Dr.WEB

Enterprise Security Suite

Руководство администратора

Dr.Web Enterprise Security Suite
Версия 12.0
Руководство администратора
23.09.2021

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1: Введение

1.1. 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 состоит из следующих основных частей:

1. **Руководство по установке** (**drweb-12.0-esuite-install-manual-ru.pdf**)

   Будет полезно руководителю организации, принимающему решение о приобретении и установке системы комплексной антивирусной защиты.

   В руководстве по установке описан процесс создания антивирусной сети и установки ее основных компонентов.

2. **Руководство администратора** (**drweb-12.0-esuite-admin-manual-ru.pdf**)

   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** (**drweb-12.0-esuite-appendices-ru.pdf**)

   Содержат техническую информацию, описывающую параметры настройки компонентов Антивируса, а также синтаксис и значения инструкций, используемых при работе с ними.

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

Также поставляются следующие Руководства:

1. **Инструкция по развертыванию антивирусной сети**

   Содержит краткую информацию по установке и первоначальной настройке компонентов антивирусной сети. За подробной информацией обращайтесь к документации администратора.

2. **Руководства по управлению станциями**

   Содержат информацию о централизованной настройке компонентов антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web.

3. **Руководства пользователя**

   Содержат информацию о настройке антивирусного решения Dr.Web, осуществляемой непосредственно на защищаемых станциях.

4. **Руководство по Web API**

   Содержит техническую информацию по интеграции Dr.Web Enterprise Security Suite со сторонним программным обеспечением посредством Web API.

5. **Руководство по базе данных Сервера Dr.Web**

   Содержит описание внутренней структуры базы данных Сервера Dr.Web и примеров её использования.

Все перечисленные Руководства поставляются в том числе в составе продукта Dr.Web Enterprise Security Suite и могут быть открыты через Центр управления безопасностью Dr.Web.

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

1.2. Условные обозначения и сокращения

Условные обозначения

В данном руководстве используются следующие 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.

Обозначение	Комментарий
`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 могут употребляться без расшифровки следующие сокращения:

- ACL — списки контроля доступа (Access Control List),
- CDN — сеть доставки контента (Content Delivery Network),
- DFS — распределенная файловая система (Distributed File System),
- DNS — система доменных имен (Domain Name System),
- FQDN — полностью определенное имя домена (Fully Qualified Domain Name),
- GUI — графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы — версия, использующая средства GUI,
- MIB — база управляющей информации (Management Information Base),
- MTU — максимальный размер полезного блока данных (Maximum Transmission Unit),
- NAP — Network Access Protection,
- 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.

Глава 2: Dr.Web Enterprise Security Suite

2.1. 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*.

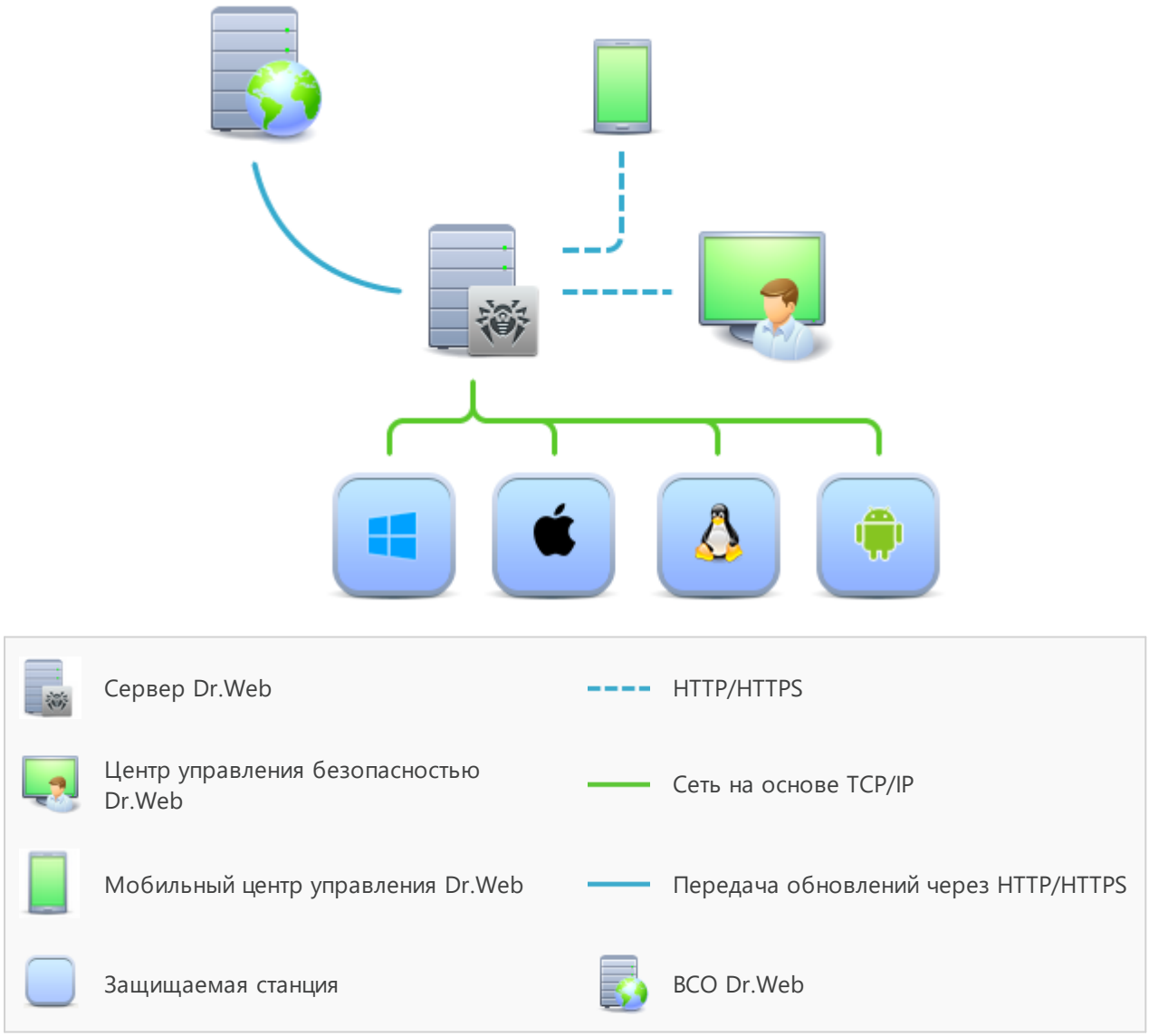


Рисунок 1-1. Логическая структура антивирусной сети

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).

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 база данных SQLite3, встроенная непосредственно в Сервер централизованной защиты.

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

- MySQL,
- Oracle,
- PostgreSQL (включая Postgres Pro),

- 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,
- Microsoft Edge,
- 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 7: 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 8: 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 6: 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 9: 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 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,
- macOS,
- ОС Android.

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 в интернет. Контроль подключения и передачи данных по интернету 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.

Контроль приложений

Осуществляет мониторинг активности всех процессов на станциях. Позволяет администратору антивирусной сети регулировать, какие приложения разрешать, а какие — запрещать запускать на защищаемых станциях.

Станции под ОС семейства UNIX

Антивирусная проверка

Сканирующее ядро. Выполняет антивирусную проверку данных (содержимого файлов, загрузочных записей дисковых устройств, иных данных, полученных от других компонентов Dr.Web для UNIX). Организует очередь проверки. Выполняет лечение тех угроз, для которых данное действие применимо.

Антивирусная проверка, управление карантином

Компонент проверки объектов файловой системы и менеджер карантина. Принимает от других компонентов Dr.Web для UNIX задания на проверку файлов. Обходит каталоги файловой системы согласно заданию, передает файлы на проверку сканирующему ядру. Выполняет удаление инфицированных файлов, перемещение их в карантин и восстановление из карантина, управляет каталогами карантина. Организует и содержит в актуальном состоянии кеш, хранящий информацию о ранее проверенных файлах и реестр обнаруженных угроз.

Используется всеми компонентами, проверяющими объекты файловой системы, такими как SpIDer Guard (для Linux, SMB, NSS).

Проверка веб-трафика

ICAP-сервер, выполняющий анализ запросов и трафика, проходящего через прокси-серверы HTTP. Предотвращает передачу инфицированных файлов и доступ к узлам сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором.

Файловый монитор для систем GNU/Linux

Монитор файловой системы Linux. Работает в фоновом режиме и отслеживает операции с файлами (такие как создание, открытие, закрытие и запуск файла) в файловых системах GNU/Linux. Посылает компоненту проверки файлов запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ.

Файловый монитор для каталогов Samba

Монитор разделяемых каталогов Samba. Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции чтения и записи) в каталогах, отведенных для файловых хранилищ SMB-сервера Samba. Отправляет компоненту проверки файлов содержимое новых и изменившихся файлов на проверку.

Файловый монитор NSS

Монитор томов NSS (Novell Storage Services). Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции записи) на томах NSS, смонтированных в указанную точку файловой системы. Отправляет содержимое новых и изменившихся файлов на проверку компоненту проверки файлов.

Проверка сетевых соединений

Компонент проверки сетевого трафика и URL. Предназначен для проверки данных, загружаемых на локальный узел из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращения соединения с узлами сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором.

Почтовый монитор

Компонент проверки почтовых сообщений. Анализирует сообщения почтовых протоколов, разбирает сообщения электронной почты и подготавливает их к проверке на наличие угроз. Может работать в двух режимах:

1. Фильтр для почтовых серверов (Sendmail, Postfix и т. п.), подключаемый через интерфейс Milter, Spamd или Rspamd.
2. Прозрачный прокси почтовых протоколов (SMTP, POP3, IMAP). В этом режиме использует SpIDer Gate.

Станции под macOS

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 SMS

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 интернету 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.

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.

Прокси-сервер позволяет использовать любой компьютер, входящий в состав антивирусной сети, в следующих целях:

- В качестве центра ретрансляции обновлений для снижения сетевой нагрузки на Сервер и соединение между Сервером и Прокси-сервером, а также для сокращения времени получения обновлений защищаемыми станциями за счет использования функции кеширования.
- В качестве центра пересылки вирусных событий от защищаемых станций на Сервер, что также снижает сетевую нагрузку и позволяет справиться, например, в случаях, когда группа станций находится в сетевом сегменте, изолированном от сегмента, в котором расположен Сервер.

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.

2.2. Системные требования

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

- Чтобы компьютеры антивирусной сети имели доступ к Серверу Dr.Web, либо к Прокси-серверу Dr.Web.
- Для совместной работы антивирусных компонентов на используемых компьютерах должны быть открыты следующие порты:

Номера портов	Протоколы	Соединения	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	• исходящие для Сервера • входящие для Агента	Для удаленной установки Агента Dr.Web.
	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		

Сервер Dr.Web

Компонент	Требования
Процессор	CPU с поддержкой инструкций SSE2 и тактовой частотой 1,3 ГГц и выше.

Компонент	Требования
Оперативная память	• Минимальные требования: 1 ГБ. • Рекомендуемые требования: от 2 ГБ.
Место на жестком диске	• Не менее 50 ГБ для ПО Сервера и дополнительное место для хранения временных файлов, например, персональных инсталляционных пакетов Агентов (примерно 17 МБ каждый) в подкаталоге `var\installers-cache` каталога установки Сервера Dr.Web. • До 5 ГБ для базы данных. • Вне зависимости от места установки Сервера, на системном диске для ОС Windows или в `/var/tmp` для ОС семейства UNIX (или в другой директории для временных файлов, если она переопределена): ▫ для установки Сервера необходимо наличие не менее 4,3 ГБ для запуска инсталлятора и распаковки временных файлов; ▫ для работы Сервера необходимо наличие свободного места на системном диске для хранения временных и рабочих файлов в зависимости от объема базы данных и настроек репозитория.
Операционная система	• Windows (полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А). • Linux, при наличии библиотеки `glibc` 2.13 или более поздней версии; включая ALT Linux 8,9, а также Astra Linux Special Edition 1.6, 1.7. • FreeBSD 11 или более поздней версии.
Поддержка виртуальных и облачных сред	Поддерживается функционирование на операционных системах, удовлетворяющих вышеперечисленным требованиям, в виртуальных и облачных средах, в том числе: • VMware; • Hyper-V; • Xen; • KVM.
Прочее	Дополнительно под ОС FreeBSD требуется наличие библиотеки `compat-10x`. Для работы с БД Oracle требуется наличие библиотеки `Linux kernel AIO access library` (`libaio`).

Сервер Dr.Web не может быть установлен на логические диски с файловыми системами, не поддерживающими символические ссылки, в частности, с файловыми системами из семейства FAT.

Административные утилиты, доступные для скачивания через Центр управления, раздел **Администрирование** → **Утилиты**, должны запускаться на компьютере, удовлетворяющем системным требованиям для Сервера Dr.Web.

Прокси-сервер Dr.Web

Компонент	Требование
Процессор	CPU с поддержкой инструкций SSE2 и тактовой частотой 1,3 ГГц и выше.
Оперативная память	Не менее 1 ГБ.
Место на жестком диске	Не менее 1 ГБ.
Операционная система	• Windows (полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А). • Linux, при наличии библиотеки `glibc` 2.13 или более поздней версии; включая ALT Linux 8, 9 и Astra Linux Special Edition 1.6, 1.7. • FreeBSD 11 или более поздней версии.

Центр управления безопасностью Dr.Web

а) Веб-браузер:

- Internet Explorer 11,
- Microsoft Edge 0.10 или более поздней версии,
- Mozilla Firefox 44 или более поздней версии,
- Google Chrome 49 или более поздней версии,
- Opera последней версии,
- Safari последней версии.

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**.

- Для корректной работы с Центром управления через веб-браузер Windows Internet Explorer по защищенному протоколу `https` необходимо установить все последние обновления веб-браузера.
- Работа с Центром управления через веб-браузер Windows Internet Explorer в режиме совместимости не поддерживается.

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

Мобильный центр управления Dr.Web

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

Операционная система	Требование	
	Версия операционной системы	**Устройство**
iOS	iOS 9 и позднее	Apple iPhone Apple iPad
Android	Android 4.1–10	–

NAP Validator

Для сервера:

- ОС Windows Server 2008.

Для агентов:

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

Агент Dr.Web и антивирусный пакет

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.

Компонент	Требование
Свободная оперативная память	Не менее 512 МБ.
Свободное место на жестком диске	1,5 ГБ для исполняемых файлов и дополнительное место 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 или более поздней версии. 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; • Outlook 2019.

- ОС семейства Linux:

Компонент	Требование
Процессор	Процессоры с архитектурой и системой команд • Intel/AMD: 32-бит (IA-32, x86) и 64-бит (x86_64, x64, amd64); • ARM64; • E2K (Эльбрус).
Свободная оперативная память	Не менее 512 МБ (рекомендуется 1 ГБ и более).
Свободное место на жестком диске	Не менее 500 МБ свободного дискового пространства на томе, на котором размещаются каталоги Антивируса.

- macOS, ОС Android: требования к конфигурации совпадают с требованиями для операционной системы.

Поддерживается функционирование Агента Dr.Web на операционных системах, удовлетворяющих вышеперечисленным требованиям, в виртуальных и облачных средах, в том числе:

- VMware;
- Hyper-V;
- Xen;

- KVM.

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

2.3. Комплект поставки

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

1. Для ОС семейства UNIX:
   - `drweb-<версия_пакета>-<сборка>-esuite-server-<версия_ОС>.tar.gz.run`

     Дистрибутив Сервера Dr.Web.*
   - `drweb-reloader-<ОС>-<разрядность>`

     Консольная версия Загрузчика репозитория Dr.Web.
2. Для ОС Windows:
   - `drweb-<версия_пакета>-<сборка>-esuite-server-<версия_ОС>.exe`

     Дистрибутив Сервера Dr.Web.*
   - `drweb-<версия_пакета>-<сборка>-esuite-agent-full-windows.exe`

     Полный инсталлятор Агента Dr.Web.
   - `drweb-reloader-windows-<разрядность>.exe`

     Консольная версия Загрузчика репозитория Dr.Web.
   - `drweb-reloader-gui-windows-<разрядность>.exe`

     Графическая версия Загрузчика репозитория Dr.Web.

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

- ПО Сервера Dr.Web для соответствующей ОС,
- данные безопасности Сервера Dr.Web,
- ПО Центра управления безопасностью Dr.Web,
- ПО Агента Dr.Web и антивирусных пакетов для станций под ОС Windows,
- модуль обновления Агента Dr.Web для Windows,
- Антиспам Dr.Web для Windows,
- вирусные базы, базы встроенных фильтров антивирусных компонентов и Антиспама Dr.Web для Windows,
- документация,
- новости компании «Доктор Веб».

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

После установки Сервера Dr.Web вы также сможете загрузить в репозиторий с серверов ВСО следующие Корпоративные продукты Dr.Web:

- Полный инсталлятор Агента Dr.Web для Windows,
- Продукты для установки на защищаемые станции под ОС UNIX (включая серверы ЛВС), Android, macOS,
- Dr.Web для IBM Lotus Domino,
- Dr.Web для Microsoft Exchange Server,
- Прокси-сервер Dr.Web,
- Агент Dr.Web для Active Directory,
- Утилита для модификации схемы Active Directory,
- Утилита для изменения атрибутов у объектов Active Directory,
- NAP Validator.

Подробная информация о работе с репозиторием Сервера приведена в **Руководстве администратора**, в разделе Управление репозиторием Сервера Dr.Web.

Глава 3: 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 https://products.drweb.com/register/v4/, 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.

3.1. 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.

3.2. Распространение лицензий по межсерверным связям

В антивирусной сети с несколькими Серверами возможна передача опционального количества лицензий между Серверами на определенный промежуток времени.

Для возможности передачи лицензий между Серверами настройте межсерверные связи как описано в разделе Настройка связей между Серверами Dr.Web.

Распространение лицензий возможно для следующих вариантов связей:

- Главный Сервер выдает лицензии, подчиненный Сервер — принимает, согласно настройкам связи для распространения лицензий (изменению не подлежат).
- Передача лицензий между равноправными Серверами. В этом случае у Сервера, который выдает лицензии, в настройках связи в разделе **Лицензии** должен быть установлен флаг **Отправлять**, а у Сервера, который получает лицензии — флаг **Принимать**.

Чтобы настроить Сервер, который будет выдавать лицензии

1. Откройте Центр управления Сервера антивирусной сети, который будет выдавать лицензии соседним Серверам.
2. В главном меню Центра управления выберите пункт **Администрирование**, в управляющем меню выберите пункт **Менеджер лицензий**.
3. Добавьте лицензионный ключ как описано в разделе Менеджер лицензий, если ключ еще не был добавлен ранее. Количество лицензий в ключе должно соответствовать общему количеству обслуживаемых станций как данным Сервером, так и всеми Серверами, которые будут получать лицензии из этого ключа.

   В общем случае может быть достаточно одного лицензионного ключа, лицензии из которого будут распределены между всеми Серверами.
4. Посчитайте, сколько лицензий из данного ключа вы можете передать соседним Серверам. При подсчете учитывайте, что с соседних Серверов также может быть передана часть лицензий другим Серверам. В этом случае передаче из ключа главного Сервера подлежит суммарное количество лицензий, которое планируется распространить далее по цепочке. Также учтите, что главный Сервер не сможет воспользоваться распространенным лицензиями до окончания срока распространения этих лицензий и их возвращения.
5. Настройте распространение лицензий на соседние Серверы из лицензионного ключа как описано в разделе Менеджер лицензий.

   В настройке **Дата окончания лицензии** задайте окончательный срок действия передачи лицензий. Срок передачи может быть как меньше срока действия самой лицензии, так и равен ей. По истечении указанного срока все лицензии будут отозваны с соседнего Сервера и вернутся в список свободных лицензий исходного лицензионного ключа. При необходимости вы сможете отредактировать этот срок в любой момент как описано в разделе Менеджер лицензий.
6. При необходимости измените настройки распространения лицензий. Для этого перейдите в раздел **Конфигурация Сервера Dr.Web**.
7. На вкладке **Лицензии** задайте следующие настройки, относящиеся к Серверу, выдающему лицензии:

- **Период автоматического продления выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на данном Сервере. После окончания этого периода осуществляется автоматическое продление выданных лицензий на тот же самый период. Автоматическое продление будет осуществляться до тех пор, пока длится срок распространения лицензий, заданный в Менеджере лицензий на шаге 5.
  Данный механизм обеспечивает возвращение лицензий на главный Сервер в том случае, если подчиненный Сервер будет отключен и не сможет вернуть выданные лицензии.
- **Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами. Синхронизация лицензий позволит определить, что количество лицензий, выданных главным Сервером и полученных подчиненным Сервером, совпадает. Данный механизм позволяет выявить сбои и случаи подлога при передаче лицензий.
- **Период создания отчета** — периодичность, с которой будут создаваться отчеты на Сервере об используемых им лицензионных ключах. Если отчет об использовании лицензий создается подчиненным Сервером, то сразу после создания осуществляется отправка этого отчета на главный Сервер. Созданные отчеты дополнительно отправляются при каждом подключении (в т.ч. перезагрузке) Сервера, а также при изменении количества выдаваемых лицензий на главном Сервере. Настройка задается на главном Сервере, но используется также и подчиненным Сервером при отправке отчетов.
- **Период подсчета активных станций** — период, в течение которого будет подсчитываться количество активных станций для создания отчета об использовании лицензий. Значение 0 предписывает учитывать в отчете все станции, вне зависимости от статуса их активности. Настройка задается на главном Сервере, но используется также и подчиненным Сервером при отправке отчетов.

8. Сохраните внесенные изменения и перезагрузите Сервер.

Чтобы настроить Сервер, который будет получать лицензии

1. Откройте Центр управления Сервера антивирусной сети, который будет получать лицензии от соседнего Сервера.
2. При необходимости измените настройки распространения лицензий. Для этого перейдите в раздел **Конфигурация Сервера Dr.Web**.
3. На вкладке **Лицензии** задайте **Интервал для предварительного продления получаемых лицензий** — промежуток времени до окончания периода автоматического продления лицензий, полученных от соседнего Сервера, начиная с которого данный Сервер запрашивает предварительное автоматическое продление этих лицензий.

   Использование данной настройки зависит от типа подключения, выбранного в настройке **Параметры соединения** при конфигурации связи между Серверами (см. раздел Настройка связей между Серверами Dr.Web):

- Для периодического типа подключения: если период переподключения, заданный в настройке связи, больше чем **Период автоматического продления выдаваемых лицензий**, заданный на Сервере, выдавшем лицензии, то автоматическое продление этих лицензий будет инициировано раньше, чем истечет **Период автоматического продления выдаваемых лицензий**.
- Для постоянного подключения: данная настройка не используется.

4. Сохраните внесенные изменения и перезагрузите Сервер.

3.3. 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 своего срока действия.

Процедура автоматического обновления лицензий

Процедура автоматического обновления лицензий запускается в следующих случаях:

- При нажатии администратором кнопки **Проверить наличие обновлений и заменить лицензионные ключи** на панели задач в Менеджере лицензий Центра управления.
- При выполнении задания **Обновление репозитория** из расписания Сервера Dr.Web. При этом должен быть установлен флаг **Обновлять лицензионные ключи** в настройках задания.

> Автоматическое обновление лицензионного ключа запускается только в том случае, когда обновляемая лицензия принадлежит этому Серверу: изначально добавлена вручную или получена через автоматическое обновление. Для лицензий, полученных с соседних Серверов через межсерверные связи, процедура автоматического обновления не запускается.

Процедура автоматического обновления лицензий содержит следующие этапы:

1. Проверка наличия лицензионного ключа на серверах компании «Доктор Веб» (ВСО).
2. Загрузка лицензионного ключа с ВСО на Сервер с последующим добавлением ключа в базу данных и Менеджер лицензий.
3. Распространение нового лицензионного ключа на объекты предыдущего ключа.

В зависимости от результатов выполнения каждого из этапов, процедура может штатно завершиться на любом из них.

Возможны следующие результаты выполнения автоматического обновления:

1. *Лицензионный ключ для автоматического обновления отсутствует на ВСО.*

   Никаких действий произведено не будет.

2. *Лицензионный ключ для автоматического обновления доступен на ВСО. Состав лицензируемых компонентов у текущего и нового ключей отличается (в новом ключе нет каких-либо компонентов, которые есть в текущем) и/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. *Лицензионный ключ для автоматического обновления доступен на ВСО. 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 автоматически удалена, когда она не будет использоваться ни одним подчиненным Сервером. Таким образом, если в момент автоматического обновления подчиненный 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 процедуры автоматического обновления лицензий 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 возможна, в частности, 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 4: Начало работы

4.1. 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 требования 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.

   При планировании антивирусной сети рекомендуется также сформировать перечень лиц, которые должны иметь доступ к Центру управления по своим должностным обязанностям, и подготовить перечень ролей со списком функциональных обязанностей, закрепленных за каждой ролью. Для каждой роли необходимо создать административную группу. Ассоциация конкретных администраторов с ролями осуществляется путем размещения их учетных записей в административных группах. При необходимости административные группы (роли) можно иерархически группировать в многоуровневую систему с возможностью индивидуальной настройки административных прав доступа для каждого уровня.

   Для корректной работы Агента Dr.Web на серверной ОС Windows, начиная с Windows Server 2016, необходимо вручную отключить Защитник Windows, используя групповые политики.

4.2. Настройка сетевых соединений

Общие сведения

К Серверу Dr.Web подключаются следующие клиенты:

- Агенты Dr.Web.
- Инсталляторы Агентов Dr.Web.
- Соседние Серверы Dr.Web.
- Прокси-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 описании 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.

4.2.1. Прямые соединения

Настройка Сервера Dr.Web

В настройках Сервера должно быть указано, какой адрес (см. документ **Приложения**, п. Приложение Д. 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`.

Порт 2193 зарегистрирован за Dr.Web Enterprise Management Service в IANA.

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 /server <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.

4.2.2. 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`.

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

4.2.3. Использование протокола SRV

Клиенты под ОС Windows поддерживают клиентский сетевой протокол *SRV* (описание формата приведено в документе **Приложения**, п. Приложение Д. 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. https://datatracker.ietf.org/doc/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`.

4.3. Обеспечение безопасного соединения

4.3.1. Шифрование и сжатие трафика

Режим шифрования используется для обеспечения безопасности данных, передаваемых по небезопасному каналу, и позволяет избежать возможного разглашения ценных сведений и подмены программного обеспечения, загружаемого на защищаемые станции.

Антивирусная сеть Dr.Web Enterprise Security Suite использует следующие криптографические средства:

- Электронная цифровая подпись (ГОСТ Р 34.10-2001).
- Асимметричное шифрование (VKO GOST R 34.10-2001 — RFC 4357).
- Симметричное шифрование (ГОСТ 28147-89).
- Криптографическая хеш-функция (ГОСТ Р 34.11-94).

Антивирусная сеть Dr.Web Enterprise Security Suite позволяет зашифровать трафик между Сервером и клиентами, к которым относятся:

- Агенты Dr.Web.
- Инсталляторы Агентов Dr.Web.
- Соседние Серверы Dr.Web.
- Прокси-серверы Dr.Web.

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 клиентах аналогичны настройкам для шифрования.

Политика согласования настроек

Политика использования шифрования и сжатия настраивается отдельно на каждом из компонентов антивирусной сети, при этом настройки остальных компонентов должны быть согласованы с настройками Сервера.

При согласовании настроек шифрования и сжатия на Сервере и клиенте следует иметь ввиду, что ряд сочетаний настроек является недопустимым, и их выбор приведет к невозможности установки соединения между Сервером и клиентом.

В таблице 4-1 приведены сведения о том, при каких настройках соединение между Сервером и клиентом будет зашифрованным/сжатым (**+**), при каких — не зашифрованным/не сжатым (**–**), и о том, какие сочетания являются недопустимыми (**Ошибка**).

Таблица 4-1. Совместимость настроек политик шифрования и сжатия

Настройки клиента	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.

Для отключения режима шифрования следует последовательно переключать Сервер и компоненты сначала в режим **Возможно**, не допуская создания несовместимых пар клиент-Сервер.

Использование сжатия уменьшает трафик, но значительно увеличивает потребление оперативной памяти и вычислительную нагрузку на компьютеры, в большей степени, чем шифрование.

Подключение через Прокси-сервер Dr.Web

При подключении клиентов к Серверу через Прокси-сервер Dr.Web необходимо учитывать настройки шифрования и сжатия на всех трех компонентах. При этом:

- Настройки Сервера и Прокси-сервера (здесь играет роль клиента) должны согласовываться по таблице 4-1.
- Настройки клиента и Прокси-сервера (здесь играет роль Сервера) должны согласовываться по таблице 4-1.

Возможность установки соединения через Прокси-сервер зависит от версий Сервера и клиента, поддерживающих определенные технологии шифрования:

- Если Сервер и клиент поддерживают TLS-шифрование, используемое в версии 12.0, то достаточно выполнения вышеописанных условий для установления работающего соединения.
- Если один из компонентов не поддерживает TLS-шифрование: на Сервере и/или клиенте установлена версия 10 и более ранняя с шифрованием по ГОСТ, то выполняется дополнительная проверка по таблице 4-2.

Таблица 4-2. Совместимость настроек политик шифрования и сжатия при использовании Прокси-сервера

Настройки соединения с клиентом	**Настройки соединения с Сервером**			
	Ничего	**Сжатие**	**Шифрование**	**Все**
Ничего	Обычный режим	Обычный режим	Ошибка	Ошибка
Сжатие	Обычный режим	Обычный режим	Ошибка	Ошибка
Шифрование	Ошибка	Ошибка	Прозрачный режим	Ошибка
Все	Ошибка	Ошибка	Ошибка	Прозрачный режим

Условные обозначения

Настройки соединений с Сервером и с клиентом	
Ничего	Ни сжатие, ни шифрование не поддерживается.
Сжатие	Поддерживается только сжатие.
Шифрование	Поддерживается только шифрование.
Все	Поддерживается и сжатие, и шифрование.
Результат соединения	
Обычный режим	Установленное соединение подразумевает работу в обычном режиме — с обработкой команд и кешированием.

Прозрачный режим	Установленное соединение подразумевает работу в прозрачном режиме — без обработки команд и без кеширования. Версия протокола шифрования выбирается минимальная: если один из компонентов (Сервер или Агент) версии 11, а другой версии 10, то устанавливается шифрование, используемое в версии 10.
Ошибка	Соединение Прокси-сервера с Сервером и с клиентом будет разорвано.

Таким образом, если Сервер и Агент разных версий: один версии 11, а другой — версии 10 и более ранней, то для установленных соединений через Прокси-сервер применяются следующие ограничения:

- Кеширование данных на Прокси-сервере возможно только в том случае, если оба соединения — и с Сервером и с клиентом установлены без использования шифрования.
- Шифрование будет использоваться, только если оба соединения — и с Сервером, и с клиентом установлены с использованием шифрования и с одинаковыми параметрами сжатия (для обоих соединений есть сжатие или для обоих — нет).

Настройки шифрования и сжатия на Dr.Web Сервере

Чтобы задать настройки сжатия и шифрования Сервера

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**.
3. На вкладке **Сеть** → **Транспорт** выберите в выпадающих списках **Шифрование** и **Сжатие** один из вариантов:
   - **Да** — шифрование (или сжатие) трафика со всеми клиентами 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 клиентов, 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 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.

Настройки шифрования и сжатия на Dr.Web Прокси-сервере

Чтобы централизовано задать настройки шифрования и сжатия для Прокси-сервера

Если Прокси-сервер не подключен к Серверу Dr.Web для удаленного управления настройками, настройте подключение как описано в **Руководстве по установке**, п. Подключение Прокси-сервера к Серверу Dr.Web.

1. Откройте Центр управления для Сервера, который является управляющим для Прокси-сервера.
2. Выберите пункт **Антивирусная сеть** в главном меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название Прокси-сервера, настройки которого вы хотите отредактировать или его первичной группы, если настройки Прокси-сервера наследуются.
3. В открывшемся управляющем меню выберите пункт **Прокси-сервер Dr.Web**. Откроется раздел настроек.
4. Перейдите на вкладку **Прослушивание**.
5. В разделе **Параметры соединения с клиентами**, в выпадающих списках **Шифрование** и **Сжатие** выберите режим шифрования и сжатия трафика для каналов между Прокси-сервером и обслуживаемыми клиентами: Агентами и инсталляторами Агентов.
6. В разделе **Параметры соединения с Серверами Dr.Web** задается список Серверов, на которые будет перенаправляться трафик. Выберите в списке нужный Сервер и нажмите кнопку ✎ на панели инструментов данного раздела, чтобы отредактировать параметры соединения с выбранным Сервером Dr.Web. В открывшемся окне, в выпадающих списках **Шифрование** и **Сжатие** выберите режим шифрования и сжатия трафика для канала между Прокси-сервером и выбранным Сервером.
7. Для сохранения заданных настроек нажмите кнопку **Сохранить**.

Чтобы локально задать настройки шифрования и сжатия для Прокси-сервера

Если Прокси-сервер подключен к управляющему Серверу Dr.Web для удаленной настройки, то конфигурационный файл Прокси-сервера будет перезаписан в соответствии с настройками, пришедшими с Сервера. В таком случае необходимо задавать настройки удаленно с Сервера или отключить настройку, разрешающую принимать конфигурацию с этого Сервера.

Описание конфигурационного файла `drwcsd-proxy.conf` приведено в документе **Приложения**, в разделе Приложении Ж4.

1. На компьютере, на котором установлен Прокси-сервер, откройте конфигурационный файл `drwcsd-proxy.conf`.

2. Отредактируйте настройки, отвечающие за сжатие и шифрование для соединений с клиентами и с Серверами.
3. Перезапустите Прокси-сервер:
   - Для ОС Windows:
     - Если Прокси-сервер запущен как сервис ОС Windows, перезапуск сервиса осуществляется штатными средствами системы.
     - Если Прокси-сервер запущен в консоли, для перезапуска нажмите CTRL+BREAK.
   - Для ОС семейства UNIX:
     - Отправьте сигнал `SIGHUP` демону Прокси-сервера.
     - Выполните следующую команду:

       Для ОС Linux:

       ```
       /etc/init.d/dwcp_proxy restart
       ```

       Для ОС FreeBSD:

       ```
       /usr/local/etc/rc.d/dwcp_proxy restart
       ```

Настройки шифрования и сжатия на станциях

Чтобы централизовано задать настройки шифрования и сжатия станций

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы.
2. В открывшемся управляющем меню выберите пункт **Параметры подключения**.
3. На вкладке **Общие**, в выпадающих списках **Режим сжатия** и **Режим шифрования** выберите один из вариантов:
   - **Да** — шифрование (или сжатие) трафика с Сервером обязательно.
   - **Возможно** — шифрование (или сжатие) будет выполняться для трафика с Сервером, если настройки Сервера этого не запрещают.
   - **Нет** — шифрование (или сжатие) не поддерживается.
4. Нажмите **Сохранить**.
5. Изменения вступят в силу, как только настройки будут переданы на станции. Если станции на момент изменения настроек отключены, изменения будут переданы, как только станции подключатся к Серверу.

Агент Dr.Web для Windows

Настройки шифрования и сжатия могут быть заданы при установке Агента:

- При дистанционной установке из Центра управления режим шифрования и сжатия задается непосредственно в настройках раздела **Установка по сети**.
- При локальной установке графический инсталлятор не предоставляет возможность изменять режим шифрования и сжатия, однако данные настройки могут быть заданы при помощи ключей командной строки при запуске инсталлятора (см. документ **Приложения**, п. 31. Сетевой инсталлятор).

После установки Агента возможность локально изменять настройки шифрования и сжатия на станции не предоставляется. По умолчанию установлен режим **Возможно** (если в процессе установки не было задано другое значение), т. е. использование шифрования и сжатия зависит от настроек со стороны Сервера. Однако, настройки на стороне Агента могут быть изменены через Центр управления (см. выше).

Антивирус Dr.Web для Android

Антивирус Dr.Web для Android не поддерживает ни шифрование, ни сжатие. Подключение будет невозможно, если задано значение **Да** для шифрования и/или сжатия на стороне Сервера или Прокси-сервера (в случае соединения через Прокси-сервер).

Антивирус Dr.Web для Linux

При установке антивируса изменение режима шифрования и сжатия не предоставляется. По умолчанию установлен режим **Возможно**.

После установки антивируса возможность локально изменять настройки шифрования и сжатия на станции предоставляется только в консольном режиме. Описание консольного режима работы и соответствующих ключей командной строки приведено в **Руководстве пользователя Dr.Web для Linux**.

Также настройки на стороне станции могут быть изменены через Центр управления (см. выше).

Антивирус Dr.Web для macOS

Возможность локально изменять настройки шифрования и сжатия на станции не предоставляется. По умолчанию установлен режим **Возможно**, т. е. использование шифрования и сжатия зависит от настроек со стороны Сервера.

Настройки на стороне станции могут быть изменены через Центр управления (см. выше).

4.3.2. Инструменты для обеспечения безопасного соединения

При установке Сервера Dr.Web создаются следующие инструменты, обеспечивающие безопасное соединение между компонентами антивирусной сети:

1. **Закрытый ключ шифрования Сервера** `drwcsd.pri`**.**

   Хранится на Сервере и не передается другим компонентам антивирусной сети.

   При утере закрытого ключа соединение между компонентами антивирусной сети необходимо восстанавливать вручную (создавать все ключи и сертификаты, а также распространять их на все компоненты сети).

   Закрытый ключ используется в следующих случаях:

   a) Создание открытых ключей и сертификатов.

   Открытый ключ шифрования и сертификат создаются автоматически из закрытого ключа в процессе установки Сервера. Закрытый ключ при этом может быть как создан новый, так и использован существующий (например, от предыдущей установки Сервера). Также ключи шифрования и сертификаты могут быть созданы в любое время при помощи серверной утилиты `drwsign` (см. документ **Приложения**, п. 37.1. Утилита генерации цифровых ключей и сертификатов).

   Информация об открытых ключах и сертификатах приведена далее.

   b) Аутентификация Сервера.

   Аутентификация Сервера удаленными клиентами осуществляется на основе электронной цифровой подписи (однократно в рамках каждого соединения).

   Сервер осуществляет цифровую подпись сообщения закрытым ключом и отправляет сообщение на сторону клиента. Клиент проверяет подпись полученного сообщения при помощи сертификата.

   c) Расшифровка данных.

   При шифровании трафика между Сервером и клиентами расшифровка данных, отправленных клиентом, осуществляется на Сервере при помощи закрытого ключа.

2. **Открытый ключ шифрования Сервера** `drwcsd.pub`**.**

   Доступен всем компонентам антивирусной сети. Открытый ключ всегда может быть сгенерирован из закрытого ключа (см. выше). При каждой генерации из одного и того же закрытого ключа получается один и тот же открытый ключ.

   Начиная с 11 версии Сервера открытый ключ используется для связи с клиентами предыдущих версий. Остальной функционал перенесен на сертификат, который, в том числе, содержит в себе открытый ключ шифрования.

3. **Сертификат Сервера** `drwcsd-certificate.pem`**.**

   Доступен всем компонентам антивирусной сети. Сертификат содержит в себе открытый ключ шифрования. Сертификат может быть сгенерирован из закрытого ключа (см. выше). При каждой генерации из одного и того же закрытого ключа получается новый сертификат.

   Клиенты, подключенные к Серверу, привязаны к конкретному сертификату, поэтому при утере сертификата на клиенте его возможно восстановить только в том случае, если тот же самый сертификат используется каким-либо другим компонентом сети: в таком случае сертификат можно скопировать на клиента с Сервера или другого клиента.

   Сертификат используется в следующих случаях:

   a) *Аутентификация Сервера.*

      Аутентификация Сервера удаленными клиентами осуществляется на основе электронной цифровой подписи (однократно в рамках каждого соединения).

      Сервер осуществляет цифровую подпись сообщения закрытым ключом и отправляет сообщение на сторону клиента. Клиент проверяет подпись полученного сообщения при помощи сертификата (в частности, открытого ключа, указанного в сертификате). В предыдущих версиях Сервера для этого использовался открытый ключ непосредственно.

      Для этого необходимо наличие на клиенте одного или нескольких доверенных сертификатов от Серверов, к которым может подключаться клиент.

   b) *Зашифровка данных*.

      При шифровании трафика между Сервером и клиентами зашифровка данных осуществляется клиентом при помощи открытого ключа.

   c) *Реализация TLS-сессии между Сервером и удаленными клиентами.*

   d) *Аутентификация Прокси-сервера.*

      Аутентификация Прокси-серверов Dr.Web удаленными клиентами осуществляется на основе электронной цифровой подписи (однократно в рамках каждого соединения).

      Прокси-сервер подписывает свои сертификаты закрытым ключом и сертификатом Сервера Dr.Web. Клиент, который доверяет сертификату Сервера Dr.Web, автоматически будет доверять сертификатам, которые им подписаны.

4. **Закрытый ключ веб-сервера.**

   Хранится на Сервере и не передается другим компонентам антивирусной сети. Подробности использования приведены далее.

5. **Сертификат веб-сервера.**

   Доступен всем компонентам антивирусной сети.

Используется для реализации TLS-сессии между веб-сервером и браузером (по HTTPS).

При установке Сервера на основе закрытого ключа веб-сервера генерируется самоподписанный сертификат, который не будет принят веб-браузерами, поскольку не был выпущен общеизвестным центром сертификации.

Чтобы защищенное соединение (HTTPS) было доступно, необходимо выполнить одно из следующих действий:

- Добавить самоподписанный сертификат в доверенные, либо в исключения для всех станций и веб-браузеров, на которых открывается Центр управления.
- Получить сертификат, подписанный общеизвестным центром сертификации.

4.3.3. Подключение клиентов к Серверу Dr.Web

Для возможности подключения к Серверу Dr.Web на стороне клиента должен присутствовать сертификат Сервера вне зависимости от того, будет ли трафик между Сервером и клиентом шифроваться.

К Серверу Dr.Web могут подключаться следующие клиенты:

- **Агенты Dr.Web.**

  Для работы Агентов в централизованном режиме с подключением к Серверу Dr.Web необходимо наличие на станции одного или нескольких доверенных сертификатов от Серверов, к которым может подключаться Агент.

  Сертификат, использованный при установке, а также сертификаты, полученные через централизованные настройки с Сервера, хранятся в реестре, но сами файлы сертификатов не используются.

  Файл сертификата в единственном экземпляре может быть добавлен при помощи ключа командной строки в каталог установки Агента (но не в реестр) и в общий список используемых сертификатов. Такой сертификат будет использоваться, в том числе, для возможности подключения к Серверу на случай ошибки в централизованных настройках.

  При отсутствии сертификата или недействительном сертификате Агент не сможет подключиться к Серверу, но продолжит функционирование и обновление в Мобильном режиме, если он разрешен для данной станции.

- **Инсталляторы Агентов Dr.Web.**

  При установке Агента на станции вместе с выбранным файлом инсталляции должен присутствовать сертификат Сервера.

  При запуске инсталляционного пакета, созданного в Центре управления, сертификат входит в состав инсталляционного пакета, и дополнительное указание файла сертификата не требуется.

После установки Агента данные сертификата заносятся в реестр, сам файл сертификата в дальнейшем не используется.

При отсутствии сертификата или недействительном сертификате инсталлятор не сможет установить Агент (относится ко всем типам инсталляционных файлов Агента).

- **Соседние Серверы Dr.Web.**

  При настройке соединения между соседними Серверами Dr.Web версии 11 и позднее необходимо на каждом из настраиваемых Серверов указать сертификат Сервера, с которым устанавливается связь (см. п. Настройка связей между Серверами Dr.Web).

  При отсутствии хотя бы одного сертификата или его недействительности установка межсерверной связи будет невозможна.

- **Прокси-серверы Dr.Web.**

  Для подключения Прокси-сервера к Серверу Dr.Web с возможностью удаленного конфигурирования через Центр управления необходимо наличие сертификата на станции с установленным Прокси-сервером. При этом Прокси-сервер также сможет поддерживать шифрование.

  При отсутствии сертификата Прокси-сервер продолжит свое функционирование, однако удаленное управление, а также шифрование и кеширование будут недоступны.

В случае штатного обновления всей антивирусной сети с предыдущей версии, которая использовала открытые ключи, на новую версию, которая использует сертификаты, никаких дополнительных действий не требуется.

Установка Агента, поставляемого с Сервером 11 версии, с подключением к Серверу 10 версии или наоборот не рекомендуется.

4.4. Интеграция Dr.Web Enterprise Security Suite с Active Directory

Если в защищаемой локальной сети используется служба Active Directory, вы можете настроить интеграцию компонентов Dr.Web Enterprise Security Suite с данной службой.

Все приведенные далее методы являются независимыми друг от друга и могут использоваться как по отдельности, так и в совокупности.

Интеграция Dr.Web Enterprise Security Suite с Active Directory осуществляется на основе следующих методов:

1. **Регистрация Сервера Dr.Web в домене Active Directory для обращения к Серверу по протоколу SRV**

   При установке Сервера Dr.Web предоставляется возможность зарегистрировать Сервер в домене Active Directory средствами установщика. В процессе регистрации на DNS-сервере создается SRV-запись, соответствующая Серверу Dr.Web. В дальнейшем возможно обращение клиентов к Серверу Dr.Web через данную SRV-запись.

   Подробнее см. разделы **Руководства по установке** Установка Сервера Dr.Web для ОС Windows и Использование протокола SRV.

2. **Синхронизация структуры антивирусной сети с доменом Active Directory**

   Возможна настройка автоматической синхронизации структуры антивирусной сети со станциями в домене Active Directory. При этом контейнеры Active Directory, содержащие компьютеры, становятся группами антивирусной сети, в которые помещаются рабочие станции.

   Для этого предоставляется задание **Синхронизация с Active Directory** в расписании Сервера. Данное задание администратор должен создать самостоятельно при помощи Планировщика заданий Сервера Dr.Web.

   Подробнее см. раздел Настройка расписания Сервера Dr.Web.

3. **Аутентификация пользователей Active Directory на Сервере Dr.Web в качестве администраторов**

   Предоставляется возможность аутентификации на Сервере Dr.Web пользователей под учетными записями Active Directory для управления антивирусной сетью. Для этого необходимо использовать один из следующих методов:

   - LDAP/AD-аутентификация. Доступна для Серверов на всех поддерживаемых ОС. Настройка доступа к Серверу для пользователей по соответствующим атрибутам Active Directory осуществляется через Центр управления. Непосредственный доступ к контроллеру домена и оснастке Active Directory не требуется — дополнительная настройка со стороны Active Directory не осуществляется.
   - Microsoft Active Directory. Доступна только для Серверов на ОС Windows, входящих в целевой домен. Настройка пользователей и групп пользователей, имеющих доступ к Серверу, осуществляется в оснастке Active Directory непосредственно. Требуется первичная настройка с помощью дополнительных утилит. Пакеты `drweb-`*`<версия_пакета>`*`-`*`<сборка>`*`-esuite-modify-ad-schema-`*`<версия_ОС>`*`.exe` и `drweb-`*`<версия_пакета>`*`-`*`<сборка>`*`-esuite-aduac-`*`<версия_ОС>`*`.msi` доступны в репозитории Сервера в **Корпоративных продуктах Dr.Web**.

