Dr.WEB

Enterprise Security Suite

Инструкция по развертыванию антивирусной сети

Dr.Web Enterprise Security Suite
Версия 12.0
Инструкция по развертыванию антивирусной сети
23.09.2021

ООО «Доктор Веб», Центральный офис в России

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

Сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

ООО «Доктор Веб»

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

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

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

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

Мы благодарны пользователям за поддержку решений семейства Dr.Web!

Содержание

Глава 1: Введение

1.1. Назначение документа

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

Документация администратора антивирусной сети состоит из следующих основных частей:

1. **Руководство по установке**
2. **Руководство администратора**
3. **Приложения**

Также дополнительно поставляются следующие Руководства:

1. **Руководства по управлению станциями**
2. **Руководства пользователя**
3. **Руководства по Web API**
4. **Руководство по базе данных Сервера Dr.Web**

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.

Обозначение	Комментарий
Антивирусная сеть	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
`C:\Windows\`	Наименования файлов и каталогов, фрагменты программного кода.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте Руководства могут употребляться без расшифровки следующие сокращения:

- ACL — списки контроля доступа (Access Control List),
- CDN — сеть доставки контента (Content Delivery Network),
- DFS — распределенная файловая система (Distributed File System),
- DNS — система доменных имен (Domain Name System),
- FQDN — полностью определенное имя домена (Fully Qualified Domain Name),
- GUI — графический пользовательский интерфейс (Graphical User Interface), GUI-версия программы — версия, использующая средства GUI,
- MIB — база управляющей информации (Management Information Base),
- MTU — максимальный размер полезного блока данных (Maximum Transmission Unit),
- NAP — Network Access Protection,
- TTL — время жизни пакета (Time To Live),
- UDS — доменный сокет UNIX (UNIX Domain Socket),
- БД, СУБД — База Данных, Система Управления Базами Данных,
- ВСО Dr.Web — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение.

Глава 2: Dr.Web Enterprise Security Suite

2.1. О продукте

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

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

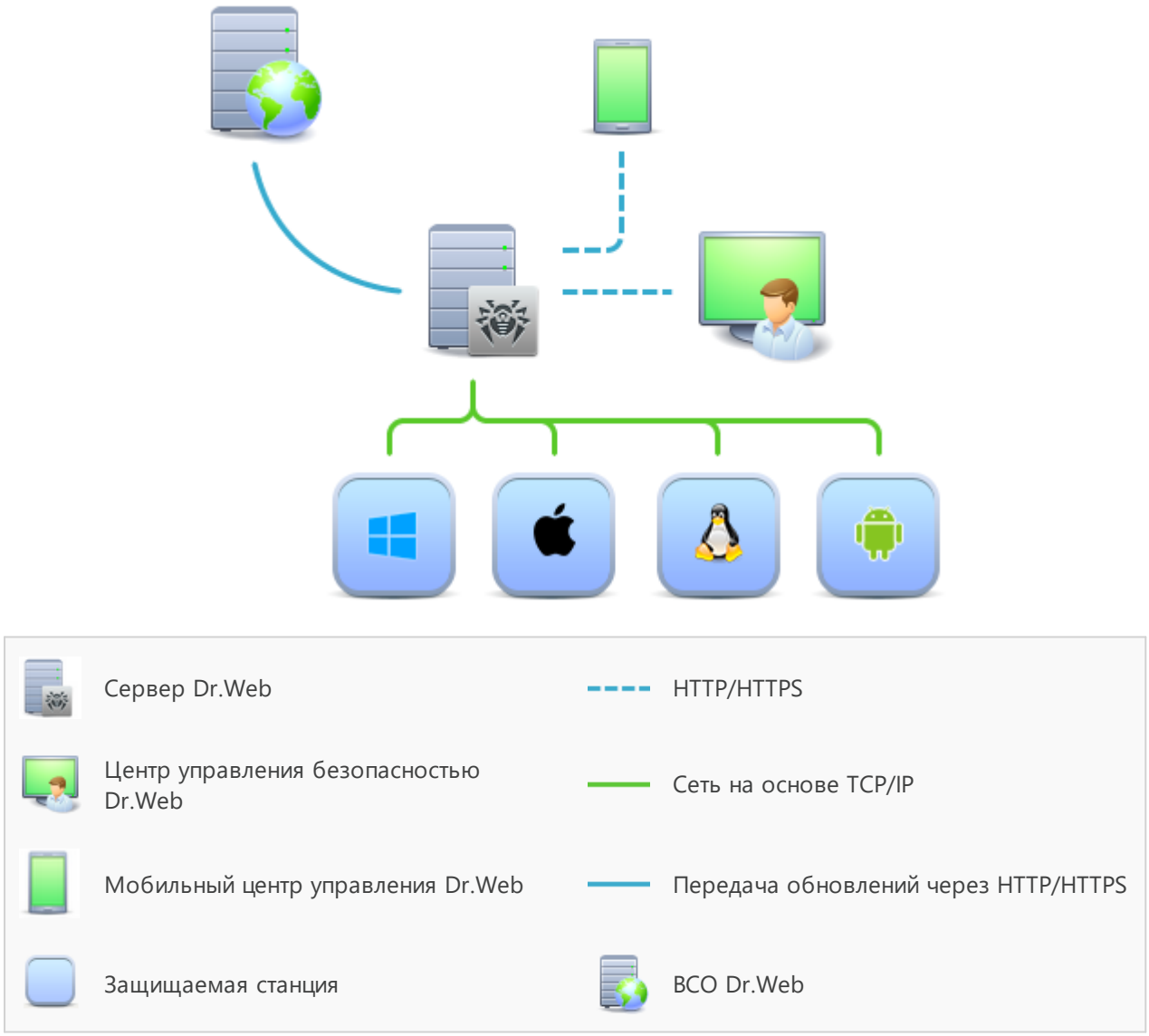

Рисунок 1-1. Логическая структура антивирусной сети

Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на компьютеры и мобильные устройства пользователей и

администраторов, а также на компьютеры, выполняющие функции серверов ЛВС. Компоненты антивирусной сети обмениваются информацией, используя сетевые протоколы TCP/IP. Антивирусное ПО на защищаемые станции возможно устанавливать (и впоследствии управлять ими) как через ЛВС, так и через интернет.

Сервер централизованной защиты

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

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

- ОС Windows,
- ОС семейства UNIX (Linux, FreeBSD).

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

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.

Центр управления централизованной защитой

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

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

- Windows Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,

- Google Chrome.

Список возможных вариантов использования приведен в п. Системные требования.

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

Мобильный центр управления централизованной защитой

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

Подключение Мобильного центра управления к Серверу осуществляется на основе учетных данных администратора антивирусной сети, в том числе по зашифрованному протоколу.

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

Защита станций сети

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

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

- ОС Windows,
- ОС семейства UNIX,
- macOS,
- ОС Android.

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

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

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

Обеспечение связи между компонентами антивирусной сети

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

Прокси-сервер Dr.Web

Прокси-сервер может опционально включаться в состав антивирусной сети. Основная задача Прокси-сервера — обеспечение связи Сервера и защищаемых станций в случае невозможности организации прямого доступа.

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.

Загрузчик репозитория

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

2.2. Системные требования

Сервер Dr.Web

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

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

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

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

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.

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

Мобильный центр управления Dr.Web

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

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

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.

- ОС семейства Linux:

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

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

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

- VMware;
- Hyper-V;
- Xen;
- KVM.

2.3. Комплект поставки

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

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

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

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

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

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

Консольная версия Загрузчика репозитория Dr.Web.

- `drweb-reploader-gui-windows-<`*разрядность*`>.exe`

  Графическая версия Загрузчика репозитория Dr.Web.

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

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

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

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

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

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

Глава 3: 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.

   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 **Руководстве по установке**, п. Установка Сервера Dr.Web.

   Вместе с Сервером устанавливается Центр управления безопасностью Dr.Web.

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

4. При необходимости установите и настройте Прокси-сервер. Описание приведено в **Руководстве по установке**, п. Установка Прокси-сервера.

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

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

   Центр управления доступен по адресу:

   `http://<Адрес_Сервера>:9080`

   или

   `https://<Адрес_Сервера>:9081`

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

   В диалоговом окне запроса на авторизацию введите регистрационные данные администратора. Данные администратора с полными правами по умолчанию:

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

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

6. Произведите начальную настройку Сервера (подробное описание настроек Сервера 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 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. Обновление может занять продолжительное время. Дождитесь окончания процесса обновления перед тем как продолжить дальнейшую настройку.

При установке Сервера версии 12 обновления продуктов репозитория **Агент Dr.Web для Android**, **Агент Dr.Web для UNIX** и **Прокси-сервер Dr.Web** по умолчанию загружаются с ВСО только при запросе этих продуктов со станций. Подробнее см. **Руководство администратора**, п. Детальная конфигурация репозитория.

Если ваш Сервер не подключен к интернету, и обновления загружаются вручную с другого Сервера или через Загрузчик репозитория, то перед тем как устанавливать или обновлять продукты, для которых 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. При наличии новой версии, обновите Сервер 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. 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 (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 и резервной копии.

7. 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.
8. Установите ПО Агента Dr.Web на рабочие станции.

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

- Если пользователи устанавливают антивирус самостоятельно, воспользуйтесь персональными инсталляционными пакетами, которые создаются через Центр управления отдельно для каждой станции. Данный тип пакетов также возможно отправить пользователям на электронную почту непосредственно из Центра управления. После установки подключение станций к Серверу осуществляется автоматически.
- 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 несколько станций одновременно (только для станций под ОС Windows) 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.
- Если необходимо уменьшить нагрузку на канал связи между Сервером и станциями в процессе установки, можете воспользоваться полным инсталлятором, который осуществляет установку Агента и компонентов защиты единовременно.
- Установка на станции под ОС Android, ОС Linux, macOS может выполняться локально по общим правилам. Также уже установленный автономный продукт может подключаться к Серверу 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.

9. Сразу после установки на компьютеры Агенты автоматически устанавливают соединение с Сервером. Авторизация антивирусных станций на Сервере 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 рабочие станции автоматически получают регистрацию при первом подключении к Серверу, и дополнительное подтверждение не требуется.
   b. При установке из инсталляторов и настройке ручного подтверждения доступа администратору необходимо вручную подтвердить новые рабочие станции для их регистрации на Сервере. При этом новые рабочие станции не подключаются автоматически, а помещаются Сервером в группу новичков.

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

Для завершения установки компонентов рабочей станции потребуется перезагрузка компьютера.

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

Приложение А. 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 **Руководстве по установке**, п. Установка Сервера Dr.Web.

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

Приложение В. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела https://support.drweb.com/;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу https://company.drweb.com/contacts/offices/.