Dr.WEB®
с 1992 года

Установка на станцию только модуля Контроль приложений и Сканера Dr.Web в Dr.Web Enterprise Security Suite 12.0

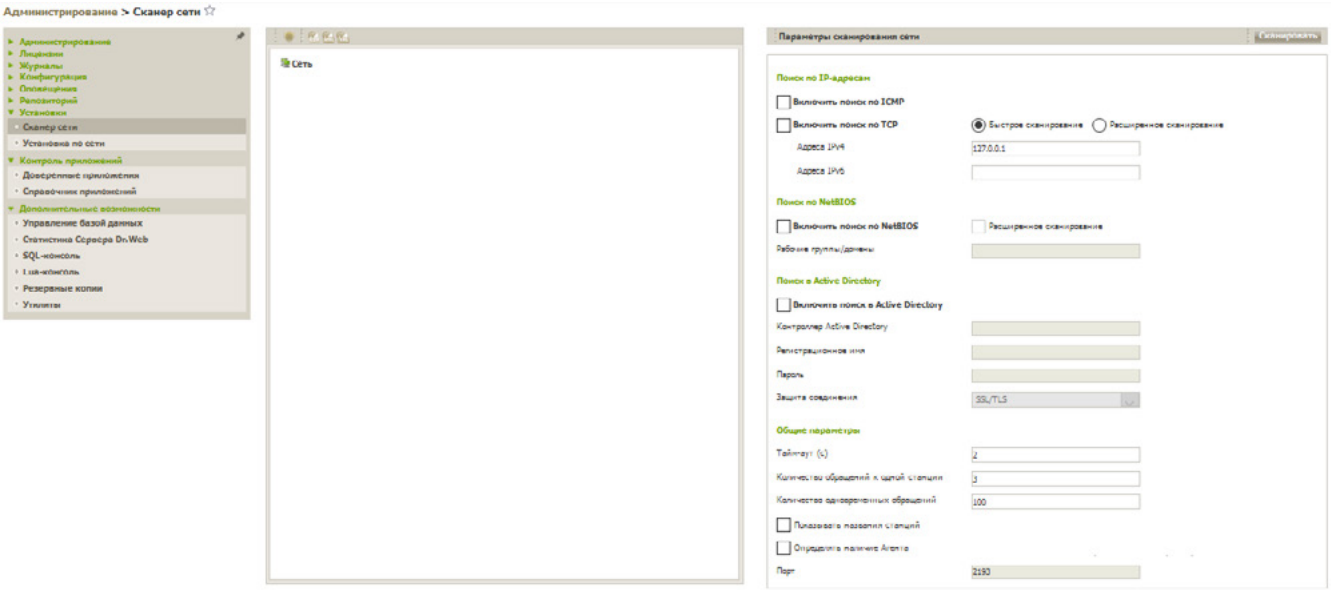
Dr.Web Enterprise Security Suite 12.0

Установка на станцию только модуля Контроль приложений и Сканера Dr.Web

В ряде случаев использование полноценной антивирусной защиты невозможно или нежелательно. Например, в случаях, когда защищаемый компьютер имеет достаточно слабую конфигурацию или для работы компьютера критично время срабатывания на определенные события. В этих условиях защита компьютера может осуществляться с помощью модулей **Контроль приложений** и **Антивирусный сканер**. Первый будет отвечать за контроль запуска только разрешенных приложений (белого списка), а с помощью второго будет проводиться периодическая антивирусная проверка

Рассмотрим процедуру установки, в ходе которой устанавливаются только эти два модуля. Для установки используем **Сканер сети**.

Переходим в раздел **Администрирование → Установка → Сканер сети**.



Сканер сети выполняет следующие действия:

- Сканирование (обзор) сети (в том числе по IP-адресам и NetBIOS) с целью обнаружения рабочих станций.
- Определение наличия Антивирусного **Агента** на станциях исходя из возможности обмена информацией (запрос-ответ) через порт udp/2193 (значение по умолчанию). Если на станции установлен запрет (например, посредством брандмауэра) приема пакетов на udp/2193, то Агент не может быть обнаружен, а следовательно, с точки зрения Сканера сети, считается, что Агент на станции не установлен.
- Поиск станций в Active Directory и LDAP, при этом поиск может осуществляться для станций, находящихся в разных доменах.

Внимание! Не рекомендуется запускать Сканер сети под ОС Windows 2000 и младше — обзор сети может быть неполным.

Параметр **Быстрое сканирование** определяет тип поиска станций в сети.
При включенной опции **Быстрое сканирование** осуществляется следующая последовательность действий.