   Выбор метода зависит от операционной системы Сервера Dr.Web и способа настройки разрешенных пользователей.

   Подробнее см. раздел Аутентификация администраторов.

4. **Удаленная установка Агентов Dr.Web на станции в домене Active Directory**

   Возможна дистанционная установка Агента Dr.Web на станции в домене Active Directory. Для этого необходимо:

   a) Произвести административную установку на целевом разделяемом ресурсе при помощи специального установщика Агента для Active Directory. Пакет `drweb-<версия_пакета>-<сборка>-esuite-agent-activedirectory.msi` доступен в репозитории Сервера в **Корпоративных продуктах Dr.Web**.

   b) Настроить соответствующие политики Active Directory для автоматической установки пакета на станции в домене.

   Подробнее см. раздел **Руководства по установке** Установка Агента Dr.Web с использованием службы Active Directory.

5. **Поиск станций домена Active Directory**

   Предоставляется возможность поиска станций домена Active Directory через Сканер сети. При этом возможно определить наличие Агента Dr.Web на найденных станциях и при его отсутствии дистанционно установить Агент через Центр управления.

   Данный подход для дистанционной установки Агентов может использоваться наряду с автоматической установкой пакетов через политики Active Directory, описанной в п. 4.

   Подробнее см. раздел Сканер сети.

6. **Поиск пользователей домена Active Directory**

   Предоставляется возможность поиска пользователей домена Active Directory для создания их персональных профилей и более тонкой настройки Офисного контроля и Контроля приложений.

   Подробнее см. **Руководство по управлению станциями для Windows**.

Глава 5: Компоненты антивирусной сети и их интерфейс

5.1. Сервер Dr.Web

Антивирусная сеть, построенная на основе Dr.Web Enterprise Security Suite 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 рекомендуется использовать внешнюю базу 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 антивирусного ПО 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,
- 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.

5.1.1. Управление Сервером Dr.Web под ОС Windows

Интерфейс и управление Сервером Dr.Web

Управление Сервером Dr.Web, как правило, осуществляется при помощи Центра управления, который служит внешним интерфейсом для Сервера.

Элементы, позволяющие осуществлять настройку и базовое управление Сервером, размещаются в главное меню ОС Windows **Программы**, в каталог **Dr.Web Server** в процессе установке Сервера:

- Каталог **Управление сервером** содержит следующие команды:
  - **Детальный журнал** — установить уровень **Все** для детализации журнала работы Сервера.
  - **Запустить** — запустить сервис Сервера.
  - **Остановить** — остановить сервис Сервера.
  - **Перезагрузить репозиторий** — перечитать репозиторий Сервера с диска.
  - **Перезагрузить шаблоны** — перечитать шаблоны оповещений администратора.
  - **Перезапустить** — перезапустить сервис Сервера.
  - **Проверить базу данных** — запустить проверку встроенной базы данных.
  - **Стандартный журнал** — установить уровень **Информация** для детализации журнала работы Сервера.

  После выполнения команд **Детальный журнал** и **Стандартный журнал** необходимо перезапустить Сервер для применения изменений. Для этого выполните команду **Перезапустить**.

  Расширенные настройки ведения журнала доступны в разделе Журнал Центра Управления.

  Соответствующие команды подробнее описаны в документе **Приложения**, п. 33. 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 Сервера Dr.Web имеет следующую структуру:

Каталог установки по умолчанию (может быть изменен при установке): `C:\Program Files\DrWeb Server`

- `bin` — исполняемые файлы Сервера Dr.Web.

- `ds-modules` — распакованные скриптовые модули.
- `etc` — основные конфигурационные файлы компонентов антивирусной сети.
- `fonts` — шрифты для PDF-документов.
- `var` — каталог содержит подкаталоги:
  - `backup` — резервные копии БД и других критичных данных.
  - `extensions` — скрипты пользовательских процедур, предназначенные для автоматизации выполнения определенных заданий.
  - `file-cache` — файловый кеш.
  - `installers-cache` — кеш для хранения персональных и групповых инсталляционных пакетов Агента при создании станций в Центре управления. Создается при создании инсталляционных пакетов.
  - `plugins` — временные объекты подключаемых модулей.
  - `objects` — кеш объектов Центра управления.
  - `reports` — временный каталог для генерации и хранения отчетов. Создается при необходимости.
  - `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 для записи пользователю, от имени которого запускается Сервер (как правило, пользователь **LocalSystem**).
  - `sessions` — сессии Центра управления.
  - `tmp` — временные файлы.
  - `twin-cache` — распакованные вирусные базы для обратной совместимости с предыдущими версиями Агентов Dr.Web. Также может содержать другие распакованные файлы из репозитория, например, инсталлятор Агента.
  - `upload` — директория для загрузки временных файлов, которые задаются через Центр управления. Создается при загрузке файлов большого объема.
- `vfs` — запакованные скриптовые модули и языковые пакеты.
- `webmin` — элементы Центра управления.
- `websockets` — скрипты для работы с веб-сокетами.

Каталог для резервного копирования (может быть изменен при удалении): *<диск_установки>*`:\Drweb Backup`.

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	
`database.conf`	шаблон настроек базы данных с параметрами по умолчанию	
`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 12.0 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	
`yalocator.apikey`	API-ключ для расширения Yandex.Locator	
`webmin.conf`	конфигурационный файл Центра управления	
`auth-ads.conf`	конфигурационный файл внешней авторизации администраторов через Active Directory	
`auth-ldap.conf`	конфигурационный файл внешней авторизации администраторов через LDAP	
`auth-ldap-rfc4515.conf`	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме	

Файл	Описание	Каталог по умолчанию
`auth-radius.conf`	конфигурационный файл внешней авторизации администраторов через RADIUS	
`database.sqlite`	встроенная БД	`var`
`drwcsd.pub`	открытый ключ шифрования	`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. 33. 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.

5.1.2. 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 и `/usr/local/drwcs` для ОС FreeBSD:

- `bin` — исполняемые файлы Сервера Dr.Web.
- `doc` — файлы лицензионных соглашений.
- `ds-modules` — распакованные скриптовые модули.
- `fonts` — шрифты для PDF-документов.
- `lib` — набор библиотек для работы Сервера.
- `vfs` — запакованные скриптовые модули и языковые пакеты.
- `webmin` — элементы Центра управления.
- `websockets` — скрипты для работы с вебсокетами.

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

- `backup` — резервные копии БД и других критичных данных.
- `coredump` — дампы падений Сервера. Создается при появлении дампов.
- `etc` — основные конфигурационные файлы компонентов антивирусной сети.
- `extensions` — скрипты пользовательских процедур, предназначенные для автоматизации выполнения определенных заданий.
- `installers-cache` — кеш для хранения персональных и групповых инсталляционных пакетов Агента при создании станций в Центре управления. Создается при создании инсталляционных пакетов.
- `file-cache` — файловый кеш.
- `log` — файлы журнала Сервера.
- `plugins` — временные объекты подключаемых модулей.
- `objects` — кеш объектов Центра управления.
- `reports` — временный каталог для генерации и хранения отчетов. Создается при необходимости.
- `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 для записи пользователю, от имени которого запускается Сервер (как правило, пользователь **drwcs**).

- `run` — ID процесса Сервера.
- `sessions` — сессии Центра управления.
- `tmp` — временные файлы.
- `twin-cache` — распакованные вирусные базы для обратной совместимости с предыдущими версиями Агентов Dr.Web. Также может содержать другие распакованные файлы из репозитория, например, инсталлятор Агента.
- `upload` — директория для загрузки временных файлов, которые задаются через Центр управления. Создается при загрузке файлов большого объема.

`/etc/opt/drweb.com/` для ОС Linux и `/usr/local/etc/drweb.com` для ОС FreeBSD:

- `software/drweb-esuite.remove` — скрипт для удаления Сервера.
- возможны дополнительные файлы и каталоги.

`/usr/local/etc/rc.d/` для ОС FreeBSD:

- `drwcsd` — 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: `/var/opt/drwcs/etc` • для ОС FreeBSD: `/var/drwcs/etc`
`certificate.pem`	сертификат для SSL	
`common.conf`	конфигурационный файл (для некоторых ОС семейства UNIX)	
`database.conf`	шаблон настроек базы данных с параметрами по умолчанию	
`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	

Файл	Описание	Каталог по умолчанию
`enterprise.key` (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 12.0 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	
`yalocator.apikey`	API-ключ для расширения Yandex.Locator	
`webmin.conf`	конфигурационный файл Центра управления	
`auth-ldap.conf`	конфигурационный файл внешней авторизации администраторов через LDAP	
`auth-ldap-rfc4515.conf`	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме	
`auth-pam.conf`	конфигурационный файл внешней авторизации администраторов через PAM	
`auth-radius.conf`	конфигурационный файл внешней авторизации администраторов через RADIUS	
`database.sqlite`	встроенная БД	• для ОС Linux: `/var/opt/drwcs` • для ОС FreeBSD: `/var/drwcs`
`drwcsd.pub`	открытый ключ шифрования	• для ОС Linux: `/opt/drwcs/webmin/install` • для ОС FreeBSD: `/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  .
- При помощи соответствующей консольной команды (также см. документ Приложения, п. 33. Сервер Dr.Web):
  - Запуск:
    - для ОС FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd start
      ```
    - для ОС Linux:
      ```
      # /etc/init.d/drwcsd start
      ```
  - Перезапуск:
    - для ОС FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd restart
      ```
    - для ОС Linux:
      ```
      # /etc/init.d/drwcsd restart
      ```
  - Останов:
    - для ОС FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd stop
      ```
    - Для ОС Linux:
      ```
      # /etc/init.d/drwcsd stop
      ```

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

5.2. 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.

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.

5.3. 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 регистрационные данные администратора. Данные администратора с полными правами по умолчанию:

- Имя — **admin**.

- Пароль:
  - для ОС Windows — пароль, который был задан при установке Сервера.
  - для ОС семейства UNIX — пароль, который был автоматически создан в процессе установки Сервера (см. также **Руководство по установке**, п. Установка Сервера Dr.Web для ОС семейства UNIX).

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** или более поздней версии 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. 5-1) делится на *заголовок главного меню* и *рабочую область*.

Главное Меню

В главном меню Центра управления доступны:

- раздел Администрирование,
- раздел Антивирусная Сеть,
- 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.

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).

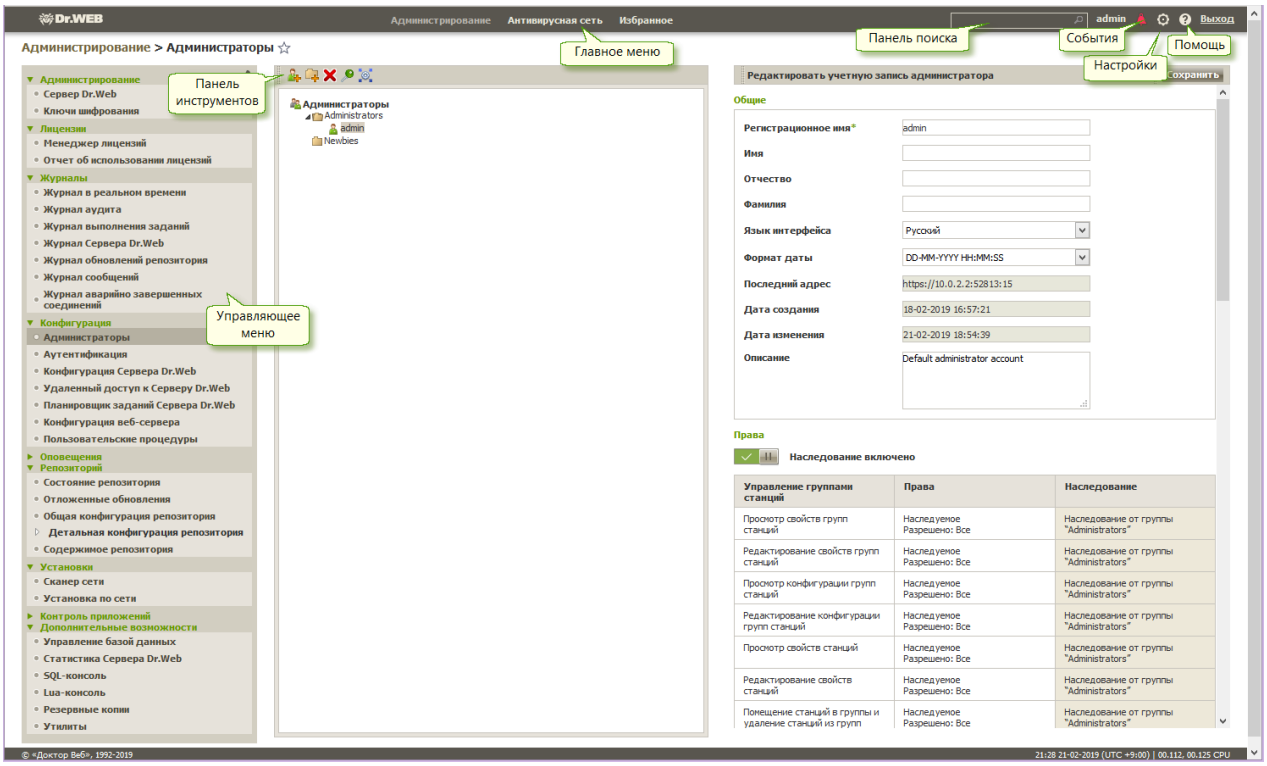


Рисунок 5-1. Окно Центра управления безопасностью Dr.Web. Нажмите на пункт главного меню для перехода к описанию

Управляющее меню

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

Управляющее меню может быть свернуто. При этом будут отображаться только названия разделов меню. При наведении курсора мыши на соответствующий раздел, отображаются пункты меню, доступные в данном разделе.

Для управления отображением управляющего меню служат иконки в правом верхнем углу:

- **Открепить меню** — снять закрепление и отображать меню в свернутом виде.
- **Закрепить меню** — закрепить развернутое положение меню.

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 связанными Серверами. Если для связи не задано имя, приводится ее идентификатор.

  При нажатии на связь возможны два варианта действий:
  - Откроется Центр управления связанного Сервера, если при настройке связи был указан IP-адрес Центра управления.
    Действие аналогично кнопке → на панели инструментов при работе со связями.
  - Если адрес Центра управления соседнего Сервера не задан для данной связи, откроется раздел настройки связей для задания IP-адреса.

5.3.1. Администрирование

Выберите пункт **Администрирование** в главном меню Центра управления.

Управляющее меню

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 , 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.

- **Ключи шифрования** — позволяет экспортировать (сохранить локально) открытый и закрытый ключи шифрования, а также сертификат Сервера.

2. **Лицензии**

- Менеджер лицензий — позволяет управлять лицензионными ключевыми файлами.
- Отчет об использовании лицензий — содержит информацию об использовании лицензий, в том числе на соседних Серверах.

3. **Журналы**

- Журнал в реальном времени — позволяет просмотреть список событий и изменений, связанных с работой Сервера, выводимых в реальном времени (сразу в момент появления события).
- 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.
- Журнал сообщений — содержит все текстовые сообщения, которые были отправлены администратором на станции антивирусной сети.
- **Журнал аварийно завершенных соединений** — содержит все случаи аварийных разрывов соединений Сервера с клиентами: станциями, инсталляторами Агентов, соседними Серверами, Прокси-серверами.

4. **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.
- Конфигурация SNMP-агента Dr.Web — открывает панель настройки параметров подключения к SNMP-агенту Dr.Web.

- Планировщик заданий Сервера Dr.Web — открывает панель настройки расписания заданий Сервера.
- Конфигурация веб-сервера — открывает панель основных настроек Веб-сервера.
- Пользовательские процедуры — открывает панель настроек пользовательских процедур.

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.
- Шаблоны сообщений — список шаблонов произвольных текстовых сообщений, отправляемых администратором на станции 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.
- **Известные хеши угроз** — позволяет производить поиск по бюллетеням с известными хешами угроз. Для поиска по полям таблицы хешей нажмите значок  . Раздел доступен, только если лицензировано использование бюллетеней известных хешей угроз. Наличие лицензии приводится в информации по лицензионному ключу, которую можно просмотреть в разделе Менеджер лицензий, параметр **Разрешенные списки бюллетеней хешей** (достаточно лицензии хотя бы в одном из лицензионных ключей, используемых Сервером).

7. **Установки**

   - 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).

8. **Контроль приложений**

   - Доверенные приложения — списки приложений, запуск которых всегда разрешен на станциях с установленным компонентом Контроль приложений (выбор разрешенных списков осуществляется в настройках профиля, назначенного на станции).
   - Справочник приложений — список всех приложений, установленных на станциях.

9. **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).

   - Резервные копии — позволяет просматривать и сохранять содержимое резервных копий критичных данных Сервера.
   - Утилиты — открывает раздел для загрузки дополнительных утилит для работы с Dr.Web Enterprise Security Suite.

5.3.2. Антивирусная сеть

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

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
   - **Идентификаторы безопасности**
   - Компоненты защиты
   - Карантин
   - Оборудование и программы
   - **Обнаруженные устройства**
   - **Сессии пользователей**
   - **Неактивные станции**
   - Свойства
   - Правила членства в группе (при выборе пользовательской группы)
   - Прокси-сервер Dr.Web (при выборе Прокси-серверов или их группы)
2. Статистика
3. **Конфигурация**
   - Прокси-сервер Dr.Web (при выборе Прокси-сервера или группы **Proxies** и ее подгрупп)
   - Права
   - Планировщик заданий
   - Устанавливаемые компоненты
   - Параметры подключения
   - Ограничения обновлений
   - **Агент Dr.Web для UNIX** — позволяет настроить периодичность отправки статистики по обнаруженным угрозам для станций под ОС семейства UNIX.
   - 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 5-1).

Таблица 5-1. Значки элементов иерархического списка

Значок	Описание
Группы. Основные значки	
	Группы, всегда отображаемые в иерархическом списке.
	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**.
	Значок правил членства отображается рядом со основным значком пользовательских групп, для которых установлены правила автоматического размещения станций в группе. Для отображения значка выберите на панели инструментов **Настройки вида дерева** → **Показывать значок правил членства**.
Рабочие станции. Основные значки	

Значок	Описание
	Доступная рабочая станция с установленным антивирусным ПО.
	Доступная рабочая станция с установленным антивирусным ПО. Серьезность состояния станции **Средняя**. Для определения действий, необходимых со стороны администратора, уточните ситуацию на данной станции в разделе Состояние. Для отображения значка выберите на панели инструментов  **Настройки вида дерева** → **Показывать серьезность состояния станций**.
	Доступная рабочая станция с установленным антивирусным ПО. Серьезность состояния станции **Максимальная** или **Высокая**. Для определения действий, необходимых со стороны администратора, уточните ситуацию на данной станции в разделе Состояние. Для отображения значка выберите на панели инструментов  **Настройки вида дерева** → **Показывать серьезность состояния станций**.
	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.
Прокси-серверы. Основные значки	
	Прокси-сервер, не подключенный к вашему Серверу.
	Прокси-сервер подключен к вашему Серверу, но заданные для него настройки не использует.
	Прокси-сервер подключен к вашему Серверу и использует заданные для него настройки.
Дополнительные значки для групп, станций и Прокси-серверов	
	Значок персональных настроек отображается на основных значках станций, групп и Прокси-серверов, для которых заданы персональные настройки (для групп в том числе, если в группе есть станции с персональными настройками). Для отображения значка выберите на панели инструментов  **Настройки вида дерева** → **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:  .
Политики	
	Политика или версия политики с настройками антивирусных компонентов станций.
Профили	

Значок	Описание
	Профиль для хранения настроек компонента Контроль приложений, активный режим.
	Профиль для хранения настроек компонента Контроль приложений, тестовый режим.
	Отключенный профиль для хранения настроек компонента Контроль приложений.
	Профиль для хранения настроек компонента Контроль приложений, для которого задана группа доверенных приложений, отсутствующая в репозитории Сервера.

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** — открыть панель свойств станции или группы в правой части окна Центра управления.

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

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

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

 **Назначить первичную группу для станций** — 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 — 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** — 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 — отправить пользователям сообщение произвольного содержания.

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

Перезагрузить станцию — удаленно запустить процесс перезагрузки станции. Требуется ли перезагрузка станции, например, в связи с обновлением/изменением антивирусных компонентов вы можете уточнить в разделе Состояние для этой станции.

Деинсталлировать Агент Dr.Web — удалить Агент и антивирусное ПО с выбранной станции или группы станций.

Установить Агент Dr.Web — открыть 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 — восстановить ранее удаленные станции. Данный пункт активен только при выборе станций из подгруппы **Deleted** в группе **Status**.

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

Отменить назначение профиля объектам — удалить профиль из списка профилей, назначенных выбранным объектам. Пункт активен при выборе объектов, для которых назначен профиль (отображаются в дереве как вложенные объекты для данного профиля).

Добавить объект сети — создать новый элемент антивирусной сети. Для этого выберите соответствующий пункт в выпадающем списке:

Создать станцию — создать новую станцию (см. **Руководство по установке**, п. Создание новой учетной записи).

Создать группу — создать новую группу станций.

Создать связь — создать связь с соседним Сервером Dr.Web.

Создать политику — создать новую политику для задания настроек станций.

Создать Прокси-сервер — создать новую учетную запись для подключения Прокси-сервера (см. **Руководство по установке**, п. Создание учетной записи Прокси-сервера).

Создать профиль — создать новый профиль для хранения настроек антивирусных компонентов станций.

Экспортировать данные:

Сохранить данные в CSV-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата CSV.

Сохранить данные в HTML-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата HTML.

Сохранить данные в XML-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата XML.

Сохранить данные в PDF-файл — 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.

Экспортировать статистику — сохранить в файл статистику работы антивирусных компонентов для выбранных объектов антивирусной сети. Для данной опции будет предложено выбрать сохраняемые разделы статистики и формат экспорта.

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.

Назначить политику — назначить выбранную политику группе или отдельным станциям. Для данной опции будет предложено выбрать объекты, которым может быть назначена выбранная политика.

Назначить профиль — назначить профиль с настройками, выбранный в дереве антивирусной сети, на объекты: станции, пользователей и группы. Для данной опции будет предложено выбрать объекты, на которые будет назначен профиль.

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. таблицу 5-1):

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:

Восстановить сбойные компоненты — принудительно восстановить состояние компонентов, работающих с ошибкой. Восстанавливается та ревизия продукта, которая в данный момент установлена на станции.

Прервать запущенные компоненты — остановить работу всех запущенных на станции антивирусных компонентов. Останавливать работу и запускать антивирусные компоненты по отдельности вы можете в разделе Компоненты защиты.

Сканировать — позволяет провести сканирование станции в одном из режимов, выбираемых в выпадающем списке:

Dr.Web Agent Сканер. 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.

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

Dr.Web Agent Сканер. 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 на Сервере станции будут автоматически удалены из предустановленной подгруппы **Newbies**. Для управления регистрацией станций выберите в выпадающем списке один из следующих вариантов:

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.

Настройки вида дерева — изменить 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. таблицу 5-1). 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 клиентов Сервера (станций, Прокси-серверов и соседних Серверов):
  - **Показывать идентификаторы клиентов** — отображать уникальные идентификаторы клиентов Сервера.
  - **Показывать названия клиентов** — отображать названия клиентов Сервера при наличии.

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

  - **Показывать адреса клиентов** — отображать IP-адреса клиентов Сервера.
  - **Показывать серверы станций** — отображать имена или IP-адреса Серверов Dr.Web, к котором подключены станции. Актуально для станций, входящих в кластер Серверов Dr.Web.
  - **Показывать серьезность состояния станций** — отображать серьезность статуса для активных станций. При этом добавится цветовая градация для станций в зависимости от их статуса (см. таблицу 5-1). Если опция отключена, то для станции со статусами, которым соответствуют значки  и  , будет отображаться общий значок  .
- для всех элементов:
  - **Показывать значок персональных настроек** — отображать маркер, обозначающий наличие персональных настроек, на значках групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов.
  - **Показывать описания** — отображать описания групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов (описания задаются в свойствах элемента).
  - **Показывать количество клиентов** — отображать количество клиентов Сервера: станций, Прокси-серверов и соседних Серверов для всех групп антивирусной сети, в которые эти клиенты входят.
  - **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 клиентов — изменить параметр, по которому осуществляется сортировка, и порядок сортировки клиентов Сервера: станций, Прокси-серверов и соседних Серверов 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 клиентов.
  - **Название** — сортировать по именам клиентов.
  - **Адрес** — сортировать по сетевым адресам клиентов. Те клиентов, у которых нет сетевого адреса, будут выводиться в произвольном порядке без сортировки.
  - **Дата создания** — сортировать по дате создания учетной записи клиента на Сервере.
  - **Дата последнего подключения** — сортировать по дате последнего подключения к Серверу.
- Для выбора порядка сортировки установите один из следующих флагов:
  - **Сортировать по возрастанию**.
  - **Сортировать по убыванию**.

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

- Если вы выбираете параметр сортировки в разделе **Настройки сортировки клиентов**, 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 клиентов**, то сортировка по этому параметру автоматически переключается на сортировку по названию клиента. Если отображение названий клиентов при этом отключено, то сортировка переключается на идентификатор клиента (название и идентификатор одновременно не могут быть отключены).

Панель свойств

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

Чтобы отобразить панель 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.

5.3.3. Избранное

Центр управления позволяет сохранять закладки на страницы интерфейса в списке избранного для удобства администрирования. Например, для быстрого перехода в наиболее часто посещаемые страницы Центра управления.

Управление списком избранного

1. В главном меню Центра управления выберите пункт **Избранное**.
2. Откроется список страниц Центра управления, добавленных в закладки.
3. Через список страниц избранного вы можете:
   - Открыть страницу, входящую в список избранного. Для этого нажмите на закладку, соответствующую этой странице в списке избранного.
   - Удалить все закладки из списка избранного. Для этого выберите пункт **Очистить избранное**.

Добавление закладки в избранное

1. Перейдите на страницу Центра управления, которую вы хотите добавить в избранное.
2. Рядом с названием страницы над управляющим меню нажмите значок ☆.
3. Откроется окно **Добавление закладки**. В поле **Имя** автоматически добавляется название страницы в формате <*Пункт главного меню*> > <*Пункт управляющего меню*>. При необходимости вы можете изменить название закладки.
4. Доступны следующие действия:
   - Чтобы сохранить страницу в списке избранного, нажмите **Добавить**. Значок рядом с названием страницы изменится на ★.
   - Чтобы закрыть окно без изменений списка избранных страниц, нажмите **Отмена**.

Редактирование и удаление закладки из избранного

1. Перейдите на страницу Центра управления, которую вы хотите отредактировать или удалить из избранного.
2. Рядом с названием страницы над управляющим меню нажмите значок ★.
3. Откроется окно **Редактирование закладки**. Доступны следующие действия:
   - Чтобы отредактировать закладку, измените ее название в поле **Имя**. Нажмите **Обновить** для применения изменений.
   - Чтобы удалить страницу из списка избранного, нажмите **Удалить**. Значок рядом с названием страницы изменится на ☆.

5.3.4. 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,
   - **Организация** — для поиска пользовательских групп, которые представляют организацию,
   - **ID станции** — для поиска станций по уникальным идентификаторам,
   - **ID группы** — для поиска групп по уникальным идентификаторам,
   - **ID пользователя** — для поиска станций по уникальным идентификаторам пользователей,
   - **Имя пользователя** — для поиска станций по имени пользователя на станции,
   - **IP-адрес** — для поиска станций по IP-адресу,
   - **MAC-адрес** — для поиска станций по MAC-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.
   - **Конфигурация** — для поиска станций по определенным значениям параметров антивирусных компонентов, установленных на станциях. При выборе данного критерия откроется панель поиска со следующими настройками:
     - **Компонент** — в выпадающем списке выберите название антивирусного компонента, в настройках которого будет осуществляться поиск. Для облегчения выбора компонента из списка можете использовать поиск: начните вводить название в поле компонента, система автоматически предложит варианты, содержащие введенные символы.
     - **Параметр** — в выпадающем списке выберите название параметра, по значениям которого доступен поиск. Поиск по параметрам со сложной структурой допустимых значений недоступен.
     - **Значение** — задайте значение параметра, выбранного выше. В зависимости от допустимых значений конкретного параметра, предоставляется либо выпадающий список с допустимыми значениями, либо поле ввода для задания значения пользователем с клавиатуры.

   Для начала поиска станций по параметрам компонентов нажмите кнопку **Поиск**.
2. Для всех критериев поиска кроме **Конфигурация** (см. выше) 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 **Ничего не найдено**.

5.3.5. 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 5-2. Список возможных оповещений о событиях в антивирусной сети

Событие	Важность	Раздел Центра управления	Описание
Оповещения о новичках	малозначительное	**Антивирусная сеть** Открывается группа **Newbies** в дереве антивирусной сети	К Серверу подключились новые станции и ожидают подтверждение доступа от администратора. Возможно в случае, если в конфигурации Сервера установлено значение

Событие	Важность	Раздел Центра управления	Описание
			Подтверждать доступ вручную для настройки **Режим регистрации новичков**.
Непрочитанные новости	малозначительное	**Поддержка** → **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.

5.3.6. 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.

Если вы выберете язык, тексты интерфейса на котором в данным момент не обновляются, вам будет предложено включить обновление для данного языка. Для этого перейдите по ссылке в раздел **Администрирование → Общая конфигурация репозитория → Сервер Dr.Web → Языки Центра управления безопасностью Dr.Web**, установите флаг для нужного вам языка и нажмите **Сохранить**. При ближайшем обновлении репозитория тексты интерфейса для выбранного языка будут обновлены. Также вы можете запустить обновление вручную в разделе **Состояние репозитория**.

- **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. 5-1). 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 клиентов Сервера (станций, Прокси-серверов и соседних Серверов):
  - **Показывать идентификаторы клиентов** — отображать уникальные идентификаторы клиентов Сервера.
  - **Показывать названия клиентов** — отображать названия клиентов Сервера.

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

  - **Показывать адреса клиентов** — отображать IP-адреса клиентов Сервера.
  - **Показывать серверы станций** — отображать имена или IP-адреса Серверов Dr.Web, к котором подключены станции. Актуально для станций, входящих в кластер Серверов Dr.Web.
  - **Показывать серьезность состояния станций** — отображать серьезность статуса для активных станций. При этом добавится цветовая градация для станций в зависимости от их статуса (см. табл. 5-1). Если опция отключена, то для станции со статусами, которым соответствуют значки и , будет отображаться общий значок .

- для всех элементов:
  - **Показывать значок персональных настроек** — отображать маркер, обозначающий наличие персональных настроек, на значках групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов.
  - **Показывать описания** — отображать описания групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов (описания задаются в свойствах элемента).
  - **Показывать количество клиентов** — отображать количество клиентов Сервера: станций, Прокси-серверов и соседних Серверов для всех групп антивирусной сети, в которые эти клиенты входят.
  - **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 клиентов

Настройки данного подраздела позволяют изменять параметр, по которому осуществляется сортировка, и порядок сортировки клиентов Сервера: станций, Прокси-серверов и соседних Серверов в дереве антивирусной сети, и аналогичны настройкам, расположенным на панели инструментов пункта **Настройки сортировки клиентов** в разделе главного меню **Антивирусная сеть**:

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

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

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 на странице **Новости** в Центре управления.

5.3.7. Помощь

Для получения помощи в процессе работы с Dr.Web Enterprise Security Suite нажмите в главном меню кнопку **Помощь**. Откроется контекстное меню, содержащее следующие пункты:

- **Документация** — открыть раздел документации администратора, соответствующий разделу Центра управления, в котором вы находитесь в данный момент. Если для текущего раздела Центра управления нет соответствующего раздела в документации, пункт **Документация** не будет отображаться в контекстном меню значка .
- **Поддержка** — открыть раздел **Поддержка** Центра управления (см. ниже).

Поддержка

Управляющее меню раздела **Поддержка** 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 М. Интеграция Web API и Dr.Web Enterprise Security Suite) в формате HTML.

- **Руководство по базе данных Сервера Dr.Web** — открыть документацию с описанием внутренней структуры базы данных Сервера Dr.Web.
- **Примечания к выпуску** — открыть раздел примечаний к выпуску Dr.Web Enterprise Security Suite для установленной у вас версии.
- **Руководства администратора по управлению станциями** — открыть документацию администратора в формате HTML по управлению станциями для соответствующей операционной системы, представленной в списке.
  В данных руководствах приведена информация о централизованной настройке антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web. Руководства описывают настройки соответствующего антивирусного решения и особенности централизованного управления данным ПО.

3. **Документация пользователя** — открыть документацию пользователя в формате HTML для соответствующей операционной системы, представленной в списке.

5.4. Компоненты Центра управления безопасностью Dr.Web

5.4.1. Сканер сети

Функции Сканера сети

- Сканирование 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.

Принцип работы Сканера сети

Сканер сети поддерживает следующие режимы поиска:

1. Поиск в Active Directory.
2. Поиск по NetBIOS.
3. Поиск по ICMP.
4. Поиск по TCP.
5. Дополнительный режим: определение наличия Агента.

Принцип действий, если все режимы включены:

1. Первые три режима запускаются параллельно. Повторный опрос уже опрошенных станций не осуществляется.

2. После окончания поиска по ICMP, включается поиск по TCP для не ответивших адресов. Если поиск по ICMP отключен, сразу включается поиск по TCP параллельно с первыми двумя режимами.

Поиск по ICMP осуществляется на основе рассылки ping-запросов, которые могут блокироваться из-за сетевых политик (в частности, из-за настроек брандмауэра).

Например:

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

3. Для станций, обнаруженных в результате поиска по первым четырем режимам, запускается опрос с целью обнаружения Агентов.

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

Установленный на защищаемой станции Агент осуществляют обработку соответствующих запросов Сканера сети, поступающих на определенный порт. По умолчанию используется порт `udp/2193`. Соответственно, этот же порт 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.

Запуск Сканера сети

Чтобы провести сканирование сети

1. Откройте окно Сканера сети. Для этого выберите пункт **Администрирование** в главном меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Сканер Сети**. Откроется окно Сканера сети.
2. Установите флаг **Включить поиск по ICMP**, чтобы осуществлять поиск станций через протокол ICMP в пределах заданных IP-адресов.
3. Установите флаг **Включить поиск по TCP**, чтобы осуществлять поиск станций через протокол TCP в пределах заданных IP-адресов.

   Задайте настройки для данного режима:

   - **Быстрое сканирование**. В режиме быстрого сканирования сети осуществляется опрос только основных портов на станциях: 445, 139, 22, 80.

- **Расширенное сканирование**. В режиме расширенного сканирования сети осуществляется проверка множества часто используемых портов. Порты сканируются в строго указанном порядке: 445, 139, 135, 1025, 1027, 3389, 22, 80, 443, 25, 21, 7, 19, 53, 110, 115, 123, 220, 464, 465, 515, 873, 990, 993, 995, 1194, 1433, 1434, 2049, 3306, 3690, 4899, 5222, 5269, 5432, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6446, 9101, 9102, 9103, 10050, 10051, 8080, 8081, 98, 2193, 8090, 8091, 24554, 60177, 60179.
- **Адреса IPv4** — список адресов IPv4:
  - одиночные адреса: `10.4.0.10`
  - диапазон через дефис: `172.16.0.1-172.16.0.123`
  - диапазон с использованием префикса сети: `192.168.0.0/24`

  При задании нескольких адресов используйте “;” или “,” в качестве разделителя.
- **Адреса IPv6** — список адресов IPv6:
  - одиночные адреса: `fe80::9109:1808:8e44:735b%3`
  - диапазон через дефис: `[FC00::0001]-[FC00::ffff]`
  - диапазон с использованием префикса сети: `[::ffff:10.0.0.1]/7`

  При задании нескольких адресов используйте “;” или “,” в качестве разделителя.

4. Установите флаг **Включить поиск по NetBIOS**, чтобы осуществлять поиск станций через протокол NetBIOS.

   Задайте настройки для данного режима:

   - **Домены** — список доменов, в которых будет осуществляться поиск станций. В качестве разделителя для нескольких доменов используйте запятую.
   - Установите флаг **Расширенное сканирование**, чтобы осуществлять расширенное сканирование с использованием информации от обозревателей сети.
5. Установите флаг **Включить поиск в Active Directory**, чтобы осуществлять поиск станций в домене Active Directory.

   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.

   Поиск станций в домене Active Directory осуществляется только по защищенному протоколу `ldaps`.

   Задайте настройки для данного режима:

   - **Контроллер Active Directory** — контроллер Active Directory, например, dc.example.com.
   - **Регистрационное имя** — регистрационное имя пользователя Active Directory.
   - **Пароль** — пароль пользователя Active Directory.

Для Серверов под ОС Windows настройки поиска в Active Directory являются необязательными. В качестве регистрационных данных по умолчанию используются данные пользователя, от имени которого запущен процесс Сервера (как правило LocalSystem).

Для Серверов под ОС семейства UNIX настройки должны быть обязательно заданы.

- В выпадающем списке **Защита соединения** выберите тип шифрованного обмена данными:
  - **STARTTLS** — переключение на защищенное соединение осуществляется через команду `STARTTLS`. По умолчанию для соединения предусматривается использование 25 порта.
  - **SSL/TLS** — открыть отдельное защищенное шифрованное соединение. По умолчанию для соединения предусматривается использование 465 порта.
  - **Нет** — не использовать шифрование. Обмен данными будет происходить по незащищенному соединению.

6. В разделе **Общие параметры** задайте настройки, используемые всеми режимами поиска:
   - **Тайм-аут (сек.)** — максимальное время ожидания ответа от станции в секундах.
   - **Количество обращений к одной станции** — максимальное количество обращений к одной станции в ожидании ответа.
   - **Количество одновременных обращений** — максимальное количество станций, к которым осуществляется одновременное обращение.
   - Установите флаг **Показывать названия станций**, чтобы для найденных станций отображался не только их IP-адрес, но и доменное имя. Если станция не зарегистрирована на DNS-сервере, то будет выводится только ее IP-адрес.
   - Установите флаг **Определять наличие Агента**, чтобы определять наличие установленного на станции Агента.

Если опция **Определять наличие Агента** отключена, для всех найденных станций будет отображаться статус , т. е. состояние антивирусного ПО на станции неизвестно.

   - **Порт** — номер порта протокола UDP по которому следует обращаться к Агентам при поиске. Диапазон значений 1-65535. По умолчанию используется порт 2193.
7. Нажмите кнопку **Сканировать**. После этого начнется сканирование сети.
8. В процессе сканирования сети в окно будет загружаться 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:

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	
	Активная станция с установленным антивирусным ПО.
	Активная станция с неподтвержденным статусом антивирусного ПО: на компьютере нет антивирусного ПО, либо наличие ПО не проверялось.

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

5.5. Схема взаимодействия компонентов антивирусной сети

На рисунке 5-2 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.

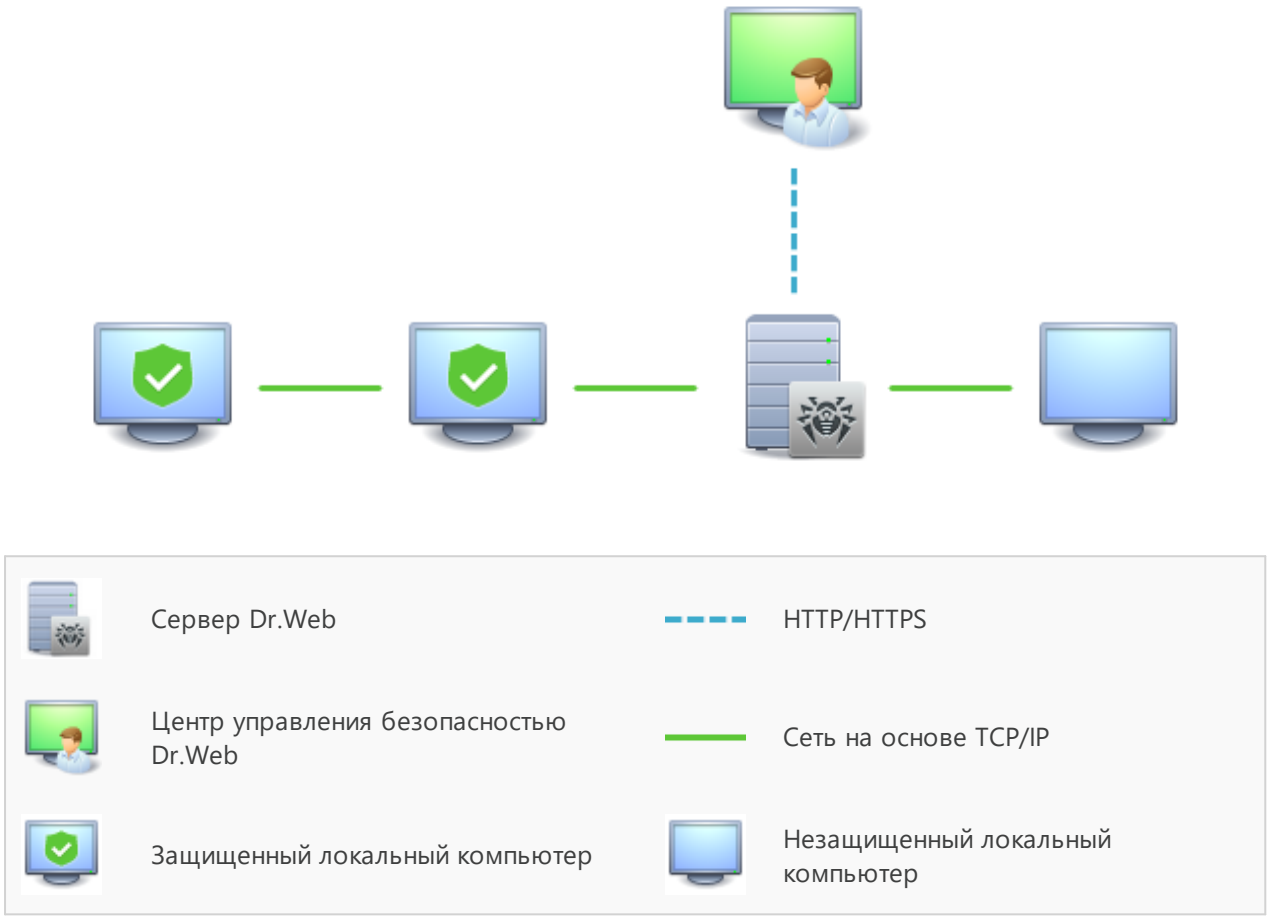


Рисунок 5-2. Структура антивирусной сети

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 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 5-3.

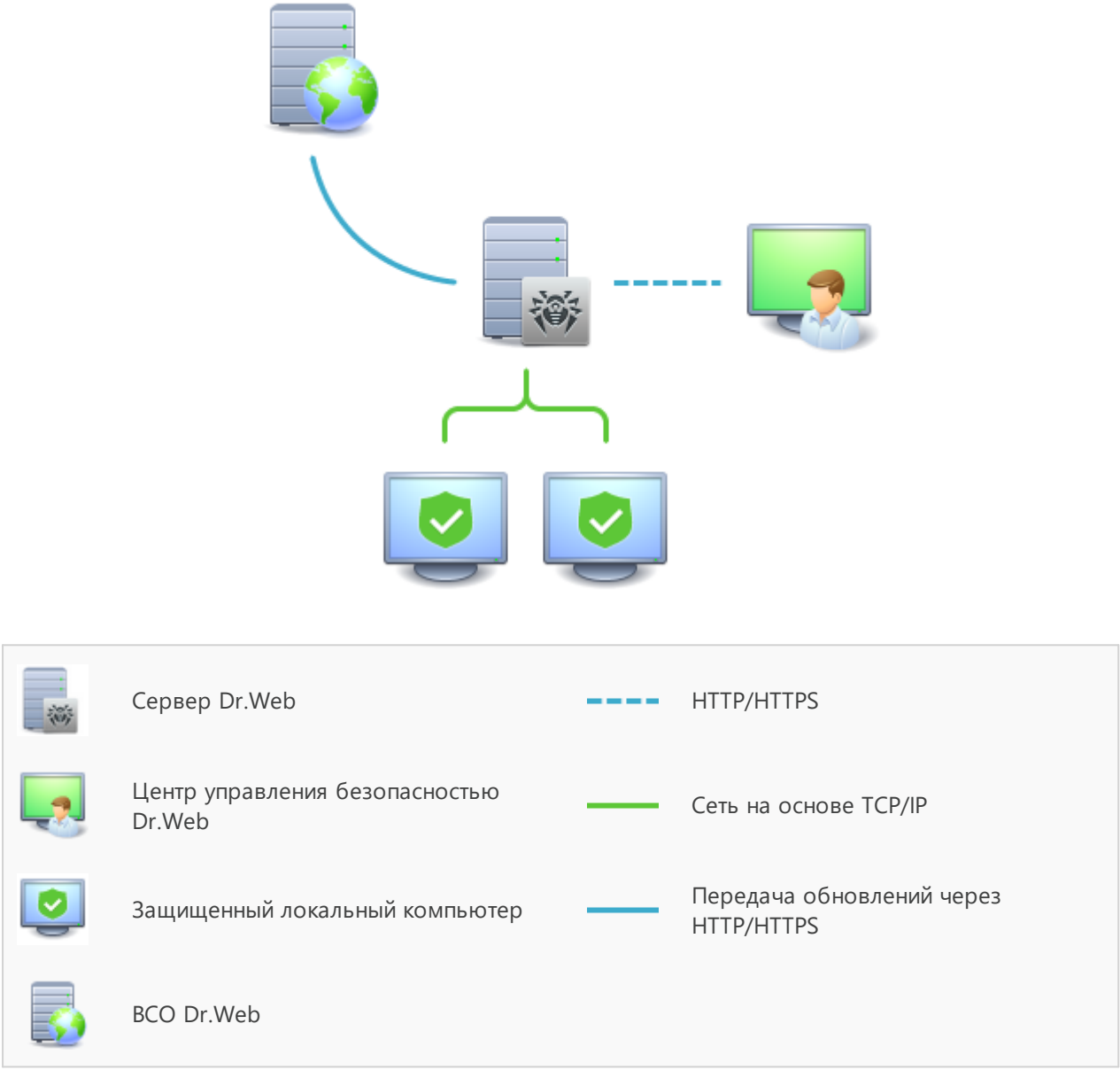


Рисунок 5-3. Логическая структура антивирусной сети

Между Сервером и рабочими станциями (сплошная тонкая линия на рисунке 5-3) 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 5-3) 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 5-3) 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 6: 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.

