



Dr.WEB

Enterprise Security Suite

Инструкция по развертыванию антивирусной сети



© «Доктор Веб», 2025. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «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 ООО «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 13.0

Инструкция по развертыванию антивирусной сети

27.05.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 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	5
1.1. Назначение документа	5
1.2. Условные обозначения и сокращения	5
Глава 2: Dr.Web Enterprise Security Suite	7
2.1. О продукте	7
2.2. Системные требования	11
2.3. Комплект поставки	23
Глава 3: Создание антивирусной сети	26
Приложение А. Лицензирование	31
Приложение Б. Техническая поддержка	33



Глава 1: Введение

1.1. Назначение документа

Инструкция по разворачиванию 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. **Руководство 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, 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:

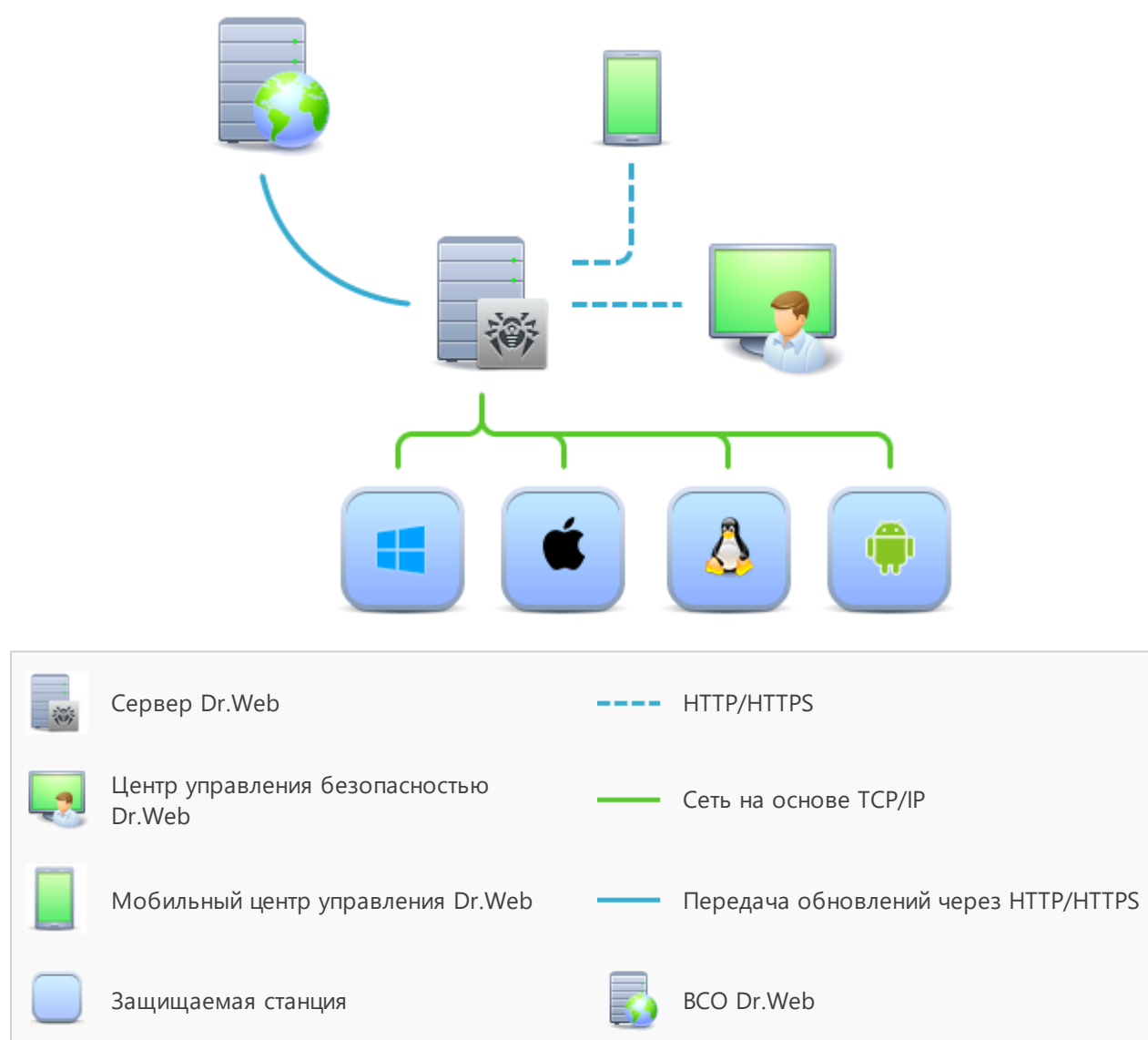
- БД, СУБД — База Данных, Система Управления Базами Данных,
- BCO Dr.Web — Всемирная Система Обновлений Dr.Web,
- ЛВС — Локальная Вычислительная Сеть,
- ОС — Операционная Система,
- ПО — Программное Обеспечение,
- ACL — списки контроля доступа (Access Control List),
- CDN — сеть доставки контента (Content Delivery Network),
- DFS — распределенная файловая система (Distributed File System),
- DN — отличительное имя, уникальный идентификатор записи в дереве LDAP (Distinguished Name),
- 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).

