Dr.WEB

Enterprise Security Suite

Руководство по установке

Dr.Web Enterprise Security Suite
Версия 13.0
Руководство по установке
12.01.2022

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**

   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**

   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**

   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 ее 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*.

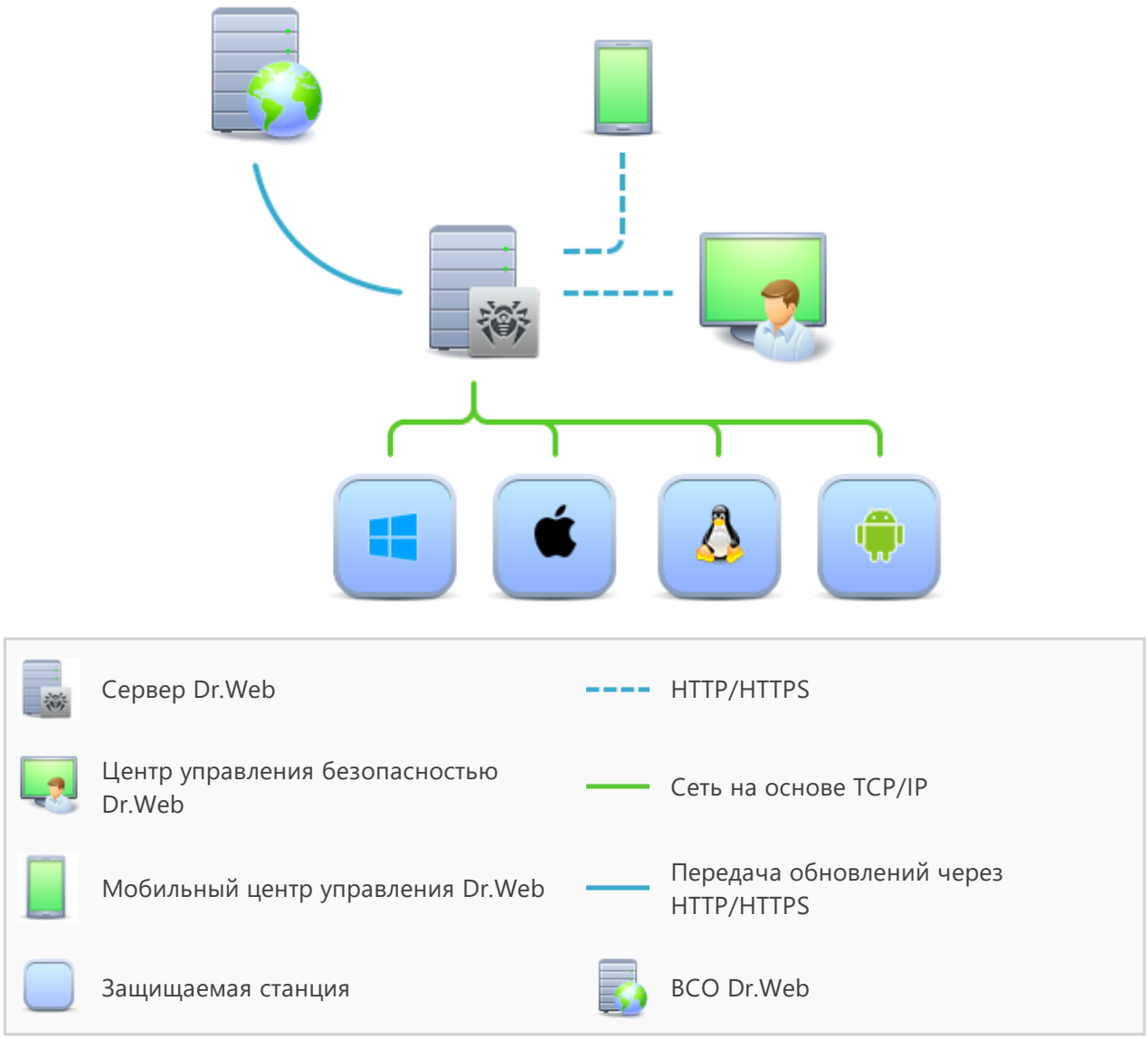

Рисунок 1-1. Логическая структура антивирусной сети

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 можно установить (и впоследствии управлять им) как через ЛВС, так и через интернет.

Сервер централизованной защиты

Сервер централизованной защиты (далее Сервер Dr.Web) 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.

Кроссплатформенность серверного программного обеспечения позволяет использовать в качестве Сервера централизованной защиты 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 централизованной защиты 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 централизованной защиты, обслуживающих защищаемые станции антивирусной сети.

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

Сервер централизованной защиты 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 централизованной защиты и предоставляет веб-интерфейс для удаленного управления Сервером централизованной защиты 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 централизованной защиты. Возможно использование Центра управления под управлением практически любой операционной системы, с полнофункциональным использованием в 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 с предварительным обзором сети для поиска компьютеров; создание дистрибутивов с уникальными идентификаторами и параметрами подключения к Серверу централизованной защиты для упрощения процесса установки Антивируса администратором или возможности установки Антивируса пользователями на станциях самостоятельно (подробную информацию см. в разделе Установка Агента Dr.Web).
- Упрощенное управление рабочими станциями антивирусной сети за счет использования механизма групп.
- 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.

- 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.
- 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.
- Гибкая система администрирования Сервера централизованной защиты 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.
- Управление лицензированием антивирусной защиты рабочих станций с разветвленной системой назначения лицензий для станций, групп станций, а также передачи лицензий между несколькими Серверами централизованной защиты при многосерверной конфигурации антивирусной сети.
- Обширный набор настроек для задания конфигурации Сервера централизованной защиты и отдельных его компонентов, в том числе: задание расписания для обслуживания; 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.

Подробная информация по использованию описанного функционала приведена в **Руководстве администратора**.

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

Мобильный центр управления централизованной защитой

В качестве отдельного компонента для мобильных устройств под управлением iOS и Android предоставляется Мобильный центр управления (*Dr.Web Mobile Control Center*). Основные требования к устройствам для работы с данным приложением приведены в п. Системные требования.

Мобильный центр управления соединяется с Сервером централизованной защиты по зашифрованному протоколу и при работе использует учетные данные администратора антивирусной сети. Мобильный центр управления поддерживает базовый набор функций Центра управления:

1. 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.
2. 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.
3. Управление станциями и группами:
   - просмотр настроек;
   - просмотр и управление составом компонентов антивирусного пакета;
   - удаление станций и групп;
   - отправка сообщений произвольного содержания на станции;
   - перезагрузка станций под управлением ОС Windows;
   - добавление станций и групп в список избранного для быстрого доступа.
4. 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 потери уведомлений в результате автоматического удаления.
5. Управление новыми станциями, ожидающими подключения к Серверу Dr.Web:
   - подтверждение доступа;
   - отклонение станций.
6. Управление станциями, на которых обновление антивирусного ПО завершилось с ошибками:
   - отображение сбойных станций;
   - обновление компонентов на сбойных станциях.
7. Управление репозиторием Сервера Dr.Web:
   - просмотр состояния продуктов в репозитории;
   - запуск обновления репозитория из Всемирной системы обновлений Dr.Web.
8. Поиск станций и групп в антивирусной сети по имени, адресу или ID.

Скачать Dr.Web Mobile Control Center вы можете из Центра управления или напрямую в магазинах приложений 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.

Кроссплатформенность 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. Поддерживается антивирусная защита почтовой системы Microsoft Outlook.

Управляющий модуль регулярно обновляет антивирусные компоненты и вирусные базы, скачивая их с Сервера централизованной защиты, а также отправляет на Сервер централизованной защиты 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 ограничение 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 Dr.Web 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 Dr.Web и соединение между Сервером Dr.Web 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 Dr.Web, 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 Dr.Web.

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 Dr.Web, не подключенном к интернету.

Сканирующий сервер Dr.Web

Сканирующий сервер Dr.Web поставляется в виде отдельного компонента. Он предназначен для работы в виртуальных окружениях. Сканирующий сервер устанавливается на отдельной виртуальной машине и обслуживает запросы на антивирусное сканирование, поступающие от других виртуальных машин.

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 Dr.Web и Прокси-сервера • исходящие для Агента	Для связи антивирусных компонентов с Сервером Dr.Web 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 Dr.Web • входящие для Агента	Для удаленной установки Агента Dr.Web.
	UDP	входящие, исходящие	
9080	HTTP	• входящие для Сервера Dr.Web • 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 Dr.Web.
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.
Оперативная память	• Минимальные требования: 1 ГБ. • Рекомендуемые требования: от 2 ГБ.
Место на жестком диске	• Не менее 50 ГБ для ПО Сервера Dr.Web 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.

Компонент	Требования
	• Вне зависимости от места установки Сервера Dr.Web, 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 Dr.Web необходимо наличие не менее 4,3 ГБ для запуска инсталлятора и распаковки временных файлов; ▫ для работы Сервера Dr.Web 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. • Linux, при наличии библиотеки `glibc` 2.13 или более поздней версии. • FreeBSD 11.3 или более поздней версии. Полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А).
Поддержка виртуальных и облачных сред	Поддерживается функционирование на операционных системах, соответствующих вышеперечисленным требованиям, в виртуальных и облачных средах, в том числе: • VMware; • Hyper-V; • Xen; • KVM.
Прочее	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, соответствующем 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.

Компонент	Требование
Оперативная память	Не менее 1 ГБ.
Место на жестком диске	Не менее 1 ГБ.
Операционная система	• Windows. • Linux, при наличии библиотеки `glibc` 2.13 или более поздней версии. • FreeBSD 11.3 или более поздней версии. Полный список поддерживаемых ОС совпадает со списком для Сервера Dr.Web и приведен в документе **Приложения**, в Приложении А).

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 Dr.Web на компьютер, в названии которого присутствует символ "_" (подчеркивание), работа с Сервером Dr.Web 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 1280×1024 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 4.1–11.0	–

NAP Validator

Для сервера:

- ОС Windows Server 2008.

Для агентов:

- ОС Windows XP SP3, ОС Windows Vista с SP2, ОС Windows Server 2008 с SP2.

Системные требования для NAP Validator совпадают с требованиями для Агента Dr.Web. Требования могут различаться в зависимости от операционной системы, на которую устанавливается антивирусное решение (полный список поддерживаемых ОС см. в документе **Приложения**, в Приложении А. Полный список поддерживаемых версий ОС):

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.
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 **Агента Dr.Web для Windows** необходимо наличие Windows Internet Explorer 6.0 или более поздней версии. 2. Для подключаемого модуля Dr.Web для Microsoft 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.

Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой Агента Dr.Web на Windows Vista, Windows 7, Windows Server 2008 или Windows Server 2008 R2 убедитесь, что в операционной системе поддерживается алгоритм шифрования SHA-256. Для этого установите все рекомендуемые обновления из Центра обновления Windows. Подробную информацию о необходимых пакетах обновлений вы можете найти на официальном сайте компании «Доктор Веб».

- 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 2 ГБ свободного дискового пространства на томе, на котором размещаются каталоги устанавливаемого продукта.

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

Поддерживается функционирование Агента Dr.Web на операционных системах, соответствующих 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).

Сканирующий сервер Dr.Web

Компонент	Требование
Гипервизор	VMware, Hyper-V, Xen, KVM
Операционная система	Linux, FreeBSD. Список поддерживаемых операционных систем аналогичен списку для антивирусного пакета для ОС UNIX.
Процессор	Процессоры с архитектурой и системой команд • Intel/AMD: 32-бит (IA-32, x86) и 64-бит (x86_64, x64, AMD64).

Компонент	Требование
Оперативная память (RAM)	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более).
Место на жестком диске	Не менее 1 ГБ свободного дискового пространства.
Сетевые подключения	Наличие сетевых подключений: • Подключение к Интернету для обновления вирусных баз и баз встроенных фильтров. • Подключение для обслуживания запросов от виртуальных агентов.

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-13.00.0-<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-13.00.0-<сборка>-esuite-server-<версия_ОС>.exe`

     Дистрибутив Сервера Dr.Web.
   - `drweb-13.00.0-<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 антивирусный пакет 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:

- Продукты для установки на защищаемые станции под ОС UNIX (включая серверы ЛВС), Android, macOS;
- Сканирующий сервер Dr.Web;
- Dr.Web для IBM Lotus Domino;
- Dr.Web для Microsoft Exchange Server;
- Прокси-сервер Dr.Web;
- Полный инсталлятор Агента 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.

Подробная информация о работе с репозиторием Сервера Dr.Web 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.

Подробная информация о принципах и особенностях лицензирования Dr.Web Enterprise Security Suite приведена в **Руководстве администратора**, в подразделах Главы 3. Лицензирование.

Использование лицензионных ключевых файлов в процессе установки программы описывается в п. Установка Сервера Dr.Web.

Использование лицензионных ключевых файлов для уже развернутой антивирусной сети описывается в **Руководстве администратора**, п. Менеджер лицензий.

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 **Руководстве администратора**, 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 Dr.Web.

   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.

   Подробное описание порядка управления административными группами и правами доступа приведено в **Руководстве администратора**, в Главе 6: Администраторы антивирусной сети

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

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

Агенты Dr.Web для станций под ОС Android, ОС Linux, macOS также могут быть установлены из пакетов для автономных продуктов и в дальнейшем подключены к централизованному Серверу Dr.Web. Описание настроек Агентов приведено в соответствующих **Руководствах пользователя**.

3. Установите основной дистрибутив Сервера Dr.Web на выбранный компьютер или компьютеры. Описание установки приведено в п. Установка Сервера Dr.Web.

   Вместе с Сервером Dr.Web устанавливается Центр управления безопасностью Dr.Web.

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

4. При необходимости установите и настройте Прокси-сервер. Описание приведено в п. Установка Прокси-сервера.

5. Если антивирусная сеть состоит из виртуальных машин, рекомендуется использовать Сканирующий сервер. Описание процедур установки и настройки приведено в п. Установка Сканирующего сервера Dr.Web.

6. Для настройки Сервера Dr.Web и антивирусного ПО на станциях необходимо подключиться к Серверу Dr.Web при помощи Центра управления безопасностью Dr.Web.

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

Центр управления доступен по адресу:

`http://`*<Адрес_Сервера_Dr.Web>*`:9080`

или

`https://`*<Адрес_Сервера_Dr.Web>*`:9081`

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

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 Dr.Web.
  - для ОС семейства UNIX — пароль, который был автоматически создан в процессе установки Сервера Dr.Web (см. также п. Установка Сервера Dr.Web для ОС семейства UNIX).

При успешном подключении к Серверу Dr.Web откроется главное окно Центра управления (подробное описание см. в **Руководстве администратора**, в п. Центр управления безопасностью Dr.Web).

Если вы установили Сканирующий сервер, то укажите его адрес в настройках станций (подробное описание см. в **Руководстве администратора,** п. Подключение станций к Сканирующему серверу).

7. Произведите начальную настройку Сервера Dr.Web (подробное описание настроек приведено в **Руководстве администратора**, в Главе 9: Настройка Сервера Dr.Web):
   a. В разделе Менеджер лицензий добавьте один или несколько лицензионных ключей и распространите их на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера Dr.Web не был задан лицензионный ключ.
   b. В разделе Общая конфигурация репозитория задайте, какие компоненты антивирусной сети будут обновляться с ВСО Dr.Web. Если антивирусная сеть будет включать защищаемые станции под ОС Android, ОС Linux, macOS, необходимо загрузить **Корпоративные продукты Dr.Web**.

      В разделе Состояние репозитория произведите обновление продуктов в репозитории Сервера Dr.Web. Обновление может занять продолжительное время. Дождитесь окончания процесса обновления перед тем как продолжить дальнейшую настройку.

При установке Сервера Dr.Web версии 13 обновления продуктов репозитория **Базы 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. Подробнее см. **Руководство администратора**, п. Детальная конфигурация репозитория.

Если ваш Сервер Dr.Web не подключен к интернету, и обновления загружаются вручную с другого Сервера Dr.Web или через Загрузчик репозитория, то перед тем как устанавливать или обновлять продукты, для которых в настройках репозитория включена опция **Обновлять только по требованию**, необходимо предварительно загрузить эти продукты в репозиторий вручную.

   c. На странице **Администрирование** → **Сервер Dr.Web** приведена информация о версии Сервера Dr.Web. При наличии новой версии, обновите Сервер Dr.Web как описано в **Руководстве администратора**, п. Обновление Сервера Dr.Web и восстановление из резервной копии.
   d. При необходимости настройте Сетевые соединения для изменения сетевых настроек по умолчанию, используемых для взаимодействия всех компонентов антивирусной сети.
   e. При необходимости настройте список администраторов Сервера Dr.Web. Также доступна внешняя аутентификация администраторов. Подробнее см. в **Руководстве администратора**, в Главе 6: Администраторы антивирусной сети.
   f. Перед началом эксплуатации антивирусного ПО рекомендуется изменить настройку каталога резервного копирования критичных данных Сервера Dr.Web (см. **Руководство администратора**, п. Настройка расписания Сервера Dr.Web). Данный каталог

желательно разместить на другом локальном диске, чтобы уменьшить вероятность одновременной потери файлов ПО Сервера Dr.Web и резервной копии.

8. Задайте настройки и конфигурацию антивирусного ПО для рабочих станций (подробное описание настройки групп и станций приведено в **Руководстве администратора**, в Главе 7 и Главе 8):
   a. При необходимости создайте пользовательские группы станций.
   b. Задайте настройки группы **Everyone** и созданных пользовательских групп. В частности настройте раздел устанавливаемых компонентов.
9. Установите ПО Агента Dr.Web на рабочие станции.

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

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

   

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

10. Сразу после установки на компьютеры Агенты автоматически устанавливают соединение с Сервером Dr.Web. Авторизация антивирусных станций на Сервере Dr.Web происходит в

соответствии с выбранной вами политикой (см. **Руководство администратора**, п. Политика подключения станций):

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

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

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

> Для завершения установки компонентов рабочей станции потребуется перезагрузка компьютера.

12. Настройка станций и антивирусного ПО возможна также после установки (подробное описание приведено в **Руководстве администратора**, в Главе 8).

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 Dr.Web:

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 Dr.Web.

   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 Dr.Web.

3. Через протокол SRV.

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

При конфигурации антивирусной сети Dr.Web Enterprise Security Suite на использование прямых соединений Служба обнаружения Сервера Dr.Web 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 Dr.Web инсталлятор автоматически добавляет порты и интерфейсы Сервера Dr.Web 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 Dr.Web 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 Dr.Web **Администрирование** → **Конфигурация Сервера Dr.Web** → вкладка **Сеть** → вкладка **Транспорт** → поле **Адрес**.

По умолчанию для "прослушивания" Сервером Dr.Web устанавливаются:

- **Адрес**: пустое значение — использовать *все сетевые интерфейсы* для данной машины, на которой установлен Сервер Dr.Web.
- **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 Dr.Web "слушал" хотя бы один TCP-порт, который должен быть известен всем клиентам.

Настройка Агента Dr.Web

При установке Агента адрес Сервера Dr.Web (IP-адрес или DNS-имя компьютера, на котором запущен Сервер Dr.Web) может быть явно указан в параметрах установки:

`drwinst /server` <*Адрес_Сервера_Dr.Web*>

При установке Агента рекомендуется использовать имя Сервера Dr.Web, 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 Dr.Web в сети (режим *Multicasting* с использованием Службы обнаружения Сервера Dr.Web).

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

В дальнейшем адрес Сервера Dr.Web 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 Dr.Web. Перед каждым установлением соединения осуществляется поиск Сервера Dr.Web в сети. Для этого клиент посылает в сеть широковещательный запрос и ожидает ответ от Сервера Dr.Web с указанием его адреса. После получения отзыва клиент устанавливает соединение с Сервером Dr.Web.

Для этого Сервер Dr.Web должен *прослушивать* сеть на подобные запросы.

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

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

1. Сервер Dr.Web регистрируется в мультикаст-группе с адресом, заданным в настройках Сервера Dr.Web.
2. Агенты, при поиске Сервера Dr.Web, посылают в сеть мультикаст-запросы на групповой адрес, заданный в п. 1.

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

Данный параметр задается в настройках Центра управления: **Администрирование** → **Конфигурация Сервера Dr.Web** → **Сеть** → **Транспорт** → **TCP/IP**. Пустое значение предписывает использовать адрес по умолчанию, указанный выше.

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 Dr.Web через SRV-записи реализуется следующим образом:

1. При установке Сервера Dr.Web 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 Dr.Web 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 Dr.Web.

   Если при обращении Сервер Dr.Web 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 Dr.Web 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 Dr.Web, 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 Dr.Web.

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

В таблице 4-1 приведены сведения о том, при каких настройках соединение между Сервером Dr.Web 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 Dr.Web		
	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 Dr.Web 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 Dr.Web через Прокси-сервер Dr.Web необходимо учитывать настройки шифрования и сжатия на всех трех компонентах. При этом:

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

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

- Если Сервер Dr.Web и клиент поддерживают TLS-шифрование, используемое в версии 13.0, то достаточно выполнения вышеописанных условий для установления работающего соединения.
- Если один из компонентов не поддерживает TLS-шифрование: на Сервере Dr.Web 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 Dr.Web			
	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 Dr.Web 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 Dr.Web или Агент) версии 13, а другой версии 10, то устанавливается шифрование, используемое в версии 10.
Ошибка	Соединение Прокси-сервера с Сервером Dr.Web и с клиентом будет разорвано.

Таким образом, если Сервер Dr.Web и Агент разных версий: один версии 13, 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 Dr.Web и с клиентом установлены без использования шифрования.
- Шифрование будет использоваться, только если оба соединения — и с Сервером Dr.Web, 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 Сервере Dr.Web

Чтобы задать настройки сжатия и шифрования Сервера Dr.Web

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 Dr.Web 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 Dr.Web не было задано другое).

При настройке шифрования и сжатия на стороне Сервера Dr.Web обратите внимание на особенности клиентов, которые планируется подключать к данному Серверу Dr.Web. Не все клиенты поддерживают шифрование и сжатия трафика.