При планировании антивирусной сети рекомендуется также сформировать перечень лиц, которые должны иметь доступ к Центру управления по своим должностным обязанностям, и подготовить перечень ролей со списком функциональных обязанностей, закрепленных за каждой ролью. Для каждой роли необходимо создать административную группу. Ассоциация конкретных администраторов с ролями осуществляется путем размещения их учетных записей в административных группах. При необходимости административные группы (роли) можно иерархически группировать в многоуровневую систему с возможностью индивидуальной настройки административных прав доступа для каждого уровня.

6.1. Аутентификация администраторов

Аутентификация администратора для подключения к Серверу Dr.Web возможна следующими способами:

- С хранением данных об администраторах в БД Сервера.
- С помощью настроек LDAP/AD, позволяющих подключение к серверам LDAP и Active Directory.
- С использованием RADIUS-протокола.
- С использованием PAM (только под ОС семейства UNIX).

При обновлении Сервера с предыдущей версии также могут быть доступны следующие типы аутентификации (если они были включены в предыдущей версии):

- С помощью Active Directory (в версиях Сервера для ОС Windows).
- С использованием LDAP-протокола.

После отключения данных типов аутентификации их разделы будут исключены из настроек Центра управления.

При первичной установке Сервера данные разделы не предоставляются.

Методы аутентификации используются последовательно согласно следующим принципам:

1. Первой всегда осуществляется попытка аутентификации администратора из БД Сервера.
2. Порядок использования методов аутентификации через внешние системы зависит от порядка их следования в настройках, задаваемых в Центре управления.
3. Методы аутентификации через внешние системы по умолчанию отключены.

Чтобы изменить порядок 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 методов аутентификации в списке разместите их путем перетаскивания мышью 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.conf`, `auth-ldap.conf`, `auth-radius.conf`, `auth-pam.conf`.

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

6.1.1. Аутентификация администраторов из БД Сервера

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

Чтобы открыть раздел управления административными учетными записями

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.

6.1.2. Аутентификация с использованием LDAP/AD

Чтобы включить аутентификацию через LDAP/AD

1. Выберите пункт **Администрирование** в главном меню Центра управления.
2. В управляющем меню выберите раздел **Аутентификация**.
3. В открывшемся окне зайдите в раздел **LDAP/AD-аутентификация**.
4. Установите флаг **Использовать LDAP/AD-аутентификацию**.
5. Нажмите кнопку **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.

Для удобства пользователя в разделе предоставляется возможность переключения между упрощенным или расширенным вариантами настроек аутентификации через LDAP/AD.

Настройки LDAP/AD-аутентификации сохраняются в файле конфигурации `auth-ldap-rfc4515.conf`.

Также предоставляются конфигурационные файлы с типовыми настройками: `auth-ldap-rfc4515-check-group.conf`, `auth-ldap-rfc4515-check-group-novar.conf`, `auth-ldap-rfc4515-simple-login.conf`.

Описание основных xml-атрибутов аутентификации приведено в документе **Приложения**, в Приложении В3.

6.1.3. Аутентификация с использованием RADIUS

Чтобы включить аутентификацию 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 кнопку **Сохранить**.
6. Для принятия изменений перезагрузите Сервер.

Для использования протокола аутентификации RADIUS необходимо развернуть сервер, реализующий этот протокол, например, freeradius (подробности см. на https://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 файл `auth-radius.conf`, 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).

6.1.4. Аутентификация с использованием PAM

Чтобы включить аутентификацию 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 кнопку **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
	Тег	Атрибут	Допустимые значения	
Флаг **Использовать PAM-аутентификацию**	<enabled>	value	yes | no	Флаг, определяющий, будет ли использоваться метод PAM-аутентификации.
Используйте *перетаскивание*	<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-

Элемент Центра управления	Элементы файла auth-pam.xml			Описание
	Тег	Атрибут	Допустимые значения	
				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.

6.1.5. Аутентификация с использованием Active Directory

Чтобы включить аутентификацию 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 кнопку **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.

Чтобы отредактировать 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-<версия_пакета>-<сборка>-esuite-modify-ad-schema-<версия_ОС>.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 12.0 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** и дополнительный атрибут **DrWebAdmin**.

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-<версия_пакета>-<сборка>-esuite-aduac-<версия_ОС>.msi` (входит в дистрибутив Dr.Web Enterprise Security Suite 12.0) 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 В1.

6.1.6. Аутентификация с использованием LDAP

Данный раздел доступен для настройки через Центр управления только при обновлении Сервера с предыдущей версии. После отключения данного типа аутентификации ее раздел будет исключен из настроек Центра управления.

При первичной установке Сервера данный раздел недоступен.

Чтобы включить аутентификацию 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 кнопку **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.conf`.

Описание основных xml-атрибутов аутентификации приведено в документе **Приложения**, в Приложении В2.

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.

6.2. Администраторы и административные группы

Чтобы открыть раздел управления административными учетными записями

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

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.

На панели инструментов раздела **Администраторы** доступны следующие опции:

 Создать учетную запись

 Создать группу

 Удалить выбранные объекты

 Изменить пароль

Распространить права администратора

6.2.1. 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.
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.

6.2.2. 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

Чтобы отредактировать права 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 В4. Подведомственные разделы прав.

   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: • **Персональное** — для данного объекта заданы собственные настройки. • **Наследуемое** — настройки унаследованы от родительской группы.	Установите/снимите флаг **Предоставить** в строке соответствующего права.
Право задается для списка объектов (станций, администраторов или групп)		
• *Предоставлено всё* — право предоставлено для всех объектов управления.	В случае объединения настроек приводятся	Нажмите на список объектов (в том числе, если задан вариант **Все**). Откроется окно с деревом

Объекты управления	Список настроек в столбце Права	Принцип задания права
• *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.	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**.	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 пуст, то результат — запрещено всё. В противном случае, результат — разрешены оставшиеся объекты.

6.3. Управление учетными записями администраторов и административными группами

6.3.1. 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**.

Чтобы добавить новую учетную запись администратора

1. Выберите пункт **Администрирование** в главном 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 полях **Пароль** и **Подтвердите 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).

Если вы выберете язык, тексты интерфейса на котором в данным момент не обновляются, вам будет предложено включить обновление для данного языка. Для этого перейдите по ссылке в раздел **Администрирование** → **Общая конфигурация репозитория** → **Сервер Dr.Web** → **Языки Центра управления безопасностью Dr.Web**, установите флаг для нужного вам языка и нажмите **Сохранить**. При ближайшем обновлении репозитория тексты интерфейса для выбранного языка будут обновлены. Также вы можете запустить обновление вручную в разделе **Состояние репозитория**.

- 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.

Чтобы у добавленного администратора была оперативная информация о событиях в антивирусной сети, рекомендуется сразу же после создания учетной записи выполнить настройку оповещений, следуя указаниям раздела Конфигурация оповещений. Для возможности создания статистических отчетов по расписанию необходимо включить оповещение **Статистический отчет**.

Добавление административных групп

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

Чтобы добавить новую учетную запись административной группы

1. Выберите пункт **Администрирование** в главном 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.

Чтобы удалить учетную запись администратора или группы

1. Выберите пункт **Администрирование** в главном 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**.

6.3.2. 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.

Чтобы отредактировать учетную запись 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**.

Чтобы отредактировать административную группу

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**.

Назначить родительскую группу для администраторов и административных групп вы можете одним из следующих способов:

- Изменить настройки администратора или группы как описано выше.
- Перетащить мышью администратора или административную группу в иерархическом списке на группу, которую хотите назначить родительской.

Чтобы распространить права администратора или группы на другого администратора или группу

1. В списке администраторов выберите один объект, права которого вы хотите распространить. Это может быть как администратор, так и группа администраторов.
2. На панели инструментов нажмите кнопку **Распространить права администратора**.
3. В открывшемся окне выберите объекты, которым вы хотите назначить права. Обратите внимание на следующие особенности:
   - Может быть выбран один или несколько объектов для назначения прав. Это могут быть как администраторы, так и группы администраторов.
   - Права сохраняются для выбранных объектов как персональные. Наследование с родительской группой разрывается.

- Назначение прав объектам, созданным по умолчанию (группы **Administrators**, **Newbies**, администратор **admin**), не допускается.
- Распространить права можно только на объекты, разрешенные в правах **Редактирование учетных записей администраторов** и **Редактирование свойств и конфигурации групп администраторов**.
- Если распространение повлечет назначение прав, которые превышают собственные права администратора, выполняющего операцию, возвращается ошибка о недостаточности прав для выполнения операции.

4. Нажмите кнопку **Распространить**.

Глава 7: Комплексное управление рабочими станциями

Для комплексного управления станциями и их настройками предоставляются следующие инструменты:

- Группы.

  Станция может входить в неограниченное количество групп. Обязательно в предустановленные группы на основе своего состояния и опционально в пользовательские группы. Однако только одна из групп является первичной.

- Политики.

  Для станции может быть назначена только одна политика или не назначено ни одной политики.

- Профили.

  Профили используются для задания настроек компонента Контроль приложений. Профили могут быть назначены как станциям и группам станций, так и отдельным пользователям.

  Чтобы контролировать запуск приложений на станциях, необходимо, чтобы для станции или пользователя станции был назначен хотя бы один активный профиль.

Типы настроек станций

- **Унаследованные настройки.**

  При создании станции настройки всегда наследуются от политики или от первичной группы. Подробная информация приведена в разделе Наследование конфигурации рабочей станции.

- **Персональные настройки.**

  В процессе работы станции наследование может быть разорвано, и установлены персональные настройки.

  Для задания персональных настроек для станции отредактируйте соответствующий раздел настроек.

  Если для станции заданы персональные настройки, то настройки назначенной политики или первичной группы и любые их изменения не будут влиять на настройки станции.

  Вы можете восстановить наследование от политики или первичной группы. Для этого нажмите кнопку **Удалить персональные настройки** на панели инструментов Центра управления в разделе соответствующих настроек или в разделе свойств станции.

> В каждом разделе настроек элементов конфигурации рабочей станции отображается информация о том, что настройки данного раздела заданы персонально или

унаследованы от соответствующего объекта.

Часть разделов с настройками может быть задана персонально, а часть — наследоваться от политики или от первичной группы, если политика не задана.

Вы можете установить разные конфигурации для разных групп и станций, изменив соответствующие настройки.

7.1. Наследование конфигурации рабочей станции

При создании станции или группы их настройки всегда наследуются:

- Новая группа наследует настройки от своей родительской группы, в которую она непосредственно входит. Если нет родительской группы (создаваемая группа является корневой в иерархическом дереве), настройки наследуются от группы **Everyone**.
- Новая станция наследует настройки от политики, которая была назначена при создании станции. Если политика не была назначена, настройки станции наследуются от одной из групп, в которую она входит. Такая группа называется *первичной*.

В процессе дальнейшей работы наследование может быть разорвано, и установлены персональные настройки станции.

Для компонента Контроль приложений принцип наследования настроек отличается от стандартного. Подробнее см. Наследование настроек для компонента Контроль приложений.

Приоритет применения настроек для станций:

1. Если у станции заданы персональные настройки, то используются персональные настройки. При этом для станции может быть назначена политика. При задании персональных настроек определенного раздела наследование настроек этого раздела разрывается.
2. Если персональные настройки отсутствуют, то используются настройки назначенной политики.
3. Если нет персональных настроек и нет назначенной политики, то станция использует настройки своей первичной группы.

Заданы персональные настройки	Назначена политика	Используемые настройки
+	+	Персональные настройки
+	–	Персональные настройки
–	+	Настройки политики

Заданы персональные настройки	Назначена политика	Используемые настройки
–	–	Настройки первичной группы

Станции может быть не назначена ни одна политика, но у станции всегда есть первичная группа.

Наследование настроек станций от политик

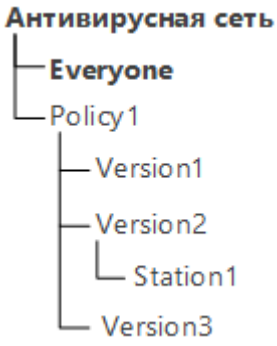
Если для станции назначена политика, устанавливается наследование настроек станции от настроек политики.

При изменениях в настройках политики эти изменения наследуются станциями, для которых эта политика назначена, за исключением случаев, когда станциям были заданы персональные настройки. При создании станции вы можете указать, какая из политик будет назначена станции. Политика может быть заменена в любое время в процессе работы. Если ни одна политика не будет назначена, настройки будут наследоваться от первичной группы.

У политик нет иерархической структуры наследования. При создании политики ее настройки копируются в качестве персональных настроек из заданного объекта (по умолчанию это политика **Default policy**). Только одна из версий политики является текущей, и ее настройки являются настройками самой политики. Только текущая версия может быть назначена станциям.

Например:

Структура иерархического списка представляет собой следующее дерево:



Для станции `Station1` назначена политика `Policy1`. Версия политики `Version2` является текущей для политики `Policy1`. Настройки версии `Version2` совпадают с настройками политики `Policy1`, которые являются персональными.

Наследование настроек станций от групп

Если для станции не назначена политика, устанавливается наследование настроек станции от настроек ее первичной группы.

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**. Первичная группа может быть заменена в любое время в процессе работы.

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**.

Возможно создание вложенных групп.

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

Например:

Структура иерархического списка представляет собой следующее дерево:

Группа `Group4` является первичной для станции `Station1`. При этом при наследовании настроек станцией `Station1` будет осуществляться поиск настроек в следующем порядке: `Station1 → Group4 → Group3 → Group2 → Group1 → Everyone`.

По умолчанию структура сети представлена таким образом, чтобы продемонстрировать вхождения станций во все группы, членом которых она является.

Если вы хотите отображать в каталоге сети членство станций только в первичных группах, на панели инструментов Центра управления в пункте **Настройки вида дерева** снимите флаг **Членство во всех группах**.

Наследование настроек для компонента Контроль приложений

Настройки профилей Контроля приложений могут быть назначены не только на станции и группы станций, но также на отдельных пользователей и группы пользователей.

Приоритет применения настроек:

1. При наличии пользовательских настроек они обладают наивысшим приоритетом.
2. При отсутствии пользовательских настроек приоритет отдается настройкам группы пользователей.
3. Если не заданы настройки для пользователей и группы пользователей, наследование осуществляется по приоритету применения настроек для станций.

7.2. Группы

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. Глава 7: Комплексное управление рабочими станциями).
- Организации (структурирования) списка рабочих станций.

Также возможно создание вложенных групп.

7.2.1. 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.

Active Directory

Группа содержит пользователей и группы пользователей, зарегистрированных в домене Active Directory. Данная группа появляется в дереве антивирусной сети после выполнения задания **Синхронизация с Active Directory** из расписания Сервера.

Configured

Группа содержит станции, для которых заданы персональные настройки.

Neighbors

Группа **Neighbors** содержит все Серверы Dr.Web, связанные с данным Сервером и служит для управления связями между Серверами в многосерверной антивирусной сети (см. п. Особенности сети с несколькими Серверами Dr.Web).

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

Группа **Neighbors** содержит вложенные группы, отражающие статус соседних Серверов, подключенных к данному Серверу:

- Группа **All neighbors** содержит все соседние Серверы, подключенные к данному Серверу.
- Группа **Children** содержит подчиненные Серверы.
- Группа **Offline** содержит неактивные в данный момент Серверы.
- Группа **Online** содержит активные в данный момент Серверы.
- Группа **Parents** содержит главные Серверы.
- Группа **Peers** содержит равноправные Серверы.

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 **macOS**. Данное семейство включает набор групп, которые соответствуют конкретной версии операционной системы macOS.
- Подгруппы семейства **UNIX**. Данное семейство включает набор групп, которые соответствуют операционным системам семейства UNIX, например, Linux, FreeBSD и т. п.
- Подгруппы семейства **Windows**. Данное семейство включает набор групп, которые соответствуют конкретной версии операционной системы Windows.
- Категория **Unknown OS**. Здесь отображаются станции, работающие под неизвестной Серверу операционной системой.

Policies

Группа, содержащая политики для настройки конфигурации станций.

Группа **Policies** будет отображаться в дереве антивирусной сети только если использование политик разрешено в конфигурации Сервера.

Profiles

Группа, содержащая профили с настройками компонента Контроль приложений для станций под ОС Windows. См. Профили.

Proxies

Группа, содержащая Прокси-серверы Dr.Web для подключения Агентов и соседних Серверов.

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 станции, регистрация которых на Сервере в данный момент не была подтверждена. При подтверждении регистрации на Сервере станции будут автоматически исключены из данной группы (подробнее см. раздел Политика подключения станций).
- Группа **Offline** содержит все неактивные в данный момент станции.
- Группа **Online** содержит все активные 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** содержит станции, подключенные в данный момент по протоколу TCP/IP версии 4.
- Группа **TCP/IP Version 6** 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 7-1 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 7-1. Группы и поддерживаемые параметры

Группа/тип групп	Параметр			
	Автоматическое членство	Управление членством	Первичная группа	Содержание настроек
Everyone	+	–	+	+
Configured	+	–	–	–
Operating System	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Ungrouped	+	–	–	–

Группа/тип групп	Параметр			
	Автоматическое членство	Управление членством	Первичная группа	Содержание настроек
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.

7.2.2. Управление группами

7.2.2.1. Создание и удаление групп

Чтобы создать новую группу

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Выберите пункт **Добавить объект сети** на панели инструментов, далее в подменю пункт **Создать группу**.

   Откроется окно создания группы.
3. Поле ввода **Идентификатор** заполняется автоматически. При необходимости его можно отредактировать в процессе создания. Идентификатор не должен включать пробелов. В дальнейшем идентификатор группы изменять нельзя.
4. Введите в поле **Название** наименование группы.
5. 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**.
6. Введите произвольный комментарий в поле **Описание**.
7. Нажмите кнопку **Сохранить**.

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

Чтобы удалить существующую группу

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

Предустановленные группы удалить невозможно.

7.2.2.2. Редактирование групп

Чтобы отредактировать настройки группы

1. Выберите пункт **Антивирусная сеть** в главном 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).

Организация

Если при создании группы вы определили группу как представителя организации или компании, то при редактировании будет доступен раздел **Организация**. В данном разделе вы можете отредактировать реквизиты организации, которую представляет данная группа. Набор реквизитов может различаться в зависимости от страны, в которой находится организация.

Назначить группу представителем организации можно только при создании группы. Отмена данного признака после создания группы также невозможна.

Конфигурация

Для подробной информации о наследовании настроек станциями от первичных групп, см. раздел Глава 7: Комплексное управление рабочими станциями.

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.	Лицензионные ключи

Значок	Настройки	Раздел с описанием
	Ограничения при распространении обновлении антивирусного ПО на станциях, которые наследуют данную настройку от группы, если она является первичной.	Ограничение обновлений рабочих станций
	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.

7.2.3. Размещение станций в 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**.

Размещение 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.

7.2.3.1. 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.

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.
3. Чтобы переместить станцию из одной пользовательской группы в другую, перетащите станцию при помощи мыши 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.

7.2.3.2. 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 **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`

Задание регулярных выражений допускается только для варианта **соответствует регулярному выражению**. Для всех остальных типов используется поиск по точному соответствию введенной строке.

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

      - 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.
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**.

7.2.4. Сравнение станций и групп

Существует возможность сравнения станций и групп по основным параметрам.

Чтобы сравнить несколько 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 данная 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.

7.2.5. 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.

Чтобы скопировать настройки

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**.

7.3. Политики

Политика представляет собой совокупность всех существующих настроек станции: права, расписание заданий, лицензионные ключи, ограничения обновлений, список устанавливаемых компонентов, конфигурация антивирусных компонентов.

Политику можно назначать только станциям.

Чтобы разрешить использование политик для настройки станций

1. Выберите пункт **Администрирование** в главном меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**.
2. На вкладке **Общие**:
   a) Установите флаг **Использовать политики**.
   b) В поле **Количество версий политики** задайте максимальное количество версий, которые могут быть созданы для каждой политики. Если при создании новой версии политики данное количество будет превышено, то будет удалена самая старая версия политики.
3. Нажмите **Сохранить** и перезапустите Сервер.
4. После разрешения использования политик создается предустановленная политика **Default policy**. Данную политику нельзя удалить, но можно редактировать и назначать станциям.

Предустановленная политика **Default policy** располагается в системной группе **Policies**, которая скрыта по умолчанию. Для отображения этой группы в иерархическом списке антивирусной сети установите опцию панели инструментов **Настройки вида дерева** → **Показывать скрытые группы**.

Для возможности управления политиками и их настройками администратору должны быть назначены права **Просмотр свойств и конфигурации политик** и **Редактирование свойств и конфигурации политик**.

Если права не назначены, то политики будут отображаться в дереве антивирусной сети и в Менеджере лицензий, но возможность просмотра их содержимого и управления ими не предоставляется.

7.3.1. Управление политиками

Создание политики

Чтобы создать новую политику

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Выберите пункт **Добавить объект сети** на панели инструментов, далее в подменю пункт **Создать политику**.

   Откроется окно создания политики.
3. Поле ввода **Идентификатор** заполняется автоматически. При необходимости его можно отредактировать в процессе создания. Идентификатор не должен включать пробелов. В дальнейшем идентификатор политики изменять нельзя.
4. В поле **Название** задайте наименование политики.
5. При создании политики ее настройки по умолчанию копируются из политики **Default policy**. Чтобы изменить объект, из которого будут копироваться настройки, нажмите на ссылку **Выбрать другой объект**. В открывшемся окне выберите объект из представленного списка. Это может быть группа, станция, другая политика или версия политики. Может быть выбран только один объект. Нажмите кнопку **Сохранить**. В окне создания политики отобразится выбранный вами объект.
6. Для создания политики с заданными настройками нажмите кнопку **Сохранить**.
7. При создании политики автоматически создается версия политики, соответствующая дате добавления самой политики.

Версии политики

Политика может содержать несколько версий, но не больше, чем указано в настройках конфигурации Сервера. Название версии политики соответствует времени ее создания.

Чтобы создать новую версию политики

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Доступ к настройкам политики осуществляется через иерархический список антивирусной сети. Отредактируйте конфигурацию политики, для которой вы хотите создать новую версию. Вы можете сделать это вручную или при помощи импорта/распространения конфигурации от другого объекта антивирусной сети (станции, группы, политики).

3. При сохранении изменений новая версия политики будет создана автоматически на основе заданных настроек политики. Созданная версия будет назначена текущей.

Только одна версия политики является текущей и может быть назначена станциям.

Настройки версии политики предоставляются только для чтения.

Чтобы изменить текущую версию политики

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В иерархическом списке выберите политику, текущую версию которой вы хотите изменить.
3. На открывшейся панели свойств политики в разделе **Общие** в выпадающем списке **Текущая версия** выберите нужную версию.
4. Нажмите кнопку **Сохранить**.

Удаление политики

Удалять политики можно как целиком, так и по версиям.

Чтобы удалить политику или версию политики

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Выберите политику или версию политики в иерархическом списке.
3. На панели инструментов нажмите **Общие** → **Удалить выбранные объекты**.

При удалении политики обратите внимание на следующие особенности:

- При удалении последней версии политики, сама политика также удаляется.
- Если удаляется текущая версия политики, то текущей становится последняя версия (с последней датой).
- Всем станциям, которым была назначена удаленная версия политики, будет назначена текущая версия этой политики.

7.3.2. Назначение политики станциям

Для станции может быть назначена только одна политика.

Станциям может быть назначена только та политика, для которой задан лицензионный ключ.

Чтобы назначить или изменить политику станции

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В иерархическом списке выберите станцию, для которой вы хотите назначить или изменить политику.
3. На открывшейся панели свойств станции в разделе **Группы** в списке **Политика** установите флаг напротив политики, которую вы хотите назначить.

   Если ранее уже была назначена политика, ее флаг будет автоматически снят, поскольку для станции может быть назначена только одна политика.

   Также вы можете снять флаги со всех политик. В этом случае настройки станции вернутся к своему предыдущему состоянию, которое было до назначения политики.
4. Нажмите кнопку **Сохранить**.

7.4. Профили

Профили определяют настройки компонента Контроль приложений, в соответствии с которыми на станциях могут запускаться или блокироваться приложения, модули, скриптовые интерпретаторы, драйверы и MSI-пакеты.

Профили создаются администратором и назначаются политикам, станциям и пользователям, в том числе группам станций и пользователей. Профили определяют режим работы Контроля приложений.

Настройка профилей осуществляется через дерево антивирусной сети:

- Все профили размещаются в предустановленной группе **Profiles**.
- Объекты, на которые назначен конкретный профиль, размещаются в дереве антивирусной сети в качестве дочерних элементов этого профиля.

Чтобы настроить Контроль приложений

1. Создайте новый профиль.
2. Задайте настройки профиля.
3. Назначьте профиль необходимым объектам.

Настройку работы профилей рекомендуется производить в тестовом режиме.

Различают следующие режимы работы профилей:

- **Отключен** — профиль не активен, настройки профиля не применяются.
- **Активный** — профиль активен, настройки применяются для объектов, на которые распространен данный профиль .
- **Тестовый** *глобальный* — профиль активен, но работает в глобальном тестовом режиме. Тестовый режим имитирует работу Контроля приложений с полным ведением журнала активности (см. События Контроля приложений), однако фактическая блокировка приложений не производится.
- **Тестовый** *для правил* — профиль активен, и на объекты распространяются настройки функционального анализа и правил. Однако, переведенные в тестовый режим правила не влияют на блокировку приложений. Результат имитируемой ими работы записывается в журнал активности (см. События Контроля приложений). Тестовый режим для правил включается и отключается в разделе настроек запрещающих и разрешающих правил.

  В таблице ниже показано какие настройки задают тот или иной режим работы профиля.

Режим **Настройка**	**Отключен**	**Активный**	**Тестовый** *глобальный*	**Тестовый** *для правил*
Общие → Включить профиль	–	+	+	+
Общие → Перевести профиль в глобальный тестовый режим	не активна	–	+	–
<Режим> → *<Правило>* → **Включить правило**	не активна	+/–	+/–	+
<Режим> → *<Правило>* → **Перевести правило в тестовый режим**	не активна	–	+/–	+

Условные обозначения

+	настройка должна быть включена
–	настройка должна быть отключена
+/–	настройка не имеет значения
не активна	настройка недоступна для редактирования

7.4.1. Создание и назначение профилей

Чтобы создать новый профиль

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне на панели инструментов выберите пункт **Добавить объект сети** → **Создать профиль**.
3. На открывшейся панели задайте **Название профиля**. В дальнейшем вы сможете его изменить при необходимости в разделе настроек Общие.
4. Нажмите кнопку **Сохранить**.
5. Новый профиль будет создан и помещен в группу **Profiles**.

Чтобы назначить профиль объекту

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в иерархическом списке выберите профиль, который вы хотите назначить.
3. На панели инструментов нажмите **Экспортировать данные** → **Назначить профиль**.

   В открывшемся окне выберите объект распространения настроек:

   - На вкладке **Active Directory** представлены списки, аналогичные списку в дереве антивирусной сети, обновляемому по заданию **Синхронизация с Active Directory** из расписания Сервера. Данные списки содержат идентичные объекты, но различаются по типу объектов, для которых будет назначен профиль:
     - В списке **Станции Active Directory** вы можете выбрать группы станций или отдельные станции, зарегистрированные в домене Active Directory.
     - В списке **Пользователи Active Directory** вы можете выбрать группы пользователей и отдельных пользователей, зарегистрированных в домене Active Directory.

     > Одни и те же объекты не должны быть выбраны в разных списках.

   - На вкладке **Антивирусная сеть** вы можете выбрать следующие объекты:
     - Группы станций. В этом случае настройки будут распространятся на учетные записи всех пользователей всех станций, входящих в данные группы.
     - Отдельные станции в группах. В этом случае настройки будут распространятся на учетные записи всех пользователей выбранных станций.
     - Политики в группе **Policies**. В этом случае настройки будут распространяться на учетные записи всех пользователей станций, которым назначена выбранная политика.

- На вкладке **Локальные пользователи** вы можете выбрать группу пользователей или отдельных пользователей на станциях. В этом случае настройки будут распространятся только на учетные записи выбранных пользователей на этих станциях.

Подробнее о приоритетах при назначении профилей см. раздел Наследование настроек для компонента Контроль приложений.

4. Нажмите кнопку **Сохранить**. Все выбранные объекты будут добавлены в список, на который распространяется настраиваемый профиль (отображаются в дереве как вложенные объекты для данного профиля).

Чтобы прекратить распространение настроек профиля на объект

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в иерархическом списке раскройте список объектов, вложенных в профиль и выберите объект, для которого вы хотите отменить назначение профиля.
3. На панели инструментов нажмите **Общие** → **Отменить назначение профиля объектам**.

7.4.2. Настройка профилей

Чтобы отредактировать настройки профиля

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Откройте раздел свойств профиля одним из следующих способов:
   a) Нажмите на название профиля в иерархическом списке антивирусной сети. В правой части окна Центра управления автоматически откроется панель со свойствами профиля.
   b) Нажмите на иконку профиля в дереве антивирусной сети или выберите профиль, затем выберите пункт **Свойства** управляющего меню. Откроется окно со свойствами профиля.
3. В разделе **Общие** задаются принципы работы профиля:
   - В поле **Название профиля** можете изменить имя профиля.
   - Установите флаг **Включить профиль**, чтобы начать использовать этот профиль.
     - Если установлен флаг **Перевести профиль в глобальный тестовый режим**, будет осуществляться только запись журнала активности как при включенных настройках. Можете использовать данный режим для отладки работы профиля.
   - В разделе Критерии функционального анализа задайте наборы предустановленных правил, по которым запуск приложений будет разрешаться или запрещаться.
4. Чтобы применить настройки, заданные в разделе **Общие**, нажмите **Сохранить** в настройках профиля.
5. В разделе **Разрешающий режим** приведена общая сводка по настройкам режима: количество созданных разрешающих правил и групп доверенных приложений,

назначенных на данный профиль. Чтобы включить или отключить режим, а также настроить правила и доверенные приложения, нажмите на ссылку Разрешающий режим для перехода в соответствующий раздел.

6. В разделе **Запрещающий режим** приведена общая сводка по настройкам режима: количество созданных запрещающих правил. Чтобы включить или отключить режим, а также настроить правила, нажмите на ссылку Запрещающий режим для перехода в соответствующий раздел.

Обратите внимание на следующие особенности работы профиля Контроля приложений:

- Если не включен ни один критерий в разделе **Критерии функционального анализа**, то сам профиль будет отключен.
- Если при задании настроек профиля ни для одного из критериев в разделе **Критерии функционального анализа** не заданы расширенные настройки и отключены запрещающий и разрешающий режимы, то данная конфигурация настроек не будет сохранена.
- Если не заданы ни разрешающие правила, ни доверенные приложения, разрешающий режим будет отключен.
- Если не заданы запрещающие правила, запрещающий режим будет отключен.

7.4.2.1. Функциональный анализ

Функциональный анализ задает набор предустановленных условий, по которым приложения разрешаются или запрещаются для запуска в соответствии с выполняемыми функциями.

Редактирование настроек функционального анализа осуществляется в разделе свойств профиля **Общие** → **Критерии функционального анализа**.

Если не включен ни один критерий в разделе **Критерии функционального анализа**, то сам профиль будет отключен.

Если ни для одного из критериев в разделе **Критерии функционального анализа** не заданы расширенные настройки и отключены запрещающий и разрешающий режимы, то сам профиль будет отключен.

Чтобы настроить функциональный анализ

1. В разделе **Критерии функционального анализа** установите флаги для категорий, которые вы хотите использовать:
   - **Запуск приложений**,
   - **Загрузка и исполнение модулей**,
   - **Запуск скриптовых интерпретаторов**,

- **Загрузка драйверов**,
- **Установка MSI-пакетов**,
- **Целостность исполняемых файлов**.

Рекомендации по использованию критериев функционального анализа приведены в документе **Приложения**, в Главе 3: Часто задаваемые вопросы. Критерии функционального анализа

> Если вы настраиваете профиль впервые, то при включении каждого из критериев автоматически включаются его разрешающие категории в расширенных настройках.
>
> Данный инструмент используется в качестве меры безопасности на случай, если после применения настроек разрешающего или запрещающего режимов окажутся заблокированы объекты операционной системы, необходимые для работы станции.
>
> В дальнейшем при необходимости вы можете отключить эти разрешающие категории в расширенных настройках.

2. Для задания расширенных настроек по выбранному критерию нажмите **Редактировать** напротив соответствующего критерия. Откроется окно со списком настроек.

   Настройки функционального анализа могут быть как запрещающими, так и разрешающими запуск приложений.

   Установите флаги для тех настроек, которые должны выполняться.

3. Если вы включите использование какого-либо из критериев, но не зададите его расширенные настройки, то контроль запуска будет производиться для всех объектов по этому критерию в соответствии с настройками разрешающего или запрещающего режимов.

   Например:

   - Если задан критерий **Запуск скриптовых интерпретаторов**, но не заданы его расширенные настройки, то будет контролироваться запуск всех скриптовых интерпретаторов в соответствии с настройками, заданными для разрешающего или запрещающего режимов.
   - Если задан критерий **Запуск скриптовых интерпретаторов** и задана его расширенная настройка **Запрещать запуск сценариев со сменных носителей**, то будет запрещен только запуск сценариев со сменных носителей.

4. Если вы зададите расширенные настройки, но не включите использование самого критерия, то ни расширенные настройки, ни сам критерий выполняться не будут.
5. Для сохранения расширенных настроек нажмите **Сохранить** в окне со списком расширенных настроек.
6. Для сохранения настроек функционального анализа нажмите **Сохранить** в окне настроек профиля.

7.4.2.2. Разрешающий режим

Разрешающий режим подразумевает, что на всех контролируемых станциях разрешается запуск только приложений из списка **Доверенные приложения** и приложений, которые соответствуют разрешающим правилам. Все остальные приложения блокируются.

Редактирование разрешающих правил и доверенных приложений осуществляется в свойствах профиля, на вкладке **Разрешающий режим**.

Чтобы использовать разрешающий режим

1. Установите флаг **Использовать разрешающий режим** на вкладке **Разрешающий режим**.
2. Задайте настройки хотя бы в одном из его разделов:
   - Разрешающие правила.
   - Доверенные приложения.
3. Нажмите **Сохранить**.

Если не заданы ни разрешающие правила, ни доверенные приложения, разрешающий режим будет отключен.

Разрешающие правила

Редактирование разрешающих правил осуществляется в разделе свойств профиля **Разрешающий режим** → **Разрешающие правила**.

Чтобы создать новое разрешающее правило

1. В разделе **Разрешающие правила** нажмите на панели инструментов кнопку ➕ **Создать правило**.
2. В окне **Добавление правила** задайте **Название правила** и нажмите **Сохранить**.
3. В списке правил выберите созданное правило и задайте его настройки на открывшейся панели свойств:
   a) Установите флаг **Включить правило**, чтобы начать использовать это правило.
   b) Если вы хотите проверить работу правила, установите флаг **Перевести правило в тестовый режим**. Приложения не будут контролироваться на станциях, однако будет осуществляться запись журнала активности как при включенных настройках. Результаты запусков и блокировок приложений в тестовом режиме работы правила будут отображаться в разделе События Контроля приложений.
   Если флаг **Перевести правило в тестовый режим** снят, правило будет работать в активном режиме с запуском приложений на станциях по заданным настройкам правила (см. также режимы работы профилей).

c) В разделе **Разрешать запуск приложений по следующим критериям** выберите опции, согласно которым запуск приложений на станциях будет разрешен.

> Также вы можете создавать разрешающие правила из разделов События Контроля приложений и Справочник приложений на основе данных, полученных со станций. При этом параметры приложений в настройках правила буду заполнены автоматически согласно выбранному приложению.

4. Нажмите **Сохранить**.

Чтобы создать дубликат разрешающего правила

1. В разделе **Разрешающие правила** в таблице правил выберите правило, которое вы хотите продублировать для этого профиля.
2. Нажмите на панели инструментов кнопку **Дублировать правило**.
3. В таблице правил появится новое правило, настройки которого будут полностью скопированы из правила, выбранного на шаге 1. В имени правила добавится цифра **1**.

Чтобы удалить разрешающее правило

1. В разделе **Разрешающие правила** в таблице правил выберите правило, которое вы хотите удалить из профиля.
2. Нажмите на панели инструментов кнопку **Удалить правило**.

Доверенные приложения

Чтобы использовать доверенные приложения, выполните одно из следующих действий:

- Если сбор доверенных приложений будет осуществляться на вашем Сервере (см. также Репозиторий доверенных приложений), активируйте сбор доверенных приложений в разделе Центра управления **Администрирование** → **Контроль приложений** → **Доверенные приложения**.
- Если доверенные приложения будут передаваться на ваш Сервер по межсерверной связи с соседнего Сервера, задайте соответствующие настройки в репозиториях Серверов, отправляющих и получающих продукт **Доверенные приложения**.

Редактирование доверенных приложений для конкретного профиля осуществляется в разделе свойств профиля **Разрешающий режим** → **Доверенные приложения**.

Таблица раздела содержит список всех групп доверенных приложений, назначенных для данного профиля.

Группа доверенных приложений (или белый список приложений) представляет собой список приложений, собранных по заданным критериям с выбранной станции или

группы станций. Эти приложения разрешены для запуска на станциях антивирусной сети, для которых назначен данный профиль при работе в разрешающем режиме.

Если ваш Сервер получает доверенные приложения по межсерверной связи с соседнего Сервера (см. Репозиторий доверенных приложений), то таблица групп может содержать записи со значком ! **Группа доверенных приложений отсутствует в репозитории Сервера**. Данные записи актуальны для групп приложений, которые были добавлены из предыдущей ревизии продукта **Доверенные приложения**, после чего была получена новая ревизия, в которую данная группа не входит. При этом, приложения могут по-прежнему сохранить работоспособность на соответствующих станциях, но чтобы предотвратить нарушения работы профиля, рекомендуется удалить такие группы из его настроек.

Чтобы добавить группу доверенных приложений в профиль

1. В разделе **Доверенные приложения** нажмите на панели инструментов кнопку ✚ **Добавить группу доверенных приложений в профиль**.
2. Откроется окно со списком всех доступных групп доверенных приложений.

При настройке разрешающего режима группы доверенных приложений выбираются из списка групп, доступных в репозитории для продукта **Доверенные приложения**.

3. Установите флаги напротив тех групп приложений, которые вы хотите добавить в профиль.
4. Нажмите **Сохранить**.

Чтобы удалить группу доверенных приложений из профиля

1. В разделе **Доверенные приложения** установите в таблице флаги для групп, которые вы хотите удалить из профиля.
2. Нажмите на панели инструментов кнопку **Удалить группу доверенных приложений**.
3. Приложения данной группы будут удалены из списка разрешенных для запуска на станциях, для которых назначен данный профиль.

При удалении из профиля сама группа доверенных приложений не удаляется. Группа остается доступна в репозитории и может быть добавлена как в данный, так и в другие профили.

7.4.2.3. Запрещающий режим

Запрещающий режим подразумевает, что на всех контролируемых станциях запрещается запуск только тех приложений, которые соответствуют запрещающим правилам. Все остальные приложения разрешаются.

Редактирование запрещающих правил осуществляется в свойствах профиля, на вкладке **Запрещающий режим**.

Чтобы использовать запрещающий режим

1. Установите флаг **Использовать запрещающий режим** на вкладке **Запрещающий режим**.
2. Создайте запрещающие правила как описано ниже.
3. Нажмите **Сохранить**.

Если не заданы запрещающие правила, запрещающий режим будет отключен.

Чтобы создать новое запрещающее правило

1. В разделе **Запрещающие правила** нажмите на панели инструментов кнопку ➕ **Создать правило**.
2. В окне **Добавление правила** задайте **Название правила** и нажмите **Сохранить**.
3. В списке правил выберите созданное правило и задайте его настройки на открывшейся панели свойств:
   a) Установите флаг **Включить правило**, чтобы начать использовать это правило.
   b) Если вы хотите проверить работу правила, установите флаг **Перевести правило в тестовый режим**. Приложения не будут контролироваться на станциях, однако будет осуществляться запись журнала активности как при включенных настройках. Результаты запусков и блокировок приложений в тестовом режиме работы правила будут отображаться в разделе События Контроля приложений.
   Если флаг **Перевести правило в тестовый режим** снят, правило будет работать в активном режиме с блокировкой приложений на станциях по заданным настройкам правила (см. также режимы работы профилей).
   c) В разделе **Запрещать запуск приложений по следующим критериям** выберите опции, согласно которым запуск приложений на станциях будет запрещен.

Также вы можете создавать запрещающие правила из разделов События Контроля приложений и Справочник приложений на основе данных, полученных со станций. При этом параметры приложений в настройках правила будут заполнены автоматически согласно выбранному приложению.

4. Нажмите **Сохранить**.

Чтобы создать дубликат запрещающего правила

1. В разделе **Запрещающие правила** в таблице правил выберите правило, которое вы хотите продублировать для этого профиля.

2. Нажмите на панели инструментов кнопку **Дублировать правило**.
3. В таблице правил появится новое правило, настройки которого будут полностью скопированы из правила, выбранного на шаге 1. В имени правила добавится цифра **1**.

Чтобы удалить запрещающее правило

1. В разделе **Запрещающие правила** в таблице правил выберите правило, которое вы хотите удалить из профиля.
2. Нажмите на панели инструментов кнопку **Удалить правило**.

Глава 8: 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.

8.1. Управление учетными записями рабочих станций

8.1.1. Политика подключения станций

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

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_ess_<ОС>_<станция>.exe` — 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.

Чтобы изменить режим доступа неподтвержденных станций

1. Выберите пункт **Антивирусная сеть** в главном 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**.

8.1.2. Удаление и восстановление станции

Удаление станций

Чтобы удалить запись о рабочей станции

1. Выберите пункт главного меню **Антивирусная сеть**.
2. В открывшемся окне в иерархическом списке выберите станцию или несколько станций, которые вы хотите удалить.
3. На панели инструментов нажмите **Общие** → **Удалить выбранные объекты**.
4. Откроется окно подтверждения удаления станции. Нажмите **ОК**.

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

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**.

8.1.3. 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).

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 кнопку **Сохранить**.

8.2. Общие настройки рабочей станции

8.2.1. 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**.

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.

8.2.1.1. Общие

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

- **Идентификатор станции** — уникальный идентификатор станции. Задается при создании учетной записи станции и в дальнейшем не подлежит изменению.
- **Название** — название станции. Задается при создании учетной записи станции и будет автоматически заменено на название компьютера после подключения Агента.
- **Дата создания** — дата создания учетной записи станции на Сервере.
- **Идентификатор безопасности** — уникальный идентификатор безопасности (SID — security identifier) учетной записи пользователя ОС Windows. Поле заполняется автоматически после подключения станции под ОС Windows к Серверу.

- **LDAP DN** — различающееся имя (distinguished name) станции под ОС Windows. Актуально для станций, входящих в ADS/LDAP-домен. Поле заполняется автоматически после подключения станции к Серверу.
- **MAC-адрес** — MAC-адрес станции. Поле заполняется автоматически после подключения станции к Серверу.
- **Дата последнего подключения** — 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 **Подтвердите 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, macOS и ОС Linux.

8.2.1.2. Конфигурация

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

Значок	Настройки	Раздел с описанием
	Права пользователей станции	Права пользователей станции
	Централизованное расписание запуска заданий на рабочей станции	Расписание заданий рабочей станции
	Лицензионные ключи для станции	Лицензионные ключи
	Ограничения при распространении обновлении антивирусного ПО	Ограничение обновлений рабочих станций

Значок	Настройки	Раздел с описанием
	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 SpIDer 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).

8.2.1.3. 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.

Чтобы настроить членство рабочей станции

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**.

8.2.1.4. Безопасность

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

Чтобы настроить ограничения доступа

1. Установите флаг **Использовать этот список доступа**, чтобы задать списки разрешенных или запрещенных адресов. Если флаг снят, все соединения будут разрешены.
2. Чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.
3. Чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.
4. 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**.

Чтобы отредактировать список адресов:

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**.

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 16777214 адресов (256*256*256-2).

   Адреса хостов в этих сетях вида: `125.*.*.*`

8.2.1.5. Прокси-сервер

В разделе **Прокси-сервер** задаются настройки Прокси-сервера Dr.Web, установленного на этой станции.

Подробная информация об установке и подключении Прокси-сервера к Серверу Dr.Web приведена в **Руководстве по установке**, п. Установка Прокси-сервера.

Если Прокси-сервер установлен на станции:

1. В поле **Идентификатор** приводится идентификатор учетной записи Прокси-сервера, созданной в Центре управления. После создания учетной записи редактирование идентификатора не предоставляется.
2. В поле **Название** вы можете изменить название учетной записи Прокси-сервера, созданной в Центре управления.
3. В полях **Пароль** и **Подтвердите пароль** вы можете изменить пароль учетной записи Прокси-сервера, созданной в Центре управления. Пароль используется для подключения Прокси-сервера к Серверу. В случае изменения пароля в Центре управления необходимо убедиться, что пароль в настройках подключения на Прокси-сервере совпадает с измененным паролем в Центре управления. В случае несовпадения паролей Прокси-сервер не сможет подключиться к Серверу для удаленного управления конфигурацией через Центр управления.
4. В разделе **Членство** задается группа, в которую входит Прокси-сервер. Для изменения группы установите флаг напротив нужной группы в приведенном списке.

   Прокси-сервер может входить только в одну группу.

   Допускается выбор предустановленной группы **Proxies** и ее подгрупп.
5. Вы можете удалить Прокси-сервер, связанный с Агентом на редактируемой станции. Для этого нажмите **Удалить Прокси-сервер**.

   После нажатия **Сохранить**, Прокси-сервер будет деинсталлирован со станции. Учетная запись Прокси-сервера — удалена с Сервера.

Если Прокси-сервер не установлен на станции:

1. Если вы хотите установить Прокси-сервер на выбранной станции, установите флаг **Создать связанный Прокси-сервер** и задайте параметры создаваемого Прокси-сервера. Параметры аналогичны параметрам при создании Прокси-сервера.
2. После нажатия **Сохранить**, будет создана учетная запись Прокси-сервера в Центре управления. После передачи настроек на станцию, Прокси-сервер будет установлен на этой станции в фоновом режиме. Агент будет подключаться к Серверу только через установленный Прокси-сервер. Использование Прокси-сервера будет прозрачно для пользователя.

8.2.1.6. 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.

Чтобы просмотреть расположение 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 OpenStreetMap 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**.

Для станций под ОС Android возможна настройка автоматического определения расположения.

Подробную информацию по использованию и настройке данной функции вы можете найти в документе **Приложения**, в разделе Автоматическое определение местоположения станции под ОС Android.

