«Доктор Веб»

Dr.Web® Enterprise Security Suite

Версия 11.0

Методическое пособие
для практических занятий по курсу

DWCERT-002-11

«Централизованно управляемая защита антивирусной сети в масштабах предприятия на базе решения Dr.Web Enterprise Security Suite»

Версия программного обеспечения	11.0.1
Версия документа	2.0
Дата последнего изменения	3 декабря 2018 года

Содержание

1. Принятые обозначения

Курсив — адреса веб-ресурсов, названия файлов и текст команд для ввода в командную строку.

Полужирный — название экранных кнопок и ключевые моменты повествования.

Внимание! — важный момент, пренебрежение которым может привести к ошибкам или проблемам в работе.

Примечание — полезная информация, которую стоит принять к сведению для более эффективного использования программы Dr.Web ESS.

2. Основные термины

Dr.Web Enterprise Security Suite (Dr.Web ESS) — антивирусный комплекс Dr.Web, предназначенный для антивирусной защиты предприятий с сетевой инфраструктурой любой сложности.

Антивирусная сеть — совокупность компонентов вычислительной сети предприятия (ПК, сервера, мобильные устройства, терминалы и т. д.), на которые установлены компоненты Dr.Web ESS, имеющая один или несколько Серверов Dr.Web и централизованно управляемая с помощью Центра управления.

Dr.Web Enterprise Server (Сервер Dr.Web) — серверная часть ESS, осуществляющая управление всем остальными компонентами антивирусной сети.

Центр управления (ЦУ) — веб-интерфейс для работы с Сервером Dr.Web и управления антивирусной сетью.

Агент Dr.Web (Агент) — клиентская часть ESS, устанавливающаяся на ПК и мобильные устройства конечных пользователей, а также сервера ЛВС.

Защищаемый объект — любой объект информационной инфраструктуры предприятия, на который распространяется защита антивирусным комплексом Dr.Web ESS.

Мобильный Агент — мобильное устройство, входящее в антивирусную сеть, но работающее вне территории предприятия и принадлежащие сотрудникам компании или находящиеся у них во временном пользовании (служебные планшеты и т. д.).

Администратор антивирусной сети (Администратор) — сотрудник организации, управляющий антивирусной защитой всей компьютерной сети предприятия или ее части.

Вирусный инцидент — ситуация, связанная с проникновением на защищаемый объект вредоносного ПО и ответной реакцией антивируса на угрозу.

3. Введение

Данный документ содержит практические рекомендации и справочные сведения, позволяющие пользователю разобраться в тонкостях развертывания и настройки антивирусного комплекса Dr.Web ESS.

Изложенный в курсе материал рассчитан на сотрудников предприятий, выполняющих роль администратора антивирусной сети, которым для выполнения своих обязанностей также необходимо иметь полномочия системного администратора или действовать совместно с администратором локальной сети.

Целью документа является подготовка пользователя к сдаче профессионального экзамена компании «Доктор Веб» «Централизованно управляемая защита антивирусной сети в масштабах предприятия на базе решения Dr.Web Enterprise Security Suite», а также применение полученных знаний для построения системы информационной защиты.

Начальные разделы документа будут также полезны руководству организации, поскольку помогут принять решение о приобретении и установке системы комплексной антивирусной защиты Dr.Web ESS. Также в плане выбора будут полезны аргументы для директоров предприятий и технических руководителей.

Внимание! Сдача экзамена по курсу DWCERT-002 «Централизованно управляемая защита антивирусной сети в масштабах предприятия на базе решения Dr.Web Enterprise Security Suite» возможна только после сдачи экзамена по курсу DWCERT-070-3 «Антивирусная система защиты предприятия». В курсе DWCERT-070-3 содержится информация о современных методах распространения киберугроз, а также меры, позволяющие предотвратить заражение.

Примечания. Возможности Dr.Web Enterprise Security Suite по защите информационной инфраструктуры предприятия не ограничиваются функционалом, описанным в данном курсе. Ознакомиться со всеми возможностями Dr.Web ESS можно, прочитав документацию по интересующему вас компоненту продукта.

Внимание! Убедитесь, что вы используете актуальную версию данного документа! Проверить это можно на официальном веб-сайте компании «Доктор Веб» https://download.drweb.ru, а также в разделе https://training.drweb.ru/external.

4. Общие сведения о Dr.Web Enterprise Security Suite

4.1. Назначение Dr.Web Enterprise Security Suite

Dr.Web ESS предназначен для организации и управления комплексной информационной защитой компьютеров, устройств и веб-сервисов предприятия. При этом необязательно, чтобы компьютеры были объединены в локальную сеть и/или имели доступ в Интернет.