Глава 2: Dr.Web Enterprise Security Suite

2.1. О продукте

Dr.Web Enterprise Security Suite предназначен для организации единой и надежной комплексной антивирусной защиты 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.



Логическая структура антивирусной сети

Антивирусная сеть Dr.Web Enterprise Security Suite имеет архитектуру *клиент-сервер*. Ее компоненты устанавливаются на станции. В данном контексте термин "станция"



обозначает защищаемое устройство в антивирусной сети, на котором установлены Агент Dr.Web и антивирусный пакет и которое выступает в качестве клиента и взаимодействует с Сервером Dr.Web. В роли станции могут выступать компьютеры, виртуальные и мобильные устройства пользователей и администраторов, а также 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 разделе [Системные требования](#).

Кроссплатформенность серверного программного обеспечения позволяет использовать в качестве Сервера Dr.Web компьютер под управлением следующих операционных систем:

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



Защита компьютера, на который устанавливается Сервер Dr.Web, не отличается от защиты рабочих станций, описанной в подразделе [Защита станций сети](#), и может быть реализована посредством установки управляющего модуля (Агента Dr.Web) и антивирусного пакета защиты.

Сервер Dr.Web хранит дистрибутивы антивирусных пакетов для различных ОС защищаемых компьютеров, обновления вирусных баз и антивирусных пакетов, лицензионные ключи и настройки антивирусных пакетов защищаемых компьютеров. Сервер Dr.Web 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 Dr.Web и хранит статистические данные по событиям антивирусной сети, настройки самого Сервера Dr.Web, параметры защищаемых станций и антивирусных компонентов, устанавливаемых на защищаемые станции.



Центр управления централизованной защитой

Центр управления безопасностью Dr.Web (далее также — Центр управления) устанавливается автоматически вместе с Сервером Dr.Web и предоставляет веб-интерфейс для удаленного управления Сервером Dr.Web и антивирусной сетью путем редактирования настроек Сервера Dr.Web, а также настроек защищаемых компьютеров, хранящихся на Сервере Dr.Web и на защищаемых компьютерах.

Центр управления может быть открыт на любом компьютере, имеющем сетевой доступ к Серверу Dr.Web. Возможно полнофункциональное использование Центра управления в следующих браузерах:

- Windows Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,
- Opera,
- Safari,
- Google Chrome,
- Яндекс.Браузер.

Полный список поддерживаемых браузеров приведен в разделе [Системные требования](#).

Частью Центра управления безопасностью является веб-сервер, который устанавливается автоматически вместе с Сервером Dr.Web. 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. Основные требования к устройствам для работы с данным приложением приведены в разделе [Системные требования](#).

Мобильный центр управления соединяется с Сервером Dr.Web по зашифрованному протоколу и при работе использует учетные данные администратора антивирусной сети.

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 Dr.Web) 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 Dr.Web, а также отправляет на Сервер Dr.Web информацию об обнаруженных угрозах на защищаемом компьютере.

В случае недоступности Сервера Dr.Web 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 Dr.Web может опционально включаться в состав антивирусной сети. Основная задача Прокси-сервера Dr.Web — обеспечение связи Сервера Dr.Web 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 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. Загрузчик репозитория может использоваться для загрузки обновлений продуктов Dr.Web Enterprise Security Suite и для размещения обновлений на Сервере Dr.Web, не подключенном к интернету.

Сканирующий сервер Dr.Web

Сканирующий сервер Dr.Web поставляется в виде отдельного компонента, предназначенного 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 Dr.Web	Для связи антивирусных компонентов с Сервером Dr.Web и межсерверных связей
	UDP	входящие, исходящие	В том числе используется Прокси-сервером для установки соединения с клиентами
			Для работы Сканера Сети
139, 445	TCP	• исходящие для Сервера Dr.Web • входящие для Агента Dr.Web	Для удаленной установки Агента Dr.Web



Номера портов	Протоколы	Соединения	Назначение
	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		
18008	UDP	• входящие, исходящие для Сканирующего сервера • входящие, исходящие для виртуального Агента Dr.Web	Для обнаружения любого доступного Сканирующего сервера виртуальными Агентами Dr.Web с использованием механизма Discovery
7090	TCP	• входящие для Сканирующего сервера • исходящие для виртуального Агента Dr.Web	Для коммуникации виртуальных Агентов Dr.Web с конкретным Сканирующим сервером

Сервер Dr.Web

Параметр	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 <code>var\installers-cache</code> каталога установки Сервера Dr.Web; • до 5 ГБ для базы данных; • вне зависимости от места установки Сервера Dr.Web, на системном диске для ОС Windows или в <code>/var/tmp</code> 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



Параметр	Требования
	системном диске для хранения временных и рабочих файлов в зависимости от объема базы данных и настроек репозитория
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, • ECP Veil, • Rosa Virtualization 2.1, 3.0
Прочее	Для работы с БД Oracle требуется наличие библиотеки <code>Linux kernel AIO access library libaio</code>). Административные утилиты, доступные для скачивания через Центр управления, раздел Администрирование → Утилиты, должны запускаться на компьютере, соответствующем системным требованиям для Сервера Dr.Web



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

Сервер Dr.Web не может быть установлен на ту же станцию, что и Прокси-сервер Dr.Web.

Для установки на Альт Linux необходимо отключить SELinux.

Для установки на ОС семейства UNIX Сервера Dr.Web и Прокси-сервера Dr.Web требуется поддержка операционной системой системы инициализации SysVinit. Если ее нет, то необходимо установить соответствующий пакет.

Список поддерживаемых операционных систем:

Windows	UNIX
<i>Для 32-разрядных систем:</i> • Windows 7, • Windows 8, • Windows 8.1, • Windows 10. <i>Для 64-разрядных систем:</i> • Windows 7,	• Linux, при наличии библиотеки <code>glibc 2.13</code> или более поздней версии, • FreeBSD 11.3 и позднее. А также специальные версии дистрибутивов Linux: ▪ Astra Linux Common Edition (Опел) 2.12, ▪ Astra Linux Special Edition 1.6 (с кумулятивным патчем 20220829SE16), ▪ Astra Linux Special Edition 1.7 (с кумулятивным патчем 20221110SE17),



Windows	UNIX
• Windows 8, • Windows 8.1, • Windows 10, • Windows 11, • Windows Server 2008 R2, • Windows Server 2012, • Windows Server 2012 R2, • Windows Server 2016, • Windows Server 2019, • Windows Server 2022, • Windows Server 2025	▪ Astra Linux Special Edition 1.8, ▪ Альт 8 СП, ▪ Альт Рабочая станция 8, ▪ Альт Рабочая станция 9, ▪ Альт Сервер 8, ▪ Альт Сервер 9, ▪ Альт Сервер 10, ▪ Гослинукс IC6, ▪ РЕД ОС 7.3 МУРОМ, ▪ РЕД ОС 8. В ОС Альт 8 СП и Гослинукс IC6 работа с мандатными уровнями доступа не поддерживается. Для ОС Astra Linux установку следует осуществлять при запуске с уровнем целостности "Высокий".

Прокси-сервер Dr.Web

Параметр	Требования
Процессор	CPU с поддержкой инструкций SSE2 и тактовой частотой 1,3 ГГц и выше
Оперативная память	Не менее 1 ГБ
Место на жестком диске	Не менее 1 ГБ
Операционная система	Список операционных систем соответствует списку для Сервера Dr.Web



Прокси-сервер Dr.Web не может быть установлен на ту же станцию, что и Сервер Dr.Web.

Центр управления безопасностью Dr.Web

Параметр	Требования
Браузер	Один из: • 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,



	• Опера последней версии, • Safari последней версии, • Яндекс.Браузер последней версии
Разрешение экрана	Рекомендуемое разрешение экрана — 1280×1024
Прочее	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



Если в вашей организации используется обратный прокси-сервер (reverse proxy) для доступа к Центру управления безопасностью Dr.Web, для работы с ним требуются определенные настройки. С примерами настроек можно ознакомиться по следующим ссылкам:

Для Nginx:

<https://nginx.org/docs/http/websocket.html>

Для Apache:

https://httpd.apache.org/docs/2.4/mod/mod_proxy_wstunnel.html

<https://www.serverlab.ca/tutorials/linux/web-servers-linux/how-to-reverse-proxy-websockets-with-apache-2-4/>



Мобильный центр управления Dr.Web

Операционная система	Требования
iOS	• Apple iPhone: iOS 9 и более поздние версии, • Apple iPad: iOS 9–12
Android	Android 5.0–14

NAP Validator

Параметр	Требования
Операционная система	Операционные системы с поддержкой технологии Network Access Protection (NAP). Минимальные требования: • Для компьютера с настроенным сервером NAP: Windows Server 2008. • Для компьютера с установленным Агентом Dr.Web: Windows Server 2008 с пакетом обновлений SP2
Прочее	Прочие системные требования для NAP Validator совпадают с требованиями для Агента Dr.Web (см. ниже). Требования могут различаться в зависимости от операционной системы, на которую устанавливается антивирусное решение

Сканирующий сервер Dr.Web

Параметр	Требования
Процессор	Процессоры с архитектурой и системой команд Intel/AMD: 32-бит (IA-32, x86) и 64-бит (x86_64, x64, AMD64)
Оперативная память	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более)
Место на жестком диске	Не менее 1 ГБ свободного дискового пространства
Гипервизор	• VMware, • Hyper-V, • Xen, • KVM



Параметр	Требования
Операционная система	Linux, FreeBSD. Список поддерживаемых операционных систем аналогичен списку для антивирусного пакета для ОС UNIX
Сетевые подключения	Наличие сетевых подключений: • подключение к Серверу Dr.Web для обновления вирусных баз и баз встроенных фильтров; • подключение для обслуживания запросов от Виртуальных агентов

Агент Dr.Web и антивирусный пакет

Требования различаются в зависимости от операционной системы, на которую устанавливается антивирусное решение.



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, брандмауэры или программы для фильтрации веб-контента).

Windows

Параметр	Требования
Процессор	С поддержкой системы команд i686
Операционная система	Для 32-разрядных операционных систем: • Windows XP с пакетом обновлений SP2 или более поздними; • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7 с пакетом обновлений SP1 или более поздними; • Windows 8; • Windows 8.1; • Windows 10 22H2 или более ранняя; • Windows Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или более поздними. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7 с пакетом обновлений SP1 или более поздними; • Windows 8;



Параметр	Требования
	• Windows 8.1; • Windows 10 22H2 или более ранняя; • Windows 11 24H2 или более ранняя; • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2 с пакетом обновлений SP1 или более поздними; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022; • Windows Server 2025
Оперативная память	512 МБ и больше
Разрешение экрана	Рекомендуется не менее 1024 × 768
Поддержка виртуальных и облачных сред	Поддерживается функционирование программы в следующих средах: • VMware; • Hyper-V; • Xen; • KVM
Прочее	Для обновления вирусных баз Dr.Web и компонентов Dr.Web требуется подключение к серверу централизованной защиты или интернету в Мобильном режиме. Для подключаемого модуля Dr.Web для Microsoft Outlook необходим установленный клиент Microsoft Outlook из состава MS Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 с пакетом обновлений SP2; • Outlook 2013; • Outlook 2016; • Outlook 2019; • Outlook 2021



Для защиты файловой системы станций под управлением ОС Windows Enterprise multi-session (Windows Enterprise for Virtual Desktops) требуется лицензия, в состав которой входит компонент **SpIDer Guard для серверов Windows**.



Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой ПО на Windows Vista, Windows 7, Windows Server 2008 или Windows Server 2008 R2 необходимо убедиться, что система поддерживает алгоритм хеширования 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»](#).

UNIX

Параметр	Требования
Платформа	Поддерживаются процессоры следующих архитектур и систем команд: • Intel/AMD: 32-бит (<i>IA-32, x86</i>); 64-бит (<i>x86-64, x64, amd64</i>); • ARM64; • E2K (<i>Эльбрус</i>); • IBM POWER9, Power10 (<i>ppc64el</i>)
Оперативная память	Не менее 500 МБ свободной оперативной памяти (рекомендуется 1 ГБ и более)
Место на жестком диске	Не менее 2 ГБ свободного дискового пространства на томе, на котором размещаются каталоги устанавливаемого продукта
Операционная система	GNU/Linux (на основе ядра версии 2.6.37 или более поздней, использующая библиотеку <code>glibc</code> версии 2.13 или более поздней, систему инициализации <code>systemd</code> версии 209 или более позднюю), FreeBSD. Перечень поддерживаемых версий операционных систем приведен ниже. Операционная система должна поддерживать механизм аутентификации PAM
Прочее	Наличие сетевого подключения: • подключение к интернету для обновления вирусных баз и компонентов антивирусного продукта; • при работе в режиме централизованной защиты достаточно только подключения к используемому серверу в рамках локальной сети, доступ в интернет не требуется

Платформа	Поддерживаемые версии GNU/Linux
x86_64	• Astra Linux Common Edition (Орел) 2.12; • Astra Linux Special Edition 1.6 (с кумулятивным патчем 20200722SE16), 1.7, 1.8; • CentOS 7, 8; • Debian 9, 10, 11, 12; • Fedora 37, 38; • Red Hat Enterprise Linux 7, 8;



Платформа	Поддерживаемые версии GNU/Linux
	• SUSE Linux Enterprise Server 12 SP3; • Ubuntu 18.04, 20.04, 22.04, 24.04; • Альт 8 СП; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10; • Гослинукс IC6; • РЕД ОС 7.2 МУРОМ, РЕД ОС 7.3 МУРОМ, РЕД ОС 8
x86	• CentOS 7; • Debian 10; • Альт 8 СП; • Альт Рабочая станция 9, 10
ARM64	• Astra Linux Special Edition (Новороссийск) 4.7; • CentOS 7, 8; • Debian 11, 12; • Ubuntu 18.04; • Альт 8 СП; • Альт Рабочая станция 9, 10; • Альт Сервер 9, 10
E2K	• Astra Linux Special Edition (Ленинград) 8.1 (с кумулятивным патчем 20200429SE81); • Альт 8 СП; • Альт Рабочая станция 10; • Альт Сервер 10; • ОПО ВК Эльбрус-8.32 ТВГИ.00311-28; • Эльбрус-Д МЦСТ 1.4
ppc64el	• CentOS 8; • Ubuntu 20.04



В ОС Альт 8 СП, Эльбрус-Д МЦСТ 1.4 и Гослинукс IC6 работа с мандатными уровнями доступа не поддерживается.

Для прочих дистрибутивов Linux, соответствующих описанным требованиям, полная совместимость с приложением не гарантируется. При возникновении проблем с совместимостью с вашим дистрибутивом обратитесь в техническую поддержку: <https://support.drweb.com>.

Платформа	Поддерживаемые версии FreeBSD
x86	11, 12, 13, 14



Платформа	Поддерживаемые версии FreeBSD
x86_64	11, 12, 13, 14



Для ОС FreeBSD установка приложения возможна только из универсального пакета.

macOS

Параметр	Требования
Устройство	Мас под управлением операционной системы macOS. Мы не гарантируем работоспособность Dr.Web на компьютерах других марок
Место на жестком диске	2 ГБ
Операционная система	• OS X 10.11 El Capitan; • macOS 10.12 Sierra; • macOS 10.13 High Sierra; • macOS 10.14 Mojave; • macOS 10.15 Catalina; • macOS 11 Big Sur; • macOS 12 Monterey; • macOS 13 Ventura; • macOS 14 Sonoma; • macOS 15 Sequoia. Мы не гарантируем работоспособность Dr.Web на модифицированных операционных системах macOS и Hackintosh

ОС Android

Параметр	Требования
Операционная система	Android версии 4.4–15
Процессор	x86/x86-64/ARMv7/ARMv8/ARMv9
Свободная оперативная память	Не менее 512 МБ
Свободная основная память	Не менее 45 МБ (для хранения данных)
Разрешение экрана	Не менее 800×480



Параметр	Требования
Прочее	Интернет-соединение (для обновления вирусных баз)

Dr.Web Mail Security Suite (Microsoft Exchange Server)

Параметр	Требования
Оперативная память	512 МБ и больше
Место на жестком диске	1 ГБ и больше
Операционная система	• Windows Server 2008 x64 с установленным пакетом обновлений SP2; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022; • Windows Server 2025
Версия Microsoft Exchange Server	• Microsoft Exchange Server 2007 x64 с установленным пакетом обновлений SP1; • Microsoft Exchange Server 2010 x64 с установленным пакетом обновлений SP1; • Microsoft Exchange Server 2013 с установленным пакетом обновлений SP1 (дополнительно требуется установка Cumulative Update 5 или запуск скрипта Exchange2013-KB2938053-Fixit ); • Microsoft Exchange Server 2016 с установленным Cumulative Update 3 (или более поздняя версия); • Microsoft Exchange Server 2019

Dr.Web Mail Security Suite (IBM Lotus Domino Windows)

Параметр	Требования
Процессор	Совместимый с системой команд i686
Оперативная память	512 МБ или больше
Место на жестком диске	750 МБ или больше. Временные файлы, создаваемые в ходе установки, потребуют дополнительного места
Разрешение экрана	Рекомендуется не менее 1280 × 1024 с поддержкой не менее



Параметр	Требования
	256 цветов
Файловая система	NTFS или FAT32
Операционная система	Для 32-разрядных операционных систем: • Windows Server 2008, • Windows Server 2008 R2. Для 64-разрядных операционных систем: • Windows Server 2008, • Windows Server 2008 R2, • Windows Server 2012, • Windows Server 2012 R2, • Windows Server 2016, • Windows Server 2019, • Windows Server 2022
Прочее ПО	ПО Lotus: • IBM Lotus Domino для Windows версии 8.5 - 9.0.1, • IBM Lotus Notes для Windows версии 7.0.2 - 9.0.1, • IBM Domino для Windows 10.1, • IBM Notes для Windows 10.0, • HCL Domino для Windows 11.0, • HCL Notes для Windows 11.0. Браузеры для работы с веб-интерфейсом: • Internet Explorer 8 или более поздней версии, • Mozilla Firefox 3 или более поздней версии, • Opera 9 или более поздней версии

2.3. Комплект поставки

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

1. Для ОС семейства UNIX:

- `drweb-esuite-server-<версия_пакета>-<сборка>-<версия_ОС>.tar.gz.run`
Дистрибутив Сервера Dr.Web.
- `drweb-reloader-<ОС>-<разрядность>`
Консольная версия Загрузчика репозитория Dr.Web.



2. Для ОС Windows:

- `drweb-esuite-server-<версия_пакета>-<сборка>-<версия_ОС>.exe`
Дистрибутив Сервера Dr.Web.
- `drweb-<версия_пакета>-<сборка>-esuite-agent-full-windows.exe`
Полный инсталлятор Агента Dr.Web.
- `drweb-reloader-windows-<разрядность>.exe`
Консольная версия Загрузчика репозитория Dr.Web.
- `drweb-reloader-gui-windows-<разрядность>.exe`
Графическая версия Загрузчика репозитория Dr.Web.

В состав дистрибутива Сервера Dr.Web входят следующие компоненты:

- ПО Сервера Dr.Web для соответствующей операционной системы;
- 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 Mail Security Suite (IBM Lotus Domino Windows);
- Dr.Web Mail Security Suite (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: Создание антивирусной сети

Краткая инструкция по развертыванию антивирусной сети:

1. Составьте план структуры антивирусной сети, включите в него все защищаемые компьютеры, виртуальные машины 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 разделе [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 станциям. 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 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**, [Глава 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 Серверу Dr.Web. Описание настроек Агентов Dr.Web 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 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 Dr.Web. Описание приведено в **Руководстве по установке**, п. [Установка Прокси-сервера Dr.Web](#).
5. Если антивирусная сеть состоит из виртуальных машин, рекомендуется использовать Сканирующий сервер. Описание процедур установки и настройки приведено в **Руководстве по установке**, 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, NetBIOS 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 **Руководство по установке**, 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 10: 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 BCO Dr.Web. Если антивирусная сеть будет включать защищаемые станции под ОС Android, ОС Linux, macOS, необходимо загрузить соответствующие **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 прежде чем продолжить дальнейшую настройку.



При установке Сервера Dr.Web обновления продуктов репозитория **Вирусные базы для Android, Базы контент-фильтров для UNIX и Прокси-сервер Dr.Web** по умолчанию загружаются с BCO 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 (см. **Руководство администратора**, п. [Настройка сетевых соединений](#)).
 - 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 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 станции.

В **Руководстве по установке**, в разделе [Инсталляционные файлы](#) ознакомьтесь со списком предоставляемых файлов для установки Агента Dr.Web. Выберите подходящий для вас вариант установки, исходя из операционной системы станции, возможности удаленной установки, варианта задания настроек Сервера Dr.Web при установке Агента Dr.Web 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 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 Dr.Web и компонентов защиты одновременно.
- 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 Dr.Web автоматически устанавливают соединение с Сервером Dr.Web. Авторизация станций антивирусной сети на Сервере Dr.Web происходит в соответствии с выбранной вами политикой (см. **Руководство администратора**, п. [Политика подключения станций](#)):
 - а. При установке из инсталляционных пакетов, а также при настройке автоматического подтверждения на Сервере Dr.Web станции автоматически получают регистрацию при первом подключении к Серверу Dr.Web, и дополнительное подтверждение не требуется.
 - б. При установке из инсталляторов и настройке ручного подтверждения доступа администратору необходимо вручную подтвердить новые станции для их регистрации на Сервере Dr.Web. При этом новые 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](#)).



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.

Демонстрационный ключевой файл

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 [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 Б. 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:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу <https://download.drweb.com/doc/>.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. 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»:

1. Заполните веб-форму в соответствующей секции раздела <https://support.drweb.com/>.
2. 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/>.