8.2.2. Компоненты защиты

Компоненты

Чтобы узнать, какие компоненты антивирусного пакета установлены на рабочей станции, а также запустить или остановить работу компонентов

1. Выберите пункт **Антивирусная сеть** в главном 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 **Компоненты защиты**.
3. Откроется окно с информацией о компонентах, установленных на выбранных станциях.

Список установленных компонентов зависит от:

- компонентов, разрешенных для использования в лицензионном ключе;
- ОС рабочей станции;
- настроек, заданных администратором на Сервере Dr.Web. 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).

4. При необходимости вы можете изменять статус работы компонентов напрямую из Центра управления. Для этого установите флаги для тех компонентов, статус работы которых вы хотите изменить, и нажмите на соответствующую кнопку на панели инструментов:
   - — остановить работу выбранных компонентов на станциях.
   - — запустить выбранные компоненты на станциях.

   При останове работы компонентов текущие сканирования будут прерваны, Сканер остановлен, работа запущенных мониторов приостановлена.

   Также вы можете остановить работу компонентов в зависимости от типа их запуска, как описано в разделе Прерывание работы запущенных компонентов по типам.

5. При необходимости вы можете экспортировать данные о статусе работы компонентов станций в файл. Для этого 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.

Вирусные базы

Чтобы узнать, какие вирусные базы установлены на рабочей станции

1. Выберите пункт **Антивирусная сеть** в главном 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 **Состояние станций** и **Состояние вирусных баз**, после чего перезагрузите Сервер.

Пункт **Вирусные базы** доступен только при выборе единичных станций.

8.2.3. 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.

Чтобы собрать информацию 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. Если перед этим вы не разрешили сбор статистики в настройках Сервера, данная настройка будет недоступна. При необходимости отредактируйте значение параметра **Период сбора информации о станциях (мин.)**.
   e) Для принятия внесенных изменений нажмите **Сохранить**. Настройки будут переданы на станции.

Чтобы просмотреть аппаратное и программное обеспечение на одной или нескольких станциях

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В иерархическом списке антивирусной сети выберите станцию или группу станций.
3. В управляющем меню, в секции **Общие** выберите пункт **Оборудование и программы**.

4. Таблица содержит следующие вкладки с информацией об аппаратном и программном обеспечении выбранных станций:
   - **Оборудование** — список аппаратного обеспечения, установленного на станциях.
   - **Программы** — список программных продуктов, установленных на станциях.
   - **Обновления Windows** — список пакетов обновлений ОС Windows, установленных на станциях.
5. Столбец **Станция** на каждой из вкладок содержит название станции, для которой приведена информация.
6. Чтобы отредактировать отображение данных в таблице:
   - При помощи значка  выберите, какие столбцы будут отображаться в таблице.
   - При помощи значка  задайте произвольную строку для поиска по всем разделам таблицы.
7. При необходимости вы можете экспортировать данные о программно-аппаратном обеспечении станции в файл. Для этого 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**.

8.3. Настройка конфигурации рабочей станции

8.3.1. Права пользователей станции

Чтобы настроить права пользователей 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, macOS, 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		
Изменение режима работы	Установите флаг, чтобы разрешить пользователям на станции устанавливать режимы работы Агента Dr.Web.	В настройках Агента, в разделе **Основные** → **Сервер** 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. • **Сервер**: недоступны настройки подключения к Серверу, флаг **Синхронизировать системное время с временем сервера** и настройка **Использовать Мобильный режим, если отсутствует подключение к серверу**. • **Самозащита**: недоступны настройки **Запрещать изменение даты и времени системы**, **Запрещать эмуляцию действий пользователя**. • **Дополнительно**: в настройках подраздела **Журнал** недоступны 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 macOS		

Флаг раздела Права	Действие флага	Результат на станции, если флаг снят
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 в мобильный режим и получать обновления непосредственно из Всемирной системы обновления Dr.Web, если отсутствует подключение к Серверу Dr.Web.	На главном экране приложения, запущенного на мобильном устройстве, раздел **Обновление** недоступен.

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 **Руководствах пользователя** продуктов Dr.Web для соответствующей операционной системы.

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.

8.3.2. 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.

Чтобы отредактировать централизованное расписание

1. Выберите пункт **Антивирусная сеть** в главном 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.

Импорт списка заданий для Сервера Dr.Web в Планировщик заданий рабочих станций и наоборот не допускается.

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**.		
Серьезность	**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**

Настройка	Действие
	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.
Выполнить задание	Выполнить выбранные в списке задания незамедлительно. При этом задание будет запущено, даже если оно запрещено для выполнения по расписанию.

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.

> Поля в интерфейсе, отмеченные знаком *, должны быть обязательно заполнены.

Чтобы отредактировать параметры 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 **Серьезность**.

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.

- Если флаг **Запускать задание асинхронно** снят, задание будет помещено в общую очередь заданий Планировщика, выполняемых последовательно. Установите флаг, чтобы выполнять данное задание параллельно вне очереди.

2. 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. • 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

Тип задания	Параметры и описание
	сразу после запуска программы, и Агент протоколирует только запуск программы.
Dr.Web Agent Сканер. Быстрое сканирование	Параметры настройки сканирования описаны в п. Настройка параметров Сканера.
Dr.Web Agent Сканер. Выборочное сканирование	
Dr.Web Agent Сканер. Полное сканирование	

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

3. 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.
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.

Режим запуска	Параметры и описание
	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.

4. 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.

8.3.3. Устанавливаемые компоненты антивирусного пакета

На серверы, выполняющие важные сетевые функции (домен-контроллеры, серверы раздачи лицензий и т. д.), не рекомендуется устанавливать компоненты SpIDer Gate, SpIDer Mail и Брандмауэр Dr.Web во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса Dr.Web.

Чтобы настроить список устанавливаемых компонентов антивирусного пакета

1. Выберите пункт **Антивирусная сеть** в главном 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 8-1 указано, будет ли установлен компонент на станции (+) в зависимости от параметров, заданных пользователем, и настроек, заданных администратором на Сервере.

Таблица 8-1.

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.

8.3.4. Параметры подключения

На вкладке **Параметры подключения** настраиваются параметры, определяющие настройки взаимодействия с Сервером:

- В поле **Сертификат** задается SSL-сертификат Сервера Dr.Web (`drwcsd-certificate.pem`). Для выбора файла сертификата нажмите кнопку  .

  На станции могут храниться одновременно несколько сертификатов, например, при переезде с одного Сервера на другой. При этом сертификаты должны быть уникальны, т. е. нельзя задать два одинаковых сертификата.

  Для добавления еще одного сертификата нажмите кнопку  и выберите файл сертификата.

  Для удаления существующего сертификата нажмите кнопку  напротив сертификата, который нужно удалить.

  Сертификат должен быть обязательно задан.

- В поле **Сервер** задается адрес Сервера Dr.Web или Прокси-сервера Dr.Web (подробнее см. Прокси-сервер Dr.Web). Данное поле может оставаться пустым. В этом случае Агент будет использовать адрес Сервера, указанный в настройках на локальной машине пользователя (адрес Сервера, с которого производилась установка).

  Может быть задан как один адрес Сервера, так и несколько адресов различных Серверов. Для добавления еще одного адреса Сервера нажмите кнопку  и введите адрес в добавленное поле. Формат задания сетевых адресов Сервера описан в документе **Приложения**, в разделе Приложении Д. Спецификация сетевого адреса.

  Пример задания адреса Сервера:

tcp/10.4.0.18:2193

tcp/10.4.0.19

10.4.0.20

Если задать некорректное/неверное значение параметра **Сервер**, то Агенты отключатся от Сервера и больше не смогут к нему подключиться. В этом случае задание адреса Сервера необходимо производить непосредственно на станции.

- В поле **Количество повторений поиска** задайте параметр, определяющий количество попыток поиска Сервера Dr.Web при подключении с использованием режима *Multicasting*.
- В поле **Тайм-аут поиска (с)** задайте промежуток между попытками поиска Сервера Dr.Web в секундах при подключении с использованием режима *Multicasting*.
- Поля **Режим сжатия** и **Режим шифрования** определяют соответствующие настройки сжатия и шифрования сетевого трафика.
- В поле **Параметры прослушивания сети** укажите UDP-порт, используемый Центром управления для поиска в сети работающих Агентов Dr.Web. Чтобы запретить прослушивание портов, введите значение **NONE**.

  Параметр задается в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Д. Спецификация сетевого адреса.

  По умолчанию используется **udp/:2193**, что означает "все интерфейсы, порт 2193".

8.3.5. Лицензионные ключи

Просмотреть и отредактировать список лицензионных ключей станции или группы можно следующими способами:

1. Через Менеджер лицензий.
2. Через конфигурацию объекта лицензирования (станции или группы) в антивирусной сети.

Чтобы отредактировать список лицензионных ключей через конфигурацию объекта лицензирования

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Откройте раздел Свойства станции или Свойства группы для объекта, лицензионные ключи которого вы хотите отредактировать.
3. В разделе конфигурация нажмите значок **Редактировать** или ссылку **Лицензионные ключи**.
4. Открывшееся окно **Лицензионные ключи** содержит список лицензионных ключей объекта, их текущий статус (унаследованы или заданы персонально), а также список всех ключей, доступных на данном Сервере. Также при необходимости вы можете напрямую перейти в Менеджер лицензий.

5. Действия над списком ключей зависят от статуса текущих лицензионных ключей объекта:

Действие	Текущие ключи унаследованы	Текущие ключи заданы персонально	Ни один ключ не задан
Добавить лицензионный ключ	Наследование будет разорвано. Новый ключ добавится в список назначенных ключей, и список ключей станет персональным.	Новый ключ добавится в список назначенных ключей.	Ключи добавятся в список лицензионных ключей объекта в качестве персональных.
Удалить лицензионный ключ	Действие недоступно.	Ключ будет удален из списка ключей объекта.	Действие недоступно.
Установить наследование	Действие недоступно.	Текущие ключи будут удалены из списка ключей объекта, задано наследование ключей от первичной/родительской группы.	Действие недоступно.
Разорвать наследование	Наследование будет разорвано. Список ключей останется неизменным, но станет персональным.	Действие недоступно.	Действие недоступно.

Текущие ключи унаследованы

Чтобы добавить лицензионный ключ

1. В окне **Лицензионные ключи**, в списке **Все ключи** выберите один или несколько лицензионных ключей, которые вы хотите добавить.
2. Нажмите  .
3. В случае, если списки устанавливаемых компонентов на станциях и в добавляемых ключах различаются, будет выведено соответствующее предупреждение и предложено отредактировать результирующий список компонентов.
4. После внесения всех необходимых изменений нажмите **Сохранить**.
5. Наследование будет разорвано. Новый ключ добавится в список назначенных ключей, и список ключей станет персональным.

Чтобы разорвать наследование без изменения списка лицензионных ключей

1. В окне **Лицензионные ключи** нажмите кнопку **Скопировать настройки из первичной группы и установить их в качестве персональных**.

2. Наследование будет разорвано. Список ключей будет скопирован из первичной/родительской группы и задан для объекта в качестве персонального.
3. Нажмите **Сохранить**.

Текущие ключи заданы персонально

Чтобы добавить лицензионный ключ

1. В окне **Лицензионные ключи**, в списке **Все ключи** выберите один или несколько лицензионных ключей, которые вы хотите добавить.
2. Нажмите  .
3. В случае, если списки устанавливаемых компонентов на станциях и в добавляемых ключах различаются, будет выведено соответствующее предупреждение и предложено отредактировать список компонентов.
4. После внесения всех необходимых изменений нажмите **Сохранить**.
5. Новый ключ добавится в список назначенных ключей.

Чтобы удалить лицензионный ключ

1. В окне **Лицензионные ключи**, в списке **Ключи объекта** нажмите  напротив тех лицензионных ключей, которые вы хотите удалить.

> Если были удалены все ключи, будет установлено наследование лицензионных ключей от первичной/родительской группы (см. также Установление наследования).

2. Нажмите **Сохранить**.
3. В случае, если списки устанавливаемых компонентов на станциях и в оставшихся ключах различаются, будет выведено соответствующее предупреждение и предложено отредактировать результирующий список компонентов.

Чтобы установить наследование

1. Установить наследование вы можете одним из следующих способов:
   - Откройте раздел Свойства станции или Свойства группы для объекта, для которого вы хотите установить наследование. В разделе конфигурация нажмите значок **Удалить ключ**.
   - В окне **Лицензионные ключи**, в списке **Ключи объекта** нажмите напротив всех назначенных лицензионных ключей. Нажмите **Сохранить**.
2. Текущие ключи будут удалены из списка ключей объекта, задано наследование ключей от первичной/родительской группы.
3. В случае, если списки устанавливаемых компонентов на станциях и в наследуемых ключах различаются, будет выведено соответствующее предупреждение и предложено отредактировать список компонентов.

Ни один ключ не задан

Ситуация возможна только в том случае, если на Сервер не был добавлен ни один лицензионный ключ или лицензионные ключи были добавлены на Сервер, но не распространены ни на один объект, в том числе на группу **Everyone**.

Чтобы добавить лицензионный ключ

1. В окне **Лицензионные ключи**, в списке **Все ключи** выберите один или несколько лицензионных ключей, которые вы хотите добавить.
2. Нажмите  .
3. Нажмите **Сохранить**.
4. Ключи добавятся в список лицензионных ключей объекта в качестве персональных.

8.4. Настройка антивирусных компонентов

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

8.4.1. 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 в интернет. Контроль подключения и передачи данных по интернету 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.

Контроль приложений

Осуществляет мониторинг активности всех процессов на станциях. Позволяет администратору антивирусной сети регулировать, какие приложения разрешать, а какие — запрещать запускать на защищаемых станциях.

Станции под ОС семейства UNIX

Dr.Web Scanning Engine

Сканирующее ядро. Выполняет антивирусную проверку данных (содержимого файлов, загрузочных записей дисковых устройств, иных данных, полученных от других компонентов Dr.Web для UNIX). Организует очередь проверки. Выполняет лечение тех угроз, для которых данное действие применимо.

Dr.Web File Checker

Компонент проверки объектов файловой системы и менеджер карантина. Принимает от других компонентов Dr.Web для UNIX задания на проверку файлов. Обходит каталоги файловой системы согласно заданию, передает файлы на проверку сканирующему ядру. Выполняет удаление инфицированных файлов, перемещение их в карантин и восстановление из карантина, управляет каталогами карантина. Организует и содержит в актуальном состоянии кеш, хранящий информацию о ранее проверенных файлах и реестр обнаруженных угроз.

Используется всеми компонентами, проверяющими объекты файловой системы, такими как SpIDer Guard (для Linux, SMB, NSS).

Dr.Web ICAPD

ICAP-сервер, выполняющий анализ запросов и трафика, проходящего через прокси-серверы HTTP. Предотвращает передачу инфицированных файлов и доступ к узлам сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором.

SpIDer Guard для Linux (только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux)

Монитор файловой системы Linux. Работает в фоновом режиме и отслеживает операции с файлами (такие как создание, открытие, закрытие и запуск файла) в файловых системах GNU/Linux. Посылает компоненту проверки файлов запросы на проверку содержимого новых и изменившихся файлов, а также исполняемых файлов в момент запуска программ.

SpIDer Guard для SMB

Монитор разделяемых каталогов Samba. Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и закрытие файла, а также операции чтения и записи) в каталогах, отведенных для файловых хранилищ SMB-сервера Samba. Отправляет компоненту проверки файлов содержимое новых и изменившихся файлов на проверку.

SpIDer Guard для NSS (только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux)

Монитор томов NSS (Novell Storage Services). Работает в фоновом режиме и отслеживает операции файловой системы (такие как создание, открытие и

закрытие файла, а также операции записи) на томах NSS, смонтированных в указанную точку файловой системы. Отправляет содержимое новых и изменившихся файлов на проверку компоненту проверки файлов.

SpIDer Gate (только в составе дистрибутивов, предназначенных для ОС семейства GNU/Linux)

Компонент проверки сетевого трафика и URL. Предназначен для проверки данных, загружаемых на локальный узел из сети и передаваемых с него во внешнюю сеть, на наличие угроз, и предотвращения соединения с узлами сети, внесенными как в нежелательные категории веб-ресурсов, так и в черные списки, формируемые системным администратором.

Dr.Web MailD

Компонент проверки почтовых сообщений. Анализирует сообщения почтовых протоколов, разбирает сообщения электронной почты и подготавливает их к проверке на наличие угроз. Может работать в двух режимах:

1. Фильтр для почтовых серверов (Sendmail, Postfix и т. п.), подключаемый через интерфейс Milter, Spamd или Rspamd.
2. Прозрачный прокси почтовых протоколов (SMTP, POP3, IMAP). В этом режиме использует SpIDer Gate.

Остальные компоненты для станций под ОС семейства UNIX являются дополнительными и служат для внутренней настройки работы антивирусного ПО.

Станции под macOS

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.

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.

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.

SpIDer Guard

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

Фильтр звонков и SMS

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 интернету 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.

8.5. Антивирусная проверка рабочих станций

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

Запуск и успешная работа Сканера возможна даже при неработоспособности Агента, в том числе при загрузке системы 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.

8.5.1. 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** в главном 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**.

8.5.2. Запуск проверки рабочей станции

Чтобы запустить антивирусную проверку рабочих станций

1. Выберите пункт **Антивирусная сеть** в главном 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:

   Dr.Web Agent Сканер. 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.

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

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

8.5.3. 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** в главном 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 8-2. Список разделов настроек сканера в зависимости от варианта запуска

Вариант запуска сканирования	Разделы настроек			
	Общие	Действия	Ограничения	Исключения
Dr.Web Agent Сканер. Выборочное сканирование	+	+	+	+

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

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

8.5.3.1. Общие

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

Настройки, которые не поддерживаются при проверке станций, работающих под ОС Android, заключены в круглые скобки **( )**.

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

- В выпадающем списке выберите один из режимов проверки:
  - **Проверка всех дисков** — провести антивирусную проверку на всех доступных локальных дисках.
    При этом станут доступны дополнительные настройки:
    - 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 **[(Проверять загружаемые 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 **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.

- **Проверка указанных путей** — провести антивирусную проверку только по указанным путям.
  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.

- Установите флаг **Использовать эвристический анализ**, чтобы Сканер осуществлял поиск неизвестных вирусов при помощи эвристического анализатора. В данном режиме возможны ложные срабатывания Сканера.
- Установите флаг **Следовать символическим ссылкам**, чтобы следовать символическим ссылкам при сканировании.
- Установите флаг **[(Прерывать проверку при переходе на питание от аккумулятора)]**, чтобы прерывать антивирусную проверку при переходе компьютера пользователя на питание от аккумулятора.
- Установите флаг **[Отключить сеть при сканировании]**, чтобы отключить компьютер от локальной сети и интернета на время сканирования.
- Установите флаг **Архивы**, чтобы искать вирусы в файлах, упакованных в файловые архивы.
- Установите флаг **(Почтовые файлы)**, чтобы проверять почтовые ящики.
- Установите флаг **[(Инсталляционные пакеты)]**, чтобы проверять пакеты для установки программ.
- 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.

- В поле **[(Количество используемых ядер)]** задайте максимальное количество ядер процессора, используемых сканером. Допускаются целые значения от 0 до 32. Значение 0 предписывает использовать все доступные ядра.

При настройке группы станций следует обратить внимание на то, что для данного параметра задается абсолютное значение, а не процентное соотношение от общего количества доступных ядер. Поэтому задание одного и того же значения может привести к различной относительной загрузке станций с разным количеством процессорных ядер.

- 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**.

8.5.3.2. Исключения

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

Чтобы отредактировать список 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,
   - Путь, заканчивающийся символом \ — данный каталог исключается из проверки,
   - Путь, не заканчивающийся символом \ — любой подкаталог, путь к которому начинается на указанную строку, исключается из проверки.

   Пример для ОС Windows: `C:\Windows` — не проверять файлы каталога `C:\Windows` и все его подкаталоги.

Пример для ОС семейства Unix: `/etc` — не проверять файлы каталога `/etc` и все его подкаталоги.

2. Маски объектов, исключаемых из проверки. Для задания масок допускается использование знаков `?` и `*`.

   Пример для ОС Windows: `C:\Windows\*\*.dll` — не проверять все файлы с расширением `dll`, расположенные во всех подкаталогах каталога `C:\Windows`.

   Пример для ОС семейства Unix: `/etc/*/*.pub` — не проверять все файлы с расширением `pub`, расположенные во всех подкаталогах каталога `/etc`.

3. Заданные в операционной системе переменные окружения в составе пути до объектов, исключаемых из проверки.

   Пример для ОС Windows: `%WINDIR%\SysWOW64\` — не проверять файлы в подкаталоге `SysWOW64` каталога `C:\Windows`.

   Пример для ОС семейства Unix: `/home/*/network` — не проверять файлы в подкаталоге `network` каталога `/home`.

4. 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 https://support.microsoft.com/en-us/topic/virus-scanning-recommendations-for-enterprise-computers-that-are-running-currently-supported-versions-of-windows-kb822158-c067a732-f24a-9079-d240-3733e39b40bc. 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$}i`	не проверять файлы подкачки ОС Windows
`qr{\\notepad\.exe$}i`	не проверять файлы `notepad.exe`
`qr{^C:}i`	не проверять вообще ничего на диске `C`

Регулярное выражение	Значение
`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 К. Использование регулярных выражений в Dr.Web Enterprise Security Suite.

8.5.3.3. Действия

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и macOS, 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.
- **Сообщать** — 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 8-3. Действия Сканера над обнаруженными вредоносными объектами

Объект	Действие				
	Лечить	**Удалять**	**Перемещать в карантин**	**Сообщать**	**Игнорировать**
Инфицированные	+/*	+	+		
Подозрительные		+	+/*		+
Неизлечимые		+	+/*		
Инсталляционные пакеты		+	+/*		
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

Чтобы задать действия над обнаруженными угрозами, используйте 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 инсталляционные пакеты** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в составе пакетов для установки программ.
- 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.

8.5.3.4. Ограничения

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и macOS, 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.

8.6. 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.

8.6.1. 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.

Чтобы просмотреть таблицы

1. Выберите пункт **Антивирусная сеть** в главном 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:

- **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.
- 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**.
- 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.
- **Заблокированные устройства** — для просмотра списка устройств, заблокированных на станциях компонентом Офисный контроль.
- **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 единичных 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.
- **События Превентивной защиты** — для просмотра информации о событиях, зафиксированных на станциях компонентом Превентивная защита.
- События Контроля приложений — для просмотра информации о событиях, зафиксированных на станциях компонентом Контроль приложений.
- **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 кнопку **Сохранить** и перезагрузите Сервер.

Таблица 8-4. Соответствие пунктов раздела Статистика и флагов раздела Статистика в конфигурации Сервера

Пункты раздела Статистика	Флаги раздела Статистика в конфигурации Сервера
Угрозы	Обнаруженные угрозы безопасности
Ошибки	Ошибки сканирования

Пункты раздела Статистика	Флаги раздела Статистика в конфигурации Сервера
Статистика сканирования	Статистика сканирования
Запуск/Завершение	Запуск/Завершение компонентов
Статистика угроз	Обнаруженные угрозы безопасности
Состояние	Состояние станций
Задания	Журнал выполнения заданий на станциях
Заблокированные устройства	Заблокированные устройства
Вирусные базы	Состояние станций Состояние вирусных баз
Модули	Список модулей станций
События Превентивной защиты	Обнаруженные угрозы безопасности
События Контроля приложений	Статистика Контроля приложений по активности процессов Статистика Контроля приложений по блокировке процессов
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.

8.6.1.1. Сводные данные

Чтобы просмотреть сводные данные

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 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. Если в отчет включена таблица с обнаруженными угрозами, на панели инструментов становятся доступны также следующие опции:

Опция	Описание
Исключить файлы из сканирования	Позволяет добавить выбранные объекты в список исключений из сканирования компонентами защиты: a) В таблице **Угрозы** установите флаг напротив одного или нескольких обнаруженных объектов. b) Нажмите кнопку . c) В открывшемся окне задайте следующие настройки: • **Исключить из сканирования и задать персональные настройки SpIDer Guard** — добавить выбранные объекты в список исключений при сканировании компонентом SpIDer Guard. При этом, если узлы сети, для которых будет изменен список исключений, наследовали настройки компонента SpIDer Guard от своих первичных групп, то для них будет разорвано наследование и установлены персональные настройки. • **Исключить из сканирования и задать персональные настройки Сканера Dr.Web** — добавить выбранные объекты в список исключений при сканировании компонентом Сканер Dr.Web. При этом, если узлы сети, для которых будет изменен список исключений, наследовали настройки компонента Сканер Dr.Web от своих первичных групп, то для них будет разорвано наследование и установлены персональные настройки. • В списке **Исключить для следующих объектов** выберите узлы сети, для которых выбранный объект будет добавлен в список исключений: либо только для станции, на которой объект был обнаружен, либо для станций и пользовательских групп, выбранных в предложенном списке. d) Нажмите кнопку **Исключить**.
Сканировать	Повторно сканировать выбранные объекты. В выпадающем меню выберите тип сканирования.

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**.

Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

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.

8.6.1.2. Статистика сканирования

Чтобы получить статистику 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.

   Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

5. Для того чтобы посмотреть подробную статистику работы конкретных антивирусных средств, нажмите на название станции в таблице. Откроется окно (или раздел текущего окна), содержащее таблицу с подробными статистическими данными.
6. Чтобы произвести сортировку данных столбца таблицы, нажмите на соответствующую стрелку (сортировка по убыванию или по возрастанию) в заголовке соответствующего столбца.
7. При необходимости сохранить таблицу статистики 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.

8. 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).

8.6.1.3. Состояние

Чтобы просмотреть сведения 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. Нажмите значок в заголовке таблицы для изменения следующих параметров фильтра:
   - В поле **Поиск** введите произвольную строку для поиска по всем разделам таблицы.
   - В списке **Серьезность** установите флаги для требуемых уровней важности сообщений: список сообщений о состоянии будет содержать только сообщения с выбранной серьезностью.
   - 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.

     Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

   - В списке **Станции** установите флаги для типов статуса станций, сообщения о которых будут отображаться в списке:
     - **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.

   Для управления настройками фильтра используйте следующие кнопки в списке фильтра:
   - **По умолчанию** — установить все настройки фильтра в значения по умолчанию.
   - **Обновить** — применить выбранные настройки фильтра.
4. 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.

5. При необходимости сохранить отчет для распечатки или дальнейшей обработки нажмите на одну из кнопок на панели управления:
   - **Сохранить данные в CSV-файл**,
   - **Сохранить данные в HTML-файл**,
   - **Сохранить данные в XML-файл**,
   - **Сохранить данные в PDF-файл**.

8.6.1.4. События Контроля приложений

Настройка получения статистики

Чтобы активировать отправку информации со станций для раздела События Контроля приложений

1. В разделе **Антивирусная сеть** выберите в дереве станции или группы станций с установленным Контролем приложений, с которых вы хотите получать информацию о запуске приложений.
2. В управляющем меню выберите пункт **Windows** → **Агент Dr.Web**.
3. На вкладке **Общие** установите флаг **Отслеживать события Контроля приложений**, чтобы отслеживать активность процессов на станциях, зафиксированную Контролем приложений, и отправлять события на Сервер. При отсутствии подключения к Серверу события накапливаются и отправляются при подключении. Если флаг снят, активность процессов игнорируется.
4. Нажмите **Сохранить**.

Чтобы активировать сбор информации Сервером для раздела События Контроля приложений

5. В разделе **Администрирование** → **Конфигурация Сервера Dr.Web** перейдите на вкладку **Статистика**.
6. Установите одну из следующих опций:
   - **Статистика Контроля приложений по активности процессов**, чтобы получать и записывать информацию по любой активности всех процессов: как разрешенных для запуска, так и запрещенных Контролем приложений. При выборе этой опции в справочник будут заноситься приложения при условии создания и назначения хотя бы одного профиля с одной или несколькими выбранными категориями критериев функционального анализа.

До создания профилей и назначения их на станции антивирусной сети, запуск всех приложений разрешается.

- **Статистика Контроля приложений по блокировке процессов**, чтобы получать и записывать информацию по активности всех процессов, запрещенных для запуска Контролем приложений. При выборе этой опции в справочник будут заноситься приложения только после создания профилей, по настройкам которых запуск приложений будет блокироваться, и назначения этих профилей на станции антивирусной сети.

Флаг **Статистика Контроля приложений по активности процессов** может значительно повысить ресурсоемкость сбора статистики по всей антивирусной сети.

7. Нажмите кнопку **Сохранить**.
8. Перезапустите Сервер.
9. После перезагрузки Сервер начнет фиксировать всю статистику по запуску приложений, присылаемую со всех станций с установленным Контролем приложений.

Просмотр статистики

Чтобы просмотреть события, зафиксированные на станциях компонентом Контроль приложений

1. В иерархическом списке выберите станцию или группу.
2. В управляющем меню в разделе **Статистика** выберите пункт **События Контроля приложений**.
3. Откроется окно, содержащее список приложений, запуск которых был запрещен или разрешен на выбранных станциях.
4. По умолчанию отображается статистика за последние сутки. Для отображения данных за определенный период 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 будет загружена таблица со статистическими данными. Описание столбцов таблицы представлено в таблице ниже.

Таблица 8-5. Описание столбцов таблицы События Контроля приложений

Название столбца	Описание
Идентификатор	Идентификатор станции
Станция	Название станции
Адрес станции	Адрес станции

Название столбца	Описание
Идентификатор безопасности	Идентификатор безопасности учетной записи пользователя
Пользователь	Пользователь рабочей станции
Тип события	Тип запущенного на станции события
Примененное действие	Действие, примененное к запущенному на станции приложению
Критерий функционального анализа	Критерий, по которому разрешается или запрещается приложение
Маска функционального анализа	Параметр критерия функционального анализа, который определяет, разрешено приложение для запуска на станции или нет
ID профиля	Идентификатор профиля
Название профиля	Название профиля
ID правила	Идентификатор правила
Название правила	Название правила
Режим работы	Режим, в котором работает правило
Путь к файлу процесса	Расположение файла процесса
Процесс	Процесс, разрешенный или запрещенный для запуска на станции
Бюллетень с хешем процесса	Бюллетень, в котором присутствует хеш файла запущенного процесса
Путь к файлу скрипта	Расположение файла скрипта
Скрипт	Файл скрипта
Бюллетень с хешем скрипта	Бюллетень, в котором присутствует хеш файла запущенного скрипта
Появление события	Дата и время появления события
Оповещение о событии	Дата и время оповещения о событии
Хеш файла (SHA-256)	Значение хеша файла по алгоритму SHA-256

Название столбца	Описание
Описание файла	Описание файла
Издатель	Издатель файла
Издатель сертификата	Удостоверяющий центр, выпустивший сертификат
Хеш сертификата (SHA-1)	Значение хеша сертификата по алгоритму SHA-1
Дата начала действия сертификата	Дата начала действия сертификата
Дата окончания действия сертификата	Дата окончания действия сертификата

Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

5. При необходимости сохранить таблицу статистики 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.

При наличии профиля или правила в тестовом режиме запускаемые на назначенных станциях приложения проверяются по всей схеме работы Контроля приложений от начала до конца. В статистике будут фиксироваться случаи совпадения приложения по всем возможным критериям: настройкам функционального анализа, правилам и группе доверенных приложений. Следовательно, одно и то же приложение может иметь несколько записей в колонке **Примененное действие**, где будет указано, что оно разрешено по одним критериям и/или заблокировано по другим.

Создание правил

Чтобы создать новое правило на основе статистики по событиям Контроля приложений

1. В разделе **Статистика** → **События Контроля приложений** выберите строку с событием о попытке запуска приложения, для которого вы хотите создать правило, контролирующее запуск.
2. При нажатии на строку таблицы откроется окно с информацией о выбранном событии.
3. Нажмите кнопку **Создать правило**.
4. Откроется окно для создания нового правила. Задайте следующие настройки:
   a) В выпадающем списке **Название профиля** выберите профиль Контроля приложений, в котором будет создано правило.
   b) В поле **Название правила** задайте название для создаваемого правила.
   c) В разделе **Тип правила** выберите тип создаваемого правила: запрещающее или разрешающее.
   d) Для опции **Режим работы** выберите, в каком режиме будет работать созданное правило (соответствует флагу **Перевести правило в тестовый режим** при создании правила из профиля):
   Если вы хотите проверить работу правила, выберите режим **Тестовый**. Приложения не будут блокироваться на станциях, однако будет осуществляться запись журнала активности как при включенных настройках. Результаты запусков и блокировок приложений в тестовом режиме работы правила будут отображаться в разделе **События Контроля приложений**.
   В режиме **Активный** правило будет работать в активном режиме с блокировкой приложений на станциях по заданным настройкам правила (см. также режимы работы профилей).
   e) В разделе **Запрещать запуск приложений по следующим критериям/Разрешать запуск приложений по следующим критериям** (в зависимости от типа правила, выбранного на шаге 4c) будут автоматически заполнены поля в соответствии с приложением, на основе которого создается правило. При необходимости можете отредактировать значения настроек.
5. Нажмите **Сохранить**. Правило будет создано в заданном профиле Контроля приложений.

8.6.2. Графики

Графики и таблицы заражений

Чтобы просмотреть общие графики и таблицы с информацией об обнаруженных заражениях

1. Выберите пункт **Антивирусная сеть** в главном 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 и численные данные:
   - **Вирусная активность** — на графике отображается общее количество вредоносных объектов, найденных в пределах каждого временного промежутка для всех выбранных станций и групп.
   - **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.
   - **Произведенные действия** — приводится список действий, произведенных над обнаруженными вредоносными объектами. На круговой диаграмме отображается процентное соотношение между всеми произведенными действиями.
   - **Наиболее атакуемые станции** — приводится список станций, на которых были обнаружены угрозы безопасности. В таблице отображается общее количество угроз для каждой станции.
3. Для просмотра 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 календарях. Для просмотра данных нажмите кнопку **Обновить**.

Графики и таблицы итоговой статистики

В пункте **Графики** раздела **Общие** и в некоторых пунктах раздела **Статистика** управляющего меню приводятся графические и численные данные. В таблице ниже приведен список возможных графиков и таблиц и соответствующих разделов управляющего меню, в которых отображаются эти элементы.

Таблица 8-6. Соответствие графиков и таблиц разделам управляющего меню

Графики и таблицы	Разделы
Вирусная активность	Графики
Наиболее распространенные угрозы	Графики Угрозы Статистика угроз
Классы угроз	Графики Статистика угроз
Наиболее атакуемые 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.

8.6.3. 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.

Чтобы просмотреть и отредактировать содержимое карантина в Центре управления

1. Выберите пункт **Антивирусная сеть** в главном 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.

   При перемещении в карантин более одной угрозы нажмите в столбце **Информация** на количество перемещенных в карантин объектов, чтобы посмотреть весь список угроз во всплывающем окне.

   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 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**.
4. Для изменения отображения данных нажмите на значок ⚙ в заголовке таблицы:
   - Задайте настройки отображения строк (наиболее актуально для длинных строк).
   - Выберите, какие столбцы будут отображаться в таблице.

5. Чтобы отфильтровать файлы карантина, нажмите значок в заголовке таблицы и задайте следующие параметры фильтрации:
   - **Поиск** — задайте произвольную строку для поиска по всем разделам таблицы. В таблице будут отображаться только строки, соответствующие результатам поиска.
   - **Переместивший компонент** — выберите компонент защиты Dr.Web, который переместил файлы в карантин.
   - **Угроза** — выберите название обнаруженной угрозы согласно классификации компании «Доктор Веб».
   - **Исходное имя** — введите исходное имя объекта до перемещения в карантин.
   - **Размер файла, Б** — при помощи ползунка задайте диапазон размеров обнаруженных объектов в байтах.

   Нажмите кнопку **Применить**, чтобы вывести файлы карантина по заданным параметрам фильтра.

   Нажмите кнопку **По умолчанию**, чтобы сбросить все параметры фильтрации в начальные значения.

   Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

6. Для управления файлами, находящимися в карантине, установите флаг для соответствующего файла, группы файлов или для всех файлов на открытой странице карантина (в заголовке таблицы). На панели инструментов выберите одно из следующих действий:

Опция	Описание
Удалить файлы	
Удалить выбранные файлы	Удалить выбранные файлы из карантина и из системы.
Удалить все файлы	Удалить из карантина и из системы все файлы, попадающие под выбранные параметры фильтрации, т. е. все файлы, отображаемые в окне карантина.
Экспорт	Скопировать и сохранить выбранные в карантине файлы.

Опция	Описание
	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».
Восстановить файлы Используйте функцию восстановления файлов из карантина только если вы уверены, что объект безопасен.	
Восстановить выбранные файлы	Восстановить первоначальное местоположение выбранных в окне файлов, т. е. восстановить файлы на станции в каталоги, в которых они находились до перемещения в карантин.
Восстановить файлы по параметрам	В открывшемся окне задайте следующие настройки: • Если выбран один объект: ▫ **Восстановить файл как** — восстановить выбранный файл из Карантина и разместить его по заданному пути и с заданным именем. В поле **Восстановить файл по следующему пути** задайте полный путь на станции, по которому будет восстановлен выбранный файл. Имя файла должно быть обязательно задано. По умолчанию подставляется первоначальное местоположение и имя файла (до перемещения). При необходимости вы можете изменить этот параметр. ▫ **Восстановить файлы по типу угрозы** — восстановить из Карантина все файлы, которым был присвоен тот же тип угрозы, что и выбранному файлу. Тип угрозы приводится в поле **Восстановить файлы, содержащие следующую угрозу**. ▫ **Восстановить файлы по пути** — восстановить из Карантина все файлы, перемещенные из определенного каталога. В поле **Восстановить все файлы, перемещенные в карантин из следующего каталога** задайте путь к каталогу на станции. Все файлы, перемещенные в Карантин из указанного каталога, будут восстановлены. По умолчанию подставляется путь до каталога, в котором находился выбранный файл. При необходимости вы можете изменить этот параметр. • Если выбрано несколько объектов:

Опция	Описание
	▫ **Восстановить файлы** — восстановить первоначальное местоположение файлов на компьютере, т.е. восстановить файлы в каталоги, в которых они находились до перемещения в Карантин. ▫ **Восстановить файлы по типу угрозы** — восстановить из Карантина все файлы, которым были присвоены те же типы угроз, что и выбранным файлам. • В списке **Восстановить на следующих объектах** выберите узлы сети, на которых выбранный объект будет восстановлен из Карантина: либо только для станции, на которой объект был обнаружен, либо для пользовательских групп, выбранных в предложенном списке. • **Добавить исключения в качестве персональных настроек SplDer Guard** — добавить выбранные объекты в список исключений при сканировании компонентом SplDer Guard. При этом, если узлы сети, для которых будет изменен список исключений, наследовали настройки компонента SplDer Guard от своих первичных групп, то для них будет разорвано наследование и установлены персональные настройки. • **Добавить исключения в качестве персональных настроек Сканера Dr.Web** — добавить выбранные объекты в список исключений при сканировании компонентом Сканер Dr.Web. При этом, если узлы сети, для которых будет изменен список исключений, наследовали настройки компонента Сканер Dr.Web от своих первичных групп, то для них будет разорвано наследование и установлены персональные настройки.
	Восстановить все файлы Восстановить первоначальное местоположение всех файлов в окне карантина, т. е. восстановить файлы на станции в каталоги, в которых они находились до перемещения в карантин.
Сканировать файлы	
	Сканировать выбранные файлы Повторно сканировать выбранные в карантине файлы.
	Сканировать все файлы Повторно сканировать все файлы в окне карантина.

На отключенные станции запрос на восстановление и повторное сканирование будет отправлен только после подключения станций к Серверу.

7. 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**.

8.7. 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. В настройках запрещены вложения (установлен флаг **Отправлять только ссылку**, см. ниже): в письме отправляются только ссылки на скачивание пакетов.
2. Операционная система станции известна (вложения разрешены):
   a) ОС Windows: к письму прикладывается инсталляционный пакет Агента Dr.Web для Windows.
   b) ОС Linux, macOS, ОС Android: к письму прикладывается инсталляционный файл Агента Dr.Web для соответствующей операционной системы и конфигурационный файл с настройками подключения к Серверу Dr.Web.
3. Операционная система станции неизвестна — новая учетная запись станции, Агент еще не установлен (вложения разрешены):
   a) Если на Сервере нет пакетов для станций под ОС Linux, macOS, ОС Android (в частности, на Сервере не загружены **Корпоративные продукты Dr.Web**): 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, macOS, 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, macOS, ОС Android, а также ссылка на скачивание инсталляционных файлов для станций под ОС Linux, macOS, ОС Android.

Чтобы разослать инсталляционные пакеты 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 **Общие**:
     - 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.
     - Установите флаг **Отправлять только ссылку**, чтобы отправлять в письме только ссылку на скачивание пакета. При этом сам файл инсталляционного пакета не будет прикладываться к письму. Данная опция может быть полезна, если почтовый сервер клиента автоматически удаляет вложения из электронных писем.
   - 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.

   Параметры отправки электронной почты настраиваются в меню **Администрирование**, в разделе **Конфигурация Сервера Dr.Web**, на вкладке **Сеть**, на внутренней вкладке Электронная почта.
4. Нажмите кнопку **Отправить**.

8.8. 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. рисунок 8-1).

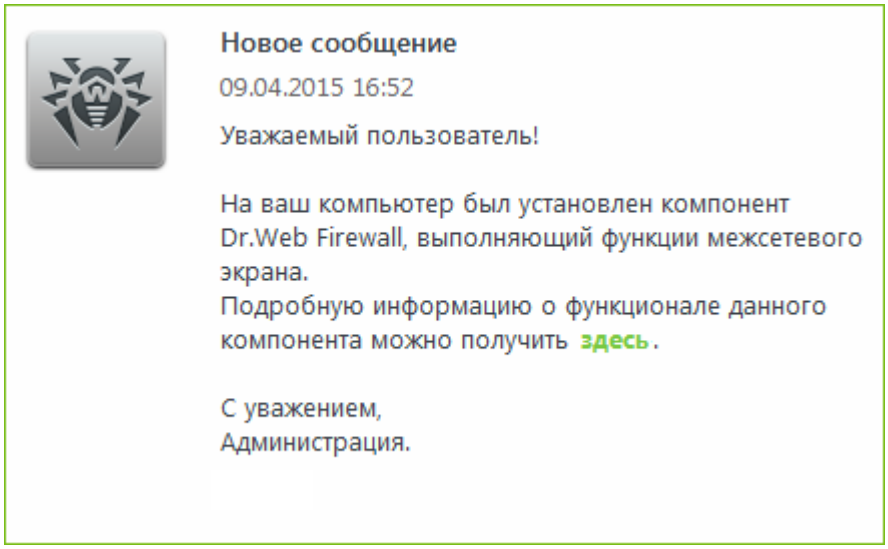


Рисунок 8-1. Окно сообщения на станции под ОС Windows

Чтобы отправить сообщение пользователю

1. Выберите пункт **Антивирусная сеть** в главном 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:
   - 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.
   - **Текст сообщения** — обязательное поле. Содержит непосредственно само сообщение длиной не более 250 символов.
   - Установите флаг **Показывать логотип в сообщении**, чтобы отображать графический объект в заголовке окна сообщения. Задайте следующие параметры логотипа:
     - 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).
     - В поле **URL-адрес для логотипа** можете задать ссылку на веб-страницу, которая будет открываться при нажатии на логотип и заголовок окна.

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:

a) В поле **Имя ссылки** укажите название ссылки — текст, который будет отображаться на месте ссылки в сообщении.

b) В поле **URL-адрес для ссылки** задайте URL-адрес веб-страницы, открываемой при клике на ссылку.

c) 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-адрес для ссылки** и **Имя ссылки**. При наличии одного или нескольких маркеров `{link}`, ссылка будет вставлена только на места маркеров.

d) Если маркер `{link}` не указан в поле **Текст сообщения**, ссылка будет вставлена единожды в конце сообщения на отдельной строке.

- 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).

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 8-1, были заданы следующие параметры:

Текст сообщения:

```
Уважаемый пользователь!


На ваш компьютер был установлен компонент Dr.Web Firewall, выполняющий
функции межсетевого экрана.

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


С уважением,

Администрация.
```

URL-адрес для ссылки: `http://drweb.com/`

Имя ссылки: `здесь`

Глава 9: Настройка Сервера Dr.Web

В данной главе приведено описание следующих возможностей по управлению параметрами работы антивирусной сети и Сервера Dr.Web:

- Управление лицензиями — параметры лицензирования;
- 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.

9.1. Управление лицензиями

9.1.1. Менеджер лицензий

Подробная информация о принципах и особенностях лицензирования Dr.Web Enterprise Security Suite приведена в разделе 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, в главном меню Центра управления выберите пункт **Администрирование**, в открывшемся окне в управляющем меню выберите пункт **Менеджер лицензий**.

Иерархический список ключей

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

Панель инструментов содержит следующие элементы управления:

Опция	Описание	Зависимость от объектов в дереве ключей
Добавить лицензионный 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 (станция, группа или политика) 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.	
Проверить наличие обновлений и заменить лицензионные ключи	Проверить наличие обновлений, располагаемых на ВСО, для всех ключей. При наличии обновлений скачать ключи и провести замену (см. Автоматическое обновление лицензий).	Опция всегда доступна. Действие распространяется на все лицензионные ключи в дереве.
Распространить ключ на соседние Серверы	Передать лицензии из выбранного ключа соседним Серверам.	Опция доступна, если в дереве выбран лицензионный ключ.

Настройки вида дерева позволяют изменять вид иерархического дерева:

- Флаг **Показывать количество лицензий** включает/отключает отображение в дереве ключей общего количества лицензий, предоставляемых лицензионными 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, станции и политики, 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 группы, содержащие объекты, для которых непосредственно назначены лицензионные ключи. При этом вложенными элементами групп являются станции и политики, входящие в данные группы, и лицензионные ключи, которые назначены для этих объектов. Данное представление дерева служит для удобства визуализации информации о лицензировании и не позволяет управлять объектами дерева.
- Для изменения внешнего вида дерева используйте следующие опции:
  - **Показывать идентификаторы клиентов** — включает/отключает отображение уникальных идентификаторов станций.
  - **Показывать названия клиентов** — включает/отключает отображение имен (названий) станций.
  - **Показывать адреса клиентов** — включает/отключает отображение IP-адресов станций.
  - **Показывать описания** — включает/отключает отображение описаний станций и групп станций.

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:

- Предоставляемое и используемое количество лицензий из данного лицензионного ключевого файла.
- 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.
- MD5-хеш лицензионного ключа.
- Разрешенные списки бюллетеней хешей для информирования о принадлежности обнаруженных угроз. Если функционал не лицензирован, данный параметр отсутствует.

  Отсутствие лицензии на бюллетени хешей не уменьшает уровень антивирусной защиты. Данная лицензия позволяет добавить оповещение администратору о том, что обнаруженная угроза присутствует в специализированных бюллетенях известных хешей угроз.