Основные задачи антивирусного комплекса:

- централизованная и удаленная (без необходимости непосредственного доступа персонала) установка и настройка антивирусных пакетов на защищаемые рабочие станции,
- централизованное обновление вирусных и антиспам-баз и программного обеспечения Dr.Web на защищаемых объектах,
- мониторинг безопасности сети и оперативная реакция на атаки и вирусные инциденты, а также контроль состояния антивирусных пакетов на всех защищаемых объектах,
- мониторинг программно-аппаратного обеспечения защищаемых станций и серверов на предмет возможных угроз и атак,
- централизованная настройка и контроль за соблюдением политик безопасности, принятых в организации.

4.2. Архитектура и состав антивирусной сети на основе Dr.Web ES

Dr.Web ES имеет архитектуру «клиент — сервер», использующую для внутрисетевого взаимодействия протокол TCP/IP. Клиентская часть представляет собой набор антивирусных Агентов, устанавливающихся на рабочие станции и другие защищаемые объекты (почтовые сервера, шлюзы и т. д.). Серверная часть состоит из Сервера Dr.Web и Центра управления (далее — ЦУ), устанавливающихся на ПК администратора антивирусной сети. В крупных сетях (более 1000 рабочих станций) может одновременно использоваться несколько Серверов Dr.Web.

В состав антивирусной сети входит несколько компонентов, выполняющих соответствующие им задачи.

4.2.1. Сервер Dr.Web

Dr.Web Enterprise Server (Сервер Dr.Web) — ключевой компонент защиты, устанавливающийся на компьютер администратора антивирусной сети. Сервер Dr.Web хранит всю информацию, необходимую для обеспечения информационной безопасности предприятия — дистрибутивы антивирусного ПО Dr.Web для всех типов применяющихся в сети ОС, репозиторий для обновления антивирусных баз, лицензионные ключевые файлы, а также установочные пакеты Агентов и наборы настроек безопасности для всех объектов сети. Там же ведется единый журнал событий антивирусной сети.

Антивирусная сеть должна иметь в своем составе хотя бы один Enterprise Сервер, в крупных сетях может использоваться несколько Enterprise Серверов.

Сервер Dr.Web выполняет следующие задачи:

- установка антивирусных пакетов (Агентов Dr.Web) на выбранный компьютер, группу компьютеров или иной компонент сети,
- мониторинг и поддержка в актуальном состоянии версий Агентов и вирусных баз на защищаемых рабочих станциях,
- обновление содержимого каталога централизованной установки и каталога обновлений,
- обновление вирусных баз и исполняемых файлов антивирусных пакетов, а также исполняемых файлов компонентов антивирусной сети на защищаемых компьютерах,
- сбор и протоколирование информации о работе антивирусных пакетов, передаваемой ему посредством ПО на защищаемых компьютерах (Агентов, подробнее см. ниже).

Протоколирование производится в общий журнал событий, реализованный в виде внешней или внутренней базы данных. Сохраняется следующая информация:

- версия антивирусных пакетов на защищаемых компьютерах,
- время и дата установки или обновления антивирусного ПО на Агентах с указанием версии,
- время и дата обновления вирусных баз с указанием их версий,
- версия ОС, установленной на защищаемых объектах, расположение системных каталогов, ключевая информация о системе,
- основные параметры аппаратного обеспечение защищаемого объекта (тип процессора, объем ОЗУ и т. д.),
- конфигурация и режимы работы Агентов Dr.Web (использование эвристических методов, список проверяемых типов файлов, действия при обнаружении компьютерных вирусов и т. п.),

- сведения о вирусных инцидентах и атаках, включая название обнаруженного вредоносного ПО, дату/время обнаружения, предпринятые действия, результат лечения и т. п.

Сервер Dr.Web оповещает администратора антивирусной сети о возникновении событий, связанных с работой антивирусной сети, посредством всплывающих уведомлений (в том числе PUSH-уведомлений, если используется Мобильный центр управления), по электронной почте и раздел уведомлений в Центре управления. Настройка событий, вызывающих направление сообщения, и прочих параметров оповещения описана в п. 7.11. «Оповещения».

Сервер Dr.Web можно установить на любом компьютере, соответствующем его системным требованиям, а не только на сервер ЛВС.

Для повышения надежности и эффективности антивирусной сети за счет распределения вычислительной нагрузки, в ней может одновременно использоваться несколько Серверов Dr.Web, один из которых будет являться основным, а остальные подчиненными. Подробнее о работе в сетях с несколькими Серверами Dr.Web изложено в документации и разделе 8.4. «Иерархия серверов» данного документа.

Управление Сервером Dr.Web осуществляется при помощи Центра управления — веб-сервиса, позволяющего удаленно управлять антивирусной сетью путем редактирования настроек всех элементов антивирусной сети. Центр управления устанавливается автоматически вместе с Сервером Dr.Web и представляет собой интерфейс для работы с ним.

Также одновременно с Сервером Dr.Web в автоматическом режиме устанавливается веб-сервер, являющийся частью Центра управления и обеспечивающий работу с Центром управления и клиентскими сетевыми соединениями.

4.2.2. Агент Dr.Web

Агент Dr.Web — это компонент, устанавливающийся на клиентские рабочие станции всех типов (с любой ОС и на любое устройство), а также серверы ЛВС, выполняющие различные задачи в вычислительной сети предприятия. Агент непосредственно отвечает за антивирусную защиту станции, его работой может управлять как администратор антивирусной сети с помощью Центра управления, так и пользователь ПК, где установлен Агент. При этом права пользователя по настройке Агента регламентируются также через ЦУ и могут быть сильно ограничены.

Для каждой ОС на Сервере Dr.Web создается дистрибутив Агента соответствующего типа. Таким образом даже если в сети используются рабочие станции с разными ОС (включая мобильные) — на все из них будут установлены соответствующие Агенты, и даже сложная по инфраструктуре сеть получит максимально простую в управлении антивирусную сеть. Администратор через Центр управления может полностью удаленно управлять действиями Агентов, как определяя стратегию антивирусной защиты, так и оперативно реагируя на произошедший вирусный инцидент.

Агент Dr.Web выполняет следующие функции:

- антивирусная защита станции, выполнение всех необходимых действий для предотвращения или устранения последствий вирусной атаки в автоматическом режиме или под управлением администратора антивирусной сети;
- выполнение заданий, получаемых от Сервера Dr.Web, таких как установка и обновление антивирусного ПО и вирусных баз, запуск сканирования и т. п.;

- отправка отч етов о работе и возникновении определенных событий (перечень настраивается администратором через ЦУ) на Сервер Dr.Web.

Хотя работа Агента подразумевает постоянное взаимодействие с Сервером Dr.Web, в случае временного отключения рабочей станции от антивирусной сети Агент использует локальную копию настроек и антивирусная защита на рабочей станции сохраняет свою функциональность (в течение срока, не превышающего срок действия пользовательской лицензии), однако обновление вирусных баз и ПО не производится.

Каждый Агент, подключенный к Серверу Dr.Web, входит в состав одной или нескольких зарегистрированных групп (подробнее см. п. 7.5. Группы станций и их использование. Предустановленные группы). Передача информации между Агентом и Сервером осуществляется по протоколу, используемому в локальной сети, как правило — TCP/IP, реже — NetBIOS.

Запущенный Агент в среде ОС Windows выводит в панель задач значок  . Через контекстное меню этого значка доступны некоторые функции управления антивирусной защитой, точный перечень которых зависит от конфигурации данной рабочей станции, заданной в ЦУ.

Вид значка зависит от того, установлено ли соединение рабочей станции с Сервером, и от других параметров. Возможные варианты и соответствующие им состояния компонентов описаны в разделе Знакомство с Агентом Dr.Web.

Компоненты Антивируса, входящие в состав Агента Dr.Web для всех ОС:

- *Dr.Web Сканер*. Компонент проверяет рабочую станцию на наличие вредоносного ПО (в том числе руткитов) по запросу пользователя, в соответствии с расписанием или по команде администратора антивирусной сети. Настройки сканера задаются через групповые или персональные настройки станции в ЦУ.
- *Страж SpIDer Guard* (файловый монитор). Постоянно находящийся в памяти ПК «сторож», проверяющий «на лету» все открываемые файлы на сменных дисках и открываемые на запись файлы на жестких дисках. Также SpIDer Guard отслеживает действия запущенных процессов и при обнаружении действий, характерных для вирусов, блокирует эти процессы с выводом соответствующего сообщения пользователю и отправкой информации в ЦУ. Присутствует во в сех типах Агентов, кроме Агент для Android.
- *HTTP-страж SpIDer Gate.* Постоянно находится в памяти компьютера и перехватывает все обращения к веб-сайтам по протоколу HTTP. Компонент нейтрализует угрозы в HTTP-трафике (в том числе отправляемых или получаемых файлах), а также блокирует доступ к подозрительным и инфицированным ресурсам.
- *Карантин.* Изолированное хранилище для зараженных и подозрительных файлов, куда они могут быть помещены для последующего анализа или передачи в службу поддержки компании «Доктор Веб».