Настройки шифрования и сжатия на Прокси-сервере Dr.Web

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 п. Подключение Прокси-сервера к Серверу Dr.Web.

1. Откройте Центр управления для Сервера Dr.Web, 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 Dr.Web, на которые будет перенаправляться трафик. Выберите в списке нужный Сервер Dr.Web 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 Dr.Web.
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 Dr.Web. В таком случае необходимо задавать настройки удаленно с Сервера Dr.Web или отключить настройку, разрешающую принимать конфигурацию с этого Сервера Dr.Web.

Описание конфигурационного файла `drwcsd-proxy.conf` приведено в документе **Приложения**, в разделе Приложении G4.

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 Dr.Web.
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 Dr.Web обязательно.
- **Возможно** — шифрование (или сжатие) будет выполняться для трафика с Сервером Dr.Web, если настройки Сервера Dr.Web 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 Dr.Web.

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. H1. 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 Dr.Web. 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 Dr.Web 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 Dr.Web.

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 Dr.Web** `drwcsd.pri`**.**

   Хранится на Сервере Dr.Web 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 Dr.Web. Закрытый ключ при этом может быть как создан новый, так и использован существующий (например, от предыдущей установки Сервера Dr.Web). Также ключи шифрования и сертификаты могут быть созданы в любое время при помощи серверной утилиты `drwsign` (см. документ **Приложения**, п. H7.1. Утилита генерации цифровых ключей и сертификатов).

   Информация об открытых ключах и сертификатах приведена далее.

   b) Аутентификация Сервера Dr.Web.

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

   Сервер Dr.Web 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 Dr.Web и клиентами расшифровка данных, отправленных клиентом, осуществляется на Сервере Dr.Web при помощи закрытого ключа.

2. **Открытый ключ шифрования Сервера Dr.Web** `*.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 Dr.Web 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 Dr.Web** `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 Dr.Web, 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 Dr.Web или другого клиента.

   Сертификат используется в следующих случаях:

   a) *Аутентификация Сервера Dr.Web.*

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

      Сервер Dr.Web 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 Dr.Web для этого использовался открытый ключ непосредственно.

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

   b) *Зашифровка данных.*

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

   c) *Реализация TLS-сессии между Сервером Dr.Web 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 Dr.Web 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 Dr.Web 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 Dr.Web вне зависимости от того, будет ли трафик между Сервером Dr.Web 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 Dr.Web, к которым может подключаться Агент.

  Сертификат, использованный при установке, а также сертификаты, полученные через централизованные настройки с Сервера Dr.Web, 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 Dr.Web на случай ошибки в централизованных настройках.

  При отсутствии сертификата или недействительном сертификате Агент не сможет подключиться к Серверу Dr.Web, 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 Dr.Web.

  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 Dr.Web указать сертификат Сервера Dr.Web, с которым устанавливается связь (см. **Руководство администратора**, 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 Dr.Web 11 версии, с подключением к Серверу Dr.Web 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 Dr.Web по протоколу SRV**

   При установке Сервера Dr.Web предоставляется возможность зарегистрировать Сервер Dr.Web 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 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 Dr.Web. Данное задание администратор должен создать самостоятельно при помощи Планировщика заданий Сервера Dr.Web.

   Подробнее см. раздел **Руководства администратора** 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 Dr.Web на всех поддерживаемых ОС. Настройка доступа к Серверу Dr.Web 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 Dr.Web на ОС Windows, входящих в целевой домен. Настройка пользователей и групп пользователей, имеющих доступ к Серверу Dr.Web, осуществляется в оснастке Active Directory непосредственно. Требуется первичная настройка с помощью дополнительных утилит. Пакеты `drweb-13.00.0-<сборка>-esuite-modify-ad-schema-<версия_ОС>.exe` и `drweb-`

`13.00.0-<сборка>-esuite-aduac-<версия_ОС>.msi` доступны в репозитории Сервера Dr.Web в **Корпоративных продуктах Dr.Web**.

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

Подробнее см. раздел **Руководства администратора** 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-13.00.0-<сборка>-esuite-agent-activedirectory.msi` доступен в репозитории Сервера Dr.Web в **Корпоративных продуктах Dr.Web**.

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

   Подробнее см. раздел 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 **Руководства администратора** 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: Установка компонентов Dr.Web Enterprise Security Suite

Перед началом установки компонентов Dr.Web Enterprise Security Suite ознакомьтесь с разделом Создание антивирусной сети.

5.1. Установка Сервера Dr.Web

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

Ход процесса установки Сервера Dr.Web зависит от того, какая версия (для ОС Windows или для ОС семейства UNIX) устанавливается.

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

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

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

Название каталога, в который ставится Сервер Dr.Web, должно быть задано на том же языке, который указан в языковых настройках ОС Windows для программ, не использующих Unicode. В противном случае установка Сервера Dr.Web не будет завершена.

Исключение — английский язык в названии каталога установки.

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

По умолчанию Сервер Dr.Web после установки запускается автоматически для версии под ОС Windows и требует запуска вручную для ОС семейства UNIX.

5.1.1. Установка Сервера Dr.Web для ОС Windows

Ниже описывается установка Сервера Dr.Web для ОС Windows.

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

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

Установка Сервера Dr.Web должна выполняться пользователем с правами администратора данного компьютера.

После установки Сервера Dr.Web необходимо произвести обновление всех компонентов Dr.Web Enterprise Security Suite (см. **Руководство администратора**, п. Ручное обновление репозитория Сервера Dr.Web).

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

На Рис. 5-1 приведена блок-схема процесса установки Сервера Dr.Web при помощи инсталлятора. Разделение установки по шагам соответствует подробному текстовому описанию процедуры, приведенному ниже.

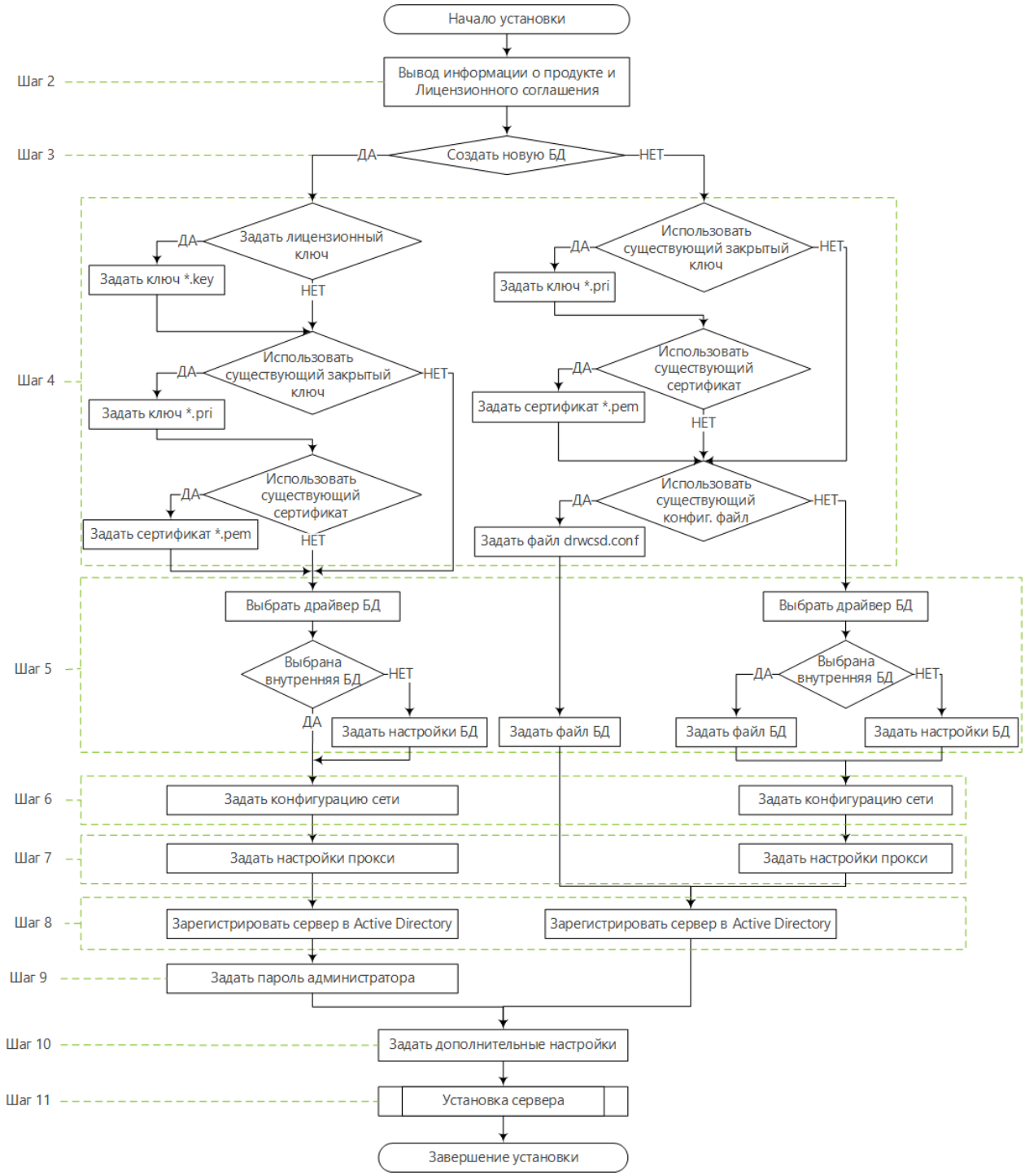

Рисунок 5-1. Схема процесса установки Сервера Dr.Web (Нажмите на блок схемы для перехода к описанию)

Чтобы установить Сервер Dr.Web на компьютер с ОС Windows

1. Запустите файл дистрибутива.

По умолчанию в качестве языка инсталлятора выбирается язык операционной системы. При необходимости вы можете изменить язык установки на любом шаге, выбрав соответствующий пункт в правом верхнем углу окна инсталлятора.

2. Откроется окно с информацией об устанавливаемом продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения установки установите флаг **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.
3. В следующем окне выберите, какую базу данных необходимо использовать для антивирусной сети:
   - **Создать новую базу данных** — для создания новой антивирусной сети.
   - **Использовать существующую базу данных** — чтобы сохранить базу данных Сервера Dr.Web от предыдущей установки. Файл базы данных вы сможете указать позднее (см. шаг **5**).
4. В следующем окне задайте настройки базы данных.

   а) Если на шаге **3** вы выбрали вариант **Создать новую базу данных**, в окне **Параметры новой баз данных** задайте следующие настройки:

   - Флаг **Задать лицензионный ключ** позволяет задать лицензионный ключевой файл Агента Dr.Web в процессе установки Сервера Dr.Web.
     - Если флаг снят, установка Сервера Dr.Web будет осуществляться без лицензионного ключа Агента. В этом случае лицензионные ключи должны быть добавлены после установки Сервера Dr.Web, через Менеджер лицензий.
     - Если флаг установлен, необходимо задать в соответствующем поле путь до файла лицензионного ключа Агента.
   - Флаг **Использовать существующий закрытый ключ шифрования** позволяет использовать существующие ключи шифрования, например, от предыдущей установки Сервера Dr.Web.
     - При первой установке Сервера Dr.Web снимите флаг **Использовать существующий закрытый ключ шифрования**. Новые ключи шифрования и сертификат будут автоматически сгенерированы в процессе установки.
     - Если вы устанавливаете Сервер Dr.Web для имеющейся антивирусной сети, установите флаг **Использовать существующий закрытый ключ шифрования** и задайте в соответствующем поле путь до файла с закрытым ключом. При этом автоматически будет создан файл с открытым ключом (содержание открытого ключа будет совпадать с содержанием предыдущего открытого ключа) и сертификат (при каждой генерации из одного и того же закрытого ключа получается новый сертификат).
     - Если вы устанавливаете Сервер Dr.Web для имеющейся антивирусной сети и используете существующий закрытый ключ шифрования, то установите флаг **Использовать существующий сертификат**, чтобы задать файл сертификата, который использовался ранее. Это позволит уже установленным Агентам подключиться к новому Серверу Dr.Web, поскольку клиенты, подключенные к Серверу Dr.Web, привязаны к конкретному сертификату (при каждой генерации из одного и того же

закрытого ключа получается новый сертификат). В противном случае после установки потребуется скопировать новый сертификат на все рабочие станции, на которых ранее были установлены Агенты Dr.Web.

- Если при извлечении открытого ключа произойдет ошибка, задайте путь до файла с соответствующим открытым ключом вручную в открывшемся поле **Открытый ключ шифрования**.

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

b) Если на шаге **3** вы выбрали вариант **Использовать существующую базу данных**, в окне **Параметры существующей баз данных** задайте следующие настройки:

- Флаг **Использовать существующий конфигурационный файл** позволяет задать настройки Сервера Dr.Web.
  - Если флаг снят, будет создан конфигурационный файл Сервера Dr.Web с настройками по умолчанию.
  - Если флаг установлен, необходимо задать в соответствующем поле путь к конфигурационному файлу с настройками Сервера Dr.Web.
- Флаг **Использовать существующий закрытый ключ шифрования** позволяет использовать существующие ключи шифрования, например, от предыдущей установки Сервера Dr.Web.
  - При первой установке Сервера Dr.Web снимите флаг **Использовать существующий закрытый ключ шифрования**. Новые ключи шифрования и сертификат будут автоматически сгенерированы в процессе установки.
  - Если вы устанавливаете Сервер Dr.Web для имеющейся антивирусной сети, установите флаг **Использовать существующий закрытый ключ шифрования** и задайте в соответствующем поле путь до файла с закрытым ключом. При этом автоматически будет создан файл с открытым ключом (содержание открытого ключа будет совпадать с содержанием предыдущего открытого ключа) и сертификат (при каждой генерации из одного и того же закрытого ключа получается новый сертификат).
  - Если вы устанавливаете Сервер Dr.Web для имеющейся антивирусной сети и используете существующий закрытый ключ шифрования, то установите флаг **Использовать существующий сертификат**, чтобы задать файл сертификата, который использовался ранее. Это позволит уже установленным Агентам подключиться к новому Серверу Dr.Web, поскольку клиенты, подключенные к Серверу Dr.Web, привязаны к конкретному сертификату (при каждой генерации из одного и того же закрытого ключа получается новый сертификат). В противном случае после установки потребуется скопировать новый сертификат на все рабочие станции, на которых ранее были установлены Агенты Dr.Web.
  - Если при извлечении открытого ключа произойдет ошибка, задайте путь до файла с соответствующим открытым ключом вручную в открывшемся поле **Открытый ключ шифрования**.

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

5. В окне **Драйвер базы данных** настраиваются параметры используемой базы данных, которые зависят от выбора типа базы данных на шаге **3** и от наличия конфигурационного файла Сервера Dr.Web, задаваемого на шаге **4**:
   - Если на шаге **3** вы выбрали вариант **Создать новую базу данных** или для варианта **Использовать существующую базу данных** на шаге **4** вы не задали путь до конфигурационного файла Сервера Dr.Web, выберите драйвер, который следует использовать. При этом:
     - Вариант **SQLite (встроенная база данных)** предписывает использовать встроенные средства Сервера Dr.Web. Задание дополнительных параметров при этом не требуется.
     - Остальные варианты подразумевают использование соответствующей внешней БД. При этом необходимо указать соответствующие параметры для настройки доступа к БД. Настройки параметров СУБД подробно описаны в приложениях (см. документ **Приложения**, п. Приложение В. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД).
   - Если на шаге **3** вы выбрали вариант **Использовать существующую базу данных** и на шаге **4** задали путь до конфигурационного файла Сервера Dr.Web, задайте путь до файла базы данных, которая будет использоваться согласно заданному конфигурационному файлу Сервера Dr.Web.
6. Если на шаге **3** вы выбрали вариант **Создать новую базу данных** или для варианта **Использовать существующую базу данных** на шаге **4** вы не задали путь до конфигурационного файла Сервера Dr.Web, откроется окно **Конфигурация сети**. В данном окне настраивается сетевой протокол для работы Сервера Dr.Web (разрешается задать только один сетевой протокол; дополнительные протоколы можно настроить в дальнейшем).

   Чтобы задать настройки сети из предустановленного набора, выберите в выпадающем списке один из следующих вариантов:
   - **Стандартная конфигурация** предписывает использование настроек по умолчанию на основе службы обнаружения Сервера Dr.Web.
   - **Ограниченная конфигурация** предписывает ограничение работы Сервера Dr.Web только внутренним сетевым интерфейсом — `127.0.0.1`. При этих настройках управление Сервером Dr.Web возможно только из Центра управления, открытого на том же компьютере, а также к Серверу Dr.Web может подключиться только Агент, запущенный на том же компьютере. В дальнейшем, после отладки настроек Сервера Dr.Web, настройки сети можно будет изменить.
   - **Пользовательская конфигурация** означает изменение следующих предустановленных настроек:

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

По умолчанию используется порт `2193`.

Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

- Установите флаг **Ограничить доступ к Серверу Dr.Web**, чтобы ограничить локальный доступ к Серверу Dr.Web. Доступ инсталляторам Агентов, Агентам и другим Серверам Dr.Web (в случае уже существующей антивирусной сети, построенной с помощью Dr.Web Enterprise Security Suite) будет запрещен. В дальнейшем эти настройки можно будет изменить через меню Центра управления **Администрирование**, пункт **Конфигурация Сервера Dr.Web**, вкладка **Модули**.
- Установите флаг **Включить службу обнаружения Сервера Dr.Web**, если хотите, чтобы Сервер Dr.Web отвечал на широковещательные и многоадресные запросы других Серверов Dr.Web по IP-адресу и имени сервиса, заданным в соответствующих полях ниже.

7. Если на шаге **3** вы выбрали вариант **Создать новую базу данных** или для варианта **Использовать существующую базу данных** на шаге **4** вы не задали путь до конфигурационного файла Сервера Dr.Web, откроется окно **Прокси-сервер** для настройки параметров использования прокси-сервера при подключении к Серверу Dr.Web:

   Чтобы подключения к Серверу Dr.Web осуществлялись через прокси-сервер, установите флаг **Использовать прокси-сервер**.

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

   Задайте следующие параметры подключения к прокси-серверу:

   - **Адрес прокси-сервера** — IP-адрес или DNS-имя прокси-сервера (обязательное поле),
   - **Имя пользователя**, **Пароль** — имя пользователя и пароль для доступа к прокси-серверу, если прокси-сервер поддерживает авторизованное подключение.
   - В выпадающем списке **Метод авторизации** выберите необходимый метод авторизации на прокси-сервере, если прокси-сервер поддерживает авторизованное подключение.

8. Если компьютер, на котором осуществляется установка Сервера Dr.Web, входит в домен Active Directory, то в следующем окне будет предложено зарегистрировать Сервер Dr.Web в домене Active Directory. В процессе регистрации в домене Active Directory на DNS-сервере создается SRV-запись, соответствующая Серверу Dr.Web. В дальнейшем возможно обращение клиентов к Серверу Dr.Web через данную SRV-запись.

   Для регистрации задайте следующие параметры:

- Установите флаг **Зарегистрировать Сервер Dr.Web в Active Directory**.
- В поле **Домен** укажите название домена Active Directory, в котором будет зарегистрирован Сервер Dr.Web. Если домен не указан, используется домен, в котором зарегистрирован компьютер, на котором осуществляется установка.
- В полях **Имя пользователя** и **Пароль** укажите учетные данные администратора домена Active Directory.

9. Если на шаге **3** вы выбрали вариант **Создать новую базу данных**, откроется окно **Пароль администратора**. Задайте пароль администратора антивирусной сети, создаваемого по умолчанию с регистрационным именем **admin** и полным набором прав для управления антивирусной сетью.
10. В следующем окне Мастер извещает о готовности к установке Сервера Dr.Web. При необходимости вы можете настроить дополнительные параметры установки. Для этого нажмите пункт **Дополнительные параметры** в нижней части окна и задайте следующие настройки:
    - На вкладке **Общее**:
        - В выпадающем списке **Язык интерфейса Центра управления безопасностью Dr.Web** выберите язык по умолчанию для интерфейса Центра управления безопасностью Dr.Web.
        - В выпадающем списке **Язык интерфейса Агента Dr.Web** выберите язык по умолчанию для интерфейса Агента Dr.Web и компонентов антивирусного пакета, устанавливаемых на станциях.
        - Установите флаг **Сделать каталог установки Агента Dr.Web общим**, чтобы изменить режим использования и наименование разделяемого ресурса для каталога установки Агента (по умолчанию задается скрытое имя разделяемого ресурса).
        - Установите флаг **Запустить Сервер Dr.Web после завершения установки**, чтобы автоматически запустить Сервер Dr.Web после установки.
        - Установите флаг **Обновить репозиторий после завершения установки**, чтобы автоматически обновить репозиторий Сервера Dr.Web сразу после завершения установки.
        - Установите флаг **Отправлять статистику в компанию «Доктор Веб»**, чтобы разрешить отправку статистики по вирусным событиям в компанию «Доктор Веб».
    - На вкладке **Путь**:
        - В поле **Каталог установки Сервера Dr.Web** задается каталог, в который осуществляется установка Сервера Dr.Web. Для изменения каталога, задаваемого по умолчанию, нажмите кнопку **Обзор** и выберите требуемый каталог.
        - В поле **Каталог для резервного копирования Сервера Dr.Web** задается каталог, в который осуществляется резервное копирование критичных данных Сервера Dr.Web согласно расписанию заданий Сервера. Для изменения каталога, задаваемого по умолчанию, нажмите кнопку **Обзор** и выберите требуемый каталог.
    - На вкладке **Журнал** вы можете задать настройки ведения журнала установки и работы Сервера Dr.Web.

После завершения настройки дополнительных компонентов нажмите кнопку **OK** для принятия внесенных изменений или кнопку **Отмена**, если не было внесено никаких изменений или для отказа от внесенных изменений.

11. Нажмите кнопку **Установить** для начала процесса установки. Дальнейшие действия программы установки не требуют вмешательства пользователя.
12. После завершения установки нажмите кнопку **Готово**.