- Список антивирусных компонентов, которые позволяет использовать данная лицензия.

Добавление нового лицензионного ключа

Чтобы добавить новый лицензионный ключ

1. В главном окне Менеджера лицензий нажмите кнопку **Добавить лицензионный ключ** на панели инструментов.
2. На открывшейся панели нажмите кнопку и выберите файл с лицензионным ключом.
3. Установите флаг:
   - **Назначить лицензионный ключ группе Everyone**, если это первый лицензионный ключ в антивирусной сети. Добавляемый ключ будет автоматически назначен группе **Everyone**.
   - **Заменить лицензионный ключ группы Everyone**, если это не первый лицензионный ключ в антивирусной сети. Текущий лицензионный ключ группы **Everyone** будет заменен добавляемым лицензионным ключом.

Если для группы **Everyone** назначено несколько лицензионных ключей, то будет заменен первый в списке.

Если вы хотите заменить определенный лицензионный ключ группы **Everyone**, воспользуйтесь процедурой Обновление лицензионного ключа.

4. Нажмите кнопку **Сохранить**.
5. Лицензионный ключ будет добавлен в дерево ключей.

   Если на шаге 3 вы не установили соответствующий флаг, то добавленный лицензионный ключ не будет 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.

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.

Чтобы заменить текущий лицензионный ключ

1. В главном окне Менеджера лицензий в дереве ключей выберите ключ, который хотите назначить объекту лицензирования: группе станций, станции или политике.
2. На панели инструментов нажмите кнопку **Распространить ключ на группы и станции**. Откроется окно с иерархическим списком антивирусной сети.

3. Выберите в списке объекты лицензирования. Для выбора нескольких объектов используйте кнопки CTRL и SHIFT.

Чтобы назначить ключ для политики, необходимо выбрать саму политику или текущую версию этой политики (ключ автоматически назначается политике при выборе ее текущей версии и наоборот).

Лицензионный ключ также может быть назначен любой версии политики, которая не является текущей. При этом ключ будет назначен только этой версии, но не самой политике. Такой ключ не будут применяться к станциям, пока текущая версия политики не будет заменена на ту, которой этот ключ назначен.

Лицензионный ключ необходимо назначать политикам или их версиям непосредственно.

4. Нажмите кнопку **Заменить лицензионный 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.

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: группе станций, станции или политике.
2. На панели инструментов нажмите кнопку **Распространить ключ на группы и станции**. Откроется окно с иерархическим списком антивирусной сети.
3. Выберите в списке объекты лицензирования. Для выбора нескольких объектов используйте кнопки CTRL и SHIFT.

Чтобы назначить ключ для политики, необходимо выбрать саму политику или текущую версию этой политики (ключ автоматически назначается политике при выборе ее текущей версии и наоборот).

Лицензионный ключ также может быть назначен любой версии политики, которая не является текущей. При этом ключ будет назначен только этой версии, но не самой политике. Такой ключ не будут применяться к станциям, пока текущая версия политики не будет заменена на ту, которой этот ключ назначен.

Лицензионный ключ необходимо назначать политикам или их версиям непосредственно.

4. Нажмите кнопку **Добавить лицензионный 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 политик, которые назначены станциям без персональных настроек лицензионного ключа, должен быть задан лицензионный ключ.

Чтобы удалить лицензионный ключ или объект из списка лицензирования

1. В главном окне Менеджера лицензий выберите лицензионный ключ, который вы хотите удалить, или объект (станцию, группу или политику), для которого назначен этот ключ, и нажмите кнопку **Удалить выбранные объекты** на панели инструментов. При этом:
   - Если была выбрана группа или станция, то она удаляется из списка объектов, на которых распространяется действие назначенного для нее ключа. Для группы или станции, у которых удаляется персональный лицензионный ключ, устанавливается наследование лицензионного ключа.
   - Если была выбрана политика, то из списка объектов, на которых назначен лицензионный ключ, также удаляется текущая версия политики. Если была выбрана текущая версия политики, то сама политика также будет удалена. Однако, при удалении версии политики, которая не является текущей, сама политика и ее текущая версия не будут удалены.
   - Если был выбран лицензионный ключ, удаляется учетная запись ключа из антивирусной сети. Для всех групп и станций, 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.

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.

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 лицензионный 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 лицензионный 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.

Редактирование лицензий, переданных на соседний Сервер

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.

Чтобы настроить устанавливаемые компоненты при выполнении данных процедур

1. В окне настроек устанавливаемых компонентов в списке объектов приведены:
   - Станции, группы и политики 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, групп и политик), 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.

Чтобы настроить устанавливаемые компоненты при выполнении данных процедур

1. В окне настроек устанавливаемых компонентов в списке объектов приведены:
   - Станции, группы и политики 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, групп и политик), 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**.

9.1.2. Отчет об использовании лицензий

Отчет об использовании лицензий содержит информацию обо всех лицензиях, используемых как данным Сервером, так и соседними Серверами, в том числе при передаче лицензии по межсерверной связи.

Отчеты создаются (и отправляются в случае соседних Серверов) в соответствии с настройками, задаваемыми в разделе **Конфигурация Сервера Dr.Web** → **Лицензии**, раздел **Настройки для отчета по использованию лицензий**.

Для того чтобы просмотреть отчет, в главном меню Центра управления выберите пункт **Администрирование**, в открывшемся окне в управляющем меню выберите пункт **Отчет об использовании лицензий**.

В данном разделе приводится следующая информация:

- Отчет обо всех лицензиях, которыми распоряжается данный Сервер. Отчет будет присутствовать также в том случае, если на Сервере не настроена ни одна связь с соседними Серверами.
- Отчеты о лицензиях, которыми распоряжаются соседние Серверы, подотчетные данному Серверу, в том числе, получающие от него лицензии по межсерверным связям. При этом будут присутствовать отчеты ото всех соседних Серверов вниз по дереву межсерверных связей.

Каждый отчет отображается в виде отдельной таблицы и содержит информацию только о лицензиях одного Сервера — автора отчета.

В заголовке таблицы приводится следующая информация:

- **Сервер Dr.Web** — имя Сервера — автора отчета.
- **Всего лицензий, полученных по связям** — общее количество лицензий, которые Сервер получил по межсерверной связи.

Таблица отчета содержит следующие данные:

- **Пользователь** — пользователь лицензионного ключа, информация о лицензиях которого приводится в строке отчета.

- **Всего лицензий** — общее количество лицензий, предоставляемых из данного лицензионного ключа на этом Сервере.
- **Доступно** — количество свободных, не использованных лицензий в данном ключе.
- **Всего используется** — общее количество лицензий, которые использовались (были выданы станциям или соседним Серверам) на момент составления отчета.
- **Используется станциями** — количество лицензий, которые используются станциями, подключенными к Серверу — автору отчета.
- **В ожидании** — количество лицензий, которые автор отчета ожидает для получения. В частности, если Сервер, использовавший некоторое количество лицензий (либо уже назначил своим станциям, либо передал по межсерверным связям), лишился части этих лицензий. Например, был заменен лицензионный ключ на ключ с меньшим количеством лицензий или было уменьшено количество лицензий, полученных от родительского Сервера.
- **Зарезервировано** — количество лицензий, которые отданы по межсерверным связям, но получатель еще не забрал назначенные ему лицензии: соседние Серверы еще не подключались для получения лицензий. Данные лицензии зарезервированы из лицензионного ключа и не могут быть отданы другим станциям или Серверам.
- **Выдано по связям** — количество лицензий, которые Сервер — автор отчета выдал по межсерверным связям своим соседним Серверам.
- **Получено по связям** — количество лицензий, которые Сервер — автор отчета получил по межсерверным связям от своих соседних Серверов.
- **Дата отчета** — дата составления отчета.

Для лицензий, используемых станциями самого Сервера — автора отчета, доступна дополнительная информация. Для ее просмотра нажмите на количество лицензий в столбце **Используется станциями** (количество лицензий должно быть не нулевым). В открывшейся таблице **Использование лицензий группами** предоставляется следующая информация:

- **Название группы** — имя группы станций, на которую были распространены лицензии.
- **Распространено лицензий** — общее количество лицензий, распространенных на группу станций.
- **Активных станций** — количество активных станций в группе. Под активными подразумеваются станции, которые были в сети за период, указанный в настройках для генерации отчета на Сервере — владельце лицензионного ключа.

9.2. Ведение журнала

9.2.1. Журнал в реальном времени

Журнал в реальном времени позволяет просмотреть список событий и изменений, связанных с работой Сервера, выводимых сразу в момент появления события.

Журнал в реальном времени отображает информацию только в Центре управления и не осуществляет запись событий в файл. Файл журнала Сервера Dr.Web ведется отдельно со своими настройками и не зависит от журнала в реальном времени и его настроек.

При переходе в другой раздел вся информация, выведенная в журнале реального времени, удаляется.

Таблица журнала содержит следующие данные:

- **Время в формате журнала** — время появления события, представленное в формате журнала Сервера Dr.Web. Может быть использовано при поиске события в файле журнала Сервера.
- **Время** — время появления события, представленное в удобной для пользователя форме.
- **Уровень** — уровень ведения журнала, в соответствии с которым произошло событие.
- **PID** — идентификатор процесса, в рамках которого произошло событие.
- **TID** — идентификатор потока, в рамках которого произошло событие.
- **Поток** — название потока, в рамках которого произошло событие.
- **Подсистема** — название подсистемы, в рамках которой произошло событие.
- **Сообщение** — текст сообщения о произошедшем событии. Нажмите на сообщение в таблице, чтобы открыть окно с полным текстом сообщения. Если текст представляет собой HTML-код, установите флаг **Форматировать как HTML-текст** для корректного отображения информации. Учтите, что если в тексте сообщения присутствует JavaScript, он будет выполнен.

Чтобы изменить отображение данных в таблице

- При помощи значка :
  - Задайте настройки отображения строк (наиболее актуально для длинных строк).
  - Выберите, какие столбцы будут отображаться в таблице.
- При помощи значка :
  - Задайте произвольную строку для поиска по всем разделам таблицы. В таблице будут отображаться только строки, соответствующие результатам поиска.
  - Чтобы отображать только конкретные уровни, установите флаги напротив нужных уровней.
  - Чтобы отображать только конкретные подсистемы, установите флаги напротив нужных подсистем.

  Чтобы в журнал писались сообщения только конкретных уровней и от конкретных подсистем, задайте настройки ведения журнала.

На панели инструментов приведены следующие элементы управления журналом:

Настроить отображение данных — открыть окно настройки ведения журнала.

Очистить таблицу — удалить все данные, показанные в таблице. Операция необратима.

Остановить сбор данных — остановить вывод информации о событиях в таблицу. Кнопка активна, когда осуществляется сбор данных. При нажатии меняется на **Запустить сбор данных**.

Запустить сбор данных — начать вывод информации о событиях в таблицу. Кнопка активна, когда сбор данных остановлен. При нажатии меняется на **Остановить сбор данных**.

Настройка ведения журнала в реальном времени

1. На панели управления нажмите **Настроить отображение данных**. Откроется окно **Настройки отображения данных**.
2. Поле **Максимальное количество записей** задает ограничение на количество записей, выводимых в таблице журнала. При достижении заданного количества старые записи удаляются при поступлении новых.
3. Поле **Частота обновления, с** определяет частоту в секундах, с которой новые записи будут выводиться в журнал.
4. Поле **Поиск по подсистемам** позволяет осуществлять поиск по названию подсистем, приведенных ниже. Может использоваться при необходимости задания уровня подробности ведения журнала определенной подсистемы в случае большого количества подсистем в списке.
5. Таблица подсистем позволяет настроить список отображаемых данных и уровень их подробности:
   a) Установите флаги напротив тех подсистем, сообщения которых будут отображаться в таблице.
   b) Для выбранных подсистем выберите уровень подробности ведения журнала.
   c) Чтобы отображать все подсистемы, установите флаг в заголовке таблицы.
   d) Чтобы задать одинаковый уровень подробности ведения журнала для всех подсистем, выберите значение в выпадающем списке напротив подсистемы **all**. При этом в таблицу будут выведены только сообщения от тех подсистем, для которых установлены флаги.
6. Нажмите кнопку **Применить**, чтобы начать выводить данные в соответствии с заданными настройками.
7. Нажмите **Закрыть**, чтобы закрыть окно без изменений в настройках отображения журнала.

9.2.2. Журнал аудита

Журнал аудита позволяет просмотреть список событий и изменений, осуществленных при помощи управляющих подсистем Dr.Web Enterprise Security Suite.

Чтобы просмотреть журнал аудита

1. Выберите пункт **Администрирование** в главном 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. Для настройки вида таблицы нажмите значок ⚙ в правом углу заголовка таблицы. В выпадающем списке вы можете настроить следующие опции:
   - Включить или отключить перенос строк для длинных сообщений.
   - Выбрать столбцы, которые будут отображаться в таблице (отмечены флагом рядом со своим названием). Для включения/отключения столбца нажмите на строку с его названием.
   - Выбрать порядок следования столбцов в таблице. Для изменения порядка перетащите соответствующий столбец в списке на требуемое место.
5. Таблица журнала содержит следующие данные:
   - **Время** — дата и время, когда было произведено действие.
   - **Состояние** — краткий результат выполнения действия:
     - **ОК** — операция выполнена успешно.
     - **неуспешно** — во время выполнения операции произошла ошибка. Операция не выполнена.
     - **инициировано** — 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.
     - **запрещено** — выполнение запрошенного действия запрещено. Например, удаление системных групп.

Для действий, завершившихся с ошибкой (значение **неуспешно** в столбце **Состояние**), строки отмечаются красным цветом.

- **Сообщение / Ошибка** — подробное описание произведенного действия или возникшей ошибки.
- **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 М. 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.

6. Для отображения только определенных данных в таблице нажмите значок в правом углу заголовка таблицы. В выпадающем списке установите флаги для данных, которые вы хотите видеть в таблице.

   Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

7. 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.

9.2.3. Журнал 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: `/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 Л. Формат файлов журнала).

Чтобы просмотреть журнал работы Сервера через Центр управления

1. Выберите пункт **Администрирование** в главном 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.

Для изменения режима ведения журнала Сервера через Центр управления воспользуйтесь разделом Журнал.

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: `/var/opt/drwcs/etc/local.conf`;
- для ОС FreeBSD: `/var/drwcs/etc/local.conf`.

Содержимое файла `local.conf`:

```
# Log level.

DRWCS_LEV=info

# 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 33.8. Описание ключей.

> 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.

9.2.4. Журнал обновлений репозитория

Журнал обновлений репозитория содержит список обновлений с ВСО, включающий подробную информацию об обновленных ревизиях продуктов.

Чтобы просмотреть журнал обновлений репозитория

1. Выберите пункт **Администрирование** в главном 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. Чтобы отображать в таблице только события определенного типа, нажмите на значок на панели инструментов. В выпадающем списке выберите нужный вариант:
   - **Показывать все события** — в таблице журнала будут отображены все события, перечисленные в группах ниже.
   - **Показывать успешные сеансы обновления** — в таблице журнала будут отображены сеансы обновления, при которых соединение с ВСО было успешно установлено, на ВСО обнаружена новая ревизия, которая была успешно загружена в репозиторий Сервера.
   - **Показывать неуспешные сеансы обновления** — в таблице журнала будут отображены сеансы обновления, при которых соединение с ВСО было успешно установлено, на ВСО обнаружена новая ревизия, но загрузка этой ревизии завершилось неудачно.
   - **Показывать неуспешные соединения с ВСО Dr.Web** — в таблице журнала будут отображены сеансы обновления, при которых соединение с ВСО не было установлено или было прекращено до получения информации о ревизиях на ВСО.
5. 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.
   - **Полученная ревизия** — 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.

6. 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**, **Хеш файла**, **Размер** и **Состояние**.
7. 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.

9.2.5. Журнал сообщений

В журнале сообщений отображаются все текстовые сообщения, которые были отправлены администратором на станции антивирусной сети (см. Отправка сообщений станциям).

Журнал отправленных сообщений содержит следующую информацию:

- **Дата отправки**.
- **Отправитель** — регистрационное имя администратора, авторизованного в Центре управления при отправке сообщения.
- **Состояние** — количество сообщений, отправленных администратором, и количество сообщений, успешно доставленных на станции. Если количество отправленных и

доставленных сообщений совпадает, то информация об этих сообщениях выделяется серым цветом.

- **Сообщение** — текст отправленного сообщения. Опционально выводится информация об остальных настройках, которые были заданы при отправке.

При клике по конкретному сообщению в таблице открывается окно с подробностями о доставке: список всех получателей и дата доставки сообщения в случае успешной операции или сообщение **Не доставлено** — в случае неуспешной.

Для управления журналом сообщений используйте следующие опции на панели инструментов:

 **Отправить выбранные сообщения повторно** — опция доступна при выборе одного или нескольких отправленных сообщений в журнале (см. процедуры ниже).

 **Сохранить выбранное сообщение как шаблон** — создать из отправленного сообщения шаблон для повторного использования в дальнейшем. Опция доступна при выборе одного сообщения в журнале. Управление сохраненными шаблонами осуществляется в разделе Шаблоны сообщений.

В выпадающем списке выберите период, в течение которого были отправлены сообщения, которые вы хотите отобразить. Тот же самый период вы можете выбрать в полях с датами, которые задаются через выпадающий календарь. Для применения выбранного периода нажмите кнопку **Обновить**.

Чтобы повторно отправить одно сообщение

1. Установите флаг напротив сообщения, которое вы хотите отправить.
2. Нажмите кнопку  **Отправить выбранные сообщения повторно**.
3. Откроется окно **Отправка сообщения**. Задайте следующие настройки:
   a) В дереве **Антивирусная сеть** будут выбраны станции, на которые данное сообщение было отправлено. Можете оставить предыдущих получателей или выбрать произвольных получателей из представленного списка: это могут быть как отдельные станции, так и группы станций.
   b) Настройки сообщения аналогичны настройкам из раздела Отправка сообщений станциям.
4. Нажмите кнопку **Отправить**.

Чтобы повторно отправить несколько сообщений

1. Установите флаги напротив сообщений, которые вы хотите отправить.
2. Нажмите кнопку  **Отправить выбранные сообщения повторно**.
3. Откроется окно **Отправка нескольких сообщений**. В разделе **Список сообщений** приведены все сообщения, которые вы выбрали для повторной отправки. Названия сообщений соответствует датам их предыдущей отправки на станции.
4. Нажмите кнопку **Отправить все**, чтобы отправить все сообщения из списка.

5. Для редактирования какого-либо из сообщений, выберите его в разделе **Список сообщений**. В разделе **Настройки сообщения** задайте следующие параметры:
   a) В дереве **Антивирусная сеть** будут выбраны станции, на которые данное сообщение было отправлено. Можете оставить предыдущих получателей или выбрать произвольных получателей из представленного списка: это могут быть как отдельные станции, так и группы станций.
   b) Настройки сообщения аналогичны настройкам из раздела Отправка сообщений станциям.
   c) Чтобы удалить выбранное сообщение из списка на отправку, нажмите кнопку **Удалить**.

9.3. 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** в главном 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.

9.3.1. Общие

На вкладке **Общие** задаются следующие настройки работы Сервера:

- **Название Сервера** — 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.

Если вы выберете язык, тексты интерфейса на котором в данным момент не обновляются, вам будет предложено включить обновление для данного языка. Для этого перейдите по ссылке в раздел **Администрирование** → **Общая конфигурация репозитория** → **Сервер Dr.Web** → **Языки Центра управления безопасностью Dr.Web**, установите флаг для нужного вам языка и нажмите **Сохранить**. При ближайшем обновлении репозитория тексты интерфейса для выбранного языка будут обновлены. Также вы можете запустить обновление вручную в разделе **Состояние репозитория**.

- **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.

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:

```
<!-- Maximum authorization queue length -->
```

```
<maximum-authorization-queue size='50'/>
```

- 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.
- Установите флаг **Автоматически создавать учетные записи станций**, чтобы автоматически создавать недостающие учетные записи станций в Центре управления при установке Агентов из группового инсталляционного пакета. Если флаг снят, установка возможна только по количеству уже созданных учетных записей в группе, инсталляционный пакет для станций которой запускается.
- 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.
- В выпадающем списке **Имя станции** задается формат отображения имен рабочих станций в каталоге антивирусной сети Центра управления.
- Через выпадающий список **Заменять имя станции** можно при необходимости задать вариант замены отображаемых имен рабочих станций на полное или частично определенное DNS-имя (при невозможности определения DNS-имен отображаются IP-адреса).

По умолчанию флаг **Заменять IP-адреса** снят, и замена имени станций не происходит. При неправильной настройке службы DNS включение этих возможностей может значительно замедлить работу Сервера. При включении любого из этих режимов рекомендуется разрешить кеширование имен на DNS-сервере.

Если в выпадающем списке **Заменять имя станции** выбран один из вариантов замены, и в антивирусной сети используется Прокси-сервер, тогда 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 **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.
- Установите флаг **Использовать политики**, чтобы разрешить использовать политики для настройки защищаемых станций (см. Политики).
  - **Количество версий политики** — максимальное количество версий, которые могут быть созданы для каждой политики.
- В поле **Количество резервных копий для версий Сервера** задайте максимальное количество хранимых резервных копий, созданных при переходе на новую ревизию Сервера через Центр управления (см. раздел Обновление Сервера Dr.Web и восстановление из резервной копии). Значение 0 предписывает хранить все резервные копии.
- Установите флаг **Использовать расширение протокола Агента для передачи файловых данных**, чтобы разрешить передачу файловых данных с Агента на Сервер по протоколу SFTP. Если флаг снят, передача данных не осуществляется.
- В поле **Количество виртуальных машин Lua** задайте максимальное количество виртуальных машин Lua, предварительно подготовленных для нужд веб-сервера.
- В поле **Скрипт для создания виртуальной машины Lua** вставьте скрипт, выполняемый при фоновом создании виртуальной машины Lua для нужд веб-сервера.

9.3.2. Трафик

9.3.2.1. Обновления

На вкладке **Обновления** задаются ограничения на объем сетевого трафика при передаче обновлений между Сервером и Агентами.

Подробнее см. в п. Ограничение трафика обновлений.

Чтобы задать ограничения на трафик обновлений Агентов

1. В поле **Количество одновременных процессов обновления** задается максимальное допустимое количество сессий раздачи обновлений, запущенных одновременно с данного Сервера. При достижении указанного ограничения запросы от Агентов

размещаются в очереди ожидания. Размер очереди ожидания не ограничен. Установите значение **0**, чтобы снять ограничение на количество одновременных процессов.

2. Установите флаг **Ограничить трафик обновлений**, чтобы ограничить объем сетевого трафика при передаче обновлений между Сервером и Агентами.

   Если флаг снят, обновления для Агентов передаются без ограничения полосы пропускания сетевого трафика.

3. 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.

   Допускается задание до пяти ограничений на скорость передачи обновлений. Для добавления еще одного поля ограничения скорости нажмите кнопку  . Для удаления ограничения нажмите кнопку  напротив ограничения, которое нужно удалить.

4. В таблице расписания задается режим ограничения обновлений отдельно на каждые 30 минут каждого дня недели.

   Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков путем перетаскивания мышью.

   Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей, начиная с варианта, при котором передача обновлений разрешена без ограничений трафика, до варианта, при котором передача обновлений запрещена.

5. После завершения редактирования, нажмите кнопку **Сохранить** для принятия внесенных изменений.

9.3.2.2. Установки

На вкладке **Установки** задаются ограничения на объем сетевого трафика при передаче данных в процессе установки Агентов Dr.Web на станциях.

Подробнее см. в п. Ограничение трафика рабочих станций.

Чтобы задать ограничения на трафик при установке Агентов

1. В поле **Количество одновременных процессов установки** задается максимальное допустимое количество сессий установки Агента, запущенных одновременно с данного Сервера. При достижении указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен. Установите значение **0**, чтобы снять ограничение на количество одновременных процессов.

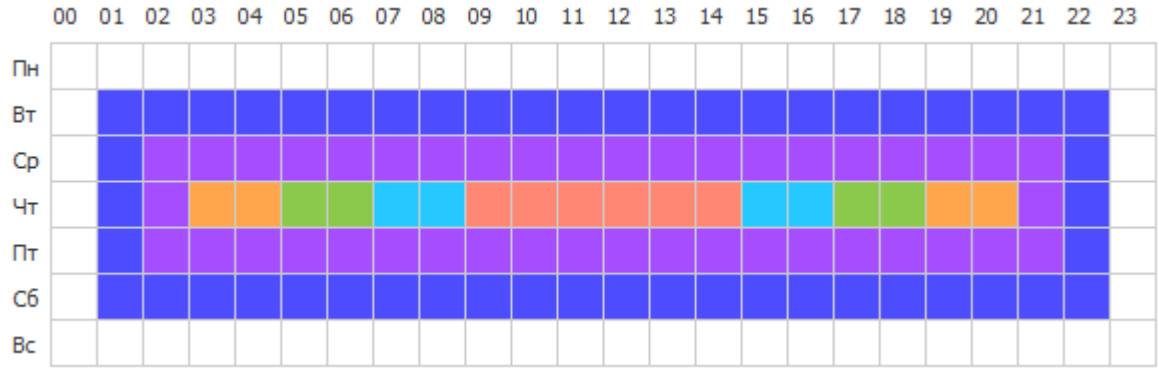
2. Установите флаг **Ограничить трафик при установке Агентов**, чтобы ограничить объем сетевого трафика при передаче данных с Сервера на станции в процессе установки Агентов Dr.Web.

   Если флаг снят, передача данных при установке Агентов осуществляется без ограничения полосы пропускания сетевого трафика.

3. Если флаг установлен, задайте в поле **Максимальная скорость передачи (КБ/с)** значение максимальной скорости передачи данных. При этом данные для установки Агентов будут передаваться в пределах заданной полосы пропускания совокупного сетевого трафика всех Агентов.

   Допускается задание до пяти ограничений на скорость передачи данных для установки Агентов. Для добавления еще одного поля ограничения скорости нажмите кнопку  . Для удаления ограничения нажмите кнопку  напротив ограничения, которое нужно удалить.

4. В таблице расписания задается режим ограничения на передачу данных отдельно на каждые 30 минут каждого дня недели.



   Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков путем перетаскивания мышью.

   Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей, начиная с варианта, при котором передача данных разрешена без ограничений трафика, до варианта, при котором передача данных запрещена.

5. После завершения редактирования, нажмите кнопку **Сохранить** для принятия внесенных изменений.

9.3.2.3. Ограничение трафика рабочих станций

В антивирусной сети Dr.Web Enterprise Security Suite существует возможность ограничить скорость передачи данных между Сервером и Агентами. Настройки делятся на ограничения передачи обновлений и ограничения при передаче данных при установках Агента.

Предоставляется возможность следующих вариантов ограничения трафика:

1. Ограничение общей скорости передачи данных всем станциям.

Настройка осуществляется в разделе конфигурации Сервера: пункт главного меню **Администрирование** → пункт управляющего меню **Конфигурация Сервера Dr.Web** → вкладка **Трафик** → внутренняя вкладка **Обновления** или **Установки** → параметр **Ограничить трафик обновлений** или **Ограничить трафик при установке Агентов** соответственно.

2. Персональное ограничение скорости передачи данных при обновлении конкретным станциям или группам станций.

   Настройка осуществляется в разделе конфигурации станций: пункт главного меню **Антивирусная сеть** → выбрать станцию или группу в иерархическом списке сети → пункт управляющего меню **Ограничения обновлений** → параметр **Ограничить трафик обновлений**.

Ограничение трафика осуществляется по следующему принципу:

1. Если включено ограничение на общую скорость передачи данных в настройках Сервера, то суммарная скорость передачи данных от Сервера всем станциям не превысит указанного значения. При этом:
   a) Вне зависимости от различий в пропускной способности каналов связи между Сервером и станциями, скорость передачи данных делится поровну между всеми станциями.
   b) Если пропускная способность канала между Сервером и станцией меньше полученного среднего значения скорости для одной станции согласно пункту a), для такой станции устанавливается ограничение передачи данных равное максимальной ширине канала до этой станции. Оставшееся значение общего ограничения аналогично пункту a) делится поровну для остальных станций.
2. Если включено персональное ограничение на скорость передачи данных в настройках группы или конкретной станций, то скорость передачи данных на эти группы или станцию не превысит указанного значения. На все остальные станции ограничение не распространяется, и передача данных осуществляется с максимальной скоростью.
3. Если включено ограничение на общую скорость передачи данных в настройках Сервера и персональное ограничение на группу или станцию, то:
   a) Скорость передачи данных на персонально ограниченные группы или станции не превысит значения, заданного в разделе настроек этих групп и станций.
   b) Для передачи данных на остальные станции, общее ограничение скорости передачи данных с учетом вычета ограничения станции из п. a) делится поровну.
   c) Если пропускная способность канала между Сервером и станцией, не ограниченной индивидуально, меньше полученного среднего значения скорости для одной станции согласно пункту b), для такой станции устанавливается ограничение передачи данных равное максимальной ширине канала до этой станции. Оставшееся значение общего ограничения аналогично пункту b) делится поровну для остальных станций, не ограниченных индивидуально.

9.3.3. Сеть

9.3.3.1. DNS

На вкладке **DNS** задаются параметры обращений к DNS-серверу:

- **Тайм-аут для DNS-запросов (с)** — 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 кеше ответов от DNS-сервера (TTL).
  - **Для положительных ответов (мин.)** — время хранения в кеше (TTL) положительных ответов от DNS-сервера в минутах.
  - **Для отрицательных ответов (мин.)** — время хранения в кеше (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.

9.3.3.2. 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. При необходимости в адресной строке допускается задание порта в формате <*адрес*>:<*порт*>. По умолчанию используется порт `3128`.
- 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

Опция		Описание
		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.
	Digest-авторизация с поддержкой IE	Использовать Digest-авторизацию. Криптографический метод авторизации. Включает поддержку браузера Internet Explorer версии 6 и более ранних.
	NTLM-авторизация	Использовать NTLM-авторизацию. Криптографический метод авторизации. Для авторизации используется протокол NTLM компании Microsoft.
	NTLM-авторизация через winbind	Использовать NTLM-авторизацию через внешнее приложение winbind. Криптографический метод авторизации.
	GSS-Negotiate авторизация	Использовать GSS-Negotiate авторизацию. Криптографический метод авторизации.

9.3.3.3. Транспорт

На вкладке **Транспорт** настраиваются параметры транспортных протоколов, используемых Сервером для соединения с клиентами.

- 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.
- 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. Шифрование и сжатие 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.

Более подробная информация приведена в разделе Шифрование и сжатие трафика.

- В поле **Ключ шифрования для мандатов TLS-сессии** задайте путь к файлу ключа шифрования для мандатов TLS-сессий. Используется для возобновления сеанса TLS на основе мандатов сессий (session tickets), которые шифруются с использованием заданного ключа.

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.
- 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`.
- **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.
- 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 Д. Спецификация сетевого адреса.

9.3.3.4. Электронная почта

На вкладке **Электронная почта** настраиваются параметры отправки электронной почты из Центра управления, например, в качестве оповещений администратора или при рассылке инсталляционных пакетов станций:

- **Электронная почта отправителя** — адрес ящика электронной почты, от имени которого будут отправляться электронные письма.

- **Адрес сервера** — 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.
- **Тайм-аут соединения с SMTP-сервером** — тайм-аут в секундах для установления соединения с SMTP-сервером. Значение — целое положительное число большее или равное 1.
- В выпадающем списке **Защита соединения** выберите тип шифрованного обмена данными:
  - **STARTTLS** — переключение на защищенное соединение осуществляется через команду `STARTTLS`. По умолчанию для соединения предусматривается использование 25 порта.
  - **SSL/TLS** — открыть отдельное защищенное шифрованное соединение. По умолчанию для соединения предусматривается использование 465 порта.
  - **Нет** — не использовать шифрование. Обмен данными будет происходить по незащищенному соединению.
- 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 LOGIN аутентификацию** для использования *LOGIN* аутентификации на почтовом сервере.
- Установите флаг **Использовать AUTH-NTLM аутентификацию** для использования *AUTH-NTLM* аутентификации на почтовом сервере.
- Установите флаг **Использовать обычную аутентификацию** для использования *plain text* аутентификации на почтовом сервере.
- Установите флаг **Проверять правильность сертификата Сервера** чтобы проверять правильность TLS-сертификата почтового сервера. В поле **Сертификат Сервера** укажите путь к корневому TLS-сертификату Сервера Dr.Web.
- Установите флаг **Отладочный режим** для получения детального журнала SMTP-сессии.
- В поле **Электронная почта получателей** можете задать адреса ящиков электронной почты, чтобы проверить отправку электронной почты. Нажмите кнопку **Отправить тестовое сообщение**, чтобы отправить тестовое письмо (аналогичное оповещению Сервера) по электронной почте в соответствии с заданными настройками в данном разделе.

9.3.3.5. 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.
- **Срок жизни** — срок жизни датаграммы при передаче данных в кластере Серверов Dr.Web.
- **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.

9.3.3.6. 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. Ж3. Конфигурационный файл download.conf).

9.3.3.7. 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**.

Основные принципы работы групповых обновлений:

1. Если групповые обновления включены, то для всех станций, подключенных к данному Серверу, обновление будет осуществляться в два этапа:
   a) Станции прослушивают заданные multicast-группы, в которые входит Сервер. При поступлении групповых обновлений, станции скачивают их через *multicast over UDP*.
   b) После передачи групповых обновлений Сервер отправляет стандартное оповещение станциям о наличии обновлений. Все, что не удалось скачать через групповые обновления, станции докачивают как при стандартном обновлении по протоколу TCP.
2. Если групповые обновления отключены, обновление для всех станций осуществляется только штатным способом — 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 избежание 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.

- **Срок жизни** — срок жизни датаграммы при передаче данных в процессе групповых обновлений.
- **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.

В разделе **Список контроля доступа** задаются ограничения на сетевые адреса станций, которые будут получать групповые обновления:

- Станции, которым разрешено получать групповые обновления, будут прослушивать заданные multicast-группы и получать обновления по стандартной схеме (см. процедура 1).
- Станции, которым запрещено получать групповые обновления, не прослушивают заданные multicast-группы на наличие обновлений, а скачивают все обновления по TCP (см. процедура 2).

Настройка списков осуществляется аналогично настройке списков раздела Безопасность.

9.3.4. Статистика

На вкладке **Статистика** задается статистическая информация, которая записывается в журнал протокола, заносится в базу данных Сервера и в дальнейшем может быть просмотрена в разделе статистики Центра управления.

Чтобы добавить в БД информацию соответствующего типа, 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 станций** — 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.

  - Установите флаг **Отслеживать эпидемии**, чтобы включить режим оповещения администратора о случаях вирусных эпидемий. Если флаг снят, оповещения о вирусных заражениях будут осуществляться в обычном режиме. При установленном флаге вы также можете задать следующие параметры отслеживания вирусных эпидемий:
    - **Период запрета на отправку оповещений** — промежуток времени в секундах после отправки оповещения об эпидемии, в течение которого не будут отправляться оповещения о единичных заражениях станций.
    - **Период подсчета зараженных станций** — промежуток времени в секундах, в течение которого должно прийти заданное количество сообщений о зараженных станциях, чтобы отправить оповещение об эпидемии.

- **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 (оповещение **Эпидемия в сети**).
- **Количество наиболее распространенных угроз** — количество наиболее часто встречающихся угроз, которые необходимо включить в отчет об эпидемиях.

▫ Установите флаг **Группировать отчеты Превентивной защиты**, чтобы присылать единый суммарный отчет о множественных событиях Превентивной защиты. Если флаг снят, события Превентивной защиты будут приходить в отдельных оповещениях вне зависимости от их количества. При установленном флаге вы также можете задать следующие параметры группировки отчетов:

- **Период запрета на отправку оповещений** — промежуток времени в секундах после отправки суммарного отчета о событиях Превентивной защиты, в течение которого не будут отправляться оповещения о единичных событиях.
- **Период подсчета событий** — промежуток времени в секундах, в течение которого должно произойти заданное количество событий Превентивной защиты, чтобы отправить суммарный отчет.
- **Количество событий** — количество событий Превентивной защиты, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единый суммарный отчет об этих событиях (оповещение **Суммарный отчет Превентивной защиты**).
- **Количество наиболее активных процессов** — количество наиболее часто встречающихся процессов, осуществивших подозрительное действие, которые необходимо включить в отчет Превентивной защиты.

▫ 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.

- **Аварийные завершения соединений** — разрешает отслеживать аварийно завершенные соединения с клиентами и иметь возможность отправлять соответствующие оповещения администратору.

  Задайте следующие настройки аварийных завершений соединений:

  ▫ **Период запрета на отправку оповещений** — промежуток времени в секундах после отправки оповещения о множественных завершениях соединений, в течение которого не будут отправляться оповещения о единичных завершенных соединениях.

  ▫ **Период подсчета завершенных соединений** — промежуток времени в секундах, в течение которого должно произойти заданное количество разрывов соединений с клиентами, чтобы отправить соответствующее оповещение.

- **Количество соединений для оповещения о единичных завершениях** — минимальное количество соединений, которые должны быть разорваны с одним адресом в течение периода подсчета, чтобы было отправлено оповещение о единичном аварийном завершении соединения (оповещение **Аварийное завершение соединения**).
- **Количество соединений для оповещения о множественных завершениях** — минимальное количество соединений, которые должны быть разорваны в течение периода подсчета, чтобы было отправлено единое оповещение о множественных аварийных завершениях соединений (оповещение **Зафиксировано большое количество аварийно завершенных соединений**).
- **Длительность коротких соединений** — если длительность завершенного соединения с клиентом меньше указанной, то при достижении заданного количества соединений будет отправлено оповещение о единичных завершениях соединений (оповещение **Аварийное завершение соединения**) вне зависимости от периода подсчета. При этом соединение не должно быть прервано в дальнейшем более продолжительными подключениями, и не должно быть отправлено оповещение о множественных аварийных завершениях соединений (оповещение **Зафиксировано большое количество аварийно завершенных соединений**).

- **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.
- **Заблокированные устройства** — разрешает мониторинг информации об устройствах, заблокированных компонентом Офисный контроль, и запись информации в базу данных.
- **Статистика Контроля приложений по активности процессов** — разрешает мониторинг информации об активности процессов на станциях, зафиксированной Контролем приложений, и запись информации в базу данных.
- **Статистика Контроля приложений по блокировке процессов** — разрешает мониторинг информации о блокировках процессов на станциях Контролем приложений и запись информации в базу данных.
- **Множественные блокировки Контролем приложений** — разрешает отслеживать множественные блокировки процессов Контролем приложений и иметь возможность отправлять соответствующие оповещения администратору.

  Задайте следующие настройки событий:

  - **Период запрета на отправку оповещений** — промежуток времени в секундах после отправки суммарного отчета о процессах, заблокированных Контролем приложений, в течение которого не будут отправляться оповещения о единичных блокировках.

  - **Период подсчета заблокированных процессов** — промежуток времени в секундах, в течение которого должно быть заблокировано заданное количество процессов, чтобы отправить суммарный отчет.
  - **Количество блокировок** — количество событий о процессах, заблокированных Контролем приложений, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единый суммарный отчет об этих событиях (оповещение **Зафиксировано большое количество блокировок Контролем приложений**).
  - **Количество наиболее распространенных профилей** — количество наиболее распространенных профилей, по которым производилась блокировка и которые необходимо включить в оповещение о множественных блокировках.
- **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**.
- **Данные о местоположении** — разрешает получать информацию о местоположении станций и записывать информацию в базу данных.

Чтобы просмотреть статистическую информацию

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 9-1. 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

Настройки Сервера	Пункты меню
Состав оборудования и программ	Общие → Оборудование и программы Общие → Обнаруженные устройства
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 Статистика → События Превентивной защиты
Ошибки сканирования	Статистика → Ошибки
Статистика сканирования	Статистика → Статистика сканирования
Инсталляции Агентов	Статистика → Инсталляции Агентов
Заблокированные устройства	Статистика → Заблокированные устройства
Статистика Контроля приложений по активности процессов	Статистика → События Контроля приложений Администрирование → Контроль приложений → Справочник приложений
Статистика Контроля приложений по блокировке процессов	
Журнал выполнения заданий на станции	Статистика → Задания
Состояние станций	Статистика → Состояние Статистика → Вирусные базы
Состояние вирусных баз	Статистика → Вирусные базы

9.3.5. 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.
- **Связи** — 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.

Чтобы настроить ограничения доступа (задаются отдельно для Агентов, Инсталляции, соседних Серверов или Службы обнаружения):

1. Установите флаг **Использовать этот список доступа**, чтобы задать списки разрешенных или запрещенных адресов. Если флаг снят, все соединения будут разрешены.
2. Чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.
3. Чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.
4. 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**.

Чтобы отредактировать список адресов:

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**.

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 16777214 адресов (256*256*256-2).

   Адреса хостов в этих сетях вида: `125.*.*.*`

9.3.6. Кеш

На вкладке **Кеш** задаются параметры очистки серверного кеша:

- **Период очистки кеша** — периодичность полной очистки кеша.
- **Файлы в карантине** — периодичность удаления файлов в Карантине на стороне Сервера.
- **Файлы репозитория** — периодичность удаления файлов в репозитории.
- **Кеш файлов** — периодичность очистки файлового кеша.
- **Инсталляционные пакеты** — периодичность удаления персональных и групповых инсталляционных пакетов.

  Нажмите кнопку  **Удалить все инсталляционные пакеты сейчас**, чтобы удалить все ранее созданные персональные и групповые инсталляционные пакеты, находящиеся в каталоге `installers-cache` каталога `var`. Обратите внимание: при обращении к данным пакетам для скачивания, они будут созданы заново, что может занять некоторое время.

При задании числовых значений обратите внимание на выдающие списки с единицами измерения периодичности.

9.3.7. 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.

Чтобы задать параметры работы с базой данных

1. В поле **Количество соединений** задайте максимально допустимое количество соединений Сервера с базой данных. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.
2. Установите флаг **Автоматически очищать базу данных после процедур обслуживания**, чтобы автоматически проводить отложенную очистку базы данных после ее инициализации, обновления и импорта. Если флаг снят, автоматическая очистка не будет выполняться. В этом случае рекомендуется настроить задание **Очистка базы данных** в расписании Сервера или выполнять очистку вручную через раздел Управление базой данных.

   Для выполнения автоматической очистки создается скрытое задание в расписании Сервера. Задание выполняется ближайшей ночью после обозначенных процедур обслуживания, в 01:17 по местному времени Сервера. Задание выполняется только в том случае, если в расписании Сервера не запланировано другого задания **Очистка базы данных** в течение ближайших суток относительно обозначенных процедур обслуживания.
3. В выпадающем списке **База данных** выберите тип базы данных:
   - **MySQL** — внешняя БД,
   - **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://docs.microsoft.com/en-US/troubleshoot/sql/general/determine-version-edition-update-level.

   - **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).

4. Задайте необходимые настройки для работы со встроенными БД:
   - При необходимости, введите в поле **Имя файла** полный путь к файлу с базой данных.
   - Задайте размер кеш-памяти БД.
   - Задайте размер кеша предкомпилированных sql-операторов.
   - В поле **Размер отображенного в память файла (Б)** задайте в байтах максимальный размер файла БД.
   - В выпадающем списке **Проверка целостности образа** выберите режим проверки целостности образа БД при запуске Сервера Dr.Web.
   - Установите флаг **Восстанавливать поврежденный образ автоматически**, чтобы автоматически восстанавливать поврежденный образ БД при запуске Сервера Dr.Web.
   - При необходимости, установите флаг **Включить WAL**, чтобы включить упреждающее журналирование. При установленном флаге вы можете настроить дополнительные параметры:
     - В поле **Максимальное число "грязных" страниц** задайте максимальное число, при достижении которого осуществляется запись страниц на диск.
     - В поле **Максимальная задержка записи страниц (с)** задайте максимальное время на которое откладывается запись страниц на диск (в секундах).
   - Задайте режим записи данных.
5. Для применения заданных настроек нажмите кнопку **Сохранить**.

Параметры для внешних БД описаны в документе **Приложения**, в разделе Приложение Б. Настройки для использования СУБД. Параметры драйверов СУБД.

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 использовать в качестве внешней базы данных БД Oracle через ODBC-подключение, то при установке (обновлении) Сервера, в настройках инсталлятора отмените установку встроенного клиента для СУБД Oracle (в разделе **Поддержка баз данных → Драйвер базы данных Oracle**).
  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.

9.3.7.1. Восстановление баз данных

В случае сбоя встроенной базы данных **SQLite3** существует возможность восстановления поврежденной базы штатными средствами.

В случае повреждения базы данных выполняется следующая последовательность действий:

1. При наличии повреждения базы данных запуск и функционирование Сервера не осуществляется:
   a) В процессе работы Сервера: если возник сбой при штатном взаимодействии со встроенной базой данных, осуществляется автоматический останов Сервера.
   b) В процессе запуска Сервера: если в настройках базы данных **SQLite3** в выпадающем списке **Проверка целостности образа** выбран вариант **Быстрая** или

Полная, то осуществляется автоматическая проверка целостности образа базы данных. При обнаружении неисправности запуск Сервера не осуществляется.

2. Для возможности запуска Сервера необходимо осуществить восстановление поврежденной базы данных:
   a) Если в настройках базы данных **SQLite3** установлен флаг **Восстанавливать поврежденный образ автоматически**, при запуске Сервера Dr.Web осуществляется автоматическое восстановление поврежденного образа базы данных.
   b) Если автоматическое восстановление образа базы данных отключено, вы можете воспользоваться ключом `repairdb` при запуске Сервера из командной строки (см. также документ **Приложения**, раздел 33.3. Команды для управления базой данных).

9.3.8. Модули

На вкладке **Модули** задается режим взаимодействия Сервера Dr.Web с другими компонентами Dr.Web Enterprise Security Suite:

- 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**.
- Установите флаг **Протокол Прокси-сервера Dr.Web** для включения протокола взаимодействия Сервера Dr.Web с Прокси-Серверами Dr.Web.
- Установите флаг **Расширение Центра управления безопасностью Dr.Web** для возможности 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 **Расширение SNMP-агента Dr.Web**, чтобы разрешить Серверу Dr.Web обмен информацией с системами сетевого управления по протоколу SNMP (см. также п. Конфигурация SNMP-агента Dr.Web).
- Установите флаг **Расширение Yandex.Locator**, чтобы разрешить использование расширения Yandex.Locator для определения местоположения мобильных устройств, подключенных к Серверу.
  - В поле **API-ключ** введите свой API-ключ, полученный через соответствующий сервис компании Яндекс.

Если вы включите расширение Yandex.Locator, но не зададите API-ключ, расширение не будет активно.

Подробную информацию по использованию и настройке расширения Yandex.Locator вы можете найти в документе **Приложения**, в разделе Автоматическое определение местоположения станции под ОС Android.

9.3.9. 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.

Чтобы просмотреть расположение 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 OpenStreetMap 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**.

9.3.10. Лицензии

На вкладке **Лицензии** задаются настройки распространения лицензий между Серверами Dr.Web, а также настройки ведения отчетов по использованию лицензий.

Настройки уведомления об ограничении по количеству лицензий в лицензионном ключе

- **Количество оставшихся лицензий** — максимальное количество оставшихся лицензий, при котором будет отправлено уведомление **Ограничение по количеству лицензий в лицензионном ключе**.
- **Процент оставшихся лицензий** — максимальный процент оставшихся лицензий, при котором будет отправлено уведомление **Ограничение по количеству лицензий в лицензионном ключе**.

Настройки для отчета по использованию лицензий

При отправке отчетов между Серверами данные настройки должны задаваться на главном Сервере, но будут использоваться подчиненными Серверами.

Если связи с соседними Серверами не настроены, данные опции используются только текущим Сервером для его личных отчетов.

- **Период создания отчета** — периодичность, с которой будут создаваться отчеты на Сервере об используемых им лицензионных ключах.

  Если отчет об использовании лицензий создается подчиненным Сервером, то сразу после создания осуществляется отправка этого отчета на главный Сервер.

  Созданные отчеты дополнительно отправляются при каждом подключении (в т.ч. перезагрузке) Сервера, а также при изменении количества выдаваемых лицензий на главном Сервере.
- **Период подсчета активных станций** — период, в течение которого будет подсчитываться количество активных станций для создания отчета об использовании лицензий. Значение 0 предписывает учитывать в отчете все станции, вне зависимости от статуса их активности.

Настройки для Сервера, выдающего лицензии

- **Период автоматического продления выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на данном Сервере. После окончания этого периода осуществляется автоматическое продление выданных лицензий на тот же самый период. Автоматическое продление будет осуществляться до тех пор, пока длится срок распространения лицензий, заданный в Менеджере лицензий на шаге 5. Данный механизм обеспечивает возвращение лицензий на главный Сервер в том

случае, если подчиненный Сервер будет отключен и не сможет вернуть выданные лицензии.

- **Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами. Синхронизация лицензий позволит определить, что количество лицензий, выданных главным Сервером и полученных подчиненным Сервером, совпадает. Данный механизм позволяет выявить сбои и случаи подлога при передаче лицензий.

Настройки для Сервера, получающего лицензии

- **Интервал для предварительного продления получаемых лицензий** — промежуток времени до окончания периода автоматического продления лицензий, полученных от соседнего Сервера, начиная с которого данный Сервер запрашивает предварительное автоматическое продление этих лицензий.

  Использование данной настройки зависит от типа подключения, выбранного в настройке **Параметры соединения** при конфигурации связи между Серверами (см. раздел Настройка связей между Серверами Dr.Web):

  - Для периодического типа подключения: если период переподключения, заданный в настройке связи, больше чем **Период автоматического продления выдаваемых лицензий**, заданный на Сервере, выдавшем лицензии, то автоматическое продление этих лицензий будет инициировано раньше, чем истечет **Период автоматического продления выдаваемых лицензий**.
  - Для постоянного подключения: данная настройка не используется.

  Подробную информацию о распространении лицензий между Серверами см. в разделе Распространение лицензий по межсерверным связям.

9.3.11. Журнал

На вкладке **Журнал** задаются настройки ведения журнала работы Сервера Dr.Web:

- В выпадающем списке **Уровень детализации журнала Сервера** выберите уровень подробности для ведения журнала работы Сервера Dr.Web.
- **Максимальное количество файлов** — максимальное количество файлов журнала (включая текущий и архивные), которые будут храниться.
- **Режим ротации журнала Сервера** — режим ротации журнала работы Сервера. Выберите одно из представленных значений:
  - **ротация по размеру** определяет ограничение на размер каждого из файлов журнала.

    Максимальный размер каждого файла — максимально допустимый размер каждого файла журнала. Когда текущий файл достигает заданного размера, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.

- **ротация по времени** определяет длительность записи каждого из файлов журнала.

  Максимальное время записи файла — максимальная длительность для записи каждого файла журнала. Когда время записи файла достигает заданной длительности, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.

- Установите флаг **Архивировать файлы журнала**, чтобы упаковывать в архив старые файлы журнала в процессе ротации.

Для применения внесенных изменений необходима перезагрузка Сервера.

Перезагрузка может быть выполнена как через Центр управления, так и при помощи соответствующей консольной команды.

Подробная информация о журнале Сервера приведена в разделе Журнал Сервера Dr.Web.

9.4. 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** в главном меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Удаленный доступ к Серверу Dr.Web**.
2. Задайте настройки протокола подключения:
   - Установите флаг **Использовать TLS**, чтобы разрешить подключение утилиты дистанционной диагностики к Серверу Dr.Web по протоколу TLS. Если флаг снят, подключение будет возможно только по протоколу TCP.
     Для подключения по протоколу TLS задайте следующие настройки:
     - **Сертификат** — файл 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.
- В поле **Ключ шифрования для мандатов TLS-сессии** задайте путь к файлу ключа шифрования для мандатов TLS-сессий. Используется для возобновления сеанса TLS на основе мандатов сессий (session tickets), которые шифруются с использованием заданного ключа.
- **Список разрешенных шифров** — строка, определяющая список шифров из пакета OpenSSL, разрешенных для использования в соединениях с клиентами. Если оставить поле пустым, будет использовано значение `DEFAULT`, что означает `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.

3. Задайте настройки интерфейса для подключения:
   - **Адрес** — IP-адрес, прослушиваемый со стороны Сервера для подключения утилиты дистанционной диагностики.
   - **Порт** — порт, прослушиваемый со стороны Сервера для подключения утилиты дистанционной диагностики. По умолчанию используется порт 10101.

   Чтобы добавить еще один интерфейс для подключения, нажмите  и задайте значения добавленных полей.

   Чтобы запретить подключение по заданному ранее интерфейсу, удалите его из списка, нажав  напротив строки с этим интерфейсом.
4. Нажмите кнопку **Сохранить**.

Описание использования консольной версии утилиты дистанционной диагностики Сервера приведено в документе **Приложения**, в разделе 37.3. Утилита дистанционной диагностики Сервера Dr.Web.

9.5. Конфигурация SNMP-агента Dr.Web

SNMP-агент Dr.Web предназначен для интеграции Dr.Web Enterprise Security Suite с системами сетевого управления посредством протокола SNMP. Такая интеграция позволяет отслеживать состояние работы компонентов Dr.Web, а также собирать статистику обнаружения и нейтрализации угроз.

Системы мониторинга или любые SNMP-менеджеры могут обратиться к Серверу Dr.Web, который предоставляет запрошенную информацию посредством расширения SNMP-агента Dr.Web.

Для ознакомления с информацией, которая может быть предоставлена SNMP-агентом Dr.Web, можете воспользоваться MIB, поставляемой вместе с Сервером. Файл `DRWEB-ESUITE-STAT-MIB.txt` располагается в подкаталоге `etc` каталога установки Сервера.

Чтобы разрешить Серверу Dr.Web обмен информацией с системами сетевого управления по протоколу SNMP необходимо включить расширение SNMP-агента Dr.Web. Для этого в разделе **Конфигурация Сервера Dr.Web**, на вкладке Модули установите флаг **Расширение SNMP-агента Dr.Web**.

Чтобы настроить параметры подключения к SNMP-агенту Dr.Web

1. Выберите пункт **Администрирование** в главном меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Конфигурация SNMP-агента Dr.Web**.
2. В поле **Сообщество** задайте имя сообщества SNMPv2c. По умолчанию **public**.
3. Задайте настройки интерфейса для подключения систем сетевого управления:
   - **Интерфейс** — IP-адрес, прослушиваемый со стороны Сервера для входящих соединений от систем сетевого управления.
   - **Порт** — порт, прослушиваемый со стороны Сервера для входящих соединений от систем сетевого управления.

   Чтобы добавить еще один интерфейс для подключения, нажмите и задайте значения добавленных полей.

   Чтобы запретить подключение по заданному ранее интерфейсу, удалите его из списка, нажав напротив строки с этим интерфейсом.
4. Установите флаг **Разрешать доступ только из локальных сетей**, чтобы разрешить подключение к SNMP-агенту Dr.Web только из локальных сетей.

   При этом заполните **Список локальных адресов**, с которых разрешено подключение систем сетевого управления к SNMP-агенту Dr.Web.
5. Нажмите кнопку **Сохранить**.

9.6. Настройка расписания Сервера Dr.Web

Чтобы настроить расписание выполнения заданий для Сервера Dr.Web

1. Выберите пункт **Администрирование** в главном 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.

   Добавить задания из расписания по умолчанию — добавить в текущее расписание все задачи из расписания по умолчанию. При этом в списке сохраняются все текущие задания и добавляются все задания из расписания по

умолчанию. Задания из расписания по умолчанию добавляются в любом случае, даже если текущее расписание уже содержит эти задания (в исходном или модифицированном виде), в том числе, полностью совпадает с расписанием по умолчанию.

Установить расписание по умолчанию — удалить все задания из текущего расписания и установить расписание заданий по умолчанию.

Расписание по умолчанию — это список заданий, создаваемых при первичной установке Сервера. Данное расписание не подлежит изменению.

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.

Импорт списка заданий для Сервера Dr.Web в Планировщик заданий рабочих станций и наоборот не допускается.

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**.		
Серьезность	**Сделать критическим**	Осуществить внеочередной запуск задания, 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**.		

Настройка	Действие
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.
Выполнить задание	Выполнить выбранные в списке задания незамедлительно. При этом задание будет запущено, даже если оно запрещено для выполнения по расписанию.

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 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.

Чтобы отредактировать параметры задания

1. На вкладке **Общие** настройте следующие параметры:
   - В поле **Название** задайте 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 **Серьезность**.

- Если флаг **Запускать задание асинхронно** снят, задание будет помещено в общую очередь заданий Планировщика, выполняемых последовательно. Установите флаг, чтобы выполнять данное задание параллельно вне очереди.

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

Тип задания	Параметры и описание
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).
Доступные лицензии заканчиваются	

Тип задания	Параметры и описание
	Задание предназначено для отправки оповещения **Количество станций в группе приближается к лицензионному ограничению**, если количество лицензий по всем ключам, назначенным выбранным группам станций заканчивается. Лицензионные ключи, назначенные на выбранные группы, могут быть также назначены на другие объекты лицензирования. Необходимо задать следующие параметры: • **Количество доступных лицензий** — максимальное количество оставшихся лицензий в лицензионных ключах, назначенных на выбранные группы, при котором администратору будет отправляться оповещение. • **Процент доступных лицензий** — максимальный процент оставшихся лицензий в лицензионных ключах, назначенных на выбранные группы, при котором администратору будет отправляться оповещение. • **Группы** — список групп, которые будут проверяться на количество оставшихся лицензий. Для выбора нескольких групп используйте кнопки CTRL и SHIFT.
Замена ключа шифрования	Задание предназначено для периодической замены следующих инструментов, обеспечивающих шифрование между компонентами: • закрытый ключ `drwcsd.pri` на Сервере, • открытый ключ `drwcsd.pub` на рабочих станциях, • сертификат `drwcsd-certificate.pem` 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 из выпадающего списка: • **Добавление нового ключа** — первый этап процедуры, на котором создается новая неактивная пара ключей шифрования и сертификат. Станции получают новый открытый ключ и сертификат, 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 и сертификат, после чего осуществляется замена действующих инструментов на новые: открытые ключи и сертификат на станциях и закрытый ключ на Сервере. Те станции, которые по каким-либо причинам не получили новые открытый ключ и сертификат, не смогут подключиться к Серверу. Для разрешения данной проблемы необходимо вручную подложить новый открытый ключ и сертификат

Тип задания	Параметры и описание
	на станции (с процедурой замены ключа на станции можно ознакомиться в документе **Приложения**, в разделе Подключение Агента Dr.Web к другому Серверу Dr.Web).
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. Если флаг **Ожидать завершения программы** снят, задание считается завершенным сразу после запуска программы, и Сервер протоколирует только запуск программы.
Окончание срока действия лицензионного ключа	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	Задание предназначено для запуска обновления продуктов репозитория с ВСО. Необходимо задать следующие параметры: • В списке **Продукт** установите флаги напротив тех продуктов репозитория, которые будут обновляться согласно этому заданию.

Тип задания	Параметры и описание
	• Установите флаг **Обновлять лицензионные ключи**, чтобы активировать процедуру автоматического обновления лицензионных ключей при обновлении репозитория. Подробная информация приведена в разделе Автоматическое обновление лицензий.
Останов Сервера	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 из базы данных. Типы удаляемых записей приведены в параметрах задания. Необходимо указать количество дней, по истечении которых записи в базе данных признаются старыми и удаляются с Сервера.

Тип задания	Параметры и описание
	Период удаления данных задается для каждого типа записей в отдельности.
Очистка старых станций	Задание предназначено для удаления устаревших станций. Необходимо указать временной период (по умолчанию 90 дней), в течение которого не посещавшие Сервер станции признаются старыми и перемещаются в группу антивирусной сети **Deleted**. Окончательное удаление таких станций из базы данных Сервера будет произведено при выполнении задания **Очистка старых записей** (срок удаления станций из группы **Deleted** задается в параметрах задания **Очистка старых записей** для типа **Удаленные станции** и отсчитывается с момента перемещения в группу **Deleted**).  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	Задание предназначено для перезапуска Сервера. Запускается без дополнительных параметров.
Пробуждение станций	

Тип задания	Параметры и описание
	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 списка адресов используйте запятую или переход на новую строку в качестве разделителя. ▫ **Группы** — список групп, станции которых необходимо включить. Чтобы изменить список групп, нажмите кнопку **Редактировать** (или идентификаторы групп, если группы уже заданы) и выберите нужные группы в открывшемся окне. 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**, для свойства **Пробуждение с помощью Magic Packet** задать **Значение** → **Включено**).
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

Тип задания	Параметры и описание
	копий (значение 0 означает отмену этого ограничения). Подробнее см. в документе **Приложения**, п. Приложение 33.5. 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:
	  ▫ **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. Необходимо задать следующие параметры:

Тип задания	Параметры и описание
	• **Контроллер Active Directory** — контроллер Active Directory, например, dc.example.com. • **Регистрационное имя** — регистрационное имя пользователя Active Directory. • **Пароль** — пароль пользователя Active Directory. Для Серверов под ОС Windows настройки не обязательны. В качестве регистрационных данных по умолчанию используются данные пользователя, от имени которого запущен процесс Сервера (как правило LocalSystem). Для Серверов под ОС семейства UNIX настройки должны быть обязательно заданы. • В выпадающем списке **Защита соединения** выберите тип шифрованного обмена данными: ▫ **STARTTLS** — переключение на защищенное соединение осуществляется через команду `STARTTLS`. По умолчанию для соединения предусматривается использование 25 порта. ▫ **SSL/TLS** — открыть отдельное защищенное шифрованное соединение. По умолчанию для соединения предусматривается использование 465 порта. ▫ **Нет** — не использовать шифрование. Обмен данными будет происходить по незащищенному соединению. 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**.

Тип задания	Параметры и описание
	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. Для возможности создания отчета необходимо, чтобы было включено оповещение **Статистический 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.

3. На вкладке **Время** настройте следующие параметры:
   - 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. 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.

4. 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.

9.7. 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** в главном 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.

9.7.1. 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.
- **Количество параллельных запросов от клиентов** — 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 сессии по HTTP/1 (с)** — тайм-аут сессии для протокола HTTP версии 1. При использовании постоянных соединений Сервер разрывает соединение, если в течение указанного времени от клиента не приходят запросы. Тайм-аут актуален до начала обмена данными в рамках сессии.
- **Минимальная скорость отправки по HTTP/1 (Б/с)** — минимальная скорость отправки данных по протоколу HTTP версии 1. Если исходящая скорость передачи по сети ниже данного значения, в соединении будет отказано. Задайте значение 0, чтобы снять данное ограничение.
- **Минимальная скорость приема по HTTP/1 (Б/с)** — минимальная скорость получения данных по протоколу HTTP версии 1. Если входящая скорость передачи по сети ниже данного значения, в соединении будет отказано. Задайте значение 0, чтобы снять данное ограничение.
- **Тайм-аут отправки по HTTP/1 (с)** — тайм-аут отправки данных в рамках открытой сессии по протоколу HTTP версии 1. Если в течение указанного времени не удалось отправить данные, сессия закрывается.
- **Тайм-аут приема по HTTP/1 (с)** — тайм-аут приема данных в рамках открытой сессии по протоколу HTTP версии 1. Если в течение указанного времени от клиента не приходят запросы, сессия закрывается. Тайм-аут актуален после начала обмена данными в рамках сессии.
- **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.
- **Включить защиту от flood-атак** — установите флаг, чтобы принимать защитные меры против flood-атак. Задайте следующие параметры обнаружения атаки:
  - **Период (с)** — промежуток времени в секундах, за который должно прийти определенное количество запросов, чтобы подтвердить flood-атаку со стороны клиента.
  - **Количество запросов** — минимальное количество запросов, которые должны прийти за определенный промежуток времени, чтобы подтвердить flood-атаку со стороны клиента.
  - **Длительность блокировки (с)** — соединения с клиентом будут запрещены в течение заданного количества секунд.

В разделе **Сжатие** задаются параметры сжатия трафика при передаче данных по каналу связи с веб-сервером через HTTP/HTTPS:

- **Максимальный размер ответа для сжатия (КБ)** — максимальный размер HTTP-ответов, которые будут сжиматься. Задайте значение 0, чтобы снять ограничение на максимальный размер HTTP-ответов, подлежащих сжатию.
- **Минимальный размер ответа для сжатия (Б)** — минимальный размер HTTP-ответов, которые будут сжиматься. Задайте значение 0, чтобы снять ограничение на минимальный размер HTTP-ответов, подлежащих сжатию.
- **Порядок использования типов сжатия**:
  - **Определяется клиентом** — порядок использования типов сжатия определяется клиентом с учетом разрешенных типов сжатия.
  - **Определяется сервером** — порядок использования типов сжатия определяется сервером с учетом разрешенных типов сжатия. В этом случае задайте порядок следования типов сжатия в списке ниже. Для изменения порядка перетащите соответствующий блок за корешок.

  Вы можете включить или отключить, а также задать порядок (для того случая, когда порядок определяется Сервером) следующие типы сжатия:
  - **Использовать сжатие GZIP** — установите флаг, что использовать этот тип сжатия. В поле **Уровень сжатия GZIP** задайте значение в диапазоне 0-9. Значение 0 означает отключить сжатие.
  - **Использовать сжатие Deflate** — установите флаг, что использовать этот тип сжатия. В поле **Уровень сжатия Deflate** задайте значение в диапазоне 0-9. Значение 0 означает отключить сжатие.
  - **Использовать сжатие Brotli** — установите флаг, что использовать этот тип сжатия. В поле **Уровень сжатия Brotli** задайте значение в диапазоне 0-11. Значение 0 означает отключить сжатие.

- **Заменять IP-адреса** — установите флаг, чтобы заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера.
- **Включить поддержку HTTP/2** — установите флаг, чтобы поддерживать обращение к веб-серверу по протоколу HTTP версии 2.
  - **Тайм-аут сессии по HTTP/2 (с)** — тайм-аут сессии для протокола HTTP версии 2. При использовании постоянных соединений сервер разрывает соединение, если в течение указанного времени от клиента не приходят запросы.
- **Поддерживать TLS-сессию активной** — установите флаг, чтобы использовать постоянное соединение для TLS. Устаревшие версии браузеров могут некорректно работать с постоянными TLS-соединениями. Отключите этот параметр, если возникают проблемы с работой по TLS протоколу.
- **Сертификат** — путь к файлу TLS-сертификата. В выпадающем списке приводятся доступные сертификаты из каталога Сервера.
- **Закрытый ключ SSL** — путь к файлу закрытого ключа TLS. В выпадающем списке приводятся доступные закрытые ключи TLS из каталога Сервера.
- **Ключ шифрования для мандатов TLS-сессии** — путь к файлу ключа шифрования для мандатов TLS-сессий. Используется для возобновления сеанса TLS на основе мандатов сессий (session tickets), которые шифруются с использованием заданного ключа.
- **Список разрешенных шифров** — строка, определяющая список шифров из пакета OpenSSL, разрешенных для использования в соединениях с клиентами. Если оставить поле пустым, будет использовано значение `DEFAULT`, что означает `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.

9.7.2. 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.

9.7.3. 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 **Прослушиваемые адреса** настраивается список интерфейсов, которые будут прослушиваться для приема соединений по протоколу HTTP:

- **Адрес** — IP-адрес сетевого интерфейса, с которого разрешен прием соединений.
- **Порт HTTP** — номер порта сетевого интерфейса, с которого разрешен прием соединений по протоколу HTTP.
- **Порт HTTPS** — 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 HTTP**: `9080` — использовать стандартный порт `9080` для протокола HTTP.
  - **Порт HTTPS**: `9081` — использовать стандартный порт `9081` для протокола HTTPS.

Для добавления новой строки адреса, нажмите кнопку  . Для удаления строки конкретного адреса нажмите кнопку  напортив удаляемого адреса.

9.7.4. Безопасность

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых веб-сервер принимает HTTP и HTTPS запросы.

Общие

- Установите флаг **Перенаправлять на защищенное соединение**, чтобы автоматически перенаправлять все соединения по HTTP на HTTPS.
- Установите флаг **Возвращать подробный заголовок**, чтобы веб-сервер возвращал подробности окружения в “Server”-заголовке.
- Установите флаг **Преобразовывать URI в нижний регистр**, чтобы преобразовывать все URI в запросах к веб-серверу в нижний регистр. Преобразованию подлежит только фрагмент иерархической части URI, содержащий путь.
- Установите флаг **Включить контроль доступа для клиентских приложений**, чтобы запретить доступ к интерфейсу Центра управления для программ-роботов и прочих клиентских приложений из списка ниже.

  Определите список запрещенных клиентских приложений:

- В поле **Имя клиентского приложения** задайте имя клиентского приложения, которому будет запрещен доступ к интерфейсу Центра управления. Чувствительно к регистру. Если не задано, используется URI приложения.
- В поле **Определяющее регулярное выражение** задайте регулярное выражение, определяющее приложение, которому будет запрещен доступ к интерфейсу Центра управления.

Ограничение доступа

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.

Чтобы отредактировать список 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 16777214 адресов (256*256*256-2).

   Адреса хостов в этих сетях вида: `125.*.*.*`

9.7.5. Модули

Не рекомендуется изменять настройки данного раздела без указаний службы технической поддержки.

В разделе **Модули** настраиваются Lua-скрипты, которые загружаются по мере исполнения других скриптов веб-интерфейса.

- Выпадающий список **Каталог скрипта в путях поиска** определяет, в какое место списка из раздела **Пути** добавить текущий каталог (каталог, в котором находится исполняемый в данный момент скрипт):
  - **первый** — в начало списка,
  - **последний** — в конец списка,
  - **не использовать** — не добавлять совсем.
- Раздел **Маски** задает множество масок, по которым ищутся модули Lua по путям, указанным в разделе **Путь**.
- Раздел **Пути** задает пути, по которым ищутся модули Lua из раздела **Маски**. Пути должны задаваться относительно корневого каталога веб-сервера.

Например:

Скрипт, расположенный по пути `var-root/webmin/esuite/include/head.ds` не будет найден без задания дополнительные настроек в разделе **Модули**.

Модули из каталогов `ds-modules` или `webmin/vfs` будут найдены без настроек в разделе **Модули**, потому что это глобальные модули, а не модули веб-интерфейса.

9.7.6. Обработчики

Настройки данного раздела, кроме подразделов **Доступ** и **Авторизация**, не рекомендуется изменять без указаний службы технической поддержки.

В разделе **Обработчики** настраивается то, каким именно образом и в каком окружении будет обрабатываться запрос, полученный от веб-клиента.

Общие

В зависимости от типа обработчика меняются доступные настройки.

Для веб-сокетов необходимый обработчик выбирается в зависимости от атрибута **Протокол**.

Для остальных типов обработчиков необходимый обработчик выбирается в зависимости от атрибута **Префикс**.

Типы используемых обработчиков выбираются в выпадающем списке **Тип**:

- **Обработчики**

  Выполняется указанный скрипт, которому в качестве параметра передаётся путь из URL. Если путь отсутствует, ему передаётся путь поля **Директория**.

  - **Префикс** — префикс пути в URL HTTP-запроса.
  - **Директория** — директория в корне веб-сервера, относительно которой считаются пути к отдаваемым файлам.
  - **Скрипт** — скрипт-обработчик.

- **Смешанные обработчики**

  В зависимости от типа файла, к которому производится запрос, ведёт себя как тип **Статические файлы** или как тип **Скрипты**.

  - **Префикс** — префикс пути в URL HTTP-запроса.
  - Список индексных файлов. Определяет, какие файлы в каком порядке будут загружаться, если веб-клиент затребует индекс директории.
  - **Скрипт** — список расширений файлов, которые необходимо считать Lua-скриптами.

- **Скрипты**

  Любой файл, к которому производится запрос, исполняется как Lua-скрипт.

  - **Префикс** — префикс пути в URL HTTP-запроса.
  - **Директория** — директория в корне веб-сервера, относительно которой считаются пути к отдаваемым файлам.

- **Статические файлы**

  Содержимое файлов отдается как есть.

  - **Префикс** — префикс пути в URL HTTP-запроса.
  - **Директория** — директория в корне веб-сервера, относительно которой считаются пути к отдаваемым файлам.
  - Список индексных файлов. Определяет, какие файлы в каком порядке будут загружаться, если веб-клиент затребует индекс директории.

- **Виртуальная файловая система**

  Аналог типа **Статические файлы**, только файлы загружаются из архива внутреннего формата `dar`, указанного в поле **Директория**.

  - **Префикс** — префикс пути в URL HTTP-запроса.
  - **Директория** — директория в корне веб-сервера, относительно которой считаются пути к отдаваемым файлам.

- **Предопределённые веб-сокеты**

  Websocket-приложение, реализуемое разделяемой библиотекой, поставляемой с сервером (`dll` или `elf shared object`). Имя файла библиотеки соответствует протоколу веб-сокета, файлы располагаются в `lib-root/websockets`.

  - **Скрипт авторизации** — имя файла Lua-скрипта, который авторизует пользователя.
  - **Протокол** — значение поля `WebSocket-Protocol`, передаваемое в HTTP-запросе подключения к вебсокету.

- **Пользовательские веб-сокеты**

  Websocket-приложение, реализуемое Lua-скриптом. Имя файла скрипта соответствует протоколу веб-сокета, файлы располагаются в `home-root/websockets`.

  - **Скрипт авторизации** — имя файла Lua-скрипта, который авторизует пользователя.
  - **Протокол** — значение поля `WebSocket-Protocol`, передаваемое в HTTP-запросе подключения к вебсокету.

Доступ

Списки контроля доступа (ACL) задают ограничения на сетевые адреса, с которых клиенты смогут получать доступ к веб-серверу.

Настройки аналогичны настройкам безопасности Сервера Dr.Web.

Если настройки не заданы, считается, что все адреса разрешены.

Авторизация

Доступна для всех типов обработчиков, кроме веб-сокетов.

Настройки раздела определяют список ресурсов, при запросах к которым нужно запрашивать basic http аутентификацию у веб-клиента.

- **Область действия** — значение, которое веб-сервер отдаст клиенту в параметре `WWW-Authenticate: Basic realm="ADMIN"`. По сути — краткое описание того, кто должен авторизоваться. К регистрационному имени отношения не имеет.

Чтобы настроить ограничения доступа для какого-либо типа соединения

1. Для того чтобы разрешать свободный доступ при подключении клиентов по HTTP или по HTTPS к определенным путям, включите эти пути в списки **HTTP: свободный доступ** или **HTTPS: свободный доступ** соответственно.
2. Для того чтобы требовать авторизацию при подключении клиентов по HTTP или по HTTPS к определенным путям, включите эти пути в списки **HTTP: запрос авторизации** или **HTTPS: запрос авторизации**.
3. При доступе к путям, не включенным ни в один из списков, авторизация требуется или нет в зависимости от того, установлен ли флаг **Приоритетность запроса авторизации**: при установленном флаге для подключения к путям, не включенным ни в один из списков (или включенным в оба), требуется авторизация. В противном случае, по таким путям разрешается свободный доступ.

Чтобы отредактировать список адресов

1. Введите в поле регулярное выражение, определяющее путь относительно директории, задаваемой в поле **Директория**.
2. Для добавления нового поля адреса, нажмите кнопку  соответствующего раздела.
3. Для удаления поля нажмите кнопку  .

9.8. 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: `/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** в главном 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. Возможность редактирования и выполнения шаблонных процедур не предоставляется.
- **IBM Syslog** — содержит шаблоны пользовательских процедур, используемых при интеграции с системой IBM Tivoli. События, соответствующие включенным процедурам, фиксируются в формате *Syslog*.

  Все события пишутся в один файл по следующему пути:

  - для ОС Windows: `var\export\tivoli\syslog\drwcs_syslog.log`
  - для ОС FreeBSD: `/var/drwcs/export/tivoli/syslog/drwcs_syslog.log`
  - для ОС Linux: `/var/opt/drwcs/export/tivoli/syslog/drwcs_syslog.log`
- **IBM W7Log** — содержит шаблоны пользовательских процедур, используемых при интеграции с системой IBM Tivoli. События, соответствующие включенным процедурам, фиксируются в формате *IBM W7Log XML*.

  Для каждого события создается отдельный файл по следующему пути:

- для ОС Windows:
  `var\export\tivoli\w7log\<название_события>_<unix_timestamp>`
- для ОС FreeBSD:
  `/var/drwcs/export/tivoli/w7log/<название_события>_<unix_timestamp>`
- для ОС Linux:
  `/var/opt/drwcs/export/tivoli/w7log/<название_события>_<unix_timestamp>`

Значок элемента дерева зависит от типа или состояния этого элемента (см. таблицу 9-7).

Таблица 9-7. 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 выбранные 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 мышью 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 будет 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.

9.9. Шаблоны сообщений

В разделе **Шаблоны сообщений** приведен список шаблонов произвольных текстовых сообщений, отправляемых администратором на станции антивирусной сети (см. Отправка сообщений станциям).

В список шаблонов сообщения могут попасть одним из следующих способов:

1. Шаблон может быть создан на основе сообщения, которое уже когда-то было отправлено администратором. Создание подобного шаблона осуществляется в разделе Журнал сообщений.
2. Может быть создан полностью новый шаблон. Для этого нажмите кнопку **Создать шаблон** на панели инструментов в разделе **Шаблоны сообщений**. Настройки сообщения аналогичны настройкам из раздела Отправка сообщений станциям.

Для управления шаблонами сообщений используйте следующие опции на панели инструментов:

Удалить — удалить выбранные шаблоны сообщений.

Создать шаблон — создать новый шаблон сообщения (см. выше).

Редактировать — редактировать настройки уже существующего шаблона. Опция доступна только при выборе одного шаблона в списке.

Отправить сообщение станциям — отправить одно или несколько сообщений станциям на основе шаблонов, выбранных в списке (см. ниже).

Чтобы отправить одно сообщение

1. Установите флаг напротив шаблона сообщения, которое вы хотите отправить.
2. Нажмите кнопку **Отправить сообщение станциям**.
3. Откроется окно **Отправка сообщения**. Задайте следующие настройки:
   a) В дереве **Антивирусная сеть** выберите получателей сообщения из представленного списка: это могут быть как отдельные станции, так и группы станций.
   b) Настройки сообщения аналогичны настройкам из раздела Отправка сообщений станциям.
4. Нажмите кнопку **Отправить**.

Чтобы отправить несколько сообщений

1. Установите флаги напротив шаблонов сообщений, которые вы хотите отправить.
2. Нажмите кнопку **Отправить сообщение станциям**.

3. Откроется окно **Отправка нескольких сообщений**. В разделе **Список сообщений** приведены все сообщения, которые вы выбрали для отправки. Названия сообщений соответствуют названиям их шаблонов.
4. Нажмите кнопку **Отправить все**, чтобы отправить все сообщения из списка.
5. Для редактирования какого-либо из сообщений, выберите его в разделе **Список сообщений**. В разделе **Настройки сообщения** задайте следующие параметры:
   a) В дереве **Антивирусная сеть** выберите получателей сообщения из представленного списка: это могут быть как отдельные станции, так и группы станций.
   b) Настройки сообщения аналогичны настройкам из раздела Отправка сообщений станциям.
   c) Чтобы удалить выбранное сообщение из списка на отправку, нажмите кнопку **Удалить**.

9.10. 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.

9.10.1. Конфигурация оповещений

Чтобы настроить оповещения о событиях в антивирусной сети

1. Выберите пункт **Администрирование** в главном меню Центра управления. В открывшемся окне выберите пункт управляющего меню **Конфигурация оповещений**.
2. Конфигурация оповещений настраивается отдельно для каждого администратора Центра управления. Имя администратора, для которого заданы отображаемые настройки, приведено в поле **Администратор, получающий оповещения**. Чтобы настроить оповещения для другого администратора, нажмите кнопку и выберите администратора в открывшемся окне.
3. При первоначальной настройке добавлен один блок (профиль) оповещений по умолчанию для главного администратора **admin**. Если список оповещений администратора пуст, нажмите **Добавить оповещение** в разделе **Список оповещений**.
4. 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.
5. 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.

6. В поле **Заголовок** задайте название добавленного блока оповещений. Это название будет использоваться, например, при настройке задания **Создание статистического отчета** 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.
7. Чтобы настроить рассылку оповещений, выберите необходимый тип отправки оповещения в выпадающем списке **Метод отправки оповещений**:
   - Агент Dr.Web — отправлять оповещений через протокол Агента.
   - Веб-консоль — отправлять оповещения для просмотра в веб-консоли.
   - Электронная почта — отправлять оповещения по электронной почте.
   - 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.
   - SNMP — отправлять оповещения через SNMP-протокол.

   Описание настроек каждого из типов отправки оповещений приведено ниже в данном разделе.
8. В списке оповещений установите флаги напротив тех оповещений, которые будут отправляться в соответствии с методом отправки текущего блока оповещений.
9. Для отправки оповещений Сервера предоставляется предопределенный набор текстовых сообщений.

   Описание предопределенных оповещений и их параметров приведено в документе **Приложения**, в Приложении Г2. Параметры шаблонов оповещений.

   Чтобы настроить конкретные оповещения, необходимо:

   a) Для возможности редактирования настроек оповещений нажмите **Переключиться в режим редактирования оповещений** в заголовке раздела.

   b) Для изменения настроек оповещений нажмите на оповещение, которое хотите отредактировать. Откроется шаблон оповещения. При необходимости отредактируйте текст отправляемого сообщения. В тексте оповещения можете использовать переменные шаблона (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 Г2. Параметры шаблонов оповещений.

c) Для оповещений по электронной почте предоставляется возможность добавить произвольные пользовательские поля в дополнительном разделе **Заголовки** в редакторе шаблона для каждого оповещения (см. п. **a)**). 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.

e) После внесения всех необходимых изменений нажмите **Выйти из режима редактирования оповещений** в заголовке раздела.

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.

10.Нажмите кнопку **Сохранить**, чтобы применить все внесенные изменения.

Оповещения через протокол Агента

Отправка оповещений через протокол Агента возможна только на Агенты Dr.Web для Windows.

Для оповещений через протокол Агента задайте следующие параметры:

- В разделе **Повторная отправка Сервером Dr.Web** задайте настройки для повторных отправок оповещения, которые предпримет Сервер в случае неудачи:
  - **Количество** — количество повторных попыток, предпринимаемых Сервером Dr.Web при неудачной отправке сообщения. По умолчанию 10.