Дополнительные компоненты:

Для ОС Windows:

- *SelfPROtect.* Обеспечивает защиту файлов и каталогов Агента от несанкционированного или ненамеренного удаления либо модификации пользователем или вредоносным ПО. При включенной системе самозащиты доступ этим ресурсам имеют только компоненты Dr.Web. Самозащита доступна только для ОС Windows.

- *Почтовый сторож SpIDer Mail* (почтовый монитор). Постоянно находится в памяти ПК и перехватывает обращения всех почтовых клиентов к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP, проверяет почту до ее получения почтовой программой.
- *Dr.Web Офисный контроль*. Постоянно находится в памяти компьютера и, при наличии соответствующих настроек, управляет доступом к сетевым и указанным локальным ресурсам. В частности, компонент позволяет контролировать доступ к веб-сайтам, разрешая или запрещая пользователям посещать определенные узлы сети Интернет, запрещает служащим доступ к нежелательной информации.
- *Сетевой экран Брандмауэр Dr.Web.* Предназначен для защиты компьютера от несанкционированного доступа извне и предотвращения утечки важных данных по сети Интернет. Компонент позволяет контролировать подключение и передачу данных по сети Интернет и блокировать подозрительные соединения на уровне пакетов и приложений.
- *Превентивная защита.* Предотвращение потенциальных угроз безопасности. Контроль доступа к критическим объектам операционной системы, контроль за загрузкой драйверов, автоматическим запуском программ и работой системных служб, а также отслеживание запущенных процессов и их блокировка в случае обнаружения вирусной активности.

Для ОС Linux:

- *Консольный сканер (управляется только на станции).* Используется для запуска из командной строки ОС проверки объектов файловой системы, активных процессов, а также удаленной проверки узлов сети на наличие угроз.
- *File Checker.* Используется Сканером, Консольным сканером, SpIDer Guard и SpIDer Gate для проверки файлов и управления Карантином.
- *Scanning Engine.* Используется для антивирусной проверки и управления вирусными базами.
- *Dr.Web ConfigD.* Координирует работу всех компонентов Dr.Web для Linux.

Для ОС Android:

- *Фильтр звонков и SMS.* Позволяет блокировать нежелательные сообщения и звонки, например рекламные рассылки, а также звонки и сообщения с неизвестных номеров.
- *Антивор.* Обнаружение местоположения или оперативная блокировка функций мобильного устройства в случае его утери или кражи.
- *URL-фильтр.* Позволяет оградить пользователя мобильного устройства от нежелательных интернет-ресурсов.
- *Брандмауэр (настройки доступны только на мобильном устройстве).* Защита мобильного устройства от несанкционированного доступа извне и предотвращение утечки важных данных по сети. Контроль подключения и передачи данных по сети Интернет и блокировка подозрительных соединений на уровне пакетов и приложений.
- *Аудитор безопасности (настройки доступны только на мобильном устройстве).* Диагностика и анализ безопасности мобильного устройства, устранение выявленных проблем и уязвимостей.
- *Фильтр приложений.* Запрет запуска на мобильном устройстве тех приложений, которые не включены в список разрешенных администратором.

4.2.3. Дополнительные компоненты

- *Прокси-сервер.* Этот компонент может опционально включаться в состав антивирусной сети. Основная задача Прокси-сервера — обеспечение связи Enterprise Сервера и Агентов в случае невозможности организации прямого доступа, например если

Enterprise Сервер и Агенты расположены в различных сетях, между которыми отсутствует маршрутизация пакетов. За счет использования функции кэширования также может быть обеспечено уменьшение сетевого трафика и времени получения обновлений Агентами.

- *NAP Validator.* Позволяет использовать технологию Microsoft Network Access Protection (NAP) для проверки работоспособности ПО защищаемых рабочих станций на основе соответствия политикам.

4.3. Системные требования

Для установки и функционирования Dr.Web Enterprise Security Suite требуется:

- чтобы Сервер Dr.Web был установлен на компьютер, имеющий доступ в Интернет, для автоматического получения обновлений с серверов ВСО (Всемирной системы обновления) Dr.Web;

Внимание! Допускается возможность распространения обновлений иным способом на Серверы, не подключенные к Интернету. В частности, при многосерверной конфигурации антивирусной сети возможно получение обновлений с ВСО только одним из Серверов с последующим ра спространением на другие Серверы, либо использование дополнительной утилиты Загрузчик репозитория Dr.Web для загрузки обновлений с ВСО через Интернет с последующим распространением на Серверы.

- чтобы компьютеры антивирусной сети имели доступ к Серверу Dr.Web либо Прокси-серверу;
- для совместной работы антивирусных компