Dr.WEB

Enterprise Security Suite

# Инструкция по развертыванию антивирусной сети

Жасағанын

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Защити созданное

Жасағаныңды қорға

Verteidige, was du erschaffen hast

Proteggi ciò che crei

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

**Товарные знаки**

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

**Ограничение ответственности**

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

**Dr.Web Enterprise Security Suite**
**Версия 10.01.0**
**Инструкция по развертыванию антивирусной сети**
**27.04.2017**

«Доктор Веб», Центральный офис в России

125040

Россия, Москва

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

Веб-сайт: http://www.drweb.com/

Телефон: +7 (495) 789-45-87

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

# «Доктор Веб»

«Доктор Веб» – российский разработчик средств информационной безопасности.

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

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

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

**Мы благодарны пользователям за поддержку решений семейства Dr.Web!**

# Содержание

# Глава 1: Dr.Web Enterprise Security Suite

## 1.1. Введение

### 1.1.1. Назначение документа

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 Dr.Web Enterprise Security Suite состоит из следующих основных частей:

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

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

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

### 1.1.2. Условные обозначения

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

**Таблица 1-1. Условные обозначения**

| **Обозначение** | **Комментарий** |
|---|---|
|  | Важное замечание или указание. |
|  | Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание. |
| *Антивирусная сеть* | Новый термин или акцент на термине в описаниях. |
| *<IP-address>* | Поля для замены функциональных названий фактическими значениями. |
| **Сохранить** | Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса. |
| CTRL | Обозначения клавиш клавиатуры. |
| `C:\Windows\` | Наименования файлов и каталогов, фрагменты программного кода. |
| Приложение А | Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы. |

## 1.2. О продукте

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

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

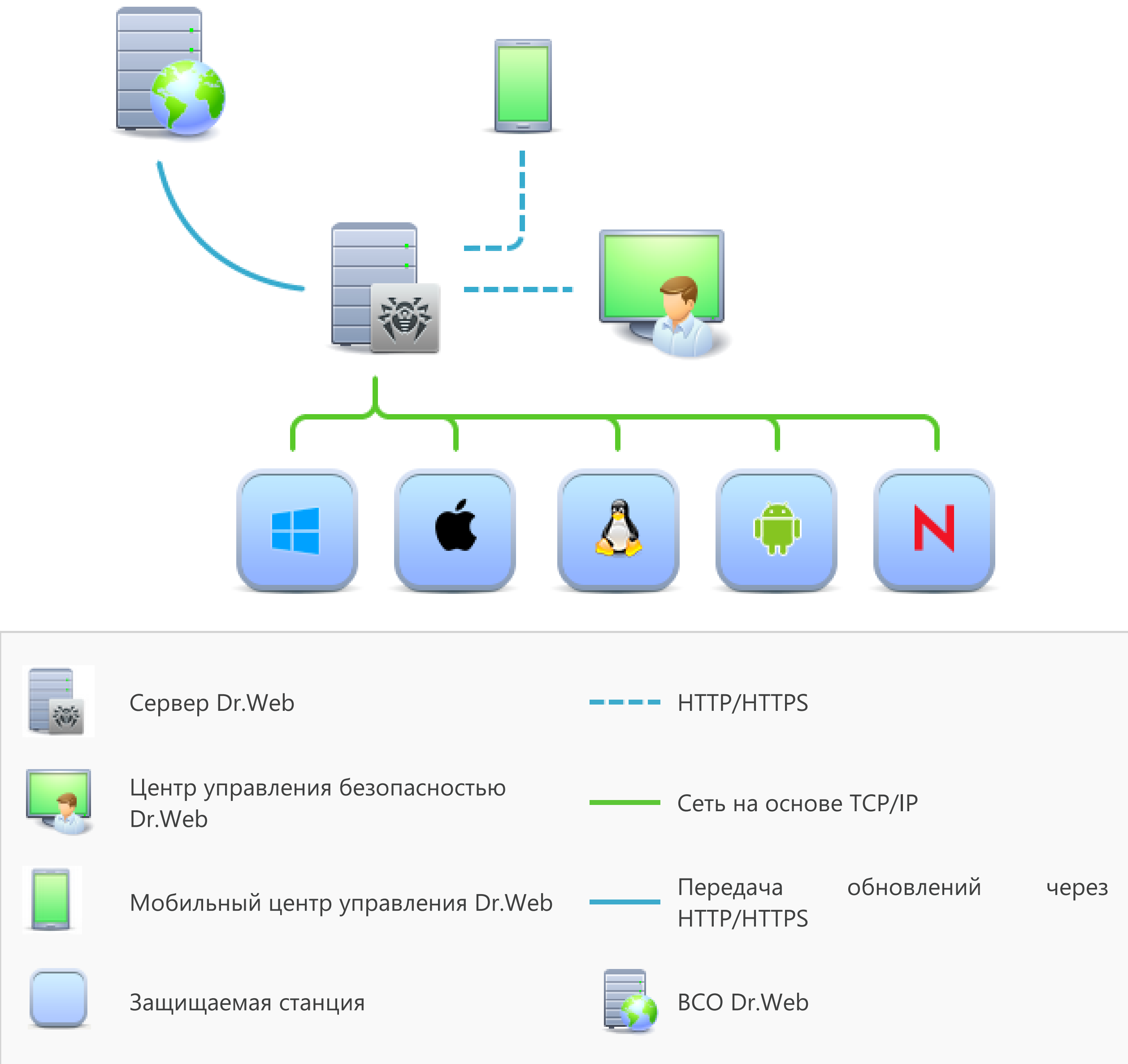


**Рисунок 1-1. Логическая структура антивирусной сети**

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

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

## Сервер централизованной защиты

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

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

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

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

## 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®,
- 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 ОС Android. Основные требования к приложению приведены в п. Системные требования.

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

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

## Защита станций сети

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

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

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

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

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

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

## 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.

# 1.3. Системные требования

**Для работы Сервера Dr.Web требуется:**

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

| Компонент | Требования |
|---|---|
| | ▫ ОС Linux;<br>▫ ОС FreeBSD;<br>▫ ОС Solaris x86.<br>• CPU V9 UltraSPARC IIIi и выше:<br>▫ ОС Solaris Sparc.<br>Полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А. |
| Оперативная память | • Минимальные требования: 1 ГБ.<br>• Рекомендуемые требования: 2 ГБ и выше. |
| Место на жестком диске | не менее 12 ГБ: до 8 ГБ для встроенной базы данных (каталог установки), до 4 ГБ в системном временном каталоге (для рабочих файлов). |

**Для работы Центра управления безопасностью Dr.Web требуется:**

a) Веб-браузер:

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

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

Установка расширения возможна на следующих веб-браузерах:

| Веб-браузер | Минимальная поддерживаемая версия | Максимальная поддерживаемая версия |
|---|---|---|
| Windows Internet Explorer | 8 | 11 |
| Mozilla Firefox | 25 | 50.0.1 |

| Веб-браузер | Минимальная поддерживаемая версия | Максимальная поддерживаемая версия |
|---|---|---|
| Google Chrome | 30 | 44.0.2403 |

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

**Для работы Мобильного центра управления Dr.Web требуется:**

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

| Операционная система | Требование | |
|---|---|---|
| | **Версия операционной системы** | **Устройство** |
| iOS | iOS® 7 и выше | Apple® iPhone®<br>Apple® iPad® |
| Android | Android 4.0 и выше | – |

**Для работы Агента Dr.Web и полного антивирусного пакета требуется:**

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

- ОС Windows:

| Компонент | Требование |
|---|---|
| Процессор | CPU с тактовой частотой 1 ГГц и выше. |
| Свободная оперативная память | Не менее 512 МБ. |
| Свободное место на жестком диске | 1 ГБ для исполняемых файлов + дополнительно для журналов работы и временных файлов. |

- ОС семейства Linux:

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

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

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

## 1.4. Комплект поставки

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

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

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

2. Для ОС Windows – в виде исполняемых файлов:

| Название файла | Компонент |
| --- | --- |
| `drweb-esuite-server-10.01.0-`*<сборка>*`-`*<версия_ОС>*`.exe` | Основной дистрибутив Сервера Dr.Web* |
| `drweb-esuite-extra-10.01.0-`*<сборка>*`-`*<версия_ОС>*`.exe` | Дополнительный дистрибутив Сервера Dr.Web |
| `drweb-esuite-proxy-10.01.0-`*<сборка>*`-`*<версия_ОС>*`.msi` | Прокси-сервер |
| `drweb-esuite-agent-activedirectory-10.01.0-`*<сборка>*`.msi` | Агент Dr.Web для Active Directory |
| `drweb-esuite-modify-ad-schema-10.01.0-`*<сборка>*`-`*<версия_ОС>*`.exe` | Утилита для модификации схемы Active Directory |
| `drweb-esuite-aduac-10.01.0-`*<сборка>*`-`*<версия_ОС>*`.msi` | Утилита для изменения атрибутов у объектов Active Directory |
| `drweb-esuite-napshv-10.01.0-`*<сборка>*`-`*<версия_ОС>*`.msi` | NAP Validator |
| `drweb-esuite-agent-full-11.00.0-`*<версия_сборки>*`-windows.exe` | Полный инсталлятор Агента Dr.Web. Также входит в состав |

| Название файла | Компонент |
|---|---|
| | дополнительного дистрибутива Сервера Dr.Web. |

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

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

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

# Глава 2: 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 требованием к этому компьютеру приведены в п. Системные требования.

   На все защищаемые станции, включая серверы ЛВС, устанавливается одна и та же версия Агента Dr.Web. Отличие составляет список устанавливаемых антивирусных компонентов, определяемый настройками на Сервере.

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

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

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

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

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

   Вместе с Сервером устанавливается Центр управления безопасностью Dr.Web.

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

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

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

   Центр управления доступен по адресу:

   `http://`<*Адрес_Сервера*>`:9080`

   или

   `https://`<*Адрес_Сервера*>`:9081`

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

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

   Имя администратора по умолчанию – **admin**.

   Пароль:

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

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

   При успешном подключении к Серверу откроется главное окно Центра управления (подробное описание см. в **Руководстве администратора**, в п. Центр управления безопасностью Dr.Web).
7. Произведите начальную настройку Сервера (подробное описание настроек Сервера приведено в **Руководстве администратора**, в Главе 8: Настройка Сервера Dr.Web):

   a. В разделе Менеджер лицензий добавьте один или несколько лицензионных ключей и распространите их на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера не был задан лицензионный ключ.

   b. В разделе Общая конфигурация репозитория задайте, какие компоненты антивирусной сети будут обновляться с ВСО Dr.Web. В разделе Состояние репозитория произведите обновление продуктов в репозитории Сервера. Обновление может занять продолжительное время. Дождитесь окончания процесса обновления перед тем как продолжить дальнейшую настройку.

   c. На странице **Администрирование** → **Сервер Dr.Web** приведена информация о версии Сервера. При наличии новой версии, обновите Сервер как описано в **Руко-**

**водстве 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 5: 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.

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

    a. При необходимости создайте пользовательские группы станций.

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

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

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

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

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

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

    > Для завершения установки компонентов рабочей станции потребуется перезагрузка компьютера.

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

# 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 http://products.drweb.com/register/, если иной адрес не указан в регистрационной карточке, прилагаемой к продукту. Зайдите на указанный сайт, заполните форму со сведениями о покупателе и введите в указанное поле регистрационный серийный номер (находится на регистрационной карточке). Архив с ключевыми файлами будет выслан по указанному вами адресу электронной почты. Вы также сможете загрузить ключевые файлы непосредственно с указанного сайта.
- Лицензионный ключевой файл может поставляться на отдельном носителе.

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

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

Подробная информация о принципах и особенностях лицензирования Dr.Web Enterprise Security Suite приведена в **Руководстве администратора**, в подразделах Главы 2. 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.ru/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу http://support.drweb.ru/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу http://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 http://support.drweb.ru/;
- 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 http://company.drweb.ru/contacts/offices/.