  - **Тайм-аут** — период в секундах, по истечении которого Сервер Dr.Web осуществляет повторную попытку отправки сообщения. По умолчанию 300 секунд.
- **Станция** — идентификатор станции, на которую будут отправляться оповещения. Идентификатор станции можно посмотреть в свойствах станции.
- **Отправить тестовое сообщение** — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений.

Оповещения, отображаемые в веб-консоли

Для оповещений, отображаемых в Веб-консоли, задайте следующие параметры:

- В разделе **Повторная отправка Сервером Dr.Web** задайте настройки для повторных отправок оповещения, которые предпримет Сервер в случае неудачи:
  - **Количество** — количество повторных попыток, предпринимаемых Сервером Dr.Web при неудачной отправке сообщения. По умолчанию 10.
  - **Тайм-аут** — период в секундах, по истечении которого Сервер Dr.Web осуществляет повторную попытку отправки сообщения. 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.

Оповещения по электронной почте

Для оповещений по электронной почте задайте следующие параметры:

- В разделе **Повторная отправка Сервером Dr.Web** задайте настройки для повторных отправок оповещения, которые предпримет Сервер в случае неудачи:
  - **Количество** — количество повторных попыток, предпринимаемых Сервером Dr.Web при неудачной отправке сообщения. По умолчанию 10.
  - **Тайм-аут** — период в секундах, по истечении которого Сервер Dr.Web осуществляет повторную попытку отправки сообщения. По умолчанию 300 секунд.
- **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  .

  Параметры отправки электронной почты настраиваются в меню **Администрирование**, в разделе **Конфигурация Сервера Dr.Web**, на вкладке **Сеть**, на внутренней вкладке Электронная почта.
- **Отправить тестовое сообщение** — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений.

Push-оповещения

Для Push-оповещений, отправляемых на Мобильный центр управления, задайте следующие параметры:

- В разделе **Повторная отправка Сервером Dr.Web** задайте настройки для повторных отправок оповещения, которые предпримет Сервер в случае неудачи:
  - **Количество** — количество повторных попыток, предпринимаемых Сервером Dr.Web при неудачной отправке сообщения. По умолчанию 10.
  - **Тайм-аут** — период в секундах, по истечении которого Сервер Dr.Web осуществляет повторную попытку отправки сообщения. По умолчанию 300 секунд.
- **Отправить тестовое сообщение** — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений.

Оповещения через SNMP протокол

Для оповещений через SNMP-протокол задайте следующие параметры:

- В разделе **Повторная отправка Сервером Dr.Web** задайте настройки для повторных отправок оповещения, которые предпримет Сервер в случае неудачи:
  - **Количество** — количество повторных попыток, предпринимаемых Сервером Dr.Web при неудачной отправке сообщения. По умолчанию 10.
  - **Тайм-аут** — период в секундах, по истечении которого Сервер Dr.Web осуществляет повторную попытку отправки сообщения. По умолчанию 300 секунд.
- В разделе **Повторная отправка SNMP-подсистемой** задайте настройки для повторных отправок оповещения, которые предпримет SNMP-подсистема в случае неудачи:
  - **Количество** — количество повторных попыток, предпринимаемых SNMP-подсистемой при неудачной отправке сообщения. По умолчанию 5.
  - **Тайм-аут** — период в секундах, по истечении которого SNMP-подсистема осуществляет повторную попытку отправки сообщения. По умолчанию 5 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.

Для получения описаний OID при разборе SNMP trap можете воспользоваться MIB, поставляемой вместе с Сервером. Файлы `DRWEB-ESUITE-NOTIFICATIONS-MIB.txt` и `DRWEB-MIB.txt` располагаются в подкаталоге `etc` каталога установки Сервера.

9.10.2. 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 веб-консоли

1. Выберите пункт **Администрирование** в главном 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 при помощи опций на панели инструментов:
   a) 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 следующие элементы панели инструментов:

      Удалить оповещения — удалить все выбранные оповещения без возможности восстановления.

      Пометить оповещения как прочитанные — отметить все выбранные оповещения как прочитанные.
   c) Для управления определенными типами оповещений установите флаги напротив оповещений соответствующих типов. При этом станут доступны следующие элементы панели инструментов:

      Неподтвержденные станции — опция доступна только при выборе оповещений с типом **Станция ожидает подтверждения**. В выпадающем списке вы можете подтвердить регистрацию или отказать в доступе к Серверу для станций из выбранных оповещений.

Сканировать — опция доступна только при выборе оповещений с типами **Эпидемия в сети**, **Ошибка сканирования**, **Обнаружена угроза безопасности**. В выпадающем списке вы можете задать параметры запуска Сканера Dr.Web на станциях из выбранных оповещений.

Управление компонентами — опция доступна только при выборе оповещений с типом **Критическая ошибка обновления станции**. В выпадающем списке вы можете задать вариант запуска обновлений антивирусного ПО на станциях из выбранных оповещений.

Перезагрузить станцию — опция доступна только при выборе оповещений с типом **Требуется перезагрузка станции для применения обновлений**. Опция инициирует перезагрузку станций из выбранных оповещений.

d) При необходимости вы можете экспортировать оповещения в файл. Экспорту подлежат оповещения, выведенные в данный момент в таблице согласно настройкам временного интервала и фильтров по столбцам таблицы (см. п. 4.b).

Для экспорта оповещений 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.

4. Для управления оповещениями при помощи опций, предоставляемых таблицей оповещений:

a) Установите значок **Хранить сообщение без автоматического удаления** 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 снимете значок напротив этих оповещений.

b) Для отображения только определенных оповещений нажмите значок в правом углу заголовка таблицы. В выпадающем списке установите флаги для тех параметров оповещений, которые вы хотите видеть в таблице.

Для фильтрации доступны следующие разделы:

Столбец	Параметр	Действие
Серьезность	**Критическая**	Отображать оповещения только с выбранным уровнем серьезности. Чтобы отобразить все оповещения, установите все флаги.
	Высокая	
	Средняя	
	Низкая	

Столбец	Параметр	Действие
	Минимальная	
Источник	**Агент**	Отображать оповещения, связанные с событиями на станциях.
	Сервер	Отображать оповещения, связанные с событиями на Сервере.

Параметры фильтра непостоянны. Их наличие или отсутствие зависит от данных, которые были получены за указанный период времени. Параметр исчезает из фильтра, если за указанный период времени не были получены соответствующие ему данные.

c) Для настройки вида таблицы нажмите значок ⚙ в правом углу заголовка таблицы. В выпадающем списке вы можете настроить следующие опции:
   - Включить или отключить перенос строк для длинных сообщений.
   - Выбрать столбцы, которые будут отображаться в таблице (отмечены флагом рядом со своим названием). Для включения/отключения столбца нажмите на строку с его названием.
   - Выбрать порядок следования столбцов в таблице. Для изменения порядка перетащите соответствующий столбец в списке на требуемое место.

9.10.3. 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** в главном 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.

9.11. 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 Сервера `var/repository`. 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.

Обновление продуктов репозитория

Обновление ревизий продуктов может осуществляться в следующих направлениях:

a) Загрузка обновлений на Сервер с ВСО Dr.Web.

Обновление репозитория Сервера с ВСО осуществляется автоматически согласно заданиям в расписании Сервера.

- Чтобы ознакомиться с заданиями по обновлению репозитория перейдите в раздел Общая конфигурация репозитория на вкладку **Планировщик заданий**.
- Чтобы изменить расписание обновлений с ВСО перейдите в раздел Настройка расписания Сервера Dr.Web.
- Чтобы проверить наличие обновлений и загрузить их вручную, перейдите в раздел Состояние репозитория и нажмите кнопку **Проверить обновления**.

См. также Обновление репозитория Сервера Dr.Web, не подключенного к интернету.

b) Распространение обновлений между различными Серверами Dr.Web в многосерверной конфигурации.

Если в вашей антивирусной сети установлено несколько Серверов Dr.Web, мы можете настроить межсерверные связи для передачи обновлений репозитория:

- При связи главный-подчиненный Серверы, получающие обновления с ВСО, будут главными, подчиненные Серверы будут получать все обновления с главных Серверов автоматически.
- При связи между равноправными Серверами, любой их них может быть назначен в качестве получающего обновления с ВСО. При этом остальные Серверы будут получать все обновления с него автоматически.

Описание настройки межсерверных связей приведено в разделе Особенности сети с несколькими Серверами Dr.Web.

Если в сети настроены межсерверные связи, и с вашего Сервера получают обновления соседние Серверы, необходимо также включить обновление систем и языков интерфейса этих соседних Серверов на вашем Сервере.

c) **Раздача обновлений с Сервера Dr.Web на рабочие станции.**

Проверка, загрузка с Сервера и установка обновлений на станциях осуществляется автоматически при каждом подключении Агентов к Серверу, а также с некоторой периодичностью в процессе работы Агентов (не настраивается и осуществляется прозрачно для администратора).

При необходимости вы можете настроить ограничения по времени и объему трафика обновлений Агентов в разделе Ограничение обновлений рабочих станций.

Настройка параметров репозитория

Репозиторий предоставляет Администратору антивирусной сети возможность настраивать следующие параметры:

- **Перечень сайтов обновления при операциях типа a).**

  Параметры подключения к ВСО настраиваются в разделе Общая конфигурация репозитория.

- **Ограничение состава продуктов, нуждающихся в синхронизации типа a).**

  Состав загружаемых с ВСО продуктов настраивается в разделах Общая конфигурация репозитория и Детальная конфигурация репозитория.

  Таким образом, администратору предоставляется возможность отслеживать только нужные ему изменения отдельных категорий продуктов.

- **Ограничение частей продукта, нуждающихся в синхронизации типа c).**

  Администратор Сервера может выбрать, что именно подлежит установке на рабочие станции. Выбор антивирусных компонентов осуществляется в разделе Устанавливаемые компоненты антивирусного пакета.

- **Контроль перехода на новые ревизии.**

  Настройка конфигурации ревизий для каждого продукта репозитория в отдельности осуществляется в разделе Детальная конфигурация репозитория.

  При этом возможно самостоятельное тестирование продуктов перед внедрением.

- **Управление содержимым репозитория на уровне каталогов и файлов.**

  Раздел Содержимое репозитория позволяет просматривать и управлять текущим содержимым репозитория на уровне каталогов и файлов репозитория: осуществлять экспорт и импорт как отдельных продуктов, так и всего содержимого репозитория и его настроек.

Состав продуктов репозитория

В настоящее время предоставляются следующие продукты:

- **Административные утилиты Dr.Web**

  Утилиты для всех поддерживаемых операционных систем:
  - Загрузчик репозитория Dr.Web (графическая и консольная версии),
  - Утилита генерации цифровых ключей и сертификатов,
  - Утилита дистанционной диагностики Сервера Dr.Web,
  - Утилита дистанционной диагностики Сервера Dr.Web для работы со скриптами,
  - Мобильный центр управления Dr.Web (ссылки на App Store и Google Play).

  Все утилиты доступны для скачивания через раздел Центра управления **Администрирование** → **Утилиты**.

- **Агент Dr.Web для Android**

  Вирусные базы для станций под ОС Android.

- **Агент Dr.Web для UNIX**

  Базы встроенных фильтров и Антиспама, а также движок Антиспама Dr.Web для UNIX.

- **Агент Dr.Web для Windows**

  ПО антивирусных компонентов для станций под ОС Windows.

- **Базы Антиспама Dr.Web**

  Базы Антиспама Dr.Web для Windows.

- **Базы SpIDer Gate**

  Базы встроенных фильтров антивирусных компонентов для Windows.

- **Вирусные базы Dr.Web**

  Вирусные базы, антивирусные движки для станций под ОС Windows и ОС семейства UNIX.

- **Данные безопасности Сервера Dr.Web**

  Набор ключей, скриптов и сертификатов, обеспечивающих безопасность при обновлении компонентов антивирусной сети и обмене данными между Сервером и Агентами.

- **Доверенные приложения**

  Группы доверенных приложений для компонента Контроль приложений для станций под ОС Windows.

  Продукт **Доверенные приложения** не обновляется с ВСО. Распространение этого продукта возможно только между соседними Серверами по межсерверной связи.

  Подробнее о настройке репозитория для продукта **Доверенные приложения** см. в разделе Доверенные приложения.

- **Известные хеши угроз**

  Списки известных хешей угроз.

- **Корпоративные продукты Dr.Web**

  Установочные пакеты для следующих продуктов:

  - Полный инсталлятор Агента Dr.Web для Windows,
  - Продукты для установки на защищаемые станции под ОС UNIX (включая серверы ЛВС), Android, macOS,
  - Dr.Web для IBM Lotus Domino,
  - Dr.Web для Microsoft Exchange Server,
  - Прокси-сервер Dr.Web — пакет для самостоятельной установки Прокси-сервера, не связанного с Агентом Dr.Web для Windows,
  - Агент Dr.Web для Active Directory,
  - Утилита для модификации схемы Active Directory,
  - Утилита для изменения атрибутов у объектов Active Directory,
  - NAP Validator.

  Все установочные пакеты корпоративных продуктов доступны для скачивания на инсталляционной странице по адресу:

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

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

- **Модуль обновления Dr.Web**

  Модуль обновления Агента Dr.Web для Windows с версии 6 до актуальной версии.

- **Новости компании «Доктор Веб»**

  Новостная лента с сайта компании «Доктор Веб».

- **Прокси-сервер Dr.Web**

  ПО для установки Прокси-сервера Dr.Web, связанного с Агентом Dr.Web для Windows.

- **Сервер Dr.Web**
  - ПО Сервера Dr.Web,
  - ПО Центра управления безопасностью Dr.Web,
  - документация.

9.11.1. Состояние репозитория

Чтобы проверить текущее состояние репозитория или обновить компоненты антивирусной сети

1. Выберите пункт **Администрирование** в главном 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 на панели инструментов:
   - Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО. Если проверяемый компонент устарел, то его обновление произойдет автоматически.
   - Нажмите одну из следующих кнопок на панели инструментов, чтобы скачать журнал обновлений репозитория:

     Сохранить данные в CSV-файл,

     Сохранить данные в HTML-файл,

     Сохранить данные в XML-файл,

     Сохранить данные в PDF-файл.
   - 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.

9.11.2. 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:
  - 05-drwmeta — данные безопасности Сервера Dr.Web,
  - 10-drwbases — вирусные базы,
  - 10-drwgatedb — базы SpIDer Gate,
  - 10-drwspamdb — базы Антиспама,
  - 10-drwupgrade — Модуль обновления Dr.Web,
  - 15-drwhashdb — Известные хеши угроз,
  - 15-drwappcntrl — Доверенные приложения компонента Контроль приложений,
  - 20-drwagent — Агент Dr.Web для Windows,
  - 20-drwandroid11 — Агент Dr.Web для Android,
  - 20-drwcs — Сервер Dr.Web,
  - 20-drwunix — Агент Dr.Web для UNIX,
  - 40-drwproxy — Прокси-сервер Dr.Web,
  - 70-drwextra — Корпоративные продукты Dr.Web,
  - 70-drwutils — Административные утилиты Dr.Web,
  - 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.

Чтобы управлять 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.

9.11.3. 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** в главном 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 кнопку **Сохранить**, чтобы сохранить все внесенные изменения в файлах конфигурации репозитория. При этом осуществляется перезагрузка текущей версии репозитория с диска.

Для применения новых настроек конфигурации репозитория требуется некоторое время. При немедленном обновлении репозитория с ВСО сразу после изменения конфигурации, могут использоваться предыдущие настройки.

9.11.3.1. ВСО Dr.Web

На вкладке **ВСО Dr.Web** осуществляется настройка параметров подключения к Всемирной системе обновлений Dr.Web. Обновления загружаются с использованием протоколов, список которых представлен в выпадающем списке **Протокол получения обновлений**:

Тип протокола	Описание
HTTP/HTTPS	Протоколы для получения обновлений с веб-сервера
FTP/FTPS	Протоколы для получения обновлений с FTP-сервера
FILE	Протокол для получения обновления из локального каталога на компьютере с установленным **Сервером Dr.Web**
CIFS/SMB	Протоколы для получения обновлений из единой файловой системы
SCP/SFTP	Протоколы для получения обновлений с использованием защищенного соединения

Чтобы отредактировать подключение к ВСО

- В выпадающем списке **Протокол получения обновлений** выберите тип протокола для получения обновлений с серверов обновлений. Для всех протоколов загрузка обновлений осуществляется согласно настройкам в разделе **Список серверов Всемирной системы обновления Dr.Web**.
- **Базовый URI** — каталог на серверах обновлений, содержащий обновления продуктов Dr.Web. При обновлении с серверов ВСО Dr.Web не следует менять данную настройку без необходимости.
- Если в списке **Протокол получения обновлений** выбран один из защищенных протоколов, поддерживающий шифрование, то в выпадающем списке **Допустимые сертификаты** выберите тип TLS-сертификатов, которые будут автоматически приниматься при установке соединения по выбранному протоколу.
- Если в списке **Допустимые сертификаты** выбран вариант **Пользовательский**, то необходимо задать путь до файла с вашим TLS-сертификатом в поле **Сертификат**.

- **Регистрационное имя** — регистрационное имя пользователя для аутентификации на сервере обновлений, если сервер требует авторизации.
- **Пароль** — пароль пользователя для аутентификации на сервере обновлений, если сервер требует авторизации.
- В выпадающем списке **Метод авторизации** выберите метод авторизации на сервере обновлений.
- В поле **Количество временно хранимых ревизий** задается количество ревизий каждого из продуктов, временно хранимых на диске, не считая ревизий, отмеченных на вкладке **Список ревизий** в разделе **Детальная конфигурация репозитория**.

  При необходимости можете задать данную настройку отдельно для каждого продукта в разделе Синхронизация, но после сохранения изменений в общей конфигурации, настройка будет заменена на общее значение.
- Установите флаг **Использовать CDN**, чтобы разрешить использование Content Delivery Network при загрузке репозитория.
- 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.

9.11.3.2. Планировщик заданий

На вкладке **Планировщик заданий** приведены все задания из расписания Сервера Dr.Web на обновление репозитория.

Создание, удаление и редактирование заданий на обновление репозитория осуществляется в разделе Планировщик заданий Сервера Dr.Web.

9.11.3.3. Агент Dr.Web

- На вкладке **Агент Dr.Web для UNIX** выберите, 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**.

- На вкладке **Агент Dr.Web для Windows** укажите, требуется ли обновление всех компонентов, устанавливаемых на рабочие станции под ОС Windows, или только вирусных баз.
- На вкладке **Языки Агента Dr.Web для Windows** задайте список языков интерфейса Агента и антивирусного пакета для ОС Windows, которые будут скачиваться с ВСО.

9.11.3.4. Сервер 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**.

- На вкладке **Языки Центра управления безопасностью Dr.Web** задайте список языков интерфейса Центра управления, которые будут скачиваться с ВСО.

  В подразделе **Используемые языки** приводится список языков, назначенных в настройках хотя бы одному администратору.

  В разделе **Неиспользуемые языки** приводится список языков, которые не назначены в настройках ни одного администратора.

9.11.3.5. 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**.

Со скачанными новостями компании «Доктор Веб» вы можете ознакомиться в разделе главного меню Центра управления **Поддержка** → **Новости**.

9.11.3.6. Инсталляционные пакеты Dr.Web

- На вкладке **Корпоративные продукты Dr.Web** в выпадающем списке выберите, какие продукты будут обновляться с ВСО:
  - **Обновлять всё** — при обновлении репозитория с ВСО будут обновляться все доступные корпоративные продукты.
  - **Обновлять только выбранные продукты** — при обновлении репозитория с ВСО будут обновляться только продукты, для которых установлены флаги в списке ниже.

  После загрузки с ВСО корпоративные продукты станут доступны на инсталляционной странице по адресу:

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

  где <*Адрес_Сервера*> — это IP-адрес или DNS-имя компьютера, на котором установлен Сервер Dr.Web; <*номер_порта*> — порт номер `9081` (или `9080` для http).
- На вкладке **Административные утилиты Dr.Web** в выпадающем списке выберите, какие утилиты будут обновляться с ВСО:
  - **Обновлять всё** — при обновлении репозитория с ВСО будут обновляться все доступные административные утилиты.
  - **Обновлять только выбранные продукты** — при обновлении репозитория с ВСО будут обновляться только утилиты, для которых установлены флаги в списке ниже.

  После загрузки с ВСО административные утилиты станут доступны в разделе **Администрирование** → **Дополнительные возможности** → Утилиты.

9.11.4. 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** в главном меню Центра управления.
2. В открывшемся окне в подразделе управляющего меню **Детальная конфигурация репозитория** выберите продукт, который вы хотите отредактировать.
3. Настройте все необходимые параметры репозитория выбранного продукта, описанные ниже.
4. На панели инструментов доступны следующие опции для управления репозиторием продукта целиком:
   - **Удалить продукт из репозитория** — полностью удалить продукт из репозитория. При этом будут удалены все ревизии продукта и отключено обновление продукта с ВСО. Кнопка доступна в том случае, если продукт еще не был удален из репозитория. После удаления продукта, кнопка меняет свое название на **Восстановить продукт в репозитории**.

После удаления продукта из репозитория вкладка **Список ревизий** будет пуста, остальные вкладки данного раздела останутся в обычном состоянии, однако их настройки не будут применяться, поскольку продукт в репозитории отсутствует.

- **Восстановить продукт в репозитории** — восстановить продукт в репозитории, если он был удален ранее при помощи кнопки **Удалить продукт из репозитория**. При этом будет включено обновление продукта с ВСО. В репозиторий будет загружена самая свежая ревизия продукта, доступная на ВСО. Обратите внимание на возможный объем загружаемых данных. Настройка загрузки обновлений осуществляется в разделе Общая конфигурация репозитория. После восстановления продукта кнопка изменит свое название на **Удалить продукт из репозитория**.
- **Сохранить и перезагрузить с диска** — сохранить все внесенные изменения. При этом осуществляется перезагрузка текущей версии репозитория с диска (см. также раздел Состояние репозитория).

9.11.4.1. Список ревизий

На вкладке **Список ревизий** приведена информация обо всех ревизиях данного продукта, доступных на данном Сервере.

Чтобы удалить какие-либо из ревизий, установите флаги напротив этих ревизий и нажмите кнопку **Удалить выбранные ревизии** на панели инструментов.

Нельзя удалить все ревизии продукта. Продукт должен содержать хотя бы одну ревизию.

Чтобы удалить продукт целиком, воспользуйтесь кнопкой **Удалить продукт из репозитория**.

Удаление ревизий — необратимая операция.

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:

Название столбца	Описание содержимого
	1. Распространяется ревизия, отмеченная маркером в столбце **Текущая**. Отмечена может быть только одна 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. См. также Откат ревизии продукта на предыдущую версию.
Хранимая	Установите маркер, чтобы сохранять данную ревизию при автоматической очистке репозитория (см. также Синхронизация). Маркер может быть установлен для нескольких ревизий одновременно. Также ни один маркер может быть не установлен. Если ревизия продукта работает стабильно, ее можно отметить как хранимую, и в случае, если с ВСО придет нестабильная ревизия, можно откатится на предыдущую.
Удерживаемая	Автоматический маркер определяет, что компоненты из данной ревизии установлены на станциях с ограничением обновлений (в разделе Ограничения обновлений установлены опции **Обновлять только базы** или **Запретить все обновления**). Такая ревизия не удаляется при автоматической очистке репозитория и может быть использована, если будет необходимо переустановить сбойные компоненты на станции или установить дополнительные компоненты из этой ревизии.
Ревизия	Дата получения ревизии продукта.

Название столбца	Описание содержимого
	Если ревизия заморожена, в данном столбце дополнительно выводится статус блокировки.

Откат ревизии продукта на предыдущую версию

Возможность откатить установленные на станциях продукты на предыдущие версии определяется следующими положениями:

- Продукты с базами компонентов (вирусные базы, базы SpIDer Gate, базы Антиспама, Агент Dr.Web для Android) всегда могут быть откачены на предыдущую версию.
- Чтобы откатить Агент Dr.Web для Windows, необходимо разрешить опцию **Разрешить переход на более ранние ревизии** в разделе Ограничения обновлений.

При откате версии Агента для Windows на предыдущую ревизию (для установки на станциях Агента более ранней версии), будет произведена принудительная перезагрузка станций с интервалом в пять минут. Изменение интервала, а также отмена перезагрузки невозможны. О предстоящей перезагрузке пользователям станции сообщается во всплывающем оповещении.

- Остальные продукты (в частности, Доверенные приложения компонента Контроль приложений) будут откатываться на предыдущую версию, если установлен флаг **Получать последние обновления** в разделе Ограничения обновлений, либо откат производится на ревизию, отмеченную маркером **Текущая** в детальной конфигурации репозитория. Во всех остальных случаях откат не производится, Сервер ожидает появления более свежей ревизии.

9.11.4.2. Синхронизация

На вкладке **Синхронизация** настраиваются параметры обновления репозитория Сервера с ВСО:

- В поле **Количество временно 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 временно хранимых ревизий продукта уже достигло максимально допустимого значения, то удаляется самая старая временно хранимая ревизия. Ревизии, помеченные как **Текущая**, **Хранимая**, **Распространяемая** и **Удерживаемая** не подлежат автоматическому удалению и не учитывается при подсчете временно хранимых ревизий.

  Данная настройка будет перезаписана на единое значение для всех продуктов в случае редактирования раздела ВСО Dr.Web.
- 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).

- Установите флаг **Обновлять только по требованию**, чтобы обновлять продукт с ВСО только при запросе этого продукта со станций. В противном случае обновления продукта не загружаются с ВСО.

  Если ваш Сервер подключен к интернету для автоматического получения обновлений репозитория с ВСО, то при использовании этой опции никаких дополнительных действий со стороны администратора не требуется: обновления будут автоматически скачаны, как только какая-либо из станций запросит обновления этого продукта с Сервера.

  Если ваш Сервер не подключен к интернету, и обновления загружаются вручную с другого Сервера или через Загрузчик репозитория, то перед тем как устанавливать или обновлять продукты, для которых включена опция **Обновлять только по требованию**, необходимо предварительно загрузить эти продукты в репозиторий вручную.

  При установке Сервера версии 12 или сразу после обновления Сервера на версию 12 обновления продуктов репозитория **Агент Dr.Web для Android**, **Агент Dr.Web для UNIX** и **Прокси-сервер Dr.Web** по умолчанию загружаются с ВСО только при запросе этих продуктов со станций.

- В подразделе **Распространение по межсерверным связям** настраиваются следующие параметры:
  - Установите флаг **Запретить передачу обновлений соседним Серверам**, чтобы запретить отправку обновлений продукта по межсерверным связям. Данная опция не влияет на настройки обновления продукта с ВСО.
  - Установите флаг **Запретить получение обновлений от соседних Серверов**, чтобы запретить прием обновлений продукта по межсерверным связям. Данная опция не влияет на настройки обновления продукта с ВСО.

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.

9.11.4.3. 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**.

9.11.4.4. 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.

Использование заморозки ревизий при переходе между мажорными версиями не рекомендуется. После отмены заморозки могут возникать проблемы при обновлении антивирусного ПО на станциях.

Чтобы использовать функционал отложенных обновлений

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 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.

9.11.5. 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

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

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:

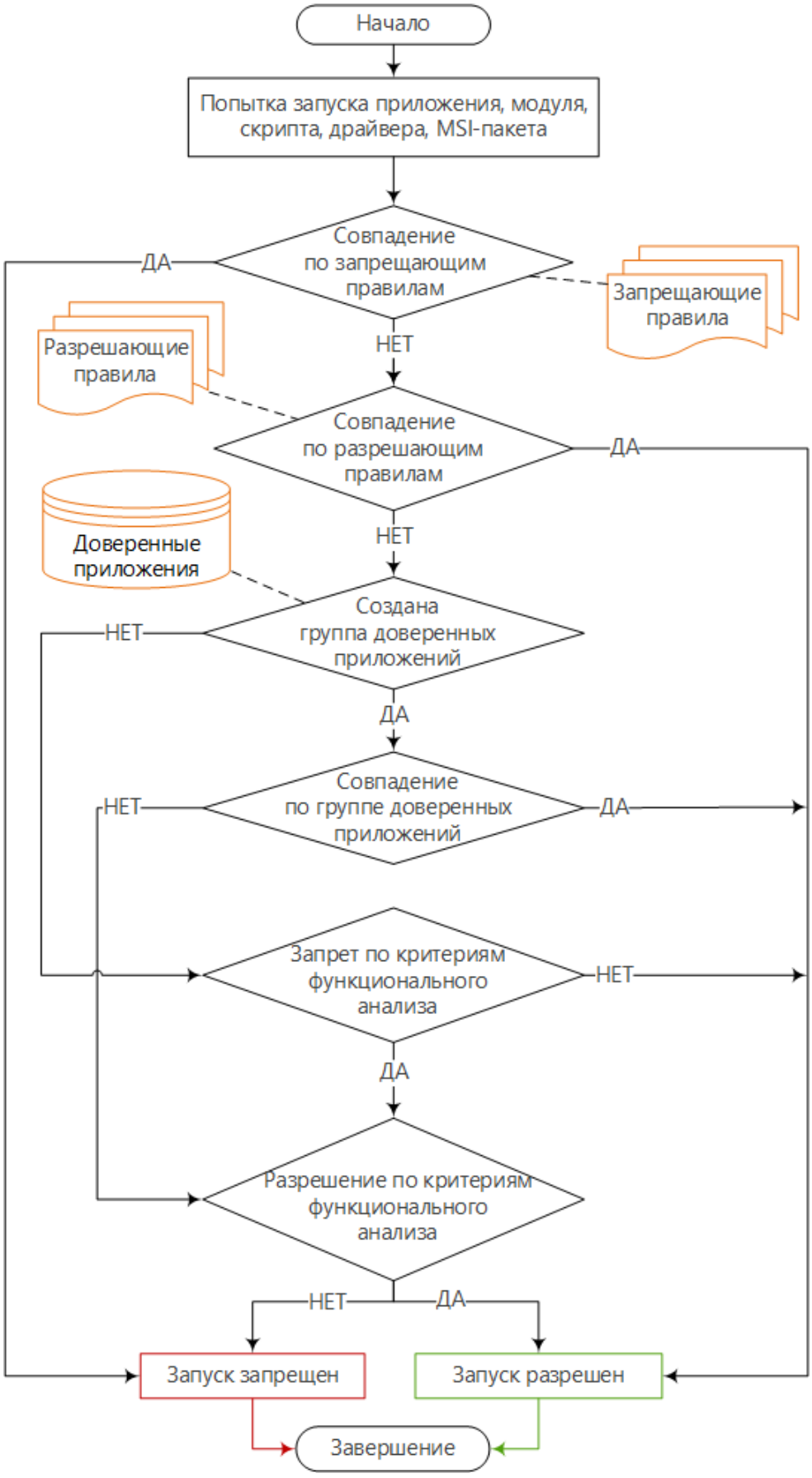
   - Весь репозиторий целиком.
   - Весь продукт целиком.
   - Вся отдельная ревизия продукта целиком.

   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.

9.12. Контроль приложений

При помощи компонента Контроль приложений вы можете регулировать, какие приложения, модули, скриптовые интерпретаторы, драйверы и MSI-пакеты разрешать, а какие — запрещать запускать на защищаемых станциях антивирусной сети, на которых установлен Агент Dr.Web для Windows.

Схема работы Контроля приложений приведена далее.



Основные инструменты Контроля приложения:

- Профили — списки правил, определяющих, какие из приложений на станциях могут быть запущены, а какие — запрещены. Профили создаются администратором и назначаются политикам, станциям и пользователям, в том числе группам станций и пользователей. Профили определяют режим работы Контроля приложений.

  Настройка профилей осуществляется через дерево сети в разделе **Антивирусная сеть**.
- Списки приложений:
  - Доверенные приложения — список приложений, который составляется по заданным правилам и собирается с выбранных станций по решению администратора. При работе в разрешающем режиме запуск этих приложений будет всегда разрешен. Конкретные группы доверенных приложений выбираются в настройках для каждого профиля индивидуально.
  - Справочник приложений — список всех приложений, установленных на защищаемых станциях. Справочник формируется автоматически в фоновом режиме и не подлежит изменению со стороны администратора.

  Настройка списков приложений осуществляется через раздел **Администрирование**.
- События Контроля приложений — информация о событиях, зафиксированных на станциях компонентом Контроль приложений.

  Просмотр событий Контроля приложений осуществляется через раздел **Антивирусная сеть** → **Статистика**.

Основные режимы работы Контроля приложений:

- *Функциональный анализ* — набор предустановленных правил, по которым приложения разрешаются или запрещаются для запуска в соответствии с выполняемыми функциями.
- *Разрешающий режим* — подразумевает, что на всех контролируемых станциях разрешается запуск только приложений из списка **Доверенные приложения** и приложений, которые соответствуют разрешающим правилам. Все остальные приложения блокируются.
- *Запрещающий режим* — подразумевает, что на всех контролируемых станциях запрещается запуск только тех приложений, которые соответствуют запрещающим правилам. Все остальные приложения разрешаются.

Разрешающий и запрещающий режимы могут быть включены или отключены как вместе, так и по отдельности.

Функциональный анализ должен быть всегда включен. Если все правила функционального анализа отключены, контроль запуска приложений не производится.

Чтобы настроить Контроль приложений

1. Создайте новый профиль.
2. Назначьте станции, пользователей и группы, на которых будут распространяться настройки созданного профиля.
3. Задайте настройки профиля.

Настройку работы профилей рекомендуется производить в тестовом режиме.

9.12.1. Тестовый режим

Чтобы убедиться в работоспособности настроенного профиля или правила, можно использовать *тестовый режим*, в котором происходит имитация работы Контроля приложений. В этом режиме приложения фактически не блокируются, но заполняется журнал активности (см. События Контроля приложений) — как если бы профиль или правило работали обычным образом.

Чтобы включить тестовый режим для профиля

1. В разделе **Общие** свойств профиля установите флаг **Включить профиль**, чтобы начать использовать этот профиль.
2. Установите флаг **Перевести профиль в глобальный тестовый режим**.
3. Нажмите **Сохранить**.

В тестовом режиме соответствующий профиль в группе **Profiles** в дереве антивирусной сети будет иметь значок . На станциях, которым назначен такой профиль, запускаемые приложения не будут блокироваться ни по заданным в профиле критериям функционального анализа, ни по разрешающим или запрещающим правилам. Вместо этого будет собираться статистика в разделе **Антивирусная сеть** → **Статистика** → **События Контроля приложений**. В данном журнале отображается подробная информация по каждому запускаемому приложению, проанализировав которую, можно изменить настройки профиля под свои нужды.

После того как вы убедитесь, что тестируемый профиль работает как нужно, необходимо перевести его из тестового режима в активный режим работы. Активный профиль имеет значок в группе **Profiles** в дереве антивирусной сети.

Чтобы отключить тестовый режим для профиля

1. В разделе **Общие** свойств профиля снимите флаг **Перевести профиль в глобальный тестовый режим**.
2. Нажмите **Сохранить**.

Тестовый режим также можно использовать для проверки работы отдельных разрешающих и запрещающих правил в профиле, без перевода в тестовый режим профиля целиком.

Чтобы включить тестовый режим для разрешающего или запрещающего правила в составе профиля

1. В разделе **Разрешающие правила** или **Запрещающие правила** свойств профиля выберите созданное правило, работу которого вы хотите протестировать.
2. В открывшихся настройках правила установите флаги **Включить правило** и **Перевести правило в тестовый режим**.
3. Нажмите **Сохранить**.

В этом режиме запускаемые на станциях программы *будут блокироваться*, однако только согласно критериям функционального анализа и тем правилам, которые не были переведены в тестовый режим. Разрешающие и запрещающие правила в тестовом режиме работают аналогично профилям в этом режиме: их настройки не влияют на блокировку программ, но результат каждого срабатывания записывается в журнал активности в разделе **События Контроля приложений**.

В отличие от тестового режима профилей, наличие правил в тестовом режиме никак не отражается на значке задействованного профиля в дереве антивирусной сети. Активный профиль с правилами в тестовом режиме будет иметь значок .

Когда вы убедитесь в должной работе тестируемого правила, необходимо перевести его из тестового режима в активный режим работы.

Чтобы отключить тестовый режим для разрешающего или запрещающего правила в составе профиля

1. В разделе **Разрешающие правила** или **Запрещающие правила** свойств профиля выберите тестируемое правило.
2. В открывшихся настройках снимите флаг **Перевести правило в тестовый режим**.
3. Нажмите **Сохранить**.

9.12.2. Доверенные приложения

Управление доверенными приложениями

Группа доверенных приложений (или белый список приложений) представляет собой список приложений, собранных по заданным критериям с выбранной станции или группы станций. Эти приложения будут разрешены для запуска на станциях

антивирусной сети, для которых они добавлены в профиль компонента Контроль приложений при работе в разрешающем режиме.

Сбор информации для формирования группы доверенных приложений является ресурсоемким процессом, который, в зависимости от заданных критериев, может существенно повлиять на быстродействие задействованного компьютера. Для снижения нагрузки на станции антивирусной сети сбор информации следует осуществлять на одной или нескольких *эталонных станциях* — компьютерах, специально выбранных для этой задачи. Идеальным кандидатом для этой роли является компьютер со свежеустановленной операционной системой, последними обновлениями и всем необходимым для работы ПО.

Для управления доверенными приложениями на Серверах, собирающих информацию, перейдите в раздел **Администрирование** → **Контроль приложений** → **Доверенные приложения**.

Таблица раздела содержит список всех актуальных групп доверенных приложений.

На панели инструментов доступны следующие кнопки управления:

➕ Создать группу доверенных приложений

🔄 Перезапустить создание группы доверенных приложений

🗑 Удалить группу доверенных приложений

Чтобы создать новую группу доверенных приложений

1. В разделе **Доверенные приложения** нажмите на панели инструментов кнопку ➕ **Создать группу доверенных приложений**.
2. В окне **Общие** задайте следующие настройки:
   - **Название группы** — название создаваемой группы доверенных приложений.
   - **Описание** — необязательное произвольное описание создаваемой группы.

   Нажмите кнопку **Далее**.
3. В окне **Параметры добавления приложений в доверенные** задайте следующие настройки, согласно которым приложения на станциях будут добавляться в создаваемую группу доверенных приложений (должно быть выбрано хотя бы по одной настройке в каждой из категорий):
   - **Область поиска** — установите флаги для тех областей, по которым будет производиться сбор информации о приложениях.

     Для опции **Искать по заданным путям** можете задать несколько путей для поиска приложений. Используйте ";" в качестве разделителя.

   - **Тип добавляемых хешей** — установите флаги для тех объектов, хеши которых будут записываться в создаваемую группу доверенных приложений.

- **Категории файлов** — установите флаги для тех файлов, которые будут учитываться при поиске.

Нажмите кнопку **Далее**.

4. В дереве сети выберите станции и группы станций, на которых будет осуществляться сбор информации о приложениях для включения их в список доверенных. Для выбора нескольких групп и станций используйте кнопки CTRL и SHIFT.

   Установите флаг **Не учитывать вложенные группы**, чтобы собирать информацию по станциям только в выбранной группе. Если флаг снят, собирается информация со всех станций в выбранной группы и ее подгруппах.

5. Нажмите кнопку **Сохранить**.
6. Начнется сбор информации о приложениях на станциях согласно заданным настройкам. Процесс может занять продолжительное время.

   Информацию о состоянии и обновлении группы доверенных приложений вы можете посмотреть:

   - в основной таблице раздела **Доверенные приложения**,
   - в дополнительной информации о группе, которая открывается при нажатии на строку, соответствующую группе в основной таблице раздела **Доверенные приложения**.

Информация о приложениях собирается в рамках текущего сеанса работы на задействованной станции. Если сбор информации не закончился, но станция была выключена или перезагружена, после включения операция начнется заново. Частично собранные данные о приложениях не сохраняются.

Чтобы запустить обновление группы доверенных приложений

1. В разделе **Доверенные приложения** в таблице раздела установите флаги для групп, которые вы хотите обновить.
2. Нажмите на панели инструментов кнопку **Перезапустить создание группы доверенных приложений**.

Чтобы удалить группу доверенных приложений

1. В разделе **Доверенные приложения** в таблице раздела установите флаги для групп, которые вы хотите удалить.
2. Нажмите на панели инструментов кнопку **Удалить группу доверенных приложений**.
3. Приложения данной группы будут удалены из списка разрешенных для запуска на станциях и сбор приложений для списка доверенных по критериям данной группы будет остановлен.

Невозможно удалить группу доверенных приложений, назначенную на профили Контроля приложений.

При удалении групп доверенных приложений создается новая ревизия в репозитории для продукта **Доверенные приложения** и распространяется на соседние Серверы. При этом может быть нарушена работа профилей Контроля приложений, для которых эта группа назначена на соседних Серверах.

Чтобы удалить информацию о приложениях на конкретной станции из группы доверенных приложений

1. В разделе **Доверенные приложения** в таблице раздела нажмите на строку с группой приложений, из которой вы хотите удалить информацию о приложениях на станции.
2. В открывшемся окне в таблице станций установите флаги для тех станций, информацию о приложениях на которых вы хотите удалить.
3. Нажмите на панели инструментов кнопку **Удалить выбранные станции**.

При удалении всех станций сама группа доверенных приложений будет удалена.

Репозиторий доверенных приложений

При настройке разрешающего режима для профиля Контроля приложений группы доверенных приложений выбираются из списка групп, доступных в репозитории для продукта **Доверенные приложения**.

Если в вашей антивирусной сети используется несколько Серверов Dr.Web, объединенных межсерверной связью, для облегчения сбора информации предоставляется возможность распределения нагрузки между вашими Серверами следующим образом:

- На одном из Серверов администратор собирает информацию с защищаемых станций. Информация автоматически размещается в репозитории Сервера в продукте **Доверенные приложения** и согласно заданным настройкам распространяется по межсерверной связи.

  Информация о доверенных приложениях может собираться на нескольких Серверах сети, но сегменты сети, обслуживаемые этими Серверами, должны быть изолированы друг от друга.
- Остальные Серверы получают обновление продукта **Доверенные приложения** по межсерверной связи согласно заданным настройкам. Настраивать сбор информации по доверенным приложениям на этих Серверах нет необходимости, поскольку в репозитории будут размещаться ревизии продукта, полученные от соседнего Сервера.

Продукт **Доверенные приложения** не обновляется с ВСО. Распространение этого продукта возможно только между соседними Серверами по межсерверной связи.

Перед началом сбора Доверенных приложений определите, какие из Серверов будут собирать информацию и отправлять ее соседним Серверам, а какие — получать ее по межсерверной связи. В зависимости от этого на каждом из Серверов необходимо произвести соответствующие настройки.

Чтобы настроить Серверы, собирающие и отправляющие доверенные приложения

1. Откройте раздел **Администрирование**.
2. Перейдите в разделе **Детальная конфигурация репозитория** → **Доверенные приложения**.
3. На вкладке **Синхронизация** снимите флаг **Запретить передачу обновлений соседним Серверам** и установите флаг **Запретить получение обновлений от соседних Серверов**.
4. Нажмите **Сохранить**.
5. Перейдите в раздел **Администрирование** → **Контроль приложений** → **Доверенные приложения** и настройте сбор доверенных приложений, как описано ниже.
6. Новая ревизия продукта **Доверенные приложения** записывается в репозиторий после получения информации ото всех станций, указанных в настройках по сбору группы доверенных приложений. После записи ревизии продукта в репозиторий, она распространяется по межсерверной связи на соседние Серверы.

Чтобы настроить Серверы, получающие доверенные приложения

1. Откройте раздел **Администрирование**.
2. Перейдите в разделе **Детальная конфигурация репозитория** → **Доверенные приложения**.
3. На вкладке **Синхронизация** снимите флаг **Запретить получение обновлений от соседних Серверов**.

   Если Сервер должен передать продукт **Доверенные приложения** другим Серверам по межсерверной связи, также снимите флаг **Запретить передачу обновлений соседним Серверам**.
4. Нажмите **Сохранить**.

9.12.3. Справочник приложений

Для просмотра справочника приложений перейдите в раздел **Администрирование** → **Контроль приложений** → **Справочник приложений**.

Справочник приложений содержит информацию о приложениях, установленных на защищаемых станциях под ОС Windows, подключенных к Серверу Dr.Web.

Справочник формируется автоматически в фоновом режиме и после сбора не подлежит изменению со стороны администратора. Информация о каждом приложении отправляется Агентом на Сервер единожды при первой активности этого приложения.

Справочник может быть использован в следующих случаях:

- Для получения информации об установленных приложениях на станциях сети.
- Для создания запрещающих и разрешающих правил. Использование справочника упрощает процесс создания правил, поскольку вся информация о приложении заполняется автоматически на основе данных о выбранном известном приложении.

Наполнение справочника приложений

Чтобы активировать отправку информации со станций для справочника приложений

1. В разделе **Антивирусная сеть** выберите в дереве станции или группы станций с установленным Контролем приложений, с которых вы хотите получать информацию об установленных на них приложениях.
2. В управляющем меню выберите пункт **Windows** → **Агент Dr.Web**.
3. На вкладке **Общие** установите флаг **Отслеживать события Контроля приложений**, чтобы отслеживать всю активность процессов на станциях, зафиксированную Контролем приложений, и отправлять события на Сервер. При отсутствии подключения к Серверу события накапливаются и отправляются при подключении. Если флаг снят, могут отправляться события только о блокировках (в зависимости от настроек в конфигурации Сервера).
4. Нажмите **Сохранить**.

Чтобы активировать сбор информации Сервером для справочника приложений

1. Откройте раздел **Администрирование** → **Конфигурация Сервера Dr.Web**.
2. Перейдите на вкладку **Статистика** и установите одну из следующих опций:
   - **Статистика Контроля приложений по активности процессов**, чтобы получать и записывать информацию по любой активности всех процессов: как разрешенных для запуска, так и запрещенных Контролем приложений. При выборе этой опции в справочник будут заноситься приложения при условии создания и назначения хотя бы одного профиля с одной или несколькими выбранными категориями критериев функционального анализа.
     До создания профилей и назначения их на станции антивирусной сети, запуск всех приложений разрешается.

- **Статистика Контроля приложений по блокировке процессов**, чтобы получать и записывать информацию по активности всех процессов, запрещенных для запуска Контролем приложений. При выборе этой опции в справочник будут заноситься приложения только после создания профилей, по настройкам которых запуск приложений будет блокироваться, и назначения этих профилей на станции антивирусной сети.

Флаг **Статистика Контроля приложений по активности процессов** может значительно повысить ресурсоемкость сбора статистики по всей антивирусной сети.

3. Нажмите кнопку **Сохранить**.
4. Перезапустите Сервер.
5. После перезагрузки Сервер начнет фиксировать статистику по запуску приложений согласно заданным настройкам, присылаемую со всех станций с установленным Контролем приложений.

Создание правил из справочника приложений

Чтобы создать новое правило на основе данных из справочника приложений

1. В разделе **Справочник приложений** выберите строку о приложений, для которого вы хотите создать правило, контролирующее запуск.
2. При нажатии на строку таблицы откроется окно с информацией о выбранном приложении.
3. Нажмите кнопку **Создать правило**.
4. Откроется окно для создания нового правила. Задайте следующие настройки:
   a) В выпадающем списке **Название профиля** выберите профиль Контроля приложений, в котором будет создано правило.
   b) В поле **Название правила** задайте название для создаваемого правила.
   c) Для опции **Тип правила** выберите тип создаваемого правила: запрещающее или разрешающее.
   d) Для опции **Режим работы** выберите, в каком режиме будет работать созданное правило (соответствует флагу **Перевести правило в тестовый режим** при создании правила из профиля):
   Если вы хотите проверить работу правила, выберите режим **Тестовый**. Приложения не будут контролироваться на станциях, однако будет осуществляться запись журнала активности как при включенных настройках. Результаты запусков и блокировок приложений в тестовом режиме работы правила будут отображаться в разделе События Контроля приложений.
   В режиме **Активный** правило будет работать в активном режиме с блокировкой приложений на станциях по заданным настройкам правила (см. также режимы работы профилей).

e) В разделе **Запрещать запуск приложений по следующим критериям/Разрешать запуск приложений по следующим критериям** (в зависимости от типа правила, выбранного на шаге 4c) будут автоматически заполнены поля в соответствии с приложением, на основе которого создается правило. При необходимости можете отредактировать значения настроек.

5. Нажмите **Сохранить**. Правило будет создано в заданном профиле Контроля приложений.

9.13. Дополнительные возможности

9.13.1. 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).
  - Команду **Анализ базы данных**. Предназначена для оптимизации базы данных Сервера посредством выполнения команды `analyze`.
  - Команду **Очистка неактивированных станций**. Предназначена для удаления учетных записей станций, которые были созданы в антивирусной сети, но ни разу не подключались к Серверу. Необходимо указать период, по истечении которого неиспользованные учетные записи будут удалены.
    Список неиспользованных учетных записей станций можно посмотреть в иерархическом списке антивирусной сети, в группе **Status** → **New**.

Чтобы выполнить команды 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.

Экспорт базы данных

Чтобы сохранить информацию из базы данных в файл

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 33.3. 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**.
     - В дереве **Антивирусная сеть** можете выбрать одну или несколько пользовательских групп. В этом случае в экспорт попадет информация только о выбранных группах и о тех станциях, для которых выбранные группы являются первичными. Если не выбрана ни одна группа, будет экспортирована информация обо всех станциях и пользовательских группах антивирусной сети.
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

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 кнопку **Сохранить**.

9.13.2. 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** в главном 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 кеша** — параметры обращения к файловому кешу компьютера, на котором установлен Сервер.
   - **Использование DNS кеша** — параметры обращения к кешу, 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 отправки статистики заражений на серверы компании «Доктор Веб».
   - **Статистика веб-сервера** — параметры обращения к Веб-серверу.
   - **Кластер** — параметры обращений по протоколу межсерверной синхронизации при использовании кластера Серверов в многосерверной конфигурации сети.
   - **Передача групповых обновлений** — параметры обмена данными при передаче групповых обновлений на рабочие станции по multicast-протоколу.
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.

9.13.3. Резервные копии

Раздел **Резервные копии** позволяет просматривать на уровне каталогов и файлов, а также сохранять локально содержимое резервных копий критичных данных Сервера.

При резервном копировании сохраняются следующие объекты: настройки репозитория, конфигурационный файлы, ключи шифрования, сертификаты, резервная копия внутренней базы данных.

Резервные копии критичных данных Сервера сохраняются в следующих случаях:

- В результате выполнения задания **Резервное копирование критичных данных сервера** согласно расписанию Сервера.
- В результате резервного копирования при запуске исполняемого файла Сервера из командной строки с ключом `backup`. Подробное описание данной команды приведено в документе **Приложения**, в разделе 33.5. Резервное копирование критичных данных Сервера Dr.Web.

Просмотр информации о резервных копиях

Чтобы просмотреть информацию о резервной копии, в иерархическом дереве выберите объект, относящийся к нужной вам резервной копии. Резервные копии размещаются в дереве согласно каталогам своего хранения: каталог по умолчанию (`var/opt/drwcs/backup` для Сервера Dr.Web под ОС семейства UNIX и `C:\DrWeb Backup` для Сервера Dr.Web под ОС Windows) и все пути сохранения резервных копий, указанные в заданиях расписания Сервера. Если в заданиях Сервера под ОС Windows указан пустой путь, по умолчанию будет использоваться каталог `C:\Program Files\DrWeb Server\var\backup`.

Просмотреть информацию можно будет только по тем резервным копиям, которые хранятся внутри каталогов Сервера.

При выборе каталогов и файлов резервных копий открывается панель свойств с информацией об объекте: **Тип**, **Размер** (только для отдельных файлов), **Дата создания** и **Дата изменения**.

Управление резервными копиями

Для управления резервными копиями используйте следующие кнопки на панели инструментов:

Резервное копирование — создать резервную копию критичных данных Сервера.

Экспортировать — сохранить резервную копию выбранного объекта на компьютере, на котором открыт Центр управления.

Удалить выбранные объекты — удалить объекты, выбранные в дереве, без возможности восстановления.

Экспорт резервной копии

Чтобы сохранить резервную копию локально

1. В иерархическом дереве выберите необходимые резервные копии (для выбора резервной копии целиком достаточно выбрать в дереве каталог, соответствующей этой резервной копии) или отдельные файлы из состава резервных копий. Для выбора нескольких объектов используйте кнопки CTRL или SHIFT.

   При экспорте обратите внимание на основные типы экспортируемых объектов:

   a) Zip-архивы резервных копий сохраняются для следующих выбранных объектов:

   - Одна или несколько резервных копий целиком (при выборе каталогов, соответствующих резервным копиям).
   - Несколько отдельных файлов из состава резервных копий.

b) Отдельные файлы из состава резервных копий. Если для экспорта был выбран только один файл, он сохраняется в исходном виде, без архивирования.

2. Нажмите кнопку **Экспортировать** на панели инструментов.
3. Задание пути для сохранения выбранных объектов осуществляется в соответствии с настройками веб-браузера, в котором открыт Центр управления.

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 33.5. Резервное копирование критичных данных Сервера Dr.Web.

9.13.4. Утилиты

Набор доступных утилит зависит от настроек репозитория Сервера. Чтобы включить или отключить получение обновлений с ВСО для утилит, доступных в данном разделе, перейдите в раздел **Администрирование** → **Общая конфигурация репозитория** → **Инсталляционные пакеты Dr.Web** → Административные утилиты Dr.Web.

В разделе **Утилиты** вы можете загрузить дополнительные утилиты для работы с Dr.Web Enterprise Security Suite:

- **Мобильный центр управления Dr.Web**

  Служит 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.

- **Утилита Dr.Web для сбора информации о системе**

  Утилита предназначена для формирования отчета о состоянии системы и всех установленных программ, включая антивирусные решения Dr.Web для защищаемых станций и ПО Сервера Dr.Web. Архив отчета может быть использован для диагностики администратором антивирусной сети, а также для предоставления в службу технической поддержки компании «Доктор Веб».

- **Утилита дистанционной диагностики Сервера Dr.Web**

  Позволяет удаленно подключаться к Серверу Dr.Web для базового управления и просмотра статистики работы. Графическая версия утилиты доступна только под ОС Windows. См. также п. Удаленный доступ к Серверу Dr.Web.

- **Утилита дистанционной диагностики Сервера Dr.Web для работы со скриптами**

  Позволяет удаленно подключаться к Серверу Dr.Web для базового управления и просмотра статистики работы. Данная версия утилиты адаптирована для использования в скриптах. См. также п. Удаленный доступ к Серверу Dr.Web.

- **Утилита генерации цифровых ключей и сертификатов**

  Позволяет генерировать ключи шифрования и цифровые сертификаты, а также осуществлять и проверять цифровую подпись файлов. Является важным средством для обеспечения безопасности соединений между компонентами антивирусной сети.

- Загрузчик репозитория Dr.Web

  Служит для скачивания продуктов Dr.Web Enterprise Security Suite из Всемирной системы обновлений. Графическая версия Загрузчика репозитория Dr.Web доступна только под ОС Windows.

- **Утилита удаления Dr.Web для Windows**

  Аварийное средство для удаления некорректных/поврежденных инсталляций ПО Агентов Dr.Web для Windows в тех случаях, когда применение штатных средств удаления недоступно или не работает. Утилита не предназначена для использования в качестве основного стандартного средства деинсталляции ПО Dr.Web.

> Для получения информации по ключам командной строки для работы с утилитами, обратитесь к документу **Приложения**, раздел **37. Утилиты**.

9.14. 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.

9.14.1. 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 9-1 представлен пример структуры сети с несколькими Серверами.

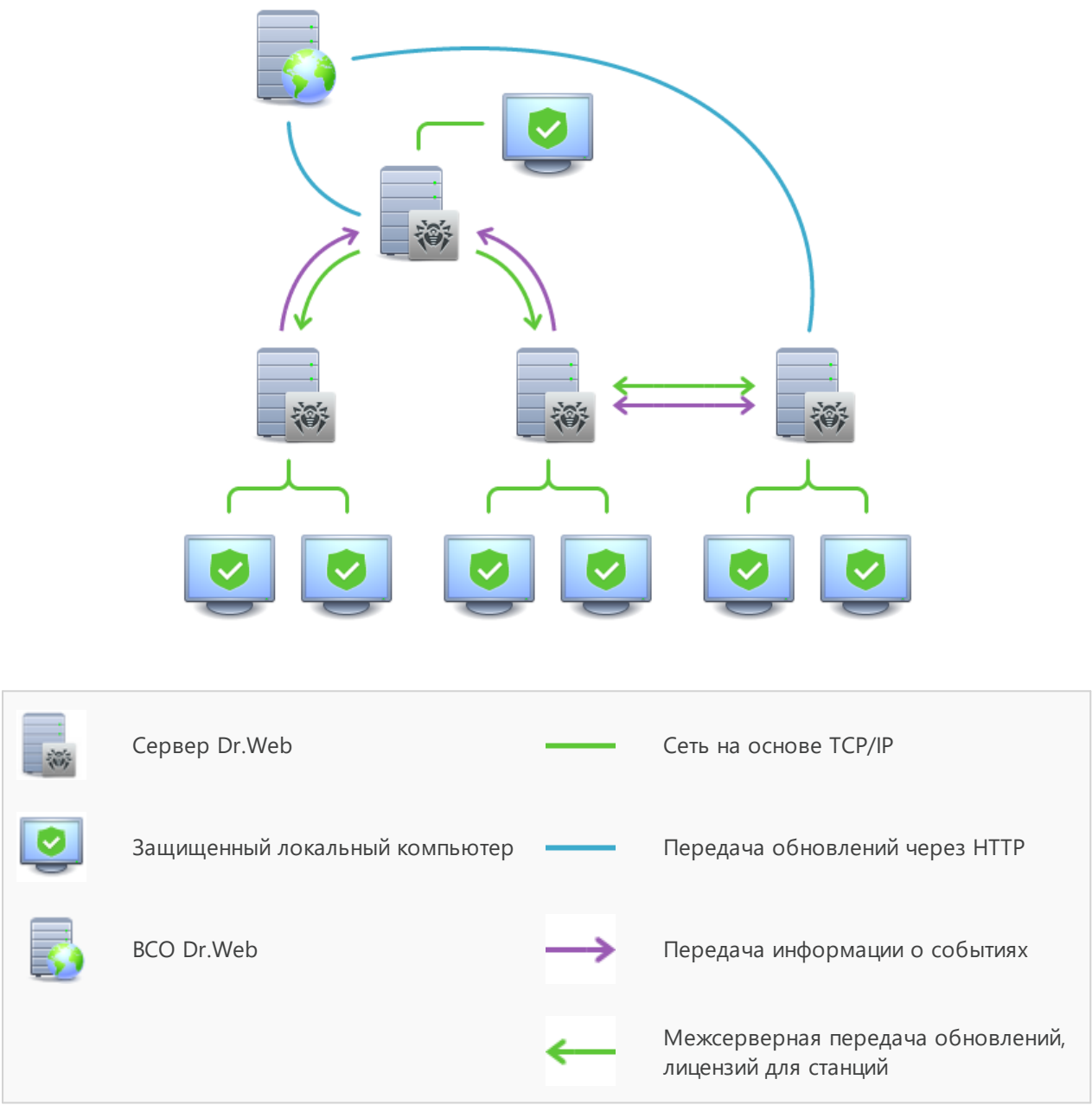


Рисунок 9-1. Сеть с несколькими Серверами

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 расписании 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.

9.14.2. 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).

При наличии межсерверных связей между Серверами Dr.Web для регистрационного имени администратора в главном меню добавляются новые функции.

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** → **Конфигурация Сервера Dr.Web** на вкладке **Общие** в поле **Название**. В данном примере назовем главный Сервер `MAIN`, а подчиненный — `AUXILIARY`.

   Заданные при настройке названия будут автоматически заменены на имена компьютеров после подключения Серверов по созданной связи.

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).
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 **Антивирусная сеть** в главном меню. Откроется окно, содержащее иерархический список антивирусной сети. Для того чтобы добавить соседний Сервер, на панели инструментов выберите **Добавить объект сети** → **Создать связь**.

   Откроется окно настройки связи 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 сертификаты Сервера Dr.Web** — список SSL-сертификатов настраиваемого Сервера. Нажмите кнопку и выберите файл сертификата `drwcsd-certificate.pem`, относящийся к текущему Серверу. Для добавления еще одного сертификата, нажмите и добавьте сертификат в новое поле.
   - **Сертификаты соседнего Сервера Dr.Web*** — список SSL-сертификатов подключаемого главного Сервера. Нажмите кнопку и выберите файл сертификата `drwcsd-certificate.pem`, относящийся к главному Серверу. Для добавления еще одного сертификата, нажмите и добавьте сертификат 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).
- **Период автоматического продления выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на данном Сервере. После окончания этого периода осуществляется автоматическое продление выданных лицензий на тот же самый период. Автоматическое продление будет осуществляться до тех пор, пока длится срок распространения лицензии. Настройка используется, если главный Сервер будет выдавать лицензии текущему Серверу.
- **Интервал для предварительного продления получаемых лицензий** — 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.
- Настройте получение оповещений администратором:
  - Установите флаг **Отправлять оповещения о событиях соседнего Сервера**, чтобы отправлять администратору оповещения о событиях, полученных от настраиваемого подчиненного Сервера. Если флаг снят, то администратор будет получать оповещения о событиях только на своем Сервере. Настроить отправку конкретных оповещений вы можете в разделе Конфигурация оповещений.
  - Установите флаг **Отправлять оповещения о событиях соседнего Сервера при обнаружении угроз по известным хешам**, чтобы отправлять администратору оповещения о событиях, полученных от настраиваемого подчиненного Сервера в случае обнаружения угроз безопасности по известным хешам угроз. Если флаг снят, то администратор будет получать оповещения о событиях только на своем Сервере. Настроить отправку конкретных оповещений вы можете в разделе Конфигурация оповещений.
    Флаг доступен, только если лицензировано использование бюллетеней

известных хешей угроз. Наличие лицензии приводится в информации по лицензионному ключу, которую можно просмотреть в разделе Менеджер лицензий, параметр **Разрешенные списки бюллетеней хешей** (достаточно лицензии хотя бы в одном из лицензионных ключей, используемых Сервером).

При включении данных опции возможно значительное увеличение получаемых оповещений.

При настройке равноправных Серверов данные опции будут доступны только если установлен флаг **Принимать** в разделе **События**.

О событиях на соседнем Сервере доступны следующие оповещения: **Обнаружена угроза безопасности**, **Отчет превентивной защиты**, **Ошибка сканирования**, **Статистика сканирования**.

О событиях на соседнем Сервере в случае обнаружения угроз безопасности по известным хешам угроз предоставляются отдельные оповещения: **Обнаружена угроза безопасности по известным хешам угроз**, **Ошибка сканирования при обнаружении угрозы по известным хешам угроз**, **Отчет Превентивной защиты об обнаружении угроз по известным хешам угроз**.

- 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 **Parents** и **Offline** (см. рис. 9-2).

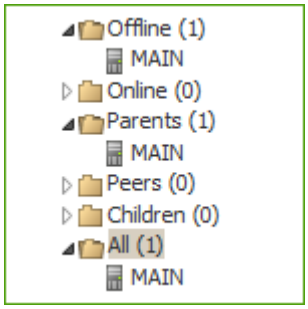


Рисунок 9-2.

6. Откройте Центр управления главного Сервера (MAIN) и добавьте подчиненный Сервер (AUXILIARY) в список соседних Серверов.

   Для этого выберите пункт **Антивирусная сеть** в главном меню. Откроется окно, содержащее иерархический список антивирусной сети. Для того чтобы добавить соседний Сервер, на панели инструментов выберите **Добавить объект сети** → **Создать связь**.

   Откроется окно настройки связи 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 сертификаты Сервера Dr.Web** — список SSL-сертификатов настраиваемого Сервера. Нажмите кнопку и выберите файл сертификата `drwcsd-certificate.pem`, относящийся к текущему Серверу. Для добавления еще одного сертификата, нажмите и добавьте сертификат в новое поле.
- **Сертификаты соседнего Сервера Dr.Web*** — список SSL-сертификатов подключаемого подчиненного Сервера. Нажмите кнопку и выберите файл сертификата `drwcsd-certificate.pem`, относящийся к подчиненному Серверу. Для добавления еще одного сертификата, нажмите и добавьте сертификат 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).
- **Период автоматического продления выдаваемых лицензий** — настройка не используется при создании связи до подчиненного Сервера.
- **Интервал для предварительного продления получаемых лицензий** — промежуток времени до окончания периода автоматического продления лицензий, начиная с которого данный подчиненный Сервер запрашивает предварительное автоматическое продление этих лицензий. Настройка используется, если подчиненный Сервер будет получать лицензии от текущего Сервера.
- **Период синхронизации лицензий** — настройка не используется при создании связи до подчиненного Сервера.
- 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.
- Опция **Отправлять оповещения о событиях соседнего Сервера** отключена и не подлежит изменению, поскольку подчиненный Сервер не получает события от главного Сервера.
- 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 **Children** и **Offline** (см. рис. 9-3).

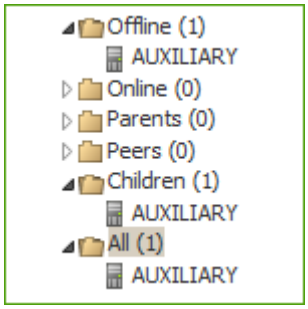


Рисунок 9-3.

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 **Offline** в папку **Online** (см. рис. 9-4).

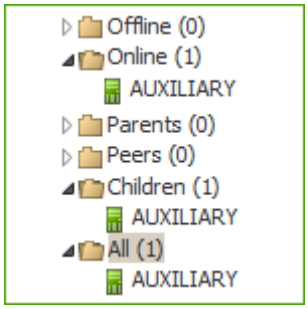


Рисунок 9-4.

8. Откройте Центр управления подчиненного Сервера (AUXILIARY) и убедитесь в том, что главный Сервер (MAIN) подключен к подчиненному (AUXILIARY) (см. рис. 9-5).

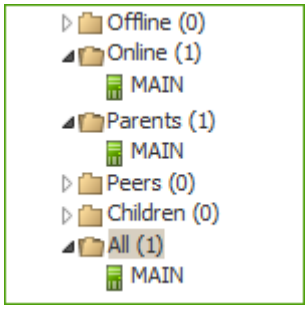


Рисунок 9-5.

Невозможно связать несколько Серверов с одинаковой парой параметров: пароль и SSL-сертификат.

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.

Однако, задание адреса подключаемого Сервера с одной из сторон является обязательным.

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 сертификаты на одном из Серверов.
- Задан неверный пароль доступа на одном из Серверов (заданы несовпадающие пароли на соединяемых Серверах).

Если необходимо установить новую межсерверную связь между Серверами 10 и 12 версий, дополнительно выполните следующие действия:

1. При создании связи укажите открытый ключ Сервера версии 12 на Сервере версии 10.
2. Сгенерируйте сертификат из закрытого ключа Сервера версии 10 при помощи утилиты `drwsign` (команда `gencert`) из состава Сервера версии 12 (см. документ **Приложения**, п. 37.1. Утилита генерации цифровых ключей и сертификатов). Укажите этот сертификат при создании связи на Сервере версии 12.

9.14.3. 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.

Чтобы просмотреть информацию о вирусных событиях на всех Серверах Dr.Web, связанных с данным

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления. В дереве антивирусной сети, в группе **Neighbors** выберите соседний Сервер, информацию которого хотите просмотреть.
2. Выберите в управляющем меню пункт **Общие** → **Оборудование и программы**, чтобы просмотреть статистику по аппаратному и программному обеспечению на защищаемых станциях, подключенных к выбранному соседнему Серверу.

   Информация, приведенная в данном разделе, аналогична информации в разделе для станций, подключенных к вашему Серверу (см. Аппаратно-программное обеспечение на станциях под ОС Windows).
3. Чтобы просмотреть статистику работы антивирусных компонентов на защищаемых станциях, подключенных к выбранному соседнему Серверу, выберите соответствующий пункт в разделе управляющего меню **Статистика**.

   Информация, приведенная в данном разделе, аналогична информации в разделе для станций, подключенных к вашему Серверу (см. Статистика).

9.14.4. 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`, а также сертификат Сервера `drwcsd-certificate.pem`.

   Если ключи шифрования и сертификат ранее не создавались, то в ходе установки первого Сервера кластера они будут сформированы автоматически.

   Получить необходимые ключи шифрования и сертификат для установки последующих Серверов кластера можно через Центр управления: меню **Администрирование** → **Ключи шифрования**. При этом в дальнейшем могут потребоваться и закрытый ключ, и сертификат: при задании закрытого ключа `drwcsd.pri` во время установки Сервера, открытый ключ `drwcsd.pub` и сертификат `drwcsd-certificate.pem` формируются автоматически, однако при генерации сертификата создается его новая версия, поэтому сертификат должен быть заменен на одну и ту же версию на всех Серверах кластера (см. Инструменты для обеспечения безопасного соединения).

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. Ж3. 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 кнопку **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) В пределах кластера не настраивается иерархическая структура Серверов. Достаточно добавить лицензионный ключ (или несколько ключей) на одном из Серверов кластера. Информация об этом лицензионном ключе будет записана в общую базу данных. Таким образом, лицензионный ключ будет использоваться всеми Серверами кластера одновременно. Общее количество лицензий, хранящихся в общей базе данных, должно соответствовать общему количеству станций, обслуживаемых всеми Серверами кластера.

Для возможности использования лицензионного ключа на всех Серверах кластера, а не только на том, на котором ключ был добавлен, остальные Серверы кластера необходимо перезагрузить после добавления ключа.

b) Возможно 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 используются Серверы как входящие в кластер, так и не входящие. В этом случае осуществляется распространение необходимого количества лицензий из лицензионного файла по межсерверной связи непосредственно в процессе работы:

   - С Сервера, не входящего в кластер, на один из Серверов кластера. Распространенные лицензии будут использоваться всеми Серверами кластера как описано в п. a).
   - С одного из Серверов кластера (т. е. из ключа, используемого всеми Серверами кластера) на Сервер, не входящий в кластер.

   Настройка распространения необходимого количества лицензий на необходимый срок осуществляется вручную администратором антивирусной сети (подробнее см. раздел Распространение лицензий по межсерверным связям).

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.

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.

9.15. Интеграция с инфраструктурой виртуальных рабочих мест

Dr.Web Enterprise Security Suite поддерживает интеграцию с инфраструктурой виртуальных рабочих мест (VDI). Такая возможность полезна при работе с *тонкими клиентами*, поддерживающими работу в терминальном режиме по протоколу RDP.

Работа антивирусной сети при этом организуется следующим образом:

1. Администратор антивирусной сети создает *эталонный образ виртуальной станции* с предустановленным ПО и Агентом Dr.Web, после чего подключает эталон к Серверу.
2. Из созданного эталона клонируются необходимые виртуальные станции.
3. По истечении заданного срока виртуальные станции удаляются. Впоследствии виртуальные станции создаются заново из эталонного образа по мере необходимости.

Чтобы подготовить антивирусную сеть к работе с VDI

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления и создайте новую станцию, которая будет служить эталонным образом.
2. Установите на созданную станцию Агент Dr.Web и все необходимое ПО. Подключите станцию к Серверу.
3. В том же разделе создайте новую группу, в которой будут размещаться виртуальные станции.

4. Настройте порядок регистрации виртуальных станций. Для этого в Центре управления перейдите в раздел **Администрирование** → Пользовательские процедуры. Добавьте новую процедуру на основе события **Новичок подключается к Серверу**. В поле **Текст процедуры** укажите:

```
local args = ... -- args.id, args.address, args.station

if args.id == '<идентификатор_эталонной_станции>' then

  return { "id", dwcore.get_uuid(), "pgroup",
"<идентификатор_первичной_группы>" }

end
```

В качестве *<идентификатора_эталонной_станции>* необходимо указать ID эталонной станции, созданной на этапе 1. В качестве *<идентификатора_первичной_группы>* укажите ID группы, созданной на этапе 3. Данная информация всегда доступна в свойствах объектов в дереве **Антивирусной сети**.

При клонировании каждая новая виртуальная станция будет получать идентификатор, совпадающий с идентификатором эталонной станции. По условиям процедуры, при подключении станции к Серверу Dr.Web для нее генерируется новый UUID, после чего станция регистрируется в первичной группе с указанным идентификатором.

При написании процедуры рекомендуется сверяться со встроенным шаблоном процедуры **Новичок подключается к Серверу**. Для уточнения информации, в том числе возможных альтернативных параметров и возвращаемых значений, в Центре управления в дереве процедур выберите **Examples of the hooks** → **Новички** → **Новичок подключается к Серверу**.

Плановое удаление неактивных виртуальных станций

Для рационального распределения лицензий, а также для предотвращения скопления в базе данных информации об удаленных виртуальных станциях, необходимо настроить задание по автоматическому удалению неактивных станций. Под неактивными подразумеваются станции, которые не подключались к Серверу в течение указанного срока.

Для подготовки задания по автоматическому удалению неактивных станций

1. В Центре управления перейдите в раздел **Администрирование** → **Планировщик заданий Сервера Dr.Web**.
2. Создайте новое задание, нажав кнопку **Создать задание** на панели инструментов.

3. На вкладке **Действие** в выпадающем списке выберите **Выполнение скрипта**, после чего импортируйте из отдельного файла, либо введите вручную следующий Lua-скрипт в поле ниже:

```
local adminName = 'admin'
-- указываем ID группы
local gid       = '<идентификатор_первичной_группы>'
-- задаем период неактивности (в секундах)
local interval  = 86400


require('st-db-state')
require('core/datetime')
require('core/admins/admins')
local lastseen = Datetime.timeUnixstampToDBFormat(Datetime.nowTimestamp() -
interval)
local stations = {}
-- выполняем запрос к базе данных
local res, err1 = DBuilder()
    :select('id, lastseenat')
    :from('stations')
    :where('gid', gid)
    :where('lastseenat '..dwcore.base64_decode('PA=='), lastseen)
    :where('state !=', st_db_state.st_db_state_logged_in)
    :get()
if res and next(res) then
  for i = 1, #res do
    table.insert(stations, res[i][1])
  end
end
-- удаляем неактивные станции
local function delete_stations(ids)
  local admin, err    = Admin:initWithLogin(adminName)
  require 'core/admins/admins'
  require('core/stations/stations')
  local status, results_stations = Stations:delete(ids, admin)
  return ''
end
return delete_stations(stations)
```

В качестве <*идентификатора_первичной_группы*> укажите ID группы, созданной на этапе 3 при подготовке к работе с VDI.

Данный скрипт обращается к базе данных, получает ID станций, не подключавшихся к Серверу в течение последних 24 часов (86400 секунд), и удаляет эти станции из группы с указанным ID.

Рекомендуется обновлять эталонный образ каждый раз после обновления антивирусных компонентов, требующего перезагрузки операционной системы. После обновления проверьте и при необходимости скорректируйте идентификатор эталонной станции в тексте процедуры.

Глава 10: Обновление компонентов Dr.Web Enterprise Security Suite в процессе работы

В данной главе описано обновление компонентов Dr.Web Enterprise Security Suite, которое осуществляется в процессе работы продукта и не подходит для перехода на новую версию.

Обновление продукта и его компонентов до новой версии описано в **Руководстве по установке**, в разделе Глава 7: 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.

Перед обновлением ПО рекомендуется настроить конфигурацию репозитория, в том числе доступ к ВСО Dr.Web (см. п. Общая конфигурация репозитория).

10.1. 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 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 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** в главном 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**.

10.2. Ручное обновление репозитория Сервера Dr.Web

Чтобы проверить текущее состояние репозитория или обновить компоненты антивирусной сети

1. Выберите пункт **Администрирование** в главном 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 на панели инструментов:
   - Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО. Если проверяемый компонент устарел, то его обновление произойдет автоматически.
   - Нажмите одну из следующих кнопок на панели инструментов, чтобы скачать журнал обновлений репозитория:
     Сохранить данные в CSV-файл,
     Сохранить данные в HTML-файл,
     Сохранить данные в XML-файл,
     Сохранить данные в PDF-файл.
   - 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.

10.3. Обновление репозитория Сервера Dr.Web по расписанию

Вы можете настроить расписание заданий на Сервере для выполнения регулярных обновлений ПО (подробнее о расписании заданий см. п. Настройка расписания Сервера Dr.Web).

Чтобы настроить расписание для обновления репозитория Сервера Dr.Web

1. Выберите пункт **Администрирование** в главном 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 новое задание, на панели инструментов нажмите кнопку **Создать задание**. При этом откроется окно редактирования задания.
3. На вкладке **Общие** настройте следующие параметры:
   - В поле **Название** задайте 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.
   - 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.
   - Если флаг **Запускать задание асинхронно** снят, задание будет помещено в общую очередь заданий Планировщика, выполняемых последовательно. Установите флаг, чтобы выполнять данное задание параллельно вне очереди.
4. На вкладке **Действие** настройте следующие параметры:
   - В выпадающем списке **Действие** выберите тип задания **Обновление репозитория**.
   - В списке **Продукт** установите флаги напротив тех продуктов репозитория, которые будут обновляться согласно этому заданию.
   - Установите флаг **Обновлять лицензионные ключи**, чтобы активировать процедуру автоматического обновления лицензионных ключей при обновлении репозитория. Подробная информация приведена в разделе Автоматическое обновление лицензий.
5. На вкладке **Время** настройте следующие параметры:
   - В выпадающем списке **Периодичность** выберите режим запуска задания и настройте время в соответствии с выбранной периодичностью.
   - 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.
6. Нажмите кнопку **Сохранить** для создания задания с заданными параметрами.

10.4. Обновление репозитория Сервера Dr.Web, не подключенного к интернету

Если Сервер Dr.Web не подключен к интернету для получения обновлений репозитория с серверов ВСО, возможны следующие варианты настройки обновления:

- Если в сети есть другой Сервер Dr.Web, подключенный к интернету для получения обновлений, настройте межсерверную связь с этим сервером как для равноправных или как главный-подчиненный, где Сервер, не подключенный к интернету, будет подчиненным. При этом Сервер, не подключенный к интернету, будет получать все обновления с главного Сервера автоматически.

  Описание настройки межсерверных связей приведено в разделе Особенности сети с несколькими Серверами Dr.Web.
- Если нет возможности настроить автоматическое обновление с другого Сервера через межсерверную связь, можно обновить репозиторий неподключенного Сервера вручную:
  - Если в сети есть другой Сервер Dr.Web, подключенный к интернету для получения обновлений, перенесите содержимое репозитория с обновляемого Сервера вручную, как описано в разделе Копирование репозитория другого Сервера Dr.Web.
  - Если в сети нет возможности подключить какой-либо из Серверов к интернету для получения обновлений, вы можете скачать репозиторий с ВСО без использования ПО Сервера. Для этого предоставляется штатная утилита Загрузчик репозитория Dr.Web.

10.4.1. 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.

Чтобы перенести обновления 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 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**.

10.4.2. 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-хеш, 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.

Состав продуктов репозитория приведен в разделе Управление репозиторием Сервера Dr.Web.

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**.

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. Выбор протокола загрузки обновлений будет зависеть от типа сервера из шага 2: HTTP/HTTPS для веб-сервера, FTP/FTPS для FTP-сервера и т. п. Исключение составляет протокол FILE — он не доступен для использования по сети (см. Создание зеркала репозитория на Сервере Dr.Web).

Создание зеркала репозитория на Сервере Dr.Web

1. Загрузите с ВСО репозиторий Сервера через утилиту Загрузчик репозитория Dr.Web.

   При загрузке выберите режим **Синхронизировать зеркало обновлений** в главном окне утилиты.

2. Загруженное зеркало разместите в произвольном каталоге на компьютере с установленным Сервером Dr.Web.

3. В разделе **Администрирование** → Общая конфигурация репозитория настройте получение обновлений с использованием протокола FILE.

   В поле **Базовый URI** необходимо указать полный локальный путь до каталога, в котором располагается зеркало. Параметр **Список серверов Всемирной системы обновления Dr.Web** при этом не используется.

Убедитесь, что зеркало располагается в каталоге с названием `12.00`. При этом путь в поле **Базовый URI** необходимо указывать вплоть до этого каталога, не включая сам каталог.

10.4.2.1. Графическая утилита

Графическая версия утилиты Загрузчик репозитория Dr.Web доступна только под ОС Windows 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.

Утилита располагается в каталоге `webmin\utilities` каталога установки Сервера. Исполняемый файл `drweb-reploader-gui-windows-<`*разрядность*`>.exe`.

Чтобы скачать репозиторий 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-хеш 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 Сервера.
      - **Синхронизировать зеркало обновлений** — осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут быть 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.

10.4.2.2. Консольная утилита

Предоставляются следующие версии консольной утилиты Загрузчик репозитория Dr.Web:

Исполняемый файл	Расположение	Описание
`drweb-reploader-<ОС>-<разрядность>`	Центр управления, раздел **Администрирование** → **Утилиты**	Независимая версия утилиты. Может запускаться из произвольного каталога и на любом компьютере с соответствующей операционной системой.
	Каталог Сервера `webmin/utilities`	
`drwreploader`	Каталог Сервера `bin`	Версия утилиты зависит от наличия серверных библиотек. Может запускаться только из каталога своего расположения.

Описание ключей командной строки для консольной версии утилиты Загрузчика репозитория приведено в документе **Приложения**, в разделе 37.5. Загрузчик репозитория Dr.Web.

10.5. Ограничение обновлений рабочих станций

При помощи Центра управления вы можете задать ограничения на объем сетевого трафика при передаче обновлений между Сервером и Агентами на защищаемых станциях в определенные промежутки времени.

Подробнее см. в п. Ограничение трафика рабочих станций.

Ограничения скорости обновлений не применяются при дополнительной установке новых компонентов, а также при обновлении, запущенном администратором при помощи опции панели инструментов **Восстановить сбойные компоненты**.

Чтобы настроить режим ограничений трафика

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:

- **Обновлять все продукты** — 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 **Снизить серьезность устаревания вирусных баз**, чтобы снизить серьезность состояний станций с устаревшими вирусными базами. Если флаг установлен, то станции с устаревшими вирусными базами будут отображаться в антивирусной сети с общим значком, а в разделе **Состояние** у станций будет серьезность **Низкая**. Если флаг снят, то станции с устаревшими вирусными базами будут отображаться в антивирусной сети со значком (если включена опция на панели инструментов **Настройки вида дерева** → **Показывать серьезность состояния станций**), а в разделе **Состояние** у станций будет серьезность **Максимальная** или **Высокая**.
4. В поле **Интервал актуальности ревизий** задается временной интервал, в течение которого ревизии продуктов, установленных на станциях, будут считаться актуальными при появлении новых ревизий в репозитории Сервера.
5. Установите флаг **Получать 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.
6. Установите флаг **Разрешить переход на более ранние ревизии**, чтобы разрешить заменять на станциях новые версии антивирусных компонентов более ранними ревизиями из репозитория Сервера согласно настройкам распространения.

   См. также Откат ревизии продукта на предыдущую версию.
7. Установите флаг **Ограничить трафик обновлений**, чтобы ограничить объем сетевого трафика при передаче обновлений между Сервером и Агентами.

   Если флаг снят, обновления для Агентов передаются без ограничения полосы пропускания сетевого трафика.

   Если флаг установлен, задайте следующие поля:

   - В поле **Скорость по умолчанию** задается значение максимальной скорости передачи обновлений, используемое по умолчанию, т. е. если не задано никакое другое ограничение (пустые белые ячейки в таблице расписания). Также значение скорости по умолчанию применяется для периодов, когда передача данных запрещена, но процесс обновления уже был запущен (см. ниже).
   - В поле **Максимальная скорость передачи (КБ/с)** задается значение максимальной скорости передачи обновлений. При этом обновления будут передаваться в

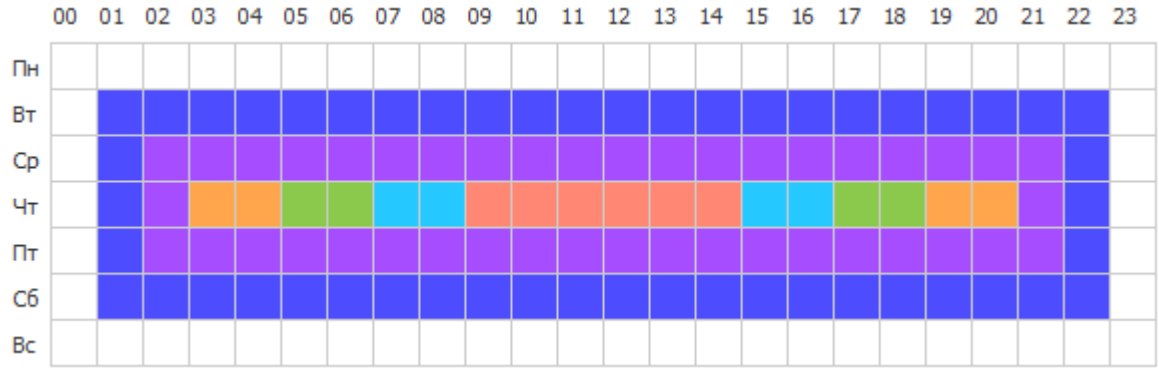
пределах заданной полосы пропускания совокупного сетевого трафика обновлений всех Агентов.

Допускается задание до пяти ограничений на скорость передачи обновлений. Для добавления еще одного поля ограничения скорости нажмите кнопку . Для удаления ограничения нажмите кнопку напротив ограничения, которое нужно удалить.

Для значений полей **Скорость по умолчанию** и **Максимальная скорость передачи (КБ/с)** существуют следующие ограничения:

- Запрещено задавать значение 0. Минимальное допустимое значение ограничения — 1 КБ/с.
- Пустое значение (поле не заполнено) снимает все ограничения на трафик обновлений для соответствующего периода времени.

В таблице расписания задается режим ограничения на передачу данных отдельно на каждые 30 минут каждого дня недели.



Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков путем перетаскивания мышью.

Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей.

В периоды времени, которые соответствуют значению **Передача данных запрещена**, запрещено начинать передачу обновлений. Если при наступлении данного периода передача обновлений уже была запущена, она не будет прервана, но максимальная скорость передачи будет ограничена значением, заданным в поле **Скорость по умолчанию**.

8. 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 политики или первичной группы — удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы.

Скопировать настройки из политики или 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.

10.6. 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.

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** → **Изменение режима работы** (для ОС Windows) или **Запуск в мобильном режиме** (для остальных операционных систем).

В Мобильном режиме Агент пытается подключиться к Серверу, делает три попытки и, если не удалось, выполняет HTTP-обновление с серверов ВСО. Попытки найти Сервер идут непрерывно с интервалом около минуты.

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 отключен, и связь Агента с Сервером возобновится.

В Мобильном режиме производится обновление только вирусных баз.

В Мобильном режиме функционирование Агента не ограничено по времени, однако обновление вирусных баз с ВСО осуществляется только до конца срока действия лицензионного ключа станции, информация о котором была сохранена Агентом при последнем подключении к Серверу (сам лицензионный ключ располагается на Сервере).

Описание настроек Мобильного режима работы на стороне Агента приведено в **Руководстве пользователя**.

Глава 11: Настройка дополнительных компонентов

11.1. Прокси-сервер Dr.Web

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

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).

Прокси-сервер позволяет использовать любой компьютер, входящий в состав антивирусной сети, в следующих целях:

- В качестве центра ретрансляции обновлений для снижения сетевой нагрузки на Сервер и соединение между Сервером и Прокси-сервером, а также для сокращения времени получения обновлений защищаемыми станциями за счет использования функции кеширования.
- В качестве центра пересылки вирусных событий от защищаемых станций на Сервер, что также снижает сетевую нагрузку и позволяет справиться, например, в случаях, когда группа станций находится в сетевом сегменте, изолированном от сегмента, в котором расположен Сервер.

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. Кеширование обновлений Агента и антивирусного пакета, передаваемых Сервером. В случае выдачи обновлений из кеша Прокси-сервера обеспечивается:
   - уменьшение сетевого трафика,
   - уменьшение времени получения обновлений Агентами.
5. Обеспечение шифрования трафика между Серверами и Агентами.

Возможно создание иерархии Прокси-серверов.

Общая схема антивирусной сети при использовании Прокси-сервера приведена на рис. 11-1.

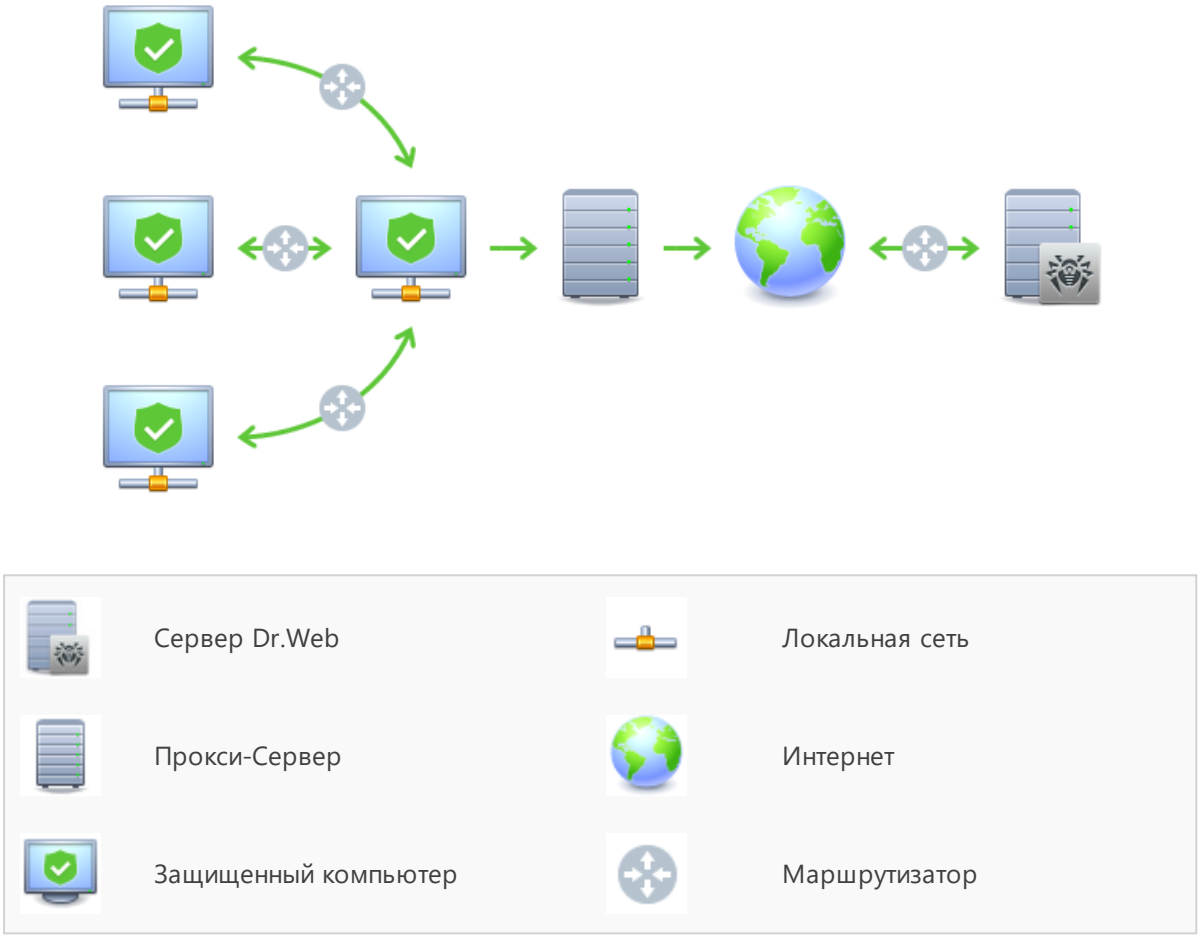


Рисунок 11-1. Схема антивирусной сети при использовании Прокси-сервера

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.conf` (см. документ **Приложения**, п. Приложение Ж4).
2. К Прокси-серверу подключается Агент Dr.Web.
3. Прокси-сервер переадресует трафик с 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 в настройках Сервера установлен флаг **Заменять NetBIOS-имена**, 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 поддерживает шифрование трафика. Для поддержки шифрования Прокси-сервер должен подключиться к Серверу (см. **Руководство по установке**, п. Подключение Прокси-сервера к Серверу Dr.Web) и подписать свой сертификат

сертификатом и закрытым ключом Сервера. Шифрование трафика между Прокси-сервером и Сервером осуществляется на основе сертификата Сервера; шифрование трафика между Прокси-сервером и Агентами осуществляется на основе сертификата Прокси-сервера, подписанного сертификатом и закрытым ключом Сервера.

Кеширование

Прокси-сервер поддерживает кеширование трафика.

Кеширование 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 кешировании:

- 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.

Установка

Установка Прокси-сервера Dr.Web и его подключение к Серверу Dr.Web подробно описаны в документе **Руководство по установке**, п. Установка Прокси-сервера Dr.Web.

Настройки

Прокси-сервер не имеет графического интерфейса. Настройки задаются одним из следующих способов:

1. Удаленно через Центр управления, если Прокси-сервер подключен к Серверу Dr.Web (см. п. Удаленная настройка Прокси-сервера).
2. Локально при помощи конфигурационного файла. Формат конфигурационного файла Прокси-сервера приведен в документе **Приложения**, п. Приложение Ж4.

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 Dr.Web).

Также для запуска Прокси-сервера под ОС Windows и ОС семейства UNIX вы можете запустить исполняемый файл `drwcsd-proxy` с соответствующими параметрами (см. Приложение 35. Прокси-сервер).

11.1.1. Удаленная настройка Прокси-сервера

После подключения Прокси-сервера Dr.Web к Серверу Dr.Web предоставляется возможность удаленной настройки Прокси-сервера через Центр управления.

Подробная информация о настройках подключения приведена в **Руководстве по установке**, п. Подключение Прокси-сервера к Серверу Dr.Web.

Прокси-сервер может получать настройки только с определенного набора подключенных к нему Серверов, которые помечены как управляющие. Если ни один Сервер не помечен управляющим, то подключение осуществляется ко всем Серверам по очереди до первого получения валидной (не пустой) конфигурации.

Чтобы задать настройки Прокси-сервера

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название Прокси-сервера или группы **Proxies** и ее подгрупп.
2. В открывшемся управляющем меню выберите пункт **Прокси-сервер Dr.Web**. Откроется раздел настроек.
3. На вкладке **Сертификат** задается список сертификатов Серверов Dr.Web. Необходимо наличие сертификатов всех Серверов, к которым подключается Прокси-сервер, и на которые перенаправляется клиентский трафик.

- Сертификат Сервера требуется для подключения к Серверу с целью удаленного управления настройками, а также для поддержки шифрования трафика между Сервером и Прокси-сервером.
- Сертификат Прокси-сервера, который подписывается сертификатом и закрытым ключом Сервера (процедура осуществляется автоматически на Сервере после подключения и не требует вмешательства администратора), требуется для подключения Агентов и для поддержки шифрования трафика между Агентами и Прокси-сервером.

4. На вкладке **Прослушивание** настраиваются параметры получения и перенаправления трафика Прокси-сервером.

   Для единых настроек прослушивания сети возможно задать единые настройки подключения всех клиентов и настройки, задаваемые отдельно для каждого из Серверов.

   Чтобы добавить еще один блок настроек, нажмите кнопку  .

   Чтобы удалить блок настроек, нажмите  рядом с блоком, который вы хотите удалить.

   Для каждого блока вы можете по отдельности настроить следующие параметры работы Прокси-сервера:

   a) В разделе настроек прослушивания:

   - В поле **Адрес для прослушивания** задайте IP-адрес, "прослушиваемый" Прокси-сервером. Значение `0.0.0.0` предписывает "прослушивать" все интерфейсы.

   Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Д. Спецификация сетевого адреса.

   - В поле **Порт** задайте номер порта, который будет "прослушиваться" Прокси-сервером. По умолчанию — порт `2193`.
   - Установите флаг **Обнаружение** для включения режима имитации Сервера. Данный режим позволяет клиентам обнаруживать Прокси-сервер в качестве Сервера Dr.Web в процессе его поиска через широковещательные запросы.
   - Установите флаг **Multicasting**, чтобы Прокси-сервер отвечал на широковещательные запросы, адресованные Серверу.
   - В поле **Multicast-группа** задайте IP-адрес многоадресной группы, в которую будет входить Прокси-сервер. Указанный интерфейс будет прослушиваться Прокси-сервером для взаимодействия с клиентами при поиске активных Серверов Dr.Web. Если поле оставить пустым, Прокси-сервер не будет входить ни в одну из многоадресных групп. По умолчанию многоадресная группа, в которую входит Сервер — `231.0.0.1`.

   b) В разделе **Параметры соединения с клиентами**:

   - В выпадающем списке **Шифрование** выберите режим шифрования трафика для каналов между Прокси-сервером и обслуживаемыми клиентами: Агентами и инсталляторами Агентов.

- В выпадающем списке **Сжатие** выберите режим сжатия трафика для каналов между Прокси-сервером и обслуживаемыми клиентами: Агентами и инсталляторами Агентов. В выпадающем списке **Уровень сжатия** выберите уровень сжатия (от 1 до 9).

c) В разделе **Параметры соединения с Серверами Dr.Web** задается список Серверов, на которые будет перенаправляться трафик.

От порядка следования Серверов в списке зависит порядок перенаправления клиентского трафика и порядок подключения Прокси-сервера к Серверам для получения настроек. Чтобы изменить порядок следования Серверов, перетащите нужные строки при помощи мыши.

Для управлениями Серверами используйте кнопки на панели инструментов списка Серверов:

 редактировать параметры соединения с выбранным Сервером Dr.Web.

 добавить параметры соединения с Сервером Dr.Web.

 удалить параметры соединения с выбранным Сервером Dr.Web.

При редактировании и создании параметров соединения с Серверами открывается окно настроек со следующими опциями:

- В выпадающем списке **С этого Сервера возможно управление настройками Прокси-сервера** выберите один из вариантов для назначения Сервера управляющим:
  Да — Сервер будет безусловным управляющим. Вы можете назначить любое количество Серверов управляющими, подключение осуществляется ко всем управляющим Серверам по порядку следования в настройках Прокси-сервера до первого получения валидной (не пустой) конфигурации.
  Нет — Сервер не будет управляющим ни при каких условиях. Также вы можете не назначать ни один из Серверов управляющим. В этом случае настройка параметров Прокси-сервера (в том числе назначение управляющих Серверов) возможна только локально через конфигурационный файл Прокси-сервера (см. документ **Приложения**, раздел Ж4. Конфигурационный файл Прокси-сервера).
  Возможно — Сервер будет управляющим только в том случае, если нет безусловных управляющих (со значением **Да** для этой настройки).
- В поле **Адрес перенаправления** задайте адрес Сервера Dr.Web, на который будут перенаправляться соединения, устанавливаемые Прокси-сервером.

Если в поле **Адрес перенаправления** не задан адрес или указано значение `udp/`, то Прокси-сервер попытается найти Сервер Dr.Web через службу обнаружения — рассылкой широковещательных запросов (см. шаг 9).

Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Д. Спецификация сетевого адреса.

- В выпадающем списке **Шифрование** выберите режим шифрования трафика для каналов связи между Прокси-сервером и заданным Сервером Dr.Web.

- В выпадающем списке **Сжатие** выберите режим сжатия трафика для каналов связи между Прокси-сервером и заданным Сервером Dr.Web. В выпадающем списке **Уровень сжатия** выберите уровень сжатия (от 1 до 9).

В таблице вы можете задать настройки ограничения передаваемого трафика аналогично настройкам Сервера, приведенным в разделах Обновления и Установки.

5. На вкладке **Кеш** задайте следующие параметры кеширования Прокси-сервера:

Установите флаг **Включить кеширование**, чтобы кешировать данные, передаваемые Прокси-сервером, и задайте следующие параметры:

- В поле **Период удаления ревизий (мин.)** задайте периодичность удаления старых ревизий из кеша в случае, если их количество превысило максимально допустимое количество сохраняемых ревизий. Значение задается в минутах. По умолчанию — 60 минут.
  - В поле **Количество сохраняемых ревизий** задайте максимальное количество ревизий каждого продукта, которые останутся в кеше после очистки. По умолчанию хранятся 3 последние ревизии, более старые ревизии удаляются.
- В поле **Период выгрузки неиспользуемых файлов (мин.)** задайте временной интервал в минутах между выгрузками неиспользуемых файлов из оперативной памяти. По умолчанию — 10 минут.
- В выпадающем списке **Режим проверки целостности** выберите режим проверки целостности данных, хранящихся в кеше:
  - **на старте** — при запуске Прокси-сервера (может занять продолжительное время).
  - **при бездействии** — во время простоя Прокси-сервера.
- Установите флаг **Использовать упреждающее кеширование**, чтобы загружать новые ревизии выбранных продуктов на Прокси-сервер с Сервера Dr.Web согласно расписанию ниже. В течение этого периода ревизии загружаются на Прокси-сервер сразу при получении их Сервером Dr.Web с ВСО. Если флаг снят, загрузка новых ревизий на Прокси-сервер осуществляется только при запросе Агентом этих ревизии с Сервера.
  - В списке ниже установите флаги для тех продуктов, для которых будет выполняться синхронизация.
  - В разделе **Расписание синхронизации репозиториев** задайте расписание, согласно которому будет осуществляться загрузка обновлений для выбранных продуктов.
    Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков путем перетаскивания мышью.
    Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей: передача данных разрешена без ограничений трафика или передача данных полностью запрещена.

6. На вкладке **События** задайте следующие параметры передачи событий:

- Установите флаг **Кешировать события**, чтобы кешировать события, полученные от Агентов. При этом события будут отправляться на Сервер каждые 15 минут в течение периода, разрешенного для отправки событий в расписании ниже. Если кеширование отключено, события будут отправляться на Сервер сразу после их получения Прокси-сервером.
- В разделе **Расписание передачи событий** задайте расписание, согласно которому будет осуществляться передача событий, полученных от Агентов.
  Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков путем перетаскивания мышью.
  Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей: передача событий разрешена без ограничений трафика или передача событий полностью запрещена.

7. На вкладке **Дамп** задайте следующие параметры:
   - Установите флаг **Создавать дампы памяти**, чтобы создавать дампы памяти в случаях возникновения критических ошибок в работе Прокси-сервера.
   - В поле **Максимальное количество дампов** задайте максимальное количество дампом памяти. При достижении заданного количества, самые старые дампы будут удаляться при создании новых. Настройка дампов памяти доступна только для ОС Windows.
8. На вкладке **DNS** настраиваются параметры обращения к DNS-серверу. Настройки аналогичны настройкам DNS для Сервера Dr.Web.
9. На вкладке **Обнаружение** настраиваются параметры хранения ответов на широковещательные запросы при поиске Серверов Dr.Web для перенаправления клиентов (см. шаг 4c).
   - **Для положительных ответов, с** — срок хранения (в секундах) списка Серверов, ответивших на широковещательный запрос при поиске Серверов Dr.Web. По истечении заданного срока запрос отправляется повторно.
   - **Для отрицательных ответов, с** — срок хранения (в секундах) информации об отсутствии Серверов Dr.Web, ответивших на широковещательный запрос. По истечении заданного срока запрос отправляется повторно.
10. На вкладке **Обновления** настраиваются параметры автоматического обновления ПО Прокси-сервера с Сервера Dr.Web:
    - Установите флаг **Включить автоматическое обновление**, чтобы автоматически загружать с Сервера Dr.Web и устанавливать новые ревизии Прокси-сервера. Расписание обновления зависит от настроек упреждающего кеширования Прокси-сервера (см. шаг 5):
      a) Если Прокси-сервер не включен в список для упреждающего кеширования (в том числе, если кеширование не используется), то обновления Прокси-сервера будут скачиваться и устанавливаться согласно расписанию автоматического обновления.
      b) Если Прокси-сервер входит в список для упреждающего кеширования, обновления Прокси-сервера будут скачиваться согласно расписанию

упреждающего кеширования. При получении новой ревизии Прокси-сервера, обновление на эту ревизию произойдет согласно расписанию автоматического обновления.

- В разделе **Расписание обновлений** задайте расписание, согласно которому будет осуществляться автоматическое обновление.
  Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков путем перетаскивания мышью.
  Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей: передача обновлений разрешена без ограничений трафика или передача обновлений полностью запрещена.

11.После завершения редактирования нажмите **Сохранить**.

11.2. 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 11-2. 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

Предметный указатель

Я