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

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

- Каталог **Управление сервером** содержит команды запуска, перезапуска и завершения работы Сервера Dr.Web, а также команды настройки ведения журнала и другие команды Сервера Dr.Web, подробнее описанные в документе **Приложения**, п. Н3. Сервер Dr.Web.
- Пункт **Веб-интерфейс** — для открытия Центра управления и подключения к Серверу Dr.Web, установленному на данном компьютере (по адресу https://localhost:9081).
- Пункт **Документация** — для открытия документации администратора в формате HTML.

Структура каталога установки Сервера Dr.Web описана в **Руководстве администратора**, в разделе Сервер Dr.Web.

5.1.2. Установка Сервера Dr.Web для ОС семейства UNIX

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

Чтобы установить Сервер Dr.Web для ОС семейства UNIX

1. Чтобы запустить установку пакета Сервера Dr.Web, выполните следующую команду:

   `./<файл_дистрибутива>.tar.gz.run`

   

   Для запуска установочного пакета можете использовать ключи командной строки. Параметры команды запуска приведены в документе **Приложения**, п. Н6. Инсталлятор Сервера Dr.Web для ОС семейства UNIX.

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

2. Далее приводится текст лицензионного соглашения. Для продолжения установки вам необходимо принять лицензионное соглашение.
3. Чтобы использовать сохраненные в резервной копии настройки предыдущей инсталляции, укажите путь к директории, где хранится резервная копия (или нажмите клавишу ENTER,

чтобы использовать каталог по умолчанию — `/var/tmp/drwcs`). Для установки Сервера Dr.Web без использования предыдущих настроек введите 0.

4. Если в системе был обнаружен дополнительный дистрибутив (extra), будет выведена информации об удалении дополнительного дистрибутива перед началом установки пакета Сервера Dr.Web. Продолжить установку без удаления дополнительного дистрибутива невозможно.
5. Далее будет произведена установка ПО, в ходе которой инсталлятор может попросить подтверждения ваших действий от имени администратора.
6. В процессе установки генерируется случайный пароль для главного администратора. После завершения установки этот пароль выводится через консоль в результатах установки Сервера Dr.Web.

В процессе установки ПО под ОС **FreeBSD** создается rc-скрипт `/usr/local/etc/rc.d/drwcsd`.

Используйте команды:

- `/usr/local/etc/rc.d/drwcsd stop` — для ручной остановки Сервера Dr.Web;
- `/usr/local/etc/rc.d/drwcsd start` — для ручного запуска Сервера Dr.Web.

Обратите внимание, что в процессе установки Сервера Dr.Web не задается лицензионный ключ. Лицензионные ключи должны быть добавлены после установки Сервера Dr.Web, через Менеджер лицензий.

Настройка Astra Linux версии 1.6 для установки Сервера Dr.Web в режиме ЗПС

В случае установки Сервера Dr.Web в среде ОС Astra Linux версии 1.6, работающей в режиме ЗПС (замкнутая программная среда), может произойти отказ в запуске программы установки из-за отсутствия открытого ключа шифрования Сервера Dr.Web в списке доверенных ключей. В этом случае необходимо перенастроить режим ЗПС, после чего запустить программу установки повторно.

Чтобы перенастроить режим ЗПС

1. Установите пакет `astra-digsig-oldkeys` с установочного диска ОС, если он еще не установлен.
2. Поместите открытый ключ шифрования Сервера Dr.Web в каталог `/etc/digsig/keys/legacy/keys` (если каталог отсутствует, его необходимо создать).
3. Выполните следующую команду:

```
# update-initramfs -k all -u
```

4. Перезагрузите систему.

5.2. Установка Агента Dr.Web

Установка Агента Dr.Web должна выполняться пользователем с правами администратора данного компьютера.

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

Агент Dr.Web 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 осуществляется в Центре управления через ЛВС. Производится администратором антивирусной сети. При этом вмешательство пользователя не требуется.

Установка Агента Dr.Web поверх автономного антивирусного продукта Dr.Web для станций под ОС Windows

При наличии на станции под ОС Windows автономного продукта Dr.Web версии 7.x-12.x, установка Агента для Dr.Web Enterprise Security Suite версии 13.0 осуществляется по следующей схеме:

- В случае запуска инсталлятора или инсталляционного пакета Агента в GUI-режиме на станции с установленным автономным продуктом версии 7.x-12.x, будет запущен инсталлятор установленного продукта. После чего пользователю будет предложено ввести код подтверждения действий и удалить продукт. После перезагрузки ОС будет запущена GUI-версия инсталлятора, который запускался изначально для установки Агента для Dr.Web Enterprise Security Suite версии 13.0.
- В случае запуска инсталлятора Агента в фоновом режиме на станции с установленным автономным продуктом версии 7.x-12.x, это не приведет к выполнению каких-либо действий. В случае удаленной установки, инсталлятор вернет сообщение Центру управления о наличии автономных продуктов предыдущих версий. В таком случае необходимо вручную удалять автономный продукт и устанавливать Агент для Dr.Web Enterprise Security Suite версии 13.0 любым из возможных способов.
- В случае запуска инсталлятора Агента как при локальной, так и удаленной установке на станции с установленным автономным продуктом версии 13.0 произойдет переключение

установленного продукта из автономного режима в режим централизованной защиты. После подключения и авторизации на Сервере Dr.Web возможно получение обновлений, новых настроек и списка устанавливаемых компонентов, в зависимости от которых может потребоваться перезагрузка.

При установке Агентов Dr.Web на сервера ЛВС и компьютеры кластера необходимо учесть:

- В случае установки на компьютеры, выполняющие роль терминальных серверов (в ОС Windows установлены службы **Terminal Services**), для обеспечения работы Агентов в терминальных сессиях пользователей установку Агентов рекомендуется осуществлять локально с помощью мастера установки и удаления программ на **Панели управления** ОС Windows. Удаленная установка в этом случае может привести к ошибкам в работе протокола Remote Desktop.
- На серверы, выполняющие важные сетевые функции (домен-контроллеры, серверы раздачи лицензий и т. д.), не рекомендуется устанавливать компоненты SpIDer Gate, Офисный контроль, SpIDer Mail и Брандмауэр Dr.Web во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса Dr.Web.
- Установка Агента на кластер должна выполняться отдельно на каждый узел кластера.
- Принципы функционирования Агента и компонентов антивирусного пакета на узле кластера аналогичны таковым на обычном сервере ЛВС, поэтому не рекомендуется устанавливать на узлы кластера компоненты SpIDer Gate, SpIDer Mail и Dr.Web Firewall.
- Если доступ к кворум-ресурсу кластера строго ограничен, рекомендуется исключить его из проверки монитором SpIDer Guard и ограничиться регулярными проверками ресурса при помощи Сканера, запускаемого по расписанию или вручную.

5.2.1. Инсталляционные файлы

Инсталляционные пакеты

Персональный инсталляционный пакет

При создании новой учетной записи станции в Центре управления генерируется персональный инсталляционный пакет для установки Агента Dr.Web. Персональный инсталляционный пакет включает в себя инсталлятор Агента Dr.Web и набор параметров для подключения и авторизации станции на Сервере Dr.Web.

Персональные инсталляционные пакеты доступны для защищаемых станций под всеми операционными системами, поддерживаемыми Dr.Web Enterprise Security Suite. Персональные инсталляционные пакеты создаются в Центре управления на основе инсталлятора Агента. Параметры для подключения и авторизации станции на Сервере Dr.Web включены в персональный инсталляционный пакет непосредственно.

Для получения персональных инсталляционных пакетов под операционными системами, отличными от ОС Windows, необходимо загрузить в репозиторий **Корпоративные продукты Dr.Web** с серверов ВСО дополнительно после установки Сервера Dr.Web.

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

Ссылка для скачивания персонального инсталляционного пакета Агента Dr.Web для конкретной станции доступна:

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

Групповой инсталляционный пакет

Групповой инсталляционный пакет Агента генерируется в Центре управления для установки на станции определенной пользовательской группы. При этом предусматривается установка Агента на все станции под одной и той же ОС из одного и того же группового инсталляционного пакета.

Групповой инсталляционный пакет включает в себя инсталлятор Агента, параметры подключения к Серверу Dr.Web, а также идентификатор и пароль пользовательской группы, в которую будет включена станция после установки Агента. Однако параметры авторизации станции на Сервере Dr.Web и сами антивирусные компоненты не входят в состав группового инсталляционного пакета.

Ссылка для скачивания группового инсталляционного пакета доступна в разделе свойств пользовательской группы.

Инсталляторы

Инсталлятор Агента отличается от инсталляционного пакета тем, что не включает в себя параметры для подключения и авторизации станции на Сервере Dr.Web.

Предоставляются следующие инсталляторы Агента Dr.Web:

- Для станций под ОС Windows доступны два типа инсталляторов:
  - *Сетевой инсталлятор* `drwinst.exe` осуществляет установку непосредственно Агента. После подключения к Серверу Dr.Web, Агент загружает и устанавливает необходимые компоненты антивирусного пакета. Возможна как локальная, так и удаленная установка

Агента при помощи сетевого инсталлятора.
Сетевой инсталлятор Агента `drwinst.exe` располагается в каталоге `webmin/install/windows` (по умолчанию скрытый разделяемый ресурс) каталога установки Сервера Dr.Web. Сетевая доступность ресурса задается на шаге 10 при установке Сервера Dr.Web. В дальнейшем вы можете изменить данный ресурс по своему усмотрению.

- *Полный инсталлятор* `drweb-13.00.0-<сборка>-esuite-agent-full-windows.exe` осуществляет установку Агента и антивирусного пакета единовременно.

- Для станций под ОС Android, ОС Linux, macOS доступен инсталлятор для установки Агента Dr.Web, аналогичный инсталлятору автономной версии.

Инсталляторы для установки Агента Dr.Web доступны на инсталляционной странице Центра управления безопасностью Dr.Web.

Для получения инсталляторов под операционными системами, отличными от ОС Windows, а также полного дистрибутива инсталлятора под ОС Windows необходимо загрузить в репозиторий **Корпоративные продукты Dr.Web** с серверов ВСО дополнительно после установки Сервера Dr.Web.

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

Инсталляционная страница

Сразу после установки Сервера Dr.Web на инсталляционной странице Центра управления безопасностью Dr.Web вы можете скачать:

1. Инсталлятор Агента Dr.Web для Windows.
2. Сертификат Сервера Dr.Web `drwcsd-certificate.pem`.

После выполнения небольшой настройки на странице также станет доступен ряд дополнительных инсталляторов. Инсталляторы для защищаемых станций под всеми ОС, поддерживаемыми Dr.Web Enterprise Security Suite, располагаются в каталогах с названиями, соответствующими названию ОС.

Инсталляционная страница доступна на любом компьютере, имеющем сетевой доступ к Серверу Dr.Web, по адресу:

`http://`*<Адрес_Сервера_Dr.Web>*`:`*<номер_порта>*`/install/`

где в качестве *<Адрес_Сервера_Dr.Web>* 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).

Чтобы настроить состав продуктов на инсталляционной странице

1. Выберите пункт **Администрирование** главного меню, после чего в управляющем меню выберите раздел **Общая конфигурация репозитория**.
2. Перейдите на вкладку **Инсталляционные пакеты Dr.Web → Корпоративные продукты Dr.Web**.
3. Нажмите на стрелку слева от названия нужного продукта и уточните операционную систему и разрядность. После установки флагов напротив всех необходимых продуктов нажмите **Сохранить**.
4. Обновите репозиторий через раздел **Состояние репозитория** в управляющем меню.
5. После загрузки с ВСО и обновления репозитория на инсталляционной странице станут доступны инсталляторы выбранных продуктов.

5.2.2. Локальная установка Агента Dr.Web

Локальная установка Агента Dr.Web осуществляется на компьютере или мобильном устройстве пользователя непосредственно. Может производиться как администратором, так и пользователем.

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

Станции под ОС Android, ОС Linux, macOS

Для локальной установки Агента Dr.Web на станции под ОС Android, ОС Linux, macOS доступны следующие средства:

- Персональный инсталляционный пакет, созданный в Центре управления.
- Групповой инсталляционный пакет, созданный в Центре управления.
- Инсталлятор Агента Dr.Web.

При выборе типа устанавливаемого пакета обратите внимание на следующие особенности:

a) При создании персонального инсталляционного пакета для установки предоставляется инсталлятор Агента Dr.Web, а также параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web.

b) При установке через инсталлятор осуществляется установка Агента Dr.Web, но параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web не предоставляются.

Станции под ОС Windows

Для локальной установки Агента Dr.Web на станции под ОС Windows доступны следующие средства:

- Персональный инсталляционный пакет, созданный в Центре управления `drweb_ess_<ОС>_<станция>.exe`.
- Групповой инсталляционный пакет, созданный в Центре управления `drweb_ess_<ОС>_<группа>.exe`.
- Полный инсталлятор Агента Dr.Web `drweb-13.00.0-<сборка>-esuite-agent-full-windows.exe`.
- Сетевой инсталлятор Агента Dr.Web `drwinst.exe`.

При выборе типа устанавливаемого пакета обратите внимание на следующие особенности:

a) При установке из персонального инсталляционного пакета параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web включены в персональный инсталляционный пакет. Установка через персональный инсталляционный пакет осуществляется на основе сетевого инсталлятора, из которого устанавливается непосредственно Агент. После подключения к Серверу Dr.Web, Агент загружает и устанавливает компоненты антивирусного пакета.

b) При установке из группового инсталляционного пакета параметры подключения к Серверу Dr.Web, а также идентификатор и пароль пользовательской группы, в которую будет включена станция после установки Агента, включены в инсталляционный пакет. Однако параметры авторизации станции на Сервере Dr.Web и сами антивирусные компоненты не входят в состав группового инсталляционного пакета. После установки Агента осуществляется подключение Агента к Серверу Dr.Web, в процессе которого определяется наличие свободных станций в пользовательской группе, групповой инсталляционный пакет которой использовался. При наличии свободных станций, параметры авторизации станции на Сервере Dr.Web предоставляются автоматически.

c) При установке через сетевой инсталлятор осуществляется установка только Агента. После подключения к Серверу Dr.Web, Агент загружает и устанавливает соответствующие компоненты антивирусного пакета. При этом параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web не предоставляются.

d) При установке через полный дистрибутив осуществляется установка Агента и антивирусного пакета единовременно. При этом параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web не предоставляются.

Сравнительные характеристики инсталляционных файлов

Инсталляционный файл		Установка Агента	Установка антивирусного пакета	Параметры подключения к Серверу Dr.Web	Параметры авторизации на Сервере Dr.Web
Инсталляционный пакет	Персональный	+	–	+	+
	Групповой	+	–	+	–
Инсталлятор	Сетевой	+	–	–	–
	Полный	+	+	–	–

Для получения инсталляторов и инсталляционных пакетов под операционными системами, отличными от ОС Windows, а также полного дистрибутива инсталлятора под ОС Windows необходимо загрузить в репозиторий **Корпоративные продукты Dr.Web** с серверов ВСО дополнительно после установки Сервера Dr.Web.

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

Запуск всех типов инсталляционных файлов Агента также возможен из командной строки с использованием ключей, приведенных в документе **Приложения**, п. H1. Сетевой инсталлятор.

5.2.2.1. Установка Агента Dr.Web при помощи персонального инсталляционного пакета

Чтобы установить Агент Dr.Web на защищаемые станции при помощи персонального инсталляционного пакета

1. При помощи Центра управления создайте учетную запись новой станции на Сервере Dr.Web.
2. Отправьте пользователю ссылку на персональный инсталляционный пакет Агента Dr.Web для соответствующей операционной системы компьютера или мобильного устройства, если установка ПО Агента Dr.Web будет осуществляться самим пользователем.

Для удобства передачи инсталляционного и конфигурационного файлов вы можете воспользоваться функцией **Рассылка инсталляционных файлов** (подробная информация приведена в **Руководстве администратора**, п. Рассылка инсталляционных файлов) для отправки сообщения с соответствующими файлами на электронную почту.

3. Произведите установку Агента Dr.Web на рабочую станцию.

Описание локальной установки Агента Dr.Web на рабочей станции приведено в **Руководстве пользователя** для соответствующей операционной системы.

Установка Агента Dr.Web должна выполняться пользователем с правами администратора данного компьютера.

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

4. Для станций под macOS настройте параметры подключения к Серверу Dr.Web локально.

   При установке Агента Dr.Web при помощи персонального инсталляционного пакета для остальных поддерживаемых систем дополнительная настройка не требуется. Параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web включены в персональный инсталляционный пакет непосредственно. После установки Агента станция автоматически подключится к Серверу Dr.Web.

Создание новой учетной записи станции

Чтобы создать учетную запись или несколько учетных записей новых станций, воспользуйтесь Центром управления безопасностью Dr.Web.

При создании учетной записи станции обратите внимание на имя Сервера Dr.Web, заданное в следующих разделах Центра управления:

1. **Администрирование** → **Конфигурация веб-сервера** → поле **Адрес Сервера Dr.Web**. Значение данного параметра подставляется при генерации ссылки на установочный пакет Агента.

   Если значение данного параметра нигде не задано, то в качестве имени Сервера Dr.Web для формирования ссылки на скачивание инсталлятора Агента задается DNS-имя (если доступно) или IP-адрес компьютера, на котором открыт Центр управления.

2. **Администрирование** → **Конфигурация Сервера Dr.Web** → Вкладка **Сеть** → вкладка **Загрузка** → поле **Адрес Сервера Dr.Web**. Значение данного параметра

прописывается в установочные пакеты Агента и определяет, к какому Серверу Dr.Web будет подключаться Агент при установке.

Если значение данного параметра нигде не задано, то при создании установочного пакета Агента, в нем прописывается адрес Сервера Dr.Web, по которому подключен Центр управления. В этом случае подключение Центра управления к Серверу Dr.Web должно осуществляться по IP-адресу для домена, в котором создается учетная запись (адрес Сервера Dr.Web не должен быть задан как loopback — `127.0.0.1`).

Чтобы создать новую учетную запись станции при помощи Центра управления безопасностью Dr.Web

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. На панели инструментов нажмите кнопку **Добавить объект сети** → **Создать станцию**. В правой части окна Центра управления откроется панель создания учетной записи станции.
3. В поле **Количество** укажите количество учетных записей, которое вам нужно создать.
4. В поле **Идентификатор** автоматически генерируется уникальный идентификатор создаваемой станции. При необходимости вы можете его изменить.
5. В поле **Название** задайте имя станции, которое будет отображаться в иерархическом списке антивирусной сети. В дальнейшем, после соединения станции с Сервером Dr.Web, данное имя может быть автоматически заменено на название станции, заданное локально.
6. В полях **Пароль** и **Подтвердите пароль** можете задать пароль для доступа станции к Серверу Dr.Web. Если пароль не указан, он будет сгенерирован автоматически.

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

7. В поле **Описание** введите дополнительную информацию о станции. Данный параметр не обязателен.
8. В разделе **Группы** задаются группы, в которые будет входить создаваемая станция.
   - В списке **Членство** вы можете настроить список пользовательских групп, в которые будет входить станция.
     По умолчанию станция входит в группу **Everyone**. В случае наличия пользовательских групп, вы можете включить в них создаваемую станцию без ограничений на количество групп, в которые входит станция. Для этого установите флаги напротив нужных пользовательских групп в списке **Членство**.

Нельзя исключить станцию из группы **Everyone** и из первичной группы.

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

- В списке **Политики** вы можете задать политику, из которой будут браться настройки создаваемой станции.
  По умолчанию политика не назначена. Для назначения политики установите флаг напротив нужной политики. Настройки станции будут унаследованы от настроек текущей версии этой политики. Для станции может быть назначено не больше одной политики.

9. В разделе **Прокси-сервер** задаются настройки Прокси-сервера Dr.Web, связанного с этой станцией.
   Если вы хотите установить Прокси-сервер на создаваемой станции, установите флаг **Создать связанный Прокси-сервер** и задайте параметры Прокси-сервера. Параметры аналогичны параметрам при создании Прокси-сервера.

При создании учетной записи станции 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 Dr.Web только через установленный Прокси-сервер. Использование Прокси-сервера будет прозрачно для пользователя.

10. При необходимости заполните раздел **Безопасность**. Описание настроек данного раздела приведено в **Руководстве администратора** в разделе Безопасность.
11. При необходимости заполните раздел **Расположение**.
12. Нажмите кнопку **Сохранить** в правом верхнем углу. Откроется окно об удачном создании новой станции, в котором также указан идентификационный номер и приведены следующие ссылки:
    - В пункте **Инсталляционный файл** — ссылка для загрузки инсталлятора Агента.
    - В пункте **Конфигурационный файл** — ссылка для загрузки файла с настройками подключения к Серверу Dr.Web станций под управлением ОС Android, macOS и ОС Linux.

Сразу после создания новой 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.

Ссылки для скачивания инсталлятора Агента и конфигурационного файла также доступны:

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

Для получения инсталляционных пакетов под операционными системами, отличными от ОС Windows, необходимо загрузить в репозиторий **Корпоративные**

продукты Dr.Web с серверов ВСО дополнительно после установки Сервера Dr.Web.

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

- В пункте **Пароль** приведен пароль для доступа данной станции к Серверу Dr.Web. Для отображения пароля нажмите .
- В пункте **Пароль Прокси-сервера** приведен пароль для доступа Прокси-сервера к Серверу Dr.Web, если станция создавалась со связанным Прокси-сервером (см. шаг 9).
- В данном окне также доступна кнопка **Установить**, предназначенная для удаленной установки Агента Dr.Web с использованием Центра управления безопасностью Dr.Web.

13. Действия по установке Агента Dr.Web на рабочей станции приведены в **Руководстве пользователя** для соответствующей операционной системы.

Настройки подключения к Серверу Dr.Web для станции под macOS

1. В меню приложения Антивирус Dr.Web нажмите пункт **Настройки** и выберите раздел **Режим**.
2. Установите флаг **Включить режим централизованной защиты**.
3. Настройки подключения к Серверу Dr.Web, такие как IP-адрес и параметры авторизации на Сервере Dr.Web, автоматически задаются из конфигурационного файла `install.cfg`, расположенного внутри персонального инсталляционного пакета.

   Чтобы использовать файл:

   a) В Менеджере Лицензий перейдите по ссылке **Другие виды активации**.

   b) В открывшееся окно перетащите файл с настройками или щелкните по пунктирной области, чтобы открыть окно для выбора файла.

   После подключения файла поля для ввода параметров подключения к Серверу Dr.Web будут заполнены автоматически.

5.2.2.2. Установка Агента Dr.Web при помощи группового инсталляционного пакета

Чтобы установить Агент Dr.Web на защищаемые станции при помощи группового инсталляционного пакета

1. При помощи Центра управления создайте новую пользовательскую группу на Сервере Dr.Web (подробное описание процедуры создания групп приведено в **Руководстве администратора**, п. Создание и удаление групп). Вы также можете использовать уже существующую группу, созданную вами ранее.

2. При необходимости, в Менеджере лицензий назначьте для группы персональный лицензионный ключ. В противном случае группа унаследует лицензионный ключ от своей родительской группы.
3. При помощи Центра управления создайте учетные записи новых станций на Сервере Dr.Web. Включите новые учетные записи станций в пользовательскую группу из шага 1 и сделайте эту группу для них первичной. В пользовательской группе возможно создание стольких станций, сколько свободных лицензий доступно данной группе.
4. В настройках группы будет доступна ссылка на групповой инсталляционный пакет. Инсталляционные пакеты будут разделены по доступным операционным системам: по одному инсталляционному пакету для каждой операционной системы.
5. Отправьте пользователям ссылку на групповой инсталляционный пакет Агента Dr.Web для соответствующей операционной системы компьютера или мобильного устройства, если установка ПО Агента Dr.Web будет осуществляться самими пользователями. При этом всем пользователям отправляется один и тот же групповой инсталляционный пакет для соответствующей операционной системы.
6. Произведите установку Агента Dr.Web на рабочую станцию.

Описание локальной установки Агента Dr.Web на рабочей станции приведено в **Руководстве пользователя** для соответствующей операционной системы.

Установка Агента Dr.Web должна выполняться пользователем с правами администратора данного компьютера.

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

7. После установки Агента осуществляется подключение Агента к Серверу Dr.Web, указанному в групповом инсталляционном пакете. В процессе первого обращения к Серверу Dr.Web определяется наличие свободных станций в пользовательской группе, групповой инсталляционный пакет которой использовался для установки Агента. Количество свободных станций определяется по количеству учетных записей в данной группе, у которых не истек срок допуска. При каждом подключении группового инсталляционного пакета количество свободных станций пересчитывается для предоставления актуальной информации.
   a) При наличии свободных станций параметры авторизации станции для подключения к Серверу Dr.Web предоставляются автоматически. Данная процедура осуществляется прозрачно для администратора и не требует дополнительного вмешательства.
   b) При отсутствии свободных станций в данной группе установка прерывается с соответствующим сообщением пользователю.

5.2.2.3. Установка Агента Dr.Web при помощи инсталлятора

Инсталлятор Агента отличается от инсталляционного пакета тем, что не включает в себя параметры подключения к Серверу Dr.Web и параметры авторизации станции на Сервере Dr.Web.

Инсталляторы для установки Агента Dr.Web доступны на инсталляционной странице Центра управления безопасностью Dr.Web.

Для получения инсталляторов под операционными системами, отличными от ОС Windows, а также полного дистрибутива инсталлятора под ОС Windows необходимо загрузить в репозиторий **Корпоративные продукты Dr.Web** с серверов ВСО дополнительно после установки Сервера Dr.Web.

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

Локальная установка на станции под ОС Android, ОС Linux, macOS

Для станций под ОС Android, ОС Linux, macOS доступен инсталлятор для установки Агента Dr.Web, аналогичный инсталлятору автономной версии.

Описание локальной установки Агента Dr.Web на рабочей станции приведено в **Руководстве пользователя** для соответствующей операционной системы.

Если осуществляется установка через инсталлятор без конфигурационного файла, вам необходимо вручную прописать на станции адрес Сервера Dr.Web для подключения станции.

Параметры авторизации можете задать вручную или не задавать. При этом возможны следующие варианты подключения к Серверу Dr.Web:

Вариант задания	Параметры авторизации
Задается вручную	Осуществляется попытка автоматической авторизации по заданным параметрам авторизации.
Не задается	Принцип авторизации на Сервере Dr.Web зависит от настроек Сервера Dr.Web для подключения новых станций (подробнее см. в **Руководстве администратора**, п. Политика подключения станций).

Для задания параметров авторизации вручную необходимо сначала создать новую учетную запись станции в Центре управления. При этом будет доступен инсталляционный пакет, содержащий конфигурационный файл с параметрами подключения и авторизации. Рекомендуется использовать инсталляционный пакет вместо инсталлятора.

Локальная установка на станции под ОС Windows

Предоставляются следующие типы инсталляторов Агента Dr.Web:

- *сетевой инсталлятор* `drwinst.exe` осуществляет установку только Агента. После подключения к Серверу Dr.Web Агент загружает и устанавливает соответствующие компоненты антивирусного пакета.
- *полный инсталлятор* `drweb-13.00.0-<сборка>-esuite-agent-full-windows.exe` осуществляет установку Агента и антивирусного пакета единовременно.

При установке через данные инсталляторы вы можете не задавать параметры подключения к Серверу Dr.Web и авторизации или задать их вручную.

Для задания параметров авторизации вручную необходимо сначала создать новую учетную запись станции в Центре управления. При этом будет доступен инсталляционный пакет. Если нет необходимости установки через полный дистрибутив или сетевой инсталлятор, рекомендуется использовать инсталляционный пакет вместо инсталлятора.

Возможны следующие варианты подключения к Серверу Dr.Web:

Вариант задания	**Адрес Сервера Dr.Web**	**Параметры авторизации**
Задается вручную	Станция обращается напрямую к заданному Серверу Dr.Web.	Осуществляется попытка автоматической авторизации по заданным параметрам авторизации.
Не задается	Агент осуществляет поиск Сервера Dr.Web в сети на основе *Службы обнаружения Сервера Dr.Web*. Осуществляется попытка подключения к первому найденному Серверу Dr.Web.	Принцип авторизации на Сервере Dr.Web зависит от настроек Сервера Dr.Web для подключения новых станций (подробнее см. в **Руководстве администратора**, п. Политика подключения станций).

В **Руководстве пользователя** для ОС Windows описаны варианты установки Агента Dr.Web при помощи полного инсталлятора и при помощи инсталляционного

пакета.

Установку через сетевой инсталлятор рекомендуется осуществлять администратору антивирусной сети.

Локальная установка при помощи сетевого инсталлятора под ОС Windows

Сетевой инсталлятор Агента `drwinst.exe` предоставляется для установки Агента только под ОС Windows.

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

Установка при помощи сетевого инсталлятора возможна в двух режимах:

1. *Фоновый режим* — запускается, если задан ключ фонового режима.
2. *Графический режим* — режим по умолчанию. Запускается, если не задан ключ фонового режима.

При помощи сетевого инсталлятора вы также можете установить Агент Dr.Web на рабочую станцию удаленно, с использованием Центра управления (см. п. Удаленная установка Агента Dr.Web).

Чтобы установить Агент Dr.Web на рабочую станцию в фоновом режиме инсталлятора

1. С компьютера, на который будет устанавливаться антивирусное ПО, войдите в сетевой каталог установки Агента (при установке Сервера Dr.Web это подкаталог `webmin/install/windows` каталога установки Сервера Dr.Web, в дальнейшем его можно переместить) или скачайте с инсталляционной страницы Центра управления исполняемый файл инсталлятора `drwinst.exe` и сертификат `drwcsd-certificate.pem`. Запустите файл `drwinst.exe` с ключом фонового режима `/silent yes`.

   По умолчанию файл `drwinst.exe`, запущенный без параметров подключения к Серверу Dr.Web, использует режим *Multicast* для сканирования сети на наличие активных Серверов Dr.Web и осуществляет попытку установки Агента с первого найденного Сервера Dr.Web в сети.

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

Если требуется установить Агент на том же компьютере, на котором установлен Сервер Dr.Web, необходимо напрямую задавать адрес Сервера Dr.Web в параметрах запуска инсталлятора, поскольку Сервер Dr.Web может быть не обнаружен при поиске через multicast-запрос.

Также файл `drwinst.exe` можно запускать с дополнительными параметрами командной строки:

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

```
drwinst /silent yes /server <DNS_имя_Сервера_Dr.Web>
```

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

- Вы также можете использовать явное указание адреса Сервера Dr.Web, например:

```
drwinst /silent yes /server 192.168.1.3
```

- Использование ключа `/regagent yes` позволяет при установке зарегистрировать Агент в списке добавления и удаления программ.

Полный список параметров Сетевого инсталлятора приведен в документе **Приложения**, п. H1. Сетевой инсталлятор.

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

Чтобы установить Агент Dr.Web на рабочую станцию в графическом режиме инсталлятора

С компьютера, на который будет устанавливаться антивирусное ПО, войдите в сетевой каталог установки Агента (при установке Сервера Dr.Web это подкаталог `webmin/install/windows` каталога установки Сервера Dr.Web, в дальнейшем его можно переместить) или скачайте с инсталляционной страницы Центра управления исполняемый файл инсталлятора `drwinst.exe` и сертификат `drwcsd-certificate.pem`. Запустите файл `drwinst.exe`.

Откроется окно мастера установки Агента Dr.Web. Дальнейшие действия по установке Агента на станцию при помощи графического режима сетевого инсталлятора аналогичны действиям при установке при помощи инсталляционного пакета, но без настроек подключения к Серверу Dr.Web, если они не были заданы в соответствующем ключе командной строки.

Описание установки Агента на рабочие станции приведено в руководстве **Агент Dr.Web для Windows. Руководство пользователя**.

5.2.3. Дистанционная установка Агента Dr.Web

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

5.2.3.1. Дистанционная установка Агента Dr.Web для ОС Windows

Дистанционная установка возможна:

- При помощи Центра управления.
- При помощи службы Active Directory, если в защищаемой локальной сети используется данная служба.

Дистанционная установка Агентов Dr.Web возможна только на рабочие станции, работающие под управлением ОС семейства Windows (см. документ **Приложения**, п. Приложение А. Полный список поддерживаемых версий ОС), за исключением редакций Starter и Home, а также ОС Linux.

Для того чтобы дистанционно установить Агент Dr.Web на рабочие станции, вы должны иметь права администратора соответствующих рабочих станций.

Для дистанционной установки через Центр управления, если рабочие станции входят в домен, и для установки используется доменная учетная запись администратора, необходимо на рабочих станциях включить общий доступ к файлам и принтерам (расположение настройки для различных версий ОС Windows см. в таблице ниже).

Если станции сети не входят в домен или используется локальная учетная запись для установки, для ряда версий ОС Windows необходима дополнительная настройка станций.

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

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

После настройки рабочей станции сети рекомендуется вернуть все измененные настройки в значения, установленные до редактирования, чтобы не нарушать базовую политику безопасности операционной системы.

При дистанционной установке Агента на рабочую станцию вне домена, и/или с использованием локальной учетной записи, необходимо на компьютере, на который будет дистанционно устанавливаться Агент, выполнить следующие действия:

ОС	**Настройка**	
Windows XP	Настроить режим доступа к общим файлам	Новый стиль: **Пуск** → **Настройка** → **Панель управления** → **Оформление и темы** → **Свойства папки** → Вкладка **Вид** → снять флаг **Использовать простой общий доступ к файлам (рекомендуется)**
		Классический стиль: **Пуск** → **Настройка** → **Панель управления** → **Свойства папки** → Вкладка **Вид** → снять флаг **Использовать простой общий доступ к файлам (рекомендуется)**
	Установить в локальных политиках режим сетевой модели аутентификации	Новый стиль: **Пуск** → **Настройка** → **Панель управления** → **Производительность и обслуживание** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности** → **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** → **Обычная - локальные пользователи удостоверяются как они сами**.
		Классический стиль: **Пуск** → **Настройка** → **Панель управления** → **Администрирование** → **Локальная политика безопасности** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности** → **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** → **Обычная - локальные пользователи удостоверяются как они сами**.
	Отключить Windows Firewall на станции перед выполнением удаленной установки.	

<table>
<tr><th>ОС</th><th colspan="2">Настройка</th></tr>
<tr><td>Windows Server 2003</td><td colspan="2">Отключить Windows Firewall на станции перед выполнением удаленной установки.</td></tr>
<tr><td rowspan="4">Windows Vista

Windows Server 2008</td><td rowspan="2">Включить общий доступ к файлам</td><td>Новый стиль:

Пуск → Настройка → Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Общий доступ и сетевое обнаружение → Общий доступ к файлам → Включить.</td></tr>
<tr><td>Классический стиль:

Пуск → Настройка → Панель управления → Центр управления сетями и общим доступом → Общий доступ и сетевое обнаружение → Общий доступ к файлам → Включить.</td></tr>
<tr><td rowspan="2">Установить в локальных политиках режим сетевой модели аутентификации</td><td>Новый стиль:

Пуск → Настройка → Панель управления → Система и ее обслуживание → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами.</td></tr>
<tr><td>Классический стиль:

Пуск → Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами.</td></tr>
<tr><td colspan="2">Создать ключ LocalAccountTokenFilterPolicy:

a) В редакторе реестра откройте ветку HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Если записи LocalAccountTokenFilterPolicy не существует, в меню Правка выберите Создать и задайте значение DWORD. Введите значение LocalAccountTokenFilterPolicy и нажмите ENTER.
b) В контекстном меню пункта LocalAccountTokenFilterPolicy выберите Изменить.
c) В поле Значение задайте значение 1 и нажмите OK.</td></tr>
</table>

ОС	Настройка	
	Перезагрузка не требуется.	
Windows 7 Windows Server 2008 R2	Включить общий доступ к файлам и принтерам	Новый стиль: **Пуск → Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа → Общий доступ к файлам и принтерам → Включить общий доступ к файлам и принтерам**.
		Классический стиль: **Пуск → Панель управления → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа → Общий доступ к файлам и принтерам → Включить общий доступ к файлам и принтерам**.
	Установить в локальных политиках режим сетевой модели аутентификации	Новый стиль: **Пуск → Панель управления → Система и безопасность → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами**.
		Классический стиль: **Пуск → Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами**.
	Создать ключ **LocalAccountTokenFilterPolicy**: a) В редакторе реестра откройте ветку **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**. Если записи **LocalAccountTokenFilterPolicy** не существует, в меню **Правка** выберите **Создать** и задайте значение **DWORD**. Введите значение **LocalAccountTokenFilterPolicy** и нажмите ENTER. b) В контекстном меню пункта **LocalAccountTokenFilterPolicy** выберите **Изменить**. c) В поле **Значение** задайте значение **1** и нажмите **OK**.	

ОС	Настройка	
	Перезагрузка не требуется.	
Windows 8 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows 10	Включить общий доступ к файлам и принтерам	Новый стиль: **Параметры → Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа → Общий доступ к файлам и принтерам → Включить общий доступ к файлам и принтерам**.
		Классический стиль: **Параметры → Панель управления → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа → Общий доступ к файлам и принтерам → Включить общий доступ к файлам и принтерам**.
	Установить в локальных политиках режим сетевой модели аутентификации	Новый стиль: **Параметры → Панель управления → Система и безопасность → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами**.
		Классический стиль: **Параметры → Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная - локальные пользователи удостоверяются как они сами**.
	Создать ключ **LocalAccountTokenFilterPolicy**: a) В редакторе реестра откройте ветку **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**. Если записи **LocalAccountTokenFilterPolicy** не существует, в меню **Правка** выберите **Создать** и задайте значение **DWORD**. Введите значение **LocalAccountTokenFilterPolicy** и нажмите ENTER. b) В контекстном меню пункта **LocalAccountTokenFilterPolicy** выберите **Изменить**. c) В поле **Значение** задайте значение **1** и нажмите **OK**.	

ОС	Настройка
	Перезагрузка не требуется.

Если для учетной записи на станции в сети задан пустой пароль, установите в локальных политиках политику доступа с пустым паролем: **Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Учетные записи: ограничить использование пустых паролей только для консольного входа → Отключить**.

5.2.3.1.1. Установка Агента Dr.Web с использованием Центра управления безопасностью Dr.Web

Возможны следующие способы дистанционной установки Агентов на рабочие станции сети:

1. Установка через Сканер сети.

   Позволяет осуществить предварительный поиск незащищенных компьютеров сети и установку на них Агентов Dr.Web.

2. Установка при помощи инструмента Установка по сети.

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

3. Установка на станции с заданными ID.

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

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

Использование Сканера Сети

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

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

Чтобы установить Агент Dr.Web с использованием Сканера сети

1. Откройте Сканер сети. Для этого выберите пункт **Администрирование** в главном меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Сканер Сети**. Откроется одноименное окно с незагруженными данными.
2. Задайте параметры для поиска станций в сети. Подробное описание настроек приведено в **Руководстве администратора**, п. Сканер сети.
3. Нажмите кнопку **Сканировать**. В окно будет загружен каталог (иерархический список) компьютеров с указанием, на каких из них антивирусное ПО установлено, а на каких — нет.
4. Разверните элементы каталога, соответствующие рабочим группам (доменам). Все элементы каталога, соответствующие рабочим группам и отдельным станциям помечаются различными значками, значение которых приведено ниже.

   Таблица 5-1. Возможные виды значков

Значок	Описание
Рабочие группы	
	Рабочие группы, содержащие в числе прочих компьютеры, на которые можно установить антивирус Dr.Web Enterprise Security Suite.
	Остальные группы, включающие компьютеры с установленным антивирусным ПО или недоступные по сети.
Рабочие станции	
	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 значком  , можно дополнительно развернуть и ознакомиться с составом установленных компонентов.
5. В окне **Сканера сети** выберите незащищенный компьютер или несколько незащищенных компьютеров (при помощи кнопок CTRL или SHIFT).
6. На панели инструментов нажмите кнопку  **Установить Агент Dr.Web**.
7. Откроется окно **Установка по сети** для формирования задания на установку Агента.
8. В поле **Адреса станций** задайте IP-адреса или DNS-имена компьютеров, на которые будет устанавливаться Агент Dr.Web. При задании нескольких станций используйте ";" или "," в качестве разделителя (количество пробелов, обрамляющих разделитель, не имеет значения).

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

Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

9. По умолчанию в поле **Сервер Dr.Web** отображается IP-адрес или DNS-имя Сервера Dr.Web, к которому подключен Центр управления. При необходимости укажите в данном поле адрес Сервера Dr.Web, с которого будет устанавливаться антивирусное ПО. При задании нескольких Серверов Dr.Web используйте ";" или "," в качестве разделителя (количество пробелов, обрамляющих разделитель, не имеет значения). Оставьте поле пустым, чтобы использовать службу обнаружения Сервера Dr.Web (режим *Multicast*).

   Удаленная установка Агента недоступна на компьютер с установленным Сервером Dr.Web, с которого запускается процесс установки.

   Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

10. В поле **Количество одновременных установок** задайте максимальное количество станций, на которых может производиться запускаемая удаленная установка.
11. Установите флаг **Установить ПО Агента Dr.Web для Windows**, чтобы задать настройки, специфичные для удаленной установки на ОС Windows.
12. По умолчанию ПО Агента будет установлено на рабочую станцию в каталог `%ProgramFiles%\DrWeb`. При необходимости задайте другой путь в поле **Каталог установки Агента Dr.Web**.

    Рекомендуется задавать полный путь для однозначного определения местоположения каталога установки. При задании пути допускается использование переменных окружения.
13. В выпадающем списке **Язык** выберите язык интерфейса для Антивируса Dr.Web, который будет устанавливаться на станциях.
14. В поле **Тайм-аут установки (с)** задайте максимальное время ожидания до завершения установки Агента в секундах. Допустимые значения: 1-600. По умолчанию задано значение 180 секунд. При малой пропускной способности канала связи между Сервером Dr.Web и Агентом рекомендуется увеличить значение данного параметра.

    При большом объеме данных время установки может превысить продолжительность сессии. Если время сессии истечет до завершения установки, процесс будет завершен автоматически, а Агент Dr.Web не будет установлен.

15. При необходимости установите флаг **Зарегистрировать Агент Dr.Web в списке установленных программ**.
16. В разделе **Устанавливаемые компоненты** выберите компоненты антивирусного пакета, которые будут устанавливаться на станциях.
17. В разделах **Сжатие** и **Шифрование** задайте параметры сжатия и шифрования трафика, используемые Сетевым инсталлятором при установке Агента и антивирусного пакета.

Данные настройки также будут использоваться Агентом для взаимодействия с Сервером Dr.Web после установки.

18. В разделе **Авторизация на удаленных станциях** укажите параметры авторизации для доступа к удаленным компьютерам, на которые будет устанавливаться Агент:
    - **Пользователь** — имя пользователя для авторизации на станциях, на которых будет производиться удаленная установка. Для доменных пользователей необходимо указывать имя домена в формате *<домен>**<пользователь>* или *<пользователь>*@*<домен>*. Для локальных пользователей необходимо указывать имя станции или имя рабочей группы в формате *<станция>**<пользователь>* или *<группа>**<пользователь>*.
    - **Пароль** — пароль пользователя на удаленном компьютере.

    Возможно задание нескольких учетных записей администратора. Для добавления еще одной учетной записи нажмите кнопку  и заполните поля с настройками для авторизации. Аналогично для каждой новой записи.

    При установке Агента сначала используется первая учетная запись из списка. Если установка под этой учетной записью завершается с ошибкой, используется следующая учетная запись и т. д.
19. После задания всех необходимых параметров нажмите **Установить**.

Для запуска установки антивирусного ПО используется встроенная служба.

Для запуска установки используется сетевой инсталлятор текущего Сервера Dr.Web, расположенный в каталоге `webmin\install\windows` каталога установки Сервера Dr.Web, и SSL-сертификат `drwcsd-certificate.pem`, расположенный в каталоге `etc` каталога установки Сервера Dr.Web.

20. Агент Dr.Web будет установлен на указанные рабочие станции. После подтверждения станции на Сервере Dr.Web (если этого требуют настройки Сервера Dr.Web, см. также **Руководство администратора** п. Политика подключения станций), автоматически будет установлен антивирусный пакет.
21. Перезагрузите компьютер по требованию Агента.

Использование инструмента Установка по сети

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

Чтобы установить Агент Dr.Web по сети

1. В главном меню выберите пункт **Администрирование**, после чего в управляющем меню выберите **Установка по сети**.
2. Дальнейшие шаги установки аналогичны шагам **8-21** процедуры выше.

Установка для учетных записей с заданными ID

При создании новой учетной записи станции:

1. Создайте новую учетную запись или несколько учетных записей рабочих станций (см. п. Создание новой учетной записи).
2. Сразу после создания учетной записи, в правой части главного окна откроется панель с заголовком **Создание станции**. Нажмите кнопку **Установить**.
3. Откроется окно Сканера сети.
4. Дальнейшие шаги установки аналогичны шагам **2-21** процедуры выше.
5. После завершения установки проверьте, что в иерархическом списке у соответствующих станций изменились значки.

При использовании существующей учетной записи станции:

1. В иерархическом списке антивирусной сети выберите новую станцию, группу станций, для которых еще не были установлены Агенты, или группу **New** (для установки на все имеющиеся новые учетные записи).
2. На панели инструментов нажмите кнопку **Установить Агент Dr.Web**.
3. Откроется окно Сканера сети.
4. Дальнейшие шаги установки аналогичны шагам **2-21** процедуры выше.
5. После завершения установки проверьте, что в иерархическом списке у соответствующих станций изменились значки.

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

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

5.2.3.1.2. Установка Агента Dr.Web с использованием службы Active Directory

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

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

Установка Агента

Чтобы установить Агент с использованием службы Active Directory

1. Скачайте инсталлятор Агента Dr.Web для сетей с **Active Directory** с инсталляционной страницы.
2. На сервере локальной сети, поддерживающем службу **Active Directory**, выполните административную установку Агента Dr.Web. Установку можно производить как в режиме командной строки **(A)**, так и в графическом режиме инсталлятора **(B)**.

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

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

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

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

Ключ `/a` запускает развертывание административного пакета.

Название пакета

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

`drweb-13.00.0-<сборка>-esuite-agent-activedirectory.msi`

Параметры

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

- `ESSERVERADDRESS=<DNS_имя>` — адрес Сервера Dr.Web, к которому будет подключаться Агент. О возможных форматах см. в документе **Приложения**, п. Приложение Е.
- `ESSERVERPATH=<полное_имя_файла>` — полный путь к сертификату Сервера Dr.Web и имя файла (по умолчанию файл `drwcsd-certificate.pem` в подкаталоге `webmin/install` каталога установки Сервера Dr.Web).
- `TARGETDIR` — сетевой каталог для образа Агента (модифицированного установочного пакета Агента), который выбирается через редактор групповых политик для назначенной установки. Данный каталог должен иметь доступ на чтение и запись. Путь к каталогу следует

указывать в формате сетевых адресов, даже если он доступен локально; каталог обязательно должен быть доступен с целевых станций.

Перед административной установкой в целевом каталоге для образа Агента (см. параметр TARGETDIR) не требуется размещать вручную файлы для установки. Инсталлятор Агента для сетей с Active Directory (`<название_пакета>.msi`) и прочие файлы, необходимые для установки Агентов на рабочие станции, будут помещены в целевой каталог автоматически в процессе административной установки. Если данные файлы в целевом каталоге присутствуют перед началом административной установки, например, от предыдущих установок, то одноименные файлы будут перезаписаны.

При необходимости производить административную установку с разных Серверов Dr.Web рекомендуется задавать разные целевые каталоги для каждого из Серверов Dr.Web.

После развертывания административного пакета, в директории `<целевой_каталог>\Program Files\DrWeb` должен располагаться только файл `README.txt`.

Примеры

```
msiexec /a ESS_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\
\win_serv\drwcs_inst\drwcsd-certificate.pem TARGETDIR=\\comp\share
```

```
msiexec /a ESS_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:
\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem"
TARGETDIR=\\comp\share
```

Те же параметры можно задать в графическом режиме инсталлятора.

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

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

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

После развертывания административного пакета, в директории: *<целевой_каталог>*\Program Files\DrWeb должен располагаться только файл README.txt.

1. Для запуска инсталлятора в графическом режиме выполните команду:

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

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

Установщик Агента использует язык, указанный в языковых настройках компьютера.

3. В новом окне укажите DNS-имя или IP-адрес Сервера Dr.Web (см. в документе **Приложения**, п. Приложение Е). Укажите местонахождение сертификата Сервера Dr.Web (drwcsd-certificate.pem). Нажмите кнопку **Далее**.
4. В следующем окне укажите сетевой каталог, в который будет записан образ Агента. Путь к образу следует указывать в формате сетевых адресов, даже если каталог доступен локально; каталог обязательно должен быть доступен с целевых станций. Нажмите кнопку **Установить**.
5. После завершения инсталляции будет автоматически вызвано окно настройки, с помощью которого вы сможете назначить установку пакетов на компьютеры сети.

Настройка установки пакета на выбранные станции

1. На **Панели управления** (или в меню **Пуск** для ОС Windows 2003/2008/2012/2012R2 Server, в меню **Пуск** → **Программы** для ОС Windows 2000 Server) выберите **Администрирование** → **Active Directory — пользователи и компьютеры** (в графическом режиме установки Агента вызов данного окна настроек осуществляется автоматически).
2. В домене, включающем компьютеры, на которые предполагается установка Агентов Dr.Web, создайте новое **Подразделение** (для ОС Windows 2000 Server — **Организационное подразделение**) с именем, например, **ESS**. Для этого в контекстном меню домена выберите **Создать** → **Подразделение**. В открывшемся окне введите название нового подразделения и нажмите **ОК**. Включите в созданное подразделение компьютеры, на которые предполагается устанавливать Агент.
3. Откройте окно редактирования групповых политик. Для этого:
   a) для ОС Windows 2000/2003 Server: в контекстном меню созданного подразделения **ESS** выберите пункт **Свойства**. В открывшемся окне свойств перейдите на вкладку **Групповая политика**.
   b) для ОС Windows 2008/2012/2012R2 Server: **Пуск** → **Администрирование** → **Управление групповой политикой**.

4. Для созданного подразделения задайте групповую политику. Для этого:
   a) В ОС Windows 2000/2003 Server: нажмите кнопку **Добавить** и создайте элемент списка с именем политики **ESS**. Дважды щелкните по нему.
   b) В ОС Windows 2008/2012/2012R2 Server: в контекстном меню созданного подразделения **ESS** выберите пункт **Создать объект GPO в этом домене и связать его**. В открывшемся окне задайте название нового объекта групповой политики и нажмите кнопку **ОК**. В контекстном меню новой групповой политики выберите пункт **Изменить**.
5. В открывшемся окне **Редактор управления групповыми политиками** внесите настройки для групповой политики, созданной в п. **4**. Для этого:
   a) В ОС Windows 2000/2003 Server: в иерархическом списке выберите элемент **Конфигурация компьютера** → **Конфигурация программ** → **Установка программ**.
   b) В ОС Windows 2008/2012/2012R2 Server: в иерархическом списке выберите элемент **Конфигурация компьютера** → **Политики** → **Конфигурация программ** → **Установка программ**.
6. В контекстном меню элемента **Установка программ** выберите пункт **Создать** → **Пакет**.
7. Далее задайте установочный пакет Агента. Для этого укажите адрес сетевого разделяемого ресурса (созданный при административной установке образ Агента). Путь к каталогу с пакетом следует указывать в формате сетевых адресов, даже если каталог доступен локально.
8. Откроется окно **Развертывание программ**. Выберите опцию **Назначенные**. Нажмите **ОК**.
9. В окне редактора управления групповыми политиками появится пункт **Dr.Web Agent**. В контекстном меню этого пункта выберите **Свойства**.
10. В открывшемся окне свойств пакета перейдите на вкладку **Развертывание**. Нажмите кнопку **Дополнительно**.
11. Откроется окно **Дополнительные параметры развертывания**.
    - Установите флаг **Не использовать языковые установки при развертывании**.
    - Если вы планируете установку Агента Dr.Web при помощи настраиваемого msi-пакета на 64-битные ОС, установите флаг **Сделать доступным это 32-битное приложение для x64 машин**.
12. Нажмите дважды **ОК**.
13. Агент Dr.Web будет установлен на выбранные компьютеры при ближайшей регистрации их в домене.

Применение политик с учетом предыдущих установок Агента

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

1. **На станции нет Агента Dr.Web**.

   После применения политик, Агент будет установлен по общим правилам.

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

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

   

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

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

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

   Повторное назначение политики к станции с Агентом Dr.Web, установленным через службу Active Directory, не осуществляется.

   Таким образом, назначение политик не приведет к изменению состояния антивирусного ПО на станции.

5.2.3.2. Дистанционная установка Агента Dr.Web для ОС семейства UNIX

Для дистанционной установки ПО Агента Dr.Web на компьютеры, работающие под управлением ОС семейства UNIX, воспользуйтесь инструментом **Установка по сети** в Центре управления безопасностью Dr.Web.

Чтобы установить Агент Dr.Web по сети

1. В главном меню выберите пункт **Администрирование**, после чего в управляющем меню выберите **Установка по сети**.
2. В поле **Адреса станций** задайте IP-адреса или DNS-имена компьютеров, на которые будет устанавливаться Агент Dr.Web. При задании нескольких станций используйте “;” или “,” в качестве разделителя (количество пробелов, обрамляющих разделитель, не имеет значения).

   

   Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

3. В поле **Сервер Dr.Web** по умолчанию отображается IP-адрес или DNS-имя Сервера Dr.Web, к которому подключен Центр управления. При необходимости укажите в данном поле адрес Сервера Dr.Web, с которого будет устанавливаться антивирусное ПО. При задании нескольких Серверов Dr.Web используйте “;” или “,” в качестве разделителя (количество пробелов, обрамляющих разделитель, не имеет значения). Оставьте поле пустым, чтобы использовать службу обнаружения Сервера Dr.Web (режим *Multicast*).

Удаленная установка Агента недоступна на компьютер с установленным Сервером, с которого запускается процесс установки.

Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

4. В поле **Количество одновременных установок** задайте максимальное количество станций, на которых может производиться запускаемая удаленная установка.
5. Установите флаг **Установить ПО Агента Dr.Web для UNIX**, чтобы задать настройки, специфичные для удаленной установки на ОС семейства UNIX.
6. В поле **Тайм-аут соединения и аутентификации (с)** задайте максимальное время ожидания установки соединения и аутентификации на удаленных станциях в секундах.
7. В поле **Тайм-аут передачи установочных пакетов (с)** укажите максимальное время ожидания завершения процесса передачи установочных пакетов в секундах.
8. В поле **Тайм-аут установки пакетов (с)** укажите максимальное время ожидания завершения установки пакетов в секундах.

При большом объеме данных время установки может превысить продолжительность сессии. Если время сессии истечет до завершения установки, процесс будет завершен автоматически, а пакеты не будут установлены.

9. Если необходимо установить продукт Dr.Web для файловых серверов UNIX вместо Агента, установите флаг **Установить Dr.Web для файловых серверов UNIX**.
10. В разделе **Авторизация на удаленных станциях** укажите параметры авторизации для доступа к удаленным компьютерам, на которые будет устанавливаться Агент:
    - **Пользователь** — имя пользователя для авторизации на станциях, на которых будет производиться удаленная установка. Для доменных пользователей необходимо указывать имя домена в формате *<домен>\<пользователь>* или *<пользователь>@<домен>*. Для локальных пользователей необходимо указывать имя станции или имя рабочей группы в формате *<станция>\<пользователь>* или *<группа>\<пользователь>*.
    - **Пароль** — пароль пользователя на удаленном компьютере.

Одновременно можно задать нескольких учетных записей для авторизации. Для добавления еще одной учетной записи нажмите кнопку  и заполните поля с настройками для авторизации.

При установке Агента будут последовательно использоваться учетные записи из списка. Если установка под одной учетной записью завершается с ошибкой, используется следующая учетная запись и т. д.

11. В разделе **Аутентификация по электронной подписи** можно задать настройки альтернативной авторизации на удаленных компьютерах с использованием ключей шифрования:

- **Пользователь** — имя пользователя для авторизации на станциях, на которых будет производиться удаленная установка. Для доменных пользователей необходимо указывать имя домена в формате *<домен>\<пользователь>* или *<пользователь>@<домен>*. Для локальных пользователей необходимо указывать имя станции или имя рабочей группы в формате *<станция>\<пользователь>* или *<группа>\<пользователь>*.
- **Открытый ключ** — путь к файлу открытого ключа шифрования Сервера Dr.Web.
- **Закрытый ключ** — путь к файлу закрытого ключа шифрования Сервера Dr.Web.
- **Пароль закрытого ключа** — пароль закрытого ключа шифрования Сервера Dr.Web (необязателен).

Как и в случае с разделом **Авторизация на удаленных станциях**, существует возможность одновременного указания нескольких учетных записей, для чего необходимо нажать кнопку  и заполнить соответствующие поля.

Если заполнены параметры авторизации в обоих разделах **Авторизация на удаленных станциях** и **Аутентификация по электронной подписи**, первыми для установки Агента будут использоваться параметры авторизации через ключи шифрования.

12. Раздел **Права суперпользователя** содержит настройки для повышения прав пользователя на удаленном компьютере до уровня, необходимого для установки Агента Dr.Web.
    - Установите флаг **Использовать команду sudo** или **Использовать команду su** для повышения прав до уровня пользователя *root* на время установки Агента.
    - В поле **Тайм-аут ввода пароля (с)** укажите максимальное время ожидания ввода пароля для использования команды *su* или *sudo* в секундах.
    - В поле **Пароль su/sudo** введите пароль для использования команды *su* или *sudo*. Нажав кнопку  , можно указать несколько паролей, которые будут перебираться поочередно. Если оставить поле пустым, но при этом будет задан пароль пользователя в разделе **Авторизация на удаленных станциях**, будет предпринята попытка выполнить команду с использованием указанного пароля.
13. В поле **Порт** раздела **Параметры подключения** укажите номер порта SSH на компьютерах, который будет использоваться для удаленной установки Агента Dr.Web. Используя кнопку  , можно перечислить несколько портов.
14. После указания всех необходимых параметров нажмите **Установить**.
15. Агент Dr.Web будет установлен на указанные рабочие станции. После подтверждения станции на Сервере Dr.Web (если этого требуют настройки Сервера Dr.Web, см. также **Руководство администратора** п. Политика подключения станций), автоматически будет установлен антивирусный пакет.
16. Перезагрузите удаленные компьютеры по требованию Агента.

5.3. Установка Сканирующего сервера Dr.Web

1. На станцию, которую вы планируете назначить Сканирующим сервером, скачайте с инсталляционной страницы установочный пакет Сканирующего сервера.
2. Скачайте сертификат Сервера централизованной защиты, к которому будет подключаться Сканирующий сервер. Для этого в управляющем меню Центра управления в разделе **Администрирование** выберите пункт **Ключи шифрования**. Установите флажок возле объекта **Сертификат** и нажмите **Экспортировать**. Загрузите сертификат на станцию, которую вы планируете назначить Сканирующим сервером.

   Сертификат также можно скачать с инсталляционной страницы. Он находится в том же каталоге, что и установочный пакет Сканирующего сервера.

3. Перейдите в каталог, куда был скачан файл установочного пакета, и разрешите его исполнение:

   ```
   # chmod +x <имя_файла>.run
   ```

4. Далее запустите процедуру установки:

   ```
   # ./<имя_файла>.run
   ```

5. Примите условия Лицензионного соглашения.
6. По завершении установки подключите станцию, которую вы планируете назначить Сканирующим сервером, к Серверу централизованной защиты, выполнив команду:

   ```
   # drweb-ctl esconnect <адрес Сервера централизованной защиты> --Certificate <путь к файлу сертификата>
   ```

   После выполнения этой команды подключение должно быть одобрено автоматически или администратором антивирусной сети, в зависимости от настроек Сервера централизованной защиты.

   Подключиться к Серверу централизованной защиты возможно и другим способом: создать учетную запись станции, которую вы планируете назначить Сканирующим сервером, после чего вы получить логин (ID станции) и пароль для подключения. Далее выполните команду:

   ```
   # drweb-ctl esconnect <адрес Сервера централизованной защиты> --login <ID станции> --password <пароль> --Certificate <путь к файлу сертификата>
   ```

7. В случае успешного подключения станция будет отмечена в дереве антивирусной сети значком  , который показывает, что Сканирующий сервер активен и готов к работе.

   На станцию, выполняющую функции Сканирующего сервера, дополнительно устанавливать Агент Dr.Web не требуется.

8. Убедитесь, что Сканирующий сервер прослушивает порты 7090 и 18080, выполнив следующую команду:

```
# netstat -l
```

Вывод этой команды должен содержать следующие строки:

```
tcp 0 0 0.0.0.0:7090 0.0.0.0:* LISTEN
udp 0 0 0.0.0.0:18008 0.0.0.0:*
```

Подробная информация о настройке Сканирующего сервера и подключении к нему станцией содержится в **Руководстве администратора Dr.Web Enterprise Security Suite**, в разделе Подключение станций к Сканирующему серверу.

5.4. Установка NAP Validator

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

Данный компонент устанавливается на компьютер с настроенным сервером NAP.

Чтобы установить NAP Validator

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

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

1. Откройте компонент настройки сервера NAP (команда `nps.msc`).
2. В разделе **Группы серверов исправления** нажмите кнопку **Добавить**.

3. В открывшемся диалоговом окне укажите название для сервера исправления и IP-адрес Сервера Dr.Web.
4. Для сохранения внесенных изменений нажмите кнопку **OK**.

5.5. Установка Прокси-сервера Dr.Web

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

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

Вы можете установить Прокси-сервер под ОС Windows одним из следующих способов:

- Автоматически в процессе установки Агента Dr.Web для Windows

  Установка осуществляется из персонального инсталляционного пакета Агента Dr.Web, при создании которого были заданы настройки для установки связанного Прокси-сервера. В этом случае установка Прокси-сервера осуществляется автоматически в фоновом режиме.
- Автоматически на станции с установленным Агентом Dr.Web для Windows

  В Центре управления для выбранной станции настройте создание связанного Прокси-сервера. Прокси-сервер будет установлен на станцию автоматически в фоновом режиме.
- Вручную при помощи графического инсталлятора

  Установка осуществляется вручную администратором на любой подходящей станции сети. Никакие другие компоненты антивирусной сети не могут быть установлены на этой станции.

Установка Прокси-сервера под ОС семейства UNIX осуществляется только вручную при помощи инсталлятора.

5.5.1. Создание учетной записи Прокси-сервера Dr.Web

Учетные записи Прокси-сервера должны быть созданы администратором на каждом Сервере Dr.Web, к которому Прокси будет подключаться (на который будет перенаправляться трафик).

Чтобы создать учетную запись Прокси-сервера при помощи Центра управления безопасностью Dr.Web

1. Для родительской группы, в которой планируется создавать Прокси-сервер, задайте настройки как описано в **Руководстве администратора** в разделе Удаленная настройка Прокси-сервера. В этом случае заданные настройки будут унаследованы Прокси-сервером при подключении. Вы также можете задать эти настройки после создания учетной записи Прокси-сервера (как для родительской группы в случае наследования, так и персонально

для самого Прокси-сервера), но до подключения Прокси-сервера к создаваемой учетной записи.

Если настройки не были заданы до подключения Прокси-сервера, то конфигурационный файл не будет скачан. Текущие настройки будут использоваться Прокси-сервером до тех пор, пока не будут заданы настройки на подключенном Сервере, при условии, что ему разрешено управление конфигурацией.

2. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
3. Действия, необходимые для создания Прокси-сервера, будут зависеть от того, хотите ли вы установить Прокси-сервер на существующую станцию с Агентом Dr.Web или установить Прокси-сервер отдельно:

№	Действия	Установить с Агентом	Установить отдельно
а)	1. В дереве антивирусной сети выберите станцию для установки связанного Прокси-сервера. 2. На панели свойств выбранной станции перейдите к разделу **Прокси-сервер**.	+	–
б)	1. В дереве антивирусной сети выберите станцию для установки связанного Прокси-сервера. 2. На панели инструментов выберите опцию **Добавить объект сети** → **Создать Прокси-сервер**.	+	+
в)	1. Убедитесь, что в дереве антивирусной сети не выбрана станция. 2. На панели инструментов выберите опцию **Добавить объект сети** → **Создать Прокси-сервер**.	+	+

Если вы создаете учетную запись Прокси-сервера для установки на станции с Агентом, сама установка Прокси-сервера будет осуществляться автоматически через Агента в фоновом режиме сразу после создания учетной записи Прокси-сервера (см. также Установка Прокси-сервера Dr.Web в процессе установки Агента Dr.Web для Windows).

Если вы создаете учетную запись Прокси-сервера для отдельной установки (без связи с Агентом), то установка Прокси-сервера должна будет осуществляться администратором вручную из инсталляционного пакета, поставляемого вместе с дистрибутивом Сервера Dr.Web.

4. В поле **Идентификатор** автоматически генерируется уникальный идентификатор создаваемой учетной записи. При необходимости вы можете его изменить.
5. В поле **Название** задайте имя Прокси-сервера, которое будет отображаться в дереве антивирусной сети.

Заданное при настройке название будет автоматически заменено на имя компьютера после подключения Прокси-сервера к Серверу Dr.Web.

6. В полях **Пароль** и **Подтвердите пароль** можете задать пароль для доступа Прокси-сервера к Серверу Dr.Web. Если пароль не указан, он будет сгенерирован автоматически.

   Идентификатор и пароль Прокси-сервера используются в единственном экземпляре. На всех Серверах Dr.Web, к которым подключается Прокси-сервер, должны быть созданы учетные записи Прокси-сервера с одинаковыми идентификационными данными (см. Подключение Прокси-сервера Dr.Web к Серверу Dr.Web).

   После создания учетной записи Прокси-сервера редактирование идентификатора будет невозможно.

7. Для шагов 3.б) и 3.в) в поле **Станция** задается существующая станция с установленным Агентом, с которой будет связан данный Прокси-сервер.

   Для шага 3.б) в поле **Станция** будет автоматически добавлен идентификатор выбранной станции.

   Для шага 3.в) поле **Станция** будет пустым.

   - Чтобы задать станцию, на которую будет установлен Прокси-сервер, нажмите  и в открывшемся окне выберите существующую станцию из дерева антивирусной сети.
   - Оставьте поле **Станция** пустым, чтобы не связывать Прокси-сервер ни с одной станцией и подключить Прокси-сервер, установленный вручную. Если поле **Станция** уже заполнено, нажмите  , чтобы удалить связанную станцию.

8. В разделе **Членство** задается группа, в которую будет входить создаваемый 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.

9. Нажмите кнопку **Сохранить**.

   Откроется окно об удачном создании учетной записи Прокси-сервера, в котором также указан пароль доступа к Серверу Dr.Web. Для отображения пароля нажмите  .

   Идентификатор и пароль учетной записи Прокси-сервера, созданной через Центр управления, нужны администратору для подключения Прокси-сервера к Серверу Dr.Web:

   - В процессе установки Прокси-сервера через графический инсталлятор.
   - Вручную после установки Прокси-сервера (только для ОС семейства UNIX).

5.5.2. Установка Прокси-сервера Dr.Web в процессе установки Агента Dr.Web для Windows

Чтобы установить Прокси-сервер Dr.Web вместе с Агентом Dr.Web для Windows

1. Задайте настройки Прокси-сервера в Центре правления как описано в **Руководстве администратора**, п. Удаленная настройка Прокси-сервера. Настройки должны задаваться для группы, в которой планируется создавать Прокси-сервер. В этом случае заданные настройки будут унаследованы им при создании. Вы также можете задать эти настройки после создания Прокси-сервера (как для группы в случае наследования, так и персонально для самого Прокси-сервера), но до подключения Прокси-сервера к создаваемой учетной записи.

   

   Если настройки не были заданы до подключения Прокси-сервера, будут использованы настройки, переданные Прокси-серверу установщиком. Эти настройки подразумевают подключение только к Серверу Dr.Web, с которого производилась установка.

2. Создайте учетную запись станции при помощи Центра управления как описано в разделе Установка Агента Dr.Web при помощи персонального инсталляционного пакета. В процессе создания станции установите флаг **Создать связанный Прокси-Сервер** и задайте предлагаемые настройки. В частности, укажите группу для размещения Прокси-сервера, для которой вы задавали настройки на шаге 1.

   

   Идентификатор Прокси-сервера возможно изменить только при создании учетной записи.

3. На станции запустите установку Агента из персонального инсталляционного пакета, созданного на шаге 2.
4. После установки Агент автоматически скачает с Сервера Dr.Web установщик Прокси-сервера и запустит его в фоновом режиме на той же станции. Сертификат и адрес Сервера Dr.Web, а также идентификационные данные для подключения к Серверу Dr.Web будут автоматически занесены в соответствующие конфигурационные файлы Прокси-сервера. В настройках Прокси-сервера для перенаправления трафика будет указан только Сервер Dr.Web, с которого производилась установка.
5. После установки Прокси-сервер подключится к Серверу Dr.Web, с которого осуществлялась установка, для получения полноценного конфигурационного файла. Если на Сервере Dr.Web не были заданы настройки на шаге 1, то конфигурационный файл не будет скачан. Конфигурация, заданная установщиком, будет использоваться до тех пор, пока не будет задана конфигурация на подключенном Сервере Dr.Web.
6. Агент будет подключаться к Серверу только через установленный Прокси-сервер. Использование Прокси-сервера будет прозрачно для пользователя.

5.5.3. Установка Прокси-сервера Dr.Web при помощи инсталлятора

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

Установка Прокси-сервера под ОС Windows

1. Создайте учетную запись Прокси-сервера при помощи Центра управления как описано в разделе Создание учетной записи Прокси-сервера Dr.Web.
2. Скачайте инсталлятор Прокси-сервера с инсталляционной страницы.
3. Скопируйте сертификат Сервера Dr.Web, к которому будет подключаться Прокси-сервер (см. Подключение Прокси-сервера Dr.Web к Серверу Dr.Web), и инсталлятор на станцию, на которой вы планируете осуществлять установку.
4. Запустите инсталлятор Прокси-сервера. Откроется окно **InstallShield Wizard**, извещающее об устанавливаемом продукте. Нажмите кнопку **Далее**.
5. В окне параметров Прокси-сервера на вкладке **Общее** задайте следующие основные параметры:
   - В поле **Путь к данным программы** при необходимости измените путь для размещения файлов, используемых Прокси-сервером: журнала работы, конфигурационных файлов, кеша. По умолчанию используется путь `%PROGRAMDATA%/Doctor Web/drwcs`. Для выбора другого пути нажмите кнопку **Обзор**.
   - В поле **Адрес для прослушивания** задайте IP-адрес, "прослушиваемый" Прокси-сервером. По умолчанию — `any (0.0.0.0)` — "прослушивать" все интерфейсы.

     

     Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

   - В поле **Порт** задайте номер порта, который будет "прослушиваться" Прокси-сервером. По умолчанию — порт `2193`.
   - Установите флаг **Включить обнаружение** для включения режима имитации Сервера Dr.Web. Данный режим позволяет клиентам обнаруживать Прокси-сервер в качестве Сервера Dr.Web в процессе его поиска через широковещательные запросы.
   - Установите флаг **Включить multicasting**, чтобы Прокси-сервер отвечал на широковещательные запросы, адресованные Серверу Dr.Web.
     - 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 Dr.Web — `231.0.0.1`.

- 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** выберите уровень сжатия (от 1 до 9).

6. 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.

   После задания настроек кеширования нажмите кнопку **Далее**.

7. Откроется окно настроек переадресации соединений:

   - В поле **Адрес перенаправления** задайте адрес Сервера Dr.Web, на который будут перенаправляться соединения, устанавливаемые Прокси-сервером. Первым в списке необходимо указать Сервер Dr.Web, к которому должен будет подключиться Прокси-сервер для получения конфигурации. Сертификат этого Сервера Dr.Web был скопирован на станцию на шаге 2.

   

   Адреса задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. 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** выберите уровень сжатия (от 1 до 9).

Чтобы добавить еще один Сервер Dr.Web в список перенаправления трафика, нажмите кнопку  и задайте настройки по списку выше.

Чтобы удалить Сервер Dr.Web из списка перенаправления трафика, нажмите кнопку  напротив Сервера Dr.Web, который вы хотите удалить.

После завершения установки Прокси-сервер подключится к первому Серверу Dr.Web, заданному в этом разделе, для получения настроек.

Если на Сервере Dr.Web задана конфигурация Прокси-сервера, все настройки, заданные в инсталляторе, будут переписаны на новую конфигурацию, полученную с Сервера Dr.Web.

После завершения редактирования настроек переадресации нажмите кнопку **Далее**.

8. Откроется окно настройки соединения с Сервером Dr.Web для удаленного управления.

   Подключение будет осуществляться к первому Серверу Dr.Web, указанному на шаге 6 для перенаправления трафика.

   - В поле **Сертификат Сервера** задайте файл сертификата, скопированного на станцию на шаге 2. Для выбора файла нажмите кнопку **Обзор**.
   - В полях **Идентификатор** и **Пароль** задайте регистрационные данные учетной записи, созданной на Сервере Dr.Web на шаге 1.

9. Откроется окно, извещающее о готовности к установке Прокси-сервера.

   Если необходимо изменить дополнительные параметры установки, в частности, каталог установки Прокси-сервера, нажмите **Дополнительные параметры**.

   Для начала установки Прокси-сервера нажмите кнопку **Установить**.

10. После завершения процесса установки нажмите кнопку **Выход**.

11. После установки Прокси-сервер подключится к Серверу Dr.Web, указанному первым на шаге 6, для получения полноценного конфигурационного файла. Если на Сервере Dr.Web не были заданы настройки, то конфигурационный файл не будет скачан. Конфигурация, заданная установщиком, будет использоваться до тех пор, пока не будет задана конфигурация на подключенном Сервере Dr.Web.

Установка Прокси-сервера под ОС семейства UNIX

1. Скачайте инсталлятор Прокси-сервера с инсталляционной страницы.
2. Запустите инсталлятор Прокси-сервера при помощи следующей команды:

   `./<файл_дистрибутива>.tar.gz.run`

3. Для продолжения установки примите лицензионное соглашение.
4. Укажите путь до сертификата Сервера Dr.Web. Сертификат также можно добавить после установки Прокси-сервера (см. Подключение Прокси-сервера Dr.Web к Серверу Dr.Web).
5. При необходимости вы можете использовать конфигурационные файлы от предыдущей установки Прокси-сервера:

- Чтобы использовать резервную копию, сохраненную по умолчанию в директории `/var/tmp/drwcsd-proxy`, нажмите ENTER.
- Чтобы использовать резервную копию из другой директории, введите путь до резервной копии вручную.
- Также вы можете установить Прокси-сервер с настройками по умолчанию, без использования резервной копии конфигурации от предыдущей установки. Для этого нажмите 0.

6. После установки Прокси-сервера при необходимости вы можете отредактировать соответствующие конфигурационные файлы вручную (см. Подключение Прокси-сервера Dr.Web к Серверу Dr.Web).

Запуск и останов

В процессе установки ПО под ОС **FreeBSD** создается `rc`-скрипт `/usr/local/etc/rc.d/dwcp_proxy`. Используйте команды:

- `/usr/local/etc/rc.d/dwcp_proxy stop` — для ручного останова Прокси-сервера;
- `/usr/local/etc/rc.d/dwcp_proxy start` — для ручного запуска Прокси-сервера.

В процессе установки ПО под ОС **Linux** будет создан `init`-скрипт для запуска и останова Прокси-сервера `/etc/init.d/dwcp_proxy`.

5.5.4. Подключение Прокси-сервера Dr.Web к Серверу Dr.Web

Начиная с версии 11, предоставляется возможность подключения Прокси-сервера Dr.Web к Серверу Dr.Web с целью удаленного управления настройками и поддержки шифрования трафика.

Настройки подключения

Для подключения Прокси-сервера к Серверу Dr.Web необходимы:

- **Сертификат Сервера Dr.Web** `drwcsd-certificate.pem`**.**

  Необходимо наличие сертификатов всех Серверов Dr.Web, к которым подключается Прокси-сервер, и на которые перенаправляется клиентский трафик.

  - Сертификат Сервера Dr.Web требуется для подключения к Серверу Dr.Web с целью удаленного управления настройками, а также для поддержки шифрования трафика между Сервером Dr.Web и Прокси-сервером.
  - Сертификат Прокси-сервера, который подписывается сертификатом и закрытым ключом Сервера Dr.Web (процедура осуществляется автоматически на Сервере Dr.Web после подключения и не требует вмешательства администратора), требуется для подключения Агентов и для поддержки шифрования трафика между Агентами и Прокси-сервером.

Все сертификаты Серверов Dr.Web хранятся на Прокси-сервере в конфигурационном файле `drwcsd-proxy-trusted.list` в следующем формате (записи сертификатов отделяются одной или более пустыми строками):

```
[<сертификат_1>]


[<сертификат_2>]


[<сертификат_3>]

...
```

- **Адрес Сервера Dr.Web.**

  Прокси-сервер подключается ко всем Серверам Dr.Web, которые указаны в его конфигурационном файле для перенаправления клиентского трафика. Однако получение настроек разрешается только с определенного набора Серверов Dr.Web, которые помечены как управляющие. Если несколько Серверов Dr.Web помечены управляющими, то подключение осуществляется ко всем Серверам Dr.Web по очереди до первого получения валидной (не пустой) конфигурации.

- **Идентификатор и пароль для доступа к Серверу Dr.Web.**

  Учетные данные доступны после создания учетной записи для Прокси-сервера через Центр управления (см. Создание учетной записи Прокси-сервера Dr.Web).

  

  Идентификатор и пароль Прокси-сервера используются в единственном экземпляре. На всех Серверах Dr.Web, к которым подключается Прокси-сервер, должны быть созданы учетные записи Прокси-сервера с одинаковыми идентификационными данными.

  Идентификационные данные хранятся на Прокси-сервере в конфигурационном файле `drwcsd-proxy.auth` в следующем формате:

```
[<ID_Прокси-сервера>]

[<Пароль_Прокси-сервера>]
```

Подключение Прокси-сервера к Серверу Dr.Web

Для возможности подключения Прокси-сервера Dr.Web необходимо включить соответствующий протокол на стороне Сервера Dr.Web. Для этого в Центре управления в разделе **Администрирование** → **Конфигурация Сервера Dr.Web** →

Модули установите флаг **Протокол Прокси-сервера Dr.Web**, сохраните настройки и перезагрузите Сервер Dr.Web.

Автоматическое подключение при установке под ОС Windows:

- Если Прокси-сервер устанавливался в процессе установки Агента или на станции с установленным Агентом, то подключение к Серверу Dr.Web осуществляется автоматически.
- Если Прокси-сервер устанавливался через графический инсталлятор под ОС Windows, то подключение к Серверу Dr.Web осуществляется автоматически с использованием параметров подключения, указанных администратором в настройках инсталлятора.

  После установки Прокси-сервера файлы для подключения к Серверу Dr.Web по умолчанию располагаются в каталоге: `C:\Program Files\Doctor Web\drwcs\etc`.

Подключение вручную при установке под ОС семейства UNIX:

1. Установите Прокси-сервер для ОС семейства UNIX согласно процедуре, описанной в разделе Установка Прокси-сервера Dr.Web при помощи инсталлятора.
2. Создайте учетную запись Прокси-сервера при помощи Центра управления как описано в разделе Создание учетной записи Прокси-сервера Dr.Web.
3. Скопируйте сертификат Сервера Dr.Web на компьютер, на котором установлен Прокси-сервер.
4. В конфигурационном файле `drwcsd-proxy-trusted.list` укажите сертификат, скопированный на компьютер на шаге 3: скопируйте содержимое файла сертификата и вставьте его в конфигурационный файл согласно формату, описанному выше.
5. В конфигурационном файле `drwcsd-proxy.auth` задайте настройки подключения к Серверу Dr.Web для учетной записи, созданной на шаге 2 согласно формату, описанному выше.

   Файлы `drwcsd-proxy-trusted.list` и `drwcsd-proxy.auth` должны располагаться в следующих директориях:

   - для ОС Linux: `/var/opt/drwcs/etc`
   - для ОС FreeBSD: `/var/drwcs/etc`

   Для файлов необходимо выставить следующие права:

```
drwcsd-proxy-trusted.list 0644 drwcs:drwcs

drwcsd-proxy.auth 0600 drwcs:drwcs
```

5.6. Коды ошибок, возвращаемые при установке

При возникновении ошибок в процессе установки будут возвращены следующие коды ошибок:

Код ошибки	Описание
0	Установка успешно завершена
1	Некорректный формат команды
2	Неизвестная ошибка
3	Недостаточно прав для завершения операции (прав для записи в реестр, создания файлов или иной операции необходимой для установки)
4	Агент Dr.Web уже установлен
5	Установка уже запущена
7	Установка отменена
9	Превышено время ожидания ответа от сервера
11	Недостаточно прав для удаления приложения
12	Версия операционной системы устарела
13	Обнаружено несовместимое приложение
14	Установка невозможна, требуется перезагрузить систему (система ожидает перезагрузки перед следующей попыткой установки)
15	Неподдерживаемая архитектура операционной системы. Поддерживаются только x86 и x86_64
16	Ваша операционная система не поддерживает алгоритм sha-2
50	Удаление версии standalone в фоновом режиме невозможно

Для выяснения причины ошибки предпочтительно смотреть записи журнала. Приведенные коды ошибок являются общими, одна ошибка может возникать вследствие разных причин.

Глава 6: Удаление компонентов Dr.Web Enterprise Security Suite

6.1. Удаление Сервера Dr.Web

6.1.1. Удаление Сервера Dr.Web для ОС Windows

Для удаления ПО Сервера Dr.Web или расширения Центра управления безопасностью Dr.Web запустите соответствующий продукту инсталляционный пакет той версии, которая у вас установлена. Инсталлятор автоматически определит программный продукт и предложит удалить его. Для удаления ПО нажмите кнопку **Удалить**.

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

При удалении Сервера Dr.Web осуществляется резервное копирование конфигурационных файлов, ключей шифрования и базы данных, только если установлена настройка **Сохранить резервную копию критических данных Сервера Dr.Web**.

6.1.2. Удаление Сервера Dr.Web для ОС семейства UNIX

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

Чтобы удалить Сервер Dr.Web версии 10 и позднее

ОС Сервера Dr.Web	Действие
FreeBSD	Запустите скрипт: `/usr/local/etc/drweb.com/software/drweb-esuite.remove`
Linux	Запустите скрипт: `/etc/opt/drweb.com/software/drweb-esuite.remove`

При удалении Сервера Dr.Web под ОС **FreeBSD** и ОС **Linux** серверные процессы будут автоматически остановлены, база данных, ключевые и конфигурационные файлы будут скопированы в каталог по умолчанию — `/var/tmp/drwcs` (список

файлов для резервного копирования приведен в разделе Обновление Сервера Dr.Web для ОС семейства UNIX).

Чтобы отменить резервное копирование, необходимо объявить переменную окружения `SKIP_BACKUP`. Значение переменной может быть любым. Например: `SKIP_BACKUP="x"`

Также можно добавить определение этой переменной в файл `common.conf`.

6.2. Удаление Агента Dr.Web

Удаление Агента Dr.Web с защищаемых станций возможно следующими способами:

- Для станций под ОС Windows:
  - По сети через Центр управления.
  - Локально на станции.
  - Через службу Active Directory, если Агент был установлен при помощи данной службы.
- Для станций под ОС Android, ОС Linux, macOS — локально на станции.

Описание удаления Агента Dr.Web на рабочих станциях под Под ОС Android, ОС Linux, macOS приведено в **Руководстве пользователя** для соответствующей операционной системы.

6.2.1. Удаление Агента Dr.Web для ОС Windows

Дистанционное удаление Агента Dr.Web и антивирусного пакета

Дистанционные установка и удаление ПО Агента возможны только в локальной сети и требуют полномочий администратора в этой сети.

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

Чтобы удалить ПО антивирусной станции удаленно (только для ОС семейства Windows)

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в каталоге антивирусной сети выберите необходимую группу или отдельные антивирусные станции.

3. На панели инструментов каталога антивирусной сети нажмите **Общие** → **Деинсталлировать Агент Dr.Web**.
4. В открывшемся окне **Деинсталляция Агента Dr.Web** при необходимости вы можете настроить параметры автоматической перезагрузки выбранных станций после удаления Агента:
   - Вариант **Сразу после деинсталляции** предписывает станции перезагрузиться через 5 минут после удаления Агента.
   - Вариант **В заданный час** позволяет конкретизировать время перезагрузки станции с шагом в 1 час.
   - Вариант **В заданный период** дает возможность указать временной отрезок, в который произойдет перезагрузка.

   При любом выбранном варианте перезагрузки пользователь станции получит своевременное уведомление от Агента в виде всплывающего окна.

Вариант перезагрузки	**Уведомление пользователя**
Не выбран	Станция не перезагружается после удаления Агента. Уведомление отсутствует.
Сразу после деинсталляции	Уведомление появляется за 5 минут до перезагрузки с указанием точного времени, когда станция будет перезагружена.
В заданный час	• **Первое уведомление** Уведомление появляется сразу же после удаления Агента и сообщает точное время, на которое была назначена перезагрузка. • **Второе уведомление** Уведомление появляется за 5 минут до перезагрузки с указанием точного времени, когда станция будет перезагружена. • **Если со станцией нет связи в заданный час** Через 15 минут после восстановления связи появляется уведомление о перезагрузке станции через ближайшие 5 минут с указанием точного времени.
В заданный период	• **Первое уведомление** Уведомление появляется сразу же после удаления Агента и сообщает точное время в рамках заданного периода, когда произойдет перезагрузка.

Вариант перезагрузки	Уведомление пользователя
	• **Второе уведомление** Уведомление появляется за 5 минут до перезагрузки с указанием точного времени, когда станция будет перезагружена. • **Если со станцией нет связи в заданный период** Через 15 минут после восстановления связи появляется уведомление о предстоящей перезагрузке на следующий день с указанием точного времени в рамках заданного периода.

5. ПО Агента и антивирусный пакет будут удалены с выбранных вами рабочих станций.

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

Локальное удаление Агента Dr.Web и антивирусного пакета

Для возможности локального удаления Агента и антивирусного пакета, данная опция должна быть разрешена на Сервере Dr.Web в разделе **Права** (см. **Руководство администратора**, п. Права пользователей станции).

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

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

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

Удаление штатными средствами ОС Windows

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

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

Для удаления Агента и антивирусного пакета штатными средствами ОС Windows воспользуйтесь элементом **Панель управления → Установка и удаление программ** (подробная инструкция приведена в **Руководстве пользователя** для Агента Dr.Web для Windows).

Удаление при помощи инсталлятора

- **Клиентский модуль win-ess-agent-setup.exe**

  Для того чтобы удалить ПО Агента и антивирусный пакет при помощи клиентского модуля, который создается при установке Агента, запустите установочный файл `win-ess-agent-setup.exe` с параметром `/instMode remove`. Дополнительно используйте параметр `/silent no`, если требуется обеспечить контроль за ходом удаления.

  Установочный файл `win-ess-agent-setup.exe` по умолчанию располагается в следующем каталоге:

  - для ОС Windows XP и ОС Windows Server 2003:
    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
  - для ОС Windows Vista или более поздней версии и для ОС Windows Server 2008 или более поздней версии:
    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  Например, для Windows 7, где `%ALLUSERPROFILE%` соответствует `C:\ProgramData`:

  ```
  C:\ProgramData\Doctor Web\Setup\win-ess-agent-setup.exe /instMode
  remove /silent no
  ```

- **Персональный инсталляционный пакет drweb_ess_<*ОС*>_<*станция*>.exe**

  Для того чтобы удалить ПО Агента и антивирусный пакет при помощи инсталляционного пакета, запустите установочный файл `drweb_ess_<ОС>_<`*станция*`>.exe` той версии продукта, которая у вас установлена.

- **Полный инсталлятор drweb-13.00.0-<*сборка*>-esuite-agent-full-windows.exe**

  Для того чтобы удалить ПО Агента и антивирусный пакет при помощи полного инсталлятора, запустите установочный файл `drweb-13.00.0-<`*сборка*`>-esuite-agent-full-windows.exe` той версии продукта, которая у вас установлена.

- **Сетевой инсталлятор drwinst.exe**

  Для того чтобы удалить ПО Агента и антивирусный пакет при помощи сетевого инсталлятора на станции локально, необходимо в каталоге установки Агента Dr.Web (по умолчанию — `C:\Program Files\DrWeb`) запустить инсталлятор `drwinst.exe` с

параметром `/instMode remove`. Дополнительно используйте параметр `/silent no`, если требуется обеспечить контроль за ходом удаления.

Например:

```
drwinst /instMode remove /silent no
```

При запуске инсталляционного пакета `drweb_ess_<ОС>_<станция>.exe`, полного инсталлятора `drweb-13.00.0-<сборка>-esuite-agent-full-windows.exe` и сетевого инсталлятора `drwinst.exe` осуществляется запуск клиентского модуля `win-ess-agent-setup.exe`, который непосредственно осуществляет удаление.

Клиентский модуль `win-ess-agent-setup.exe`, запущенный без параметров, определяет установленный продукт и запускается в режиме изменения/удаления. Для запуска сразу в режиме удаления используйте ключ `/instMode remove`.

6.2.2. Удаление Агента Dr.Web с использованием службы Active Directory

Для возможности удаления Агента данная опция должна быть разрешена на Сервере Dr.Web в разделе **Права** (см. **Руководство администратора**, п. Права пользователей станции).

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

6.3. Удаление Сканирующего сервера Dr.Web

Операцию удаления необходимо выполнять от имени суперпользователя (**root**).

Перед удалением Сканирующего сервера убедитесь, что в антивирусной сети нет станций, настроенных на взаимодействие с ним. В противном случае эти станции останутся без защиты.

Чтобы удалить Сканирующий сервер Dr.Web

1. На виртуальной машине, назначенной Сканирующим сервером, перейдите в директорию `/opt/drweb.com/bin`.
2. Запустите скрипт `uninst.sh`.
3. На экране появится текст приглашения к удалению. Чтобы начать процедуру удаления, ответьте *Yes* или *Y* на вопрос "Do you want to continue?". Чтобы отказаться от удаления Сканирующего сервера Dr.Web, введите *No* или *N*. В этом случае работа программы удаления будет завершена.
4. После подтверждения запустится процедура удаления всех Сканирующего сервера Dr.Web. При этом на экран будут выдаваться записи, фиксируемые в журнал и отражающие ход процесса удаления.
5. По окончании процесса программа удаления завершит работу автоматически.

6.4. Удаление Прокси-сервера Dr.Web

Прокси-сервер может быть удален одним из следующих способов:

1. Локально.

   Локальное удаление осуществляется администратором непосредственно на компьютере, на котором установлен Прокси-сервер.

2. Дистанционно.

   Дистанционное удаление Прокси-сервера осуществляется в Центре управления через ЛВС и доступно в том случае, когда Прокси-сервер подключен к Серверу Dr.Web.

6.4.1. Локальное удаление Прокси-сервера Dr.Web

Удалить Прокси-сервер Dr.Web локально с компьютера можно только в том случае, если его установка также производилась локально, при помощи инсталлятора. В ином случае необходимо следовать инструкциям из раздела Дистанционное удаление Прокси-сервера Dr.Web.

Для ОС Windows

При удалении Прокси-сервера его конфигурационные файлы не удаляются и остаются в каталоге `%ALLUSERSPROFILE%\Doctor Web\`.

Установленный на ОС Windows Прокси-сервер Dr.Web можно удалить штатными средствами операционной системы или при помощи инсталлятора.

Удаление штатными средствами

Воспользуйтесь элементом **Панель управления → Установка и удаление программ** (**Программы и компоненты** для ОС Windows 2008 или более поздней версии).

Удаление при помощи инсталлятора

- **Клиентский модуль proxy-setup.exe**

  Для удаления при помощи клиентского модуля, который создается при установке Прокси-сервера, запустите установочный файл `proxy-setup.exe` с параметром `/instMode remove`. Дополнительно используйте параметр `/silent no`, если требуется обеспечить контроль за ходом удаления.

  Установочный файл `proxy-setup.exe` по умолчанию располагается в следующем каталоге:

  - для ОС Windows XP и ОС Windows Server 2003: `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\drweb-win-proxy\`
  - для ОС Windows Vista или более поздней версии и для ОС Windows Server 2008 или более поздней версии: `%ALLUSERSPROFILE%\Doctor Web\Setup\drweb-win-proxy\`

  Пример команды для запуска модуля на Windows 10, где `%ALLUSERPROFILE%` соответствует `C:\ProgramData`:

  ```
  C:\ProgramData\Doctor Web\Setup\drweb-win-proxy\proxy-setup.exe /instMode remove /silent no
  ```

- **Инсталлятор drweb-proxy-<*версия_пакета*>-<*сборка*>-windows-nt-<*разрядность*>.exe**

  Для того чтобы удалить Прокси-сервер при помощи инсталлятора, скачайте с инсталляционной страницы и запустите установочный файл `drweb-proxy-<версия_пакета>-<сборка>-windows-nt-<разрядность>.exe`. Следуйте инструкциям.

Для ОС семейства UNIX

При удалении Прокси-сервера в каталог `/var/tmp/drwcsd-proxy` автоматически сохраняется резервная копия конфигурационных файлов.

ОС Прокси-сервера	Действие
FreeBSD	Запустите скрипт: `/usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove`
Linux	Запустите скрипт: `/etc/opt/drweb.com/software/drweb-proxy.remove`

6.4.2. Дистанционное удаление Прокси-сервера Dr.Web

Дистанционное удаление Прокси-сервера доступно в том случае, когда Прокси-сервер подключен к Серверу Dr.Web (см. Подключение Прокси-сервера Dr.Web к Серверу Dr.Web).

При удалении учетной записи Прокси-сервера в Центре управления осуществляется удаление самого Прокси-сервера со станции.

Чтобы удалить Прокси-сервер

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в иерархическом списке нажмите на название одного или нескольких Прокси-серверов, которых вы хотите удалить.
3. На панели инструментов нажмите **Общие** → **Удалить выбранные объекты**.
4. Откроется окно подтверждения удаления объекта. Нажмите **ОК**.

Чтобы удалить Прокси-сервер, который установлен на связанной станции

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Откройте раздел свойств станции, на которой установлен Прокси-сервер, 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. В окне свойств станции перейдите в раздел **Прокси-сервер**.

4. Нажмите **Удалить Прокси-сервер**.
5. Нажмите **Сохранить**. Прокси-сервер будет деинсталлирован со станции. Учетная запись Прокси-сервера — удалена с Сервера Dr.Web.

Глава 7: Обновление компонентов Dr.Web Enterprise Security Suite

Обновление Сервера Dr.Web с версий 11.X до версии 13.0 доступно через Центр управления. Описание процедуры приведено в **Руководстве администратора**, в разделе Обновление Сервера Dr.Web и восстановление из резервной копии.

Перед началом обновления Dr.Web Enterprise Security Suite и его отдельных компонентов обратите внимание на следующие важные особенности:

- Перед началом обновления настоятельно рекомендуется проверить корректность настроек протокола TCP/IP для возможности доступа в интернет. В частности, должна быть включена и содержать корректные настройки служба DNS.
- Перед обновлением Сервера Dr.Web рекомендуется обновить все компоненты антивирусной сети Dr.Web Enterprise Security Suite, включая Агент Dr.Web, до последней доступной на ВСО версии.
- При многосерверной конфигурации антивирусной сети необходимо учитывать, что между Серверами Dr.Web версии 13 и Серверами Dr.Web версий 6 передача межсерверных обновлений не осуществляется, и межсерверная связь используется только для передачи статистики. Для обеспечения передачи межсерверных обновлений необходимо обновить все Серверы Dr.Web. Если необходимо оставить в составе антивирусной сети Серверы Dr.Web предыдущих версий для подключения Агентов, установленных на ОС, не поддерживаемых версией 13 (см. п. Обновление Агентов Dr.Web), то Серверы Dr.Web версий 6 и Серверы Dr.Web версии 13 должны получать обновления независимо.
- Обновление кластера Серверов Dr.Web с версии 10 до версии 13 необходимо проводить по отдельности, т.е. поочередно выводить узлы из кластера, переключать на внутреннюю базу данных и обновлять, после чего один за другим подключать обратно к общему кластеру.
- Для антивирусной сети, в которой используется Прокси-сервер Dr.Web, при обновлении компонентов до версии 13.0 необходимо также произвести обновление Прокси-сервера до версии 13.0. В противном случае подключение Агентов, поставляемых с версией 13.0, к Серверу Dr.Web версии 13.0 будет невозможно. Рекомендуется производить обновление в следующем порядке: Сервер Dr.Web → Прокси-сервер Dr.Web → Агент Dr.Web.
- При обновлении Сервера Dr.Web с версии 6 до версии 13 настройки работы Сервера Dr.Web через прокси-сервер не сохраняются. После установки версии 13 необходимо задать настройки подключения через прокси-сервер вручную (см. **Руководство администратора**, п. Прокси).
- При обновлении Сервера Dr.Web все настройки репозитория не переносятся в новую версию (сбрасываются в значения по умолчанию), однако осуществляется их резервное копирование. При необходимости задайте настройки репозитория вручную после обновления Сервера Dr.Web.
- При обновлении Сервера Dr.Web до версии 13 обновления продуктов репозитория **Базы 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. Подробнее см. **Руководство администратора**, п. Детальная конфигурация репозитория.

Если ваш Сервер Dr.Web не подключен к интернету, и обновления загружаются вручную с другого Сервера Dr.Web или через Загрузчик репозитория, то перед тем как устанавливать или обновлять продукты, для которых в настройках репозитория включена опция **Обновлять только по требованию**, необходимо предварительно загрузить эти продукты в репозиторий вручную.

7.1. Обновление Сервера Dr.Web для ОС Windows

Обновление Сервера Dr.Web с версии 6, 10 или 11 до версии 13 и в пределах версии 13 осуществляется автоматически средствами инсталлятора.

Обновление Сервера Dr.Web с версий 11.X до версии 13.0 также доступно через Центр управления. Описание процедуры приведено в **Руководстве администратора**, в разделе Обновление Сервера Dr.Web и восстановление из резервной копии.

Перед началом обновления Сервера Dr.Web обратите внимание на раздел Обновление Агента Dr.Web.

Обновление Сервера Dr.Web в пределах версии 13 также возможно осуществлять при помощи Центра управления. Описание процедуры приведено в **Руководстве администратора**, в разделе Обновление Сервера Dr.Web и восстановление из резервной копии.

Не все обновления Сервера Dr.Web в пределах версии 13 содержат файл дистрибутива. Некоторые их них возможно установить только через Центр управления.

Сохранение файлов конфигурации

При обновлении Сервера Dr.Web до версии 13 средствами инсталлятора конфигурационные файлы сохраняются в каталог, заданный для резервного копирования:

- При обновлении с версии 6: в каталог *<диск_установки>*`:\DrWeb Backup`.
- При обновлении с версий 10, 11 и в пределах версии 13: в каталог, который задается в настройке **Сохранить резервную копию критических данных Сервера Dr.Web** в процессе обновления (по умолчанию *<диск_установки>*`:\DrWeb Backup`).

При обновлении Сервера Dr.Web с версии 6 сохраняются следующие конфигурационные файлы:

Файл	**Описание**
`agent.key` (имя может отличаться)	лицензионный ключ Агента
`auth-ads.xml`	конфигурационный файл внешней авторизации администраторов через Active Directory
`auth-ldap.xml`	конфигурационный файл внешней авторизации администраторов через LDAP
`auth-radius.xml`	конфигурационный файл внешней авторизации администраторов через RADIUS
`drwcsd.conf` (имя может отличаться)	конфигурационный файл Сервера Dr.Web
`dbinternal.dbs`	встроенная БД
`drwcsd.pri`	закрытый ключ шифрования
`drwcsd.pub` (имя может отличаться)	открытый ключ шифрования
`enterprise.key` (имя может отличаться)	лицензионный ключ Сервера Dr.Web
`webmin.conf`	конфигурационный файл Центра управления

При обновлении Сервера Dr.Web с версии 10 сохраняются следующие конфигурационные файлы:

Файл	**Описание**
`agent.key` (имя может отличаться)	лицензионный ключ Агента
`auth-ads.xml`	конфигурационный файл внешней авторизации администраторов через Active Directory
`auth-ldap.xml`	конфигурационный файл внешней авторизации администраторов через LDAP

Файл	Описание
auth-radius.xml	конфигурационный файл внешней авторизации администраторов через RADIUS
enterprise.key (имя может отличаться)	лицензионный ключ Сервера Dr.Web. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера Dr.Web 13.0 отсутствует
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера Dr.Web
drwcsd.conf.distr	шаблон конфигурационного файла Сервера Dr.Web с параметрами по умолчанию
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub (имя может отличаться)	открытый ключ шифрования
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера Dr.Web
webmin.conf	конфигурационный файл Центра управления
openssl.cnf	сертификат Сервера Dr.Web для HTTPS

При обновлении Сервера Dr.Web с версии 11 и в пределах версии 13 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ads.conf	конфигурационный файл внешней авторизации администраторов через Active Directory
auth-radius.conf	конфигурационный файл внешней авторизации администраторов через RADIUS
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
auth-ldap-rfc4515-check-group.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory
auth-ldap-rfc4515-check-group-novar.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory с использованием переменных
auth-ldap-rfc4515-simple-login.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме
auth-pam.conf	конфигурационный файл внешней авторизации администраторов через PAM
enterprise.key (имя может отличаться)	лицензионный ключ Сервера Dr.Web. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера Dr.Web 13.0 отсутствует
drwcsd-certificate.pem	сертификат Сервера Dr.Web
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера Dr.Web
drwcsd.conf.distr	шаблон конфигурационного файла Сервера Dr.Web с параметрами по умолчанию
drwcsd.pri	закрытый ключ шифрования
dbexport.gz	экспорт базы данных
drwcsd.pub (имя может отличаться)	открытый ключ шифрования
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера Dr.Web
openssl.cnf	сертификат Сервера Dr.Web для HTTPS
webmin.conf	конфигурационный файл Центра управления
yalocator.apikey	API-ключ для Расширения Yandex.Locator

Если вы планируете использовать файлы конфигурации от Сервера Dr.Web версии 6, обратите внимание:

1. Лицензионный ключ Сервера Dr.Web более не используется (см. п. Лицензирование).
2. Встроенная база данных обновляется, а конфигурационный файл Сервера Dr.Web конвертируется средствами инсталлятора. Данные файлы не подлежат замене на автоматически сохраненные копии при переходе с Сервера Dr.Web версии 6.

При необходимости сохраните другие важные для вас файлы в другом месте, отличном от каталога установки Сервера Dr.Web, например, шаблоны отчетов, находящиеся в каталоге `\var\templates`.

Сохранение базы данных

База данных MS SQL CE начиная с версии Сервера Dr.Web 10 более не поддерживается. При автоматическом обновлении Сервера Dr.Web средствами инсталлятора осуществляется автоматическое конвертирование базы данных MS SQL CE во встроенную базу `SQLite`.

Перед обновлением убедитесь, что в СУБД Microsoft SQL указана сортировка с учетом регистра (суффикс `_CS`) и с учетом диакритических знаков (суффикс `_AS`). В противном случае автоматическое обновление будет невозможно.

Перед обновлением также убедитесь, что используемая СУБД поддерживается Сервером Dr.Web версии 13. В противном случае автоматическое обновление будет невозможно. Список поддерживаемых СУБД приведен в документе **Приложения**, в Приложении В. Настройки для использования СУБД. Параметры драйверов СУБД.

Перед обновлением ПО Dr.Web Enterprise Security Suite рекомендуется выполнить резервное копирование базы данных.

Чтобы сохранить базу данных

1. Остановите Сервер Dr.Web.
2. Экспортируйте базу данных в файл:
   - для Сервера Dr.Web до версии 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all exportdb <каталог_резервной_копии>\esbase.es
```

- для Сервера Dr.Web, начиная с версии 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all modexecdb database-export <каталог_резервной_копии>\esbase.es
```

Для Серверов Dr.Web, использующих внешнюю базу данных, рекомендуется использовать штатные средства, поставляемые вместе с базой данных.

Убедитесь, что экспорт базы данных Dr.Web Enterprise Security Suite завершился успешно. Отсутствие резервной копии БД не позволит восстановить Сервер Dr.Web в случае непредвиденных обстоятельств.

Обновление Сервера Dr.Web

Для обновления Сервера Dr.Web запустите файл дистрибутива. Дальнейшие шаги зависят от обновляемой версии.

По умолчанию в качестве языка инсталлятора выбирается язык операционной системы. При необходимости вы можете изменить язык установки на любом шаге, выбрав соответствующий пункт в правом верхнем углу окна инсталлятора.

При использовании внешней базы данных Сервера Dr.Web в процессе обновления также выберите вариант **Использовать существующую базу данных**.

Если вы планируете использовать в качестве внешней базы данных БД Oracle через ODBC-подключение, то при установке (обновлении) Сервера Dr.Web, 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 Oracle через ODBC будет невозможна из-за конфликта библиотек.

При обновлении с версии 6

1. Откроется окно, извещающее о наличии установленного ПО Сервера Dr.Web предыдущей версии и предоставляющее краткое описание процесса обновления до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Обновить**.

2. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флаг **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.
3. В последующих шагах осуществляется настройка Сервера Dr.Web аналогично процессу Установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера Dr.Web, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.
4. Для начала процесса удаления Сервера Dr.Web предыдущей версии и установки Сервера Dr.Web версии 13.0 нажмите кнопку **Установить**.

   В процессе удаления Сервера Dr.Web автоматически сохраняются файлы конфигурации в каталог <*диск_установки*>:\DrWeb Backup.

При обновлении с версии 10.0

1. Откроется окно, извещающее о наличии установленного ПО Сервера Dr.Web предыдущей версии и предоставляющее краткое описание процесса обновления до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Обновить**.
2. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флаг **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.
3. В последующих шагах осуществляется настройка Сервера Dr.Web аналогично процессу Установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера Dr.Web, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.
4. Для начала процесса удаления Сервера Dr.Web предыдущей версии и установки Сервера Dr.Web версии 13.0 нажмите кнопку **Установить**.
5. В процессе обновления откроется окно с настройкой резервного копирования критичных данных перед удалением Сервера Dr.Web предыдущей версии. Рекомендуется установить флаг **Сохранить резервную копию критических данных Сервера Dr.Web**. При необходимости можете изменить каталог для резервного копирования, заданный по умолчанию (<*диск_установки*>:\DrWeb Backup).

При обновлении с версии 10.0.1, 10.1, 11 и в пределах версии 13

1. Откроется окно, извещающее о наличии установленного ПО Сервера Dr.Web предыдущей версии и предоставляющее краткое описание процесса обновления до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Обновить**.

2. Откроется окно с настройкой резервного копирования критичных данных перед удалением Сервера Dr.Web предыдущей версии. Рекомендуется установить флаг **Сохранить резервную копию критических данных Сервера Dr.Web**. При необходимости можете изменить каталог для резервного копирования, заданный по умолчанию (<*диск_установки*>`:\DrWeb Backup`). Для начала процесса удаления предыдущей версии Сервера Dr.Web нажмите **Удалить**.
3. После завершения удаления предыдущей версии Сервера Dr.Web начнется установка новой версии. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флаг **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.
4. В последующих шагах осуществляется настройка Сервера Dr.Web с использованием существующей базы данных (аналогично процессу Установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии). Инсталлятор автоматически определяет каталог установки Сервера Dr.Web, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.
5. Для начала процесса установки Сервера Dr.Web версии 13.0 нажмите кнопку **Установить**.

После завершения обновлений Серверов Dr.Web антивирусной сети необходимо:

1. Повторно задать настройки шифрования и сжатия у связанных Серверов Dr.Web (см. **Руководство администратора**, раздел Настройка связей между Серверами Dr.Web).
2. Очистить кеш веб-браузера, используемого для подключения к Центру управления.

7.2. Обновление Сервера Dr.Web для ОС семейства UNIX

Обновление Сервера Dr.Web до версии 13.0 зависит от исходной версии:

- Обновление с версии 6.0.4 на версию 13.0 осуществляется только вручную.
- Обновление с версий 10.X на версию 13.0 автоматически при помощи инсталлятора поверх установленной версии возможно не для всех ОС семейства UNIX. Поэтому под ОС семейства UNIX, в которых невозможно произвести автоматическое обновление поверх уже установленного пакета, необходимо осуществить обновление вручную.
- Обновление Сервера Dr.Web с версий 11.X и в пределах версии 13.0 для одинаковых типов пакетов осуществляется автоматически при помощи инсталлятора для всех ОС семейства UNIX. При желании вы также можете осуществить обновление вручную.
- Обновление Сервера Dr.Web с версий 11.X до версии 13.0 также доступно через Центр управления. Описание процедуры приведено в **Руководстве администратора**, в разделе Обновление Сервера Dr.Web и восстановление из резервной копии.

При обновлении Сервера Dr.Web под ОС семейства UNIX с версии 10 и младше настройки из раздела Центра управления **Конфигурация веб-сервера** (файл `webmin.conf`) не будут перенесены в версию 13.

Настройки в этом разделе будут сброшены в значения по умолчанию. Если вы хотите использовать настройки предыдущей версии, задайте их вручную после обновления Сервера Dr.Web в соответствующем разделе Центра управления на основе данных из резервной копии конфигурационного файла.

Перед началом обновления Сервера Dr.Web обратите внимание на раздел Обновление Агента Dr.Web.

Обновление Сервера Dr.Web в пределах версии 13 также возможно осуществлять при помощи Центра управления. Описание процедуры приведено в **Руководстве администратора**, в разделе Обновление Сервера Dr.Web и восстановление из резервной копии.

Не все обновления Сервера Dr.Web в пределах версии 13 содержат файл дистрибутива. Некоторые их них возможно установить только через Центр управления.

Сохранение файлов конфигурации

При удалении и автоматическом обновлении Сервера Dr.Web до версии 13 конфигурационные файлы сохраняются в каталог, заданный для резервного копирования по умолчанию: `/var/tmp/drwcs/`.

При удалении Сервера Dr.Web версии 6 сохраняются следующие конфигурационные файлы:

Файл	Описание
`agent.key` (имя может отличаться)	лицензионный ключ Агента
`certificate.pem`	сертификат для SSL
`common.conf`	конфигурационный файл (для некоторых ОС семейства UNIX)
`dbinternal.dbs`	встроенная БД
`drwcsd.conf` (имя может отличаться)	конфигурационный файл Сервера Dr.Web
`drwcsd.pri`	закрытый ключ шифрования

Файл	Описание
drwcsd.pub (имя может отличаться)	открытый ключ шифрования
enterprise.key (имя может отличаться)	лицензионный ключ Сервера Dr.Web
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления

При удалении Сервера Dr.Web версии 10 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ldap.xml	конфигурационный файл внешней авторизации администраторов через LDAP
auth-pam.xml	конфигурационный файл внешней авторизации администраторов через PAM
auth-radius.xml	конфигурационный файл внешней авторизации администраторов через RADIUS
certificate.pem	сертификат для SSL
common.conf	конфигурационный файл (для некоторых ОС семейства UNIX)
dbexport.gz	экспорт базы данных (создается в процессе удаления Сервера Dr.Web командой drwcs.sh xmlexportdb)
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера Dr.Web
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub (имя может отличаться)	открытый ключ шифрования

Файл	Описание
`enterprise.key` (имя может отличаться)	лицензионный ключ Сервера Dr.Web. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера Dr.Web 13.0 отсутствует
`frontdoor.conf`	конфигурационный файл для утилиты дистанционной диагностики Сервера Dr.Web
`local.conf`	настройки журнала Сервера Dr.Web
`private-key.pem`	закрытый ключ RSA
`webmin.conf`	конфигурационный файл Центра управления
`*.dbs` `*.sqlite`	встроенная БД

При удалении Сервера Dr.Web версий 11 и 13 сохраняются следующие конфигурационные файлы:

Файл	Описание
`agent.key` (имя может отличаться)	лицензионный ключ Агента
`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
`certificate.pem`	сертификат для SSL
`common.conf`	конфигурационный файл (для некоторых ОС семейства UNIX)
`dbexport.gz`	экспорт базы данных (создается в процессе удаления Сервера Dr.Web командой `drwcs.sh xmlexportdb`)
`download.conf`	сетевые настройки для формирования инсталляционных пакетов Агента

Файл	Описание
drwcsd-certificate.pem	сертификат Сервера Dr.Web
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера Dr.Web
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub (имя может отличаться)	открытый ключ шифрования
enterprise.key (имя может отличаться)	лицензионный ключ Сервера Dr.Web. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера Dr.Web 13.0 отсутствует
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера Dr.Web
local.conf	настройки журнала Сервера Dr.Web
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления
yalocator.apikey	API-ключ для Расширения Yandex.Locator

При автоматическом обновлении, в каталог для резервного копирования сохраняются следующие файлы:

Для Сервера Dr.Web версии 10:

Файл	Описание
auth-ldap.xml	конфигурационный файл внешней авторизации администраторов через LDAP
auth-pam.xml	конфигурационный файл внешней авторизации администраторов через PAM
auth-radius.xml	конфигурационный файл внешней авторизации администраторов через RADIUS
db.backup.gz	экспорт базы данных (создается в процессе обновления Сервера Dr.Web командой drwcs.sh exportdb)

Для Сервера Dr.Web версий 11 и 13:

Файл	Описание
`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
`db.backup.gz`	экспорт базы данных (создается в процессе обновления Сервера Dr.Web командой `drwcs.sh exportdb`)

Если вы планируете использовать файлы конфигурации от Сервера Dr.Web версии 6, обратите внимание:

1. Лицензионный ключ Сервера Dr.Web более не используется (см. п. Лицензирование).
2. Встроенная база данных обновляется, а конфигурационный файл Сервера Dr.Web конвертируется средствами инсталлятора. Данные файлы не подлежат замене на автоматически сохраненные копии при переходе с Сервера Dr.Web версии 6.

Сохранение базы данных

Перед обновлением ПО Dr.Web Enterprise Security Suite рекомендуется выполнить резервное копирование базы данных.

Чтобы сохранить базу данных

1. Остановите Сервер Dr.Web.
2. Экспортируйте базу данных в файл:
   - Для ОС FreeBSD:
     - для Сервера Dr.Web до версии 13

       ```
       # /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
       ```

     - для Сервера Dr.Web, начиная с версии 13

```
# /usr/local/etc/rc.d/drwcsd modexecdb database-
export /var/tmp/esbase.es
```

- Для ОС Linux:
  - для Сервера Dr.Web до версии 13
    ```
    # /etc/init.d/drwcsd exportdb /var/tmp/esbase.es
    ```
  - для Сервера Dr.Web, начиная с версии 13
  - ```
    # /etc/init.d/drwcsd modexecdb database-
    export /var/tmp/esbase.es
    ```

Для Серверов Dr.Web, использующих внешнюю базу данных, рекомендуется использовать штатные средства, поставляемые вместе с базой данных.

Убедитесь, что экспорт базы данных Dr.Web Enterprise Security Suite завершился успешно. Отсутствие резервной копии БД не позволит восстановить Сервер Dr.Web в случае непредвиденных обстоятельств.

Автоматическое обновление

При обновлении Сервера Dr.Web с версии 10 до версии 13 (кроме Серверов Dr.Web, установленных под ОС **Linux** из пакетов `*.rpm.run` и `*.deb.run`) вместо удаления старой версии и установки новой версии Сервера Dr.Web возможно автоматическое пакетное обновление. Для этого запустите установку соответствующего пакета Сервера Dr.Web.

Обновление Сервера Dr.Web с версии 11 и в пределах версии 13 для одинаковых типов пакетов осуществляется автоматически для всех ОС семейства UNIX.

При этом конфигурационные файлы будут автоматически конвертированы и размещены в требуемых директориях. Также дополнительно сохраняются некоторые конфигурационные файлы в каталоге для резервного копирования.

Ручное обновление

Если произвести обновление Сервера Dr.Web версии 6.0.4 и старше поверх уже установленного пакета невозможно, необходимо удалить ПО Сервера Dr.Web более ранних версий, сохранив резервную копию, и установить ПО версии 13 на основе сохраненной резервной копии.

Чтобы обновить Сервер Dr.Web

1. Остановите Сервер Dr.Web.
2. Если вы хотите использовать в дальнейшем какие-либо файлы (помимо тех файлов, которые будут автоматически сохранены в процессе удаления Сервера Dr.Web на шаге **3**), создайте резервные копии этих файлов вручную, например, шаблонов отчетов и т. п.
    ```

3. Удалите ПО Сервера Dr.Web (см. п. Удаление Сервера Dr.Web для ОС семейства UNIX®). При этом будет автоматически предложено сохранить резервные копии файлов. Для этого достаточно ввести путь для сохранения или принять путь, предлагаемый по умолчанию.
4. Осуществите установку Сервера Dr.Web версии 13.0 согласно штатной процедуре установки (см. п. Установка Сервера Dr.Web для ОС семейства UNIX®) на основе резервной копии из шага **3**. Все сохраненные конфигурационный файлы и встроенная база данных (в случае использования встроенной БД) будут автоматически конвертированы для использования Сервером Dr.Web версии 13.0. Без автоматической конвертации использование базы данных (в случае использования встроенной БД) и некоторых конфигурационных файлов Сервера Dr.Web предыдущих версий невозможно.

   Если вы сохраняли какие-либо файлы вручную, разместите их в те же директории, где они находились в предыдущей версии Сервера Dr.Web.

   

   Для всех сохраненных от предыдущей версии Сервера Dr.Web файлов (см. шаг 4) необходимо установить в качестве владельца файлов пользователя, выбранного при установке новой версии Сервера Dr.Web (по умолчанию — **drwcs**).

5. Запустите Сервер Dr.Web.
6. Настройте обновление репозитория и обновите его полностью.

   

   После завершения обновлений Серверов Dr.Web антивирусной сети необходимо повторно задать настройки шифрования и сжатия у связанных Серверов Dr.Web (см. **Руководство администратора**, раздел Настройка связей между Серверами Dr.Web).

7.3. Обновление Агентов Dr.Web

Описание обновления Агентов после обновления ПО Сервера Dr.Web приведены для следующих вариантов:

1. Обновление Агентов Dr.Web для станций под ОС Windows,
2. Обновление Агентов Dr.Web для станций под ОС Android,
3. Обновление Агентов Dr.Web для станций под ОС Linux и macOS.

7.3.1. Обновление Агентов Dr.Web для станций под ОС Windows

Обновление Агентов, поставляемых с Dr.Web Enterprise Security Suite 10

Обновление Агентов, поставляемых с версией Dr.Web Enterprise Security Suite 10, осуществляется автоматически.

После автоматического обновления на станции выводится всплывающее оповещение о необходимости перезагрузки; в Центре управления в статусе станции отмечается необходимость перезагрузки после обновления. Для завершения обновления перезагрузите станцию локально или удаленно через Центр управления.

В случае подключения станции к Серверу Dr.Web через Прокси-сервер Dr.Web версии 10 или более ранней, перед обновлением Агента необходимо обновить Прокси-сервер до версии 13 или удалить Прокси-сервер.

Автоматическое обновление Агентов, поставляемых с Dr.Web Enterprise Security Suite 6

Для возможности автоматического обновления необходимо выполнение следующих условий:

1. Агенты должны быть установлены на компьютерах, работающих под ОС семейства Windows, поддерживаемых для установки Агентов для Dr.Web Enterprise Security Suite версии 13.0 (см. документ **Приложения**, п. Приложение А. Полный список поддерживаемых версий ОС).
2. При выполнении автоматического обновления возможны следующие варианты действий в зависимости от настроек Сервера Dr.Web:
   a) Автоматическое обновление осуществляется, если при обновлении Сервера Dr.Web были сохранены ключи шифрования и сетевые настройки предыдущего Сервера Dr.Web.
   b) При автоматическом обновлении необходима ручная настройка, если при обновлении Сервера Dr.Web были заданы новые ключи шифрования и сетевые настройки Сервера Dr.Web.

В процессе автоматического обновления обратите внимание на следующие особенности:

1. После удаления Агента оповещение о необходимости перезагрузки на станции не отображается. Администратор должен сам инициировать перезагрузку станции.
2. В промежутке между удалением старой версии Агента и установкой новой версии станции будут находиться без антивирусной защиты.
3. После обновления Агента без перезагрузки станции функционирование антивирусного ПО будет ограничено. При этом не обеспечивается полная антивирусная защита станции. Необходимо, чтобы пользователь выполнил перезагрузку станции по требованию Агента.

Автоматическое обновление Агентов осуществляется по следующей схеме:

1. При запуске обновления удаляется старая версия Агента.
2. Осуществляется перезагрузка станции вручную.

3. Осуществляется установка новой версии Агента. Для этого автоматически создается задание в расписании Сервера Dr.Web.
4. После завершения обновления Агента, станция автоматически подключается к Серверу Dr.Web. В разделе **Состояние** Центра управления для обновленной станции будет отображаться уведомление о необходимости перезагрузки. Необходимо выполнить перезагрузку станции.

Автоматическое обновление Агентов с ручной настройкой осуществляется по следующей схеме:

1. Вручную измените настройки подключения к новому Серверу Dr.Web и замените открытый ключ шифрования на станции.
2. После изменения настроек на станции и подключения станции к Серверу Dr.Web, запустится процесс обновления Агента.
3. При запуске обновления удаляется старая версия Агента.
4. Осуществляется перезагрузка станции вручную.
5. Осуществляется установка новой версии Агента. Для этого автоматически создается задание в расписании Сервера Dr.Web.
6. После завершения обновления Агента, станция автоматически подключается к Серверу Dr.Web. В разделе **Состояние** Центра управления для обновленной станции будет отображаться уведомление о необходимости перезагрузки. Необходимо выполнить перезагрузку станции.

Ручное обновление Агентов, поставляемых с Dr.Web Enterprise Security Suite 6

Если установка новой версии Агента при автоматическом обновлении по какой-либо причине была неуспешна, то дальнейшие попытки установки осуществляться не будут. На станции не будет установлено антивирусное ПО, и в Центре управления такая станция будет отображаться как отключенная.

В таком случае необходимо произвести установку Агента самостоятельно. При этом после установки нового Агента потребуется объединить новую и старую станции в Центре управления, в иерархическом списке антивирусной сети.

Если обновление не поддерживается

Если Агенты установлены на станциях с операционными системами, не поддерживаемыми для установки Агентов для Dr.Web Enterprise Security Suite версии 13.0, никакие действия по обновлению осуществляться не будут.

Агенты, установленные на неподдерживаемых ОС, не смогут получать обновления (в том числе обновления вирусных баз) от нового Сервера Dr.Web. Если требуется наличие Агентов

под неподдерживаемыми ОС, необходимо оставить в составе антивирусной сети Серверы Dr.Web предыдущих версий, к которым подключены эти Агенты. При этом Серверы Dr.Web версий 6 и Серверы Dr.Web версии 13.0 должны получать обновления независимо.

Рекомендации по обновлению Агентов, установленных на станциях, выполняющих важные функции ЛВС, приведены в документе **Приложения**, раздел Обновление Агентов на серверах ЛВС.

7.3.2. Обновление Агентов Dr.Web для станций под ОС Android

Dr.Web Enterprise Security Suite 13.0 поддерживает работу с Агентом Dr.Web для Android, начиная с версии 12.2.

Обновить Агент Dr.Web для Android на мобильных устройствах можно

1. Автоматически. Начиная с версии 12.6.4, Агент Dr.Web для Android обновляется самостоятельно, когда с Сервера Dr.Web приходит информация о наличии новой версии. Чтобы настроить автоматическое обновление, убедитесь, что в настройках репозитория Сервера Dr.Web в Центре управления указано обновлять продукт Dr.Web для Android (**Администрирование** → **Общая конфигурация репозитория** → **Инсталляционные пакеты Dr.Web** → **Корпоративные продукты Dr.Web**), а в настройках Dr.Web для Android в Центре управления установлен соответствующий флаг (**Антивирусная сеть** → группа станций или единичная станция под управлением ОС Android → **Dr.Web для Android** → **Обновления** → **Проверять наличие новой версии**).
2. Вручную, установив на мобильное устройство инсталляционный пакет новой версии. Для этого убедитесь, что в настройках репозитория Сервера Dr.Web в Центре управления указано обновлять продукт Dr.Web для Android (**Администрирование** → **Общая конфигурация репозитория** → **Инсталляционные пакеты Dr.Web** → **Корпоративные продукты Dr.Web**), после чего скачайте сформированный пакет в Центре управления в свойствах станции или на странице **Администрирование** → **Корпоративные продукты**.

Начиная с 12 версии у Сервера централизованной защиты есть возможность обновления приложения Dr.Web Security Space для Android, при условии, что данная версия приложения была установлена с Сервера централизованной защиты.

7.3.3. Обновление Агентов Dr.Web для станций под ОС Linux и macOS

Агенты, установленные на станциях под ОС семейства Linux и macOS, подключатся к Серверу Dr.Web версии 13.0, если выполняются следующие условия:

1. Агенты должны быть установлены на компьютерах, работающих под ОС, поддерживаемых для установки Агентов для Dr.Web Enterprise Security Suite версии 13.0 (см. документ **Приложения**, п. Приложение А. Полный список поддерживаемых версий ОС).
2. На станциях должны быть заданы ключи шифрования и сетевые настройки обновленного Сервера Dr.Web.

После подключения станций к обновленному Серверу Dr.Web:

1. На станциях осуществится обновление только вирусных баз. Автоматическое обновление самого антивирусного ПО не осуществляется.
2. Если на станциях установлена последняя версия ПО, то никаких действий более не требуется.
3. Если ПО на станциях устарело, скачайте установочный пакет новой версии Агента в Центре управления в свойствах станции или на инсталляционной странице. Обновите ПО станций вручную, как описано в соответствующих **Руководствах пользователя**.

7.4. Обновление Прокси-сервера Dr.Web

7.4.1. Обновление Прокси-сервера Dr.Web в процессе работы

Обновление Прокси-сервера может осуществляться автоматически в процессе работы.

Если Сервер Dr.Web под ОС семейства UNIX был ранее обновлен с версии 11.0 или 11.0.1, автоматическое обновление Прокси-сервера Dr.Web будет невозможно. Для снятия этого ограничения необходимо в разделе **Администрирование** → **Детальная конфигурация репозитория** → **Прокси-сервер Dr.Web** → **Синхронизация** в поле **Обновлять только следующие файлы** вручную удалить суффикс `^win.*`.

При изначальной установке Сервера Dr.Web версии 11.0.2 ограничения на автоматическое обновление Прокси-сервера не накладываются.

Расписание обновления зависит от настроек упреждающего кеширования Прокси-сервера:

1. 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.
2. 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.

Настроить автоматическое обновление вы можете одним их следующих способов:

- Через настройки Прокси-сервера в Центре управления управляющего Сервера Dr.Web, в разделе **Обновления**. Подробное описание приведено в документе **Руководство администратора**, в разделе Удаленная настройка Прокси-сервера.
- Через конфигурационный файл Прокси-сервера `drwcsd-proxy.conf`. Подробное описание приведено в документе **Приложения**, п. Приложение G4.

7.4.2. Обновление Прокси-сервера Dr.Web через инсталлятор

Конфигурационные файлы Прокси-сервера

Конфигурационные файлы Прокси-сервера версии 11 и старше:

Файл	Описание
`drwcsd-proxy.conf`	конфигурационный файл Прокси-сервера (см. документ **Приложения**, п. Приложение G4)
`drwcsd-proxy.auth`	идентификационные данные (ID и пароль) для доступа к Серверам Dr.Web
`drwcsd-proxy-trusted.list`	список доверенных сертификатов Серверов Dr.Web
`drwcsd-proxy-signed.list`	список подписанных сертификатов Прокси-сервера
`drwcsd-proxy.pri`	закрытый ключ шифрования Прокси-сервера

Обновление Прокси-сервера под ОС Windows

Обновление осуществляется автоматически средствами инсталлятора.

Чтобы обновить Прокси-сервер версии 11 и старше

1. Запустите файл дистрибутива Прокси-сервера.
2. Откроется окно, которое извещает о наличии установленного ПО Прокси-сервера предыдущей версии и предлагает обновление до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Upgrade**.
3. Откроется окно с информацией об удалении Прокси-сервера предыдущей версии. Для начала процесса удаления нажмите **Uninstall**.
4. После завершения удаления предыдущей версии Прокси-сервера начнется установка новой версии. Откроется окно с информацией о продукте. Нажмите кнопку **Next**.
5. В последующих шагах осуществляется настройка Прокси-сервера аналогично процессу Установки Прокси-сервера Dr.Web на основе конфигурационных файлов от предыдущей версии. Инсталлятор автоматически определяет каталог установки Прокси-сервера и расположение конфигурационных файлов от предыдущей установки. При необходимости вы можете изменять настройки, подхваченные из файлов, которые были автоматически найдены инсталлятором.
6. Для начала процесса установки Прокси-сервера нажмите кнопку **Install**.

Обновление Прокси-сервера под ОС семейства UNIX

Чтобы обновить Прокси-сервер версии 11.0 или более ранней

При обновлении Прокси-сервера осуществляется удаление конфигурационных файлов. При необходимости сохраните конфигурационные файлы вручную перед началом обновления.

1. Для запуска процесса обновления запустите файл дистрибутива Прокси-сервера: `./<файл_дистрибутива>.tar.gz.run`
2. После завершения обновления при необходимости перенесите вручную настройки из конфигурационных файлов, сохраненных перед началом обновления, в новые конфигурационные файлы.

Чтобы обновить Прокси-сервер версии 11.0.1

1. Для запуска процесса обновления запустите файл дистрибутива Прокси-сервера: `./<файл_дистрибутива>.tar.gz.run`
2. В процессе удаления предыдущей версии будут автоматически сохранены конфигурационные файлы Прокси-сервера.
3. В процессе обновления будет предложено использовать конфигурационные файлы от предыдущей установки Прокси-сервера, сохраненные при резервном копировании:
   - Чтобы использовать резервную копию, сохраненную по умолчанию в директории `/var/tmp/drwcsd-proxy`, нажмите ENTER.

- Чтобы использовать резервную копию из другой директории, введите путь до резервной копии вручную.
- Также вы можете установить Прокси-сервер с настройками по умолчанию, без использования резервной копии конфигурации от предыдущей установки. Для этого нажмите 0.

Предметный указатель

Предметный указатель