1. На машины сети рассылаются ping-запросы.
2. Только для машин, ответивших на ping-запросы, осуществляется параллельный опрос с целью обнаружения Агентов.
3. Процедура определения наличия Агента осуществляется по общим правилам.

Ping-запросы могут блокироваться из-за сетевых политик (например, настроек брандмауэра), в этом случае нужно использовать альтернативный метод последовательного опроса всех станций на наличие агента. При обычном сканировании не рассылаются ping-запросы, а последовательно опрашиваются все станции на наличие Агента. Этот метод может использоваться в случае блокирования ping-запросов в связи с используемыми сетевыми политиками (если в сети есть станции, на которых заблокированы ping-запросы (так, например, Windows Vista и старше при установках сети типа **Общедоступная сеть**, **Домашняя сеть** или **Кафе** блокирует ping-запросы)). Метод может использоваться как дополнение к быстрому сканированию. Проверка в случае быстрого сканирования идет параллельно, в случае расширенного — последовательно, что влияет на скорость работы.

Максимальное время сканирования рассчитывается следующим образом:

- при обычном сканировании: *<N> * <timeout>*,
- при быстром сканировании: *<N>/40 + 2*<timeout>*,

где: *<N>* — количество станций, *<timeout>* — значение, задаваемое в поле **Тайм-аут**.

В поле Сети ведите параметр вашей сети/сетей в формате:

- через дефис (например, 10.4.0.1-10.4.0.10),
- через запятую и пробел (например, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
- с использованием префикса сети (например, 10.4.0.0/24).

При необходимости можно изменить номер порта и значение тайм-аута.

Нажмите **Сканировать**.

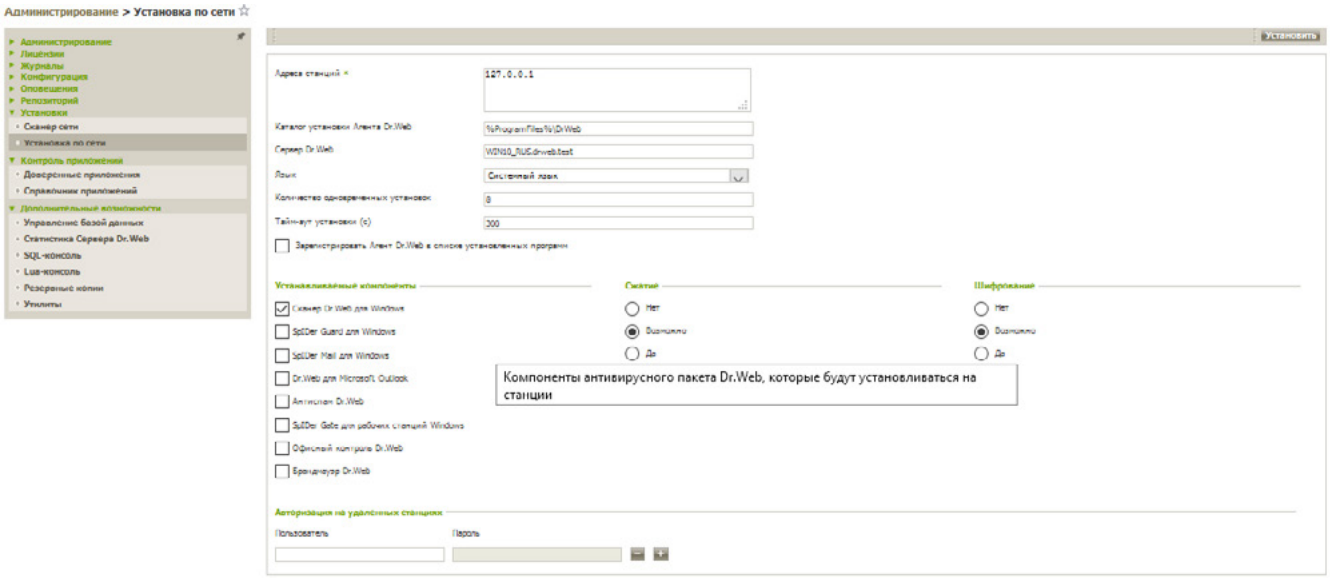
По завершении сканирования в окно будет выведен иерархический список компьютеров с указанием, на каких из них антивирусное ПО установлено, а на каких — нет. Все элементы каталога, соответствующие рабочим группам и отдельным станциям, помечаются различными значками, значение которых приведено в документации.

При необходимости разверните элементы каталога, соответствующие рабочим группам (доменам).

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

При нажатии на значок компонента станции, подключенной к данному Серверу, будет выведено окно настроек данного компонента.

Выберите одну или несколько незащищенных станций и нажмите .



В открывшемся окне выберите параметры установки, включая устанавливаемые компоненты.

В поле **Адреса станций** указывается IP-адрес компьютера (компьютеров), на которые будет устанавливаться антивирусное ПО. При установке ПО Агента сразу на несколько компьютеров вы можете указать несколько IP-адресов компьютеров в следующем формате:

- через дефис (например, 10.4.0.1-10.4.0.10),
- через запятую и пробел (например, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90),
- с использованием префикса сети (например, 10.4.0.0/24)

Вместо IP-адресов вы можете указать доменные имена компьютеров.

По умолчанию в поле **Сервер** отображается IP-адрес или DNS-имя **Сервера Dr.Web**, к которому подключен Центр управления. При необходимости укажите в данном поле адрес Сервера, с которого будет устанавливаться антивирусное ПО.

В разделе **Авторизация на удаленных станциях** вы можете указать параметры авторизации Агента на Сервере. Если не заполнены соответствующие поля, то параметры авторизации будут заданы автоматически.

В разделах **Шифрование** и **Сжатие** вы можете разрешить использование шифрования и сжатия трафика между Агентом и Сервером.

В дальнейшем эти параметры можно изменить в настройках **Агента** и свойствах станции.

Для установки отметьте только Сканер Dr.Web для Windows.

Нажмите **Установить**.

Внимание! Для удаленной установки на станцию серверу требуется доступ к директории admin$\TEMP станции. В случае отсутствия доступа установка завершиться не сможет. Доступ к данному ресурсу может быть, в частности, заблокирован функцией контроля учетных записей Windows (UAC).

Внимание! После изменения уровня параметров управления учетными записями требуется перезагрузка станции для их применения.

При настройках Сервера Dr.Web по умолчанию администратору необходимо вручную

подтвердить новые рабочие станции для их регистрации на Сервере (подробнее о политике подключения новых станций см. п. «Политика подключения новых станций»). При этом новые рабочие станции не подключаются автоматически, а помещаются Сервером в подгруппу New группы **Status**.

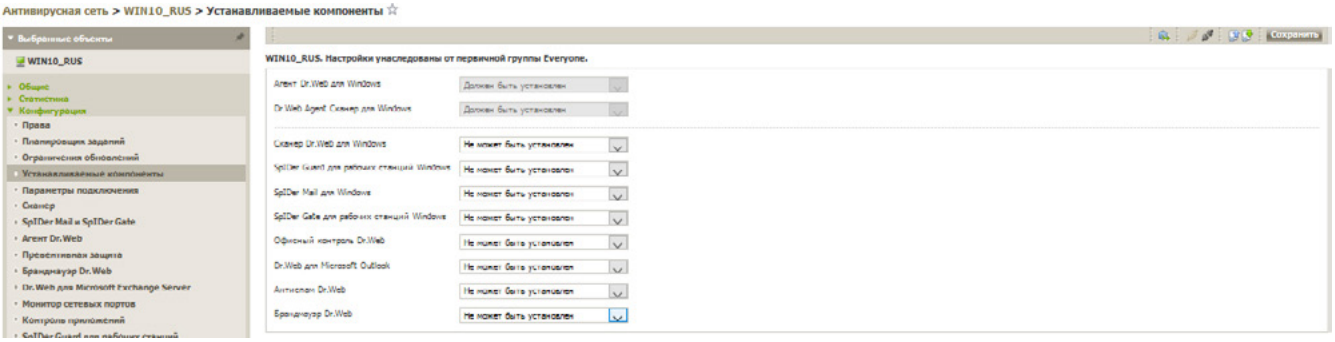
Поскольку в ходе установки происходят проверка целостности продукта, скачивание новых компонентов с Сервера, копирование компонентов в репозиторий и установка из репозитория с постапдейтом, процедура установки занимает некоторое время. В течение периода подгрузки всех необходимых файлов станция будет сообщать об ошибке обновления и находиться в соответствующей подгруппе (**Update Errors**) группы Status. Статус автоматически изменится после завершения установки. Не рекомендуется инициировать обновления всех компонентов / сбойных компонентов — это приведет только к показу сообщения **Операция инициирована**.

Для завершения установки некоторых компонентов антивирусной рабочей станции может потребоваться перезагрузка компьютера. В этом случае на фоне значка **Агента** на Панели задач появится восклицательный знак в желтом треугольнике или (для более ранних версий ОС Windows) программа установки вызовет соответствующее информационное окно.

В случае необходимости вы также можете удалить компоненты антивирусной защиты, оставив только модули Контроля приложений и Антивирусного сканера.

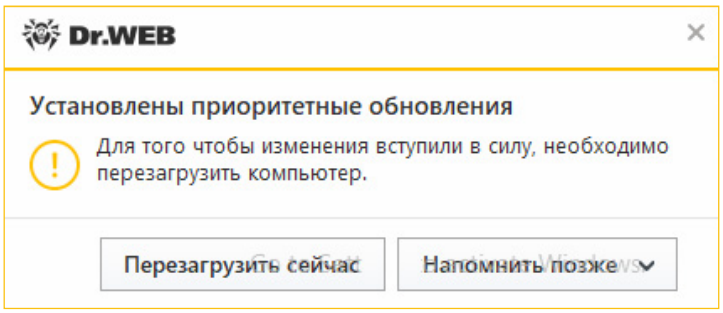
Для этого нужно выбрать нужные группы или отдельные станции и перейти в раздел **Устанавливаемые компоненты**.

Для всех доступных для удаления компонентов выбираем в выпадающих списках Н**е может быть установлен**.

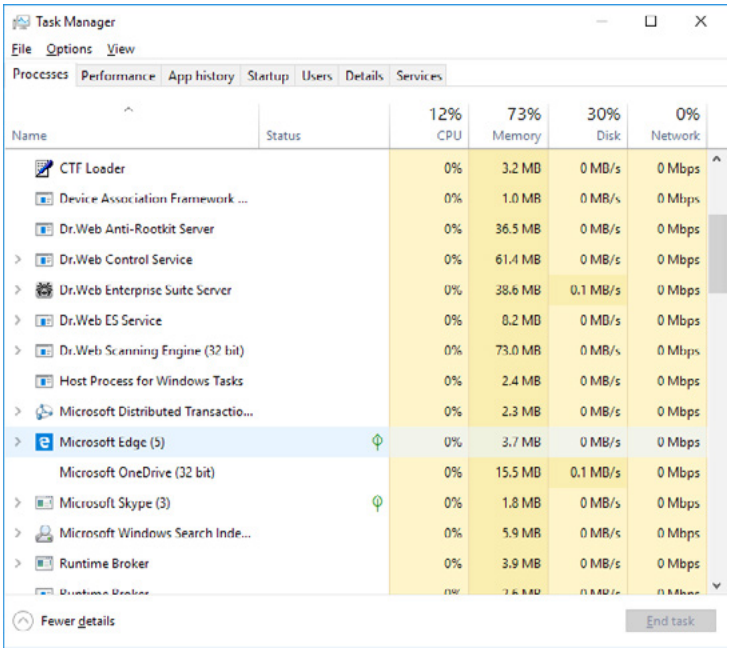


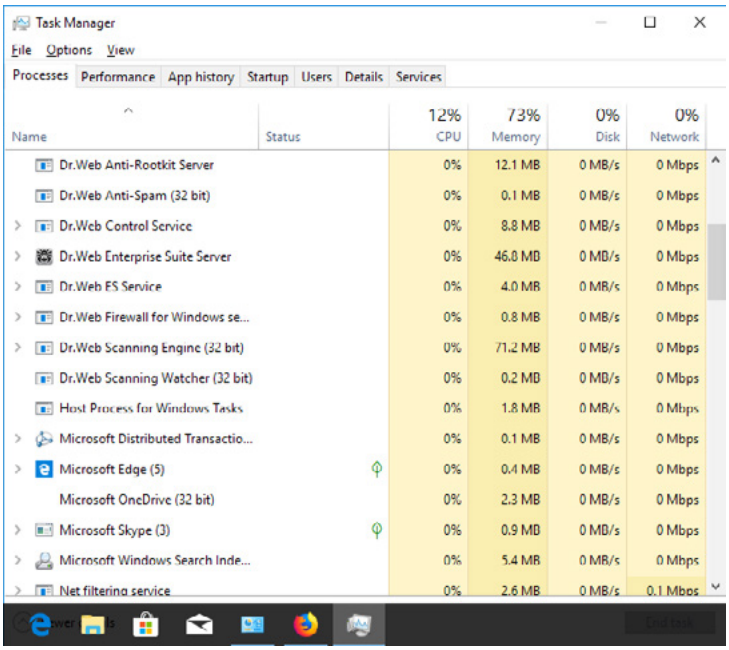
Нажимаем **Сохранить**.

Будет произведено удаление модулей и в случае необходимости выдан запрос на перезагрузку.



Если открыть после перезагрузки **Менеджер процессов**, то в списке процессов защиты будут находиться только процессы сканирующего модуля и антивирусного агента. Отметим, что в связи с отсутствием постоянной антивирусной защиты их наличие не оказывает влияния на быстродействие компьютера.





О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Его использование позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  - информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  - отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный) | Факс: +7 495 789–45–97
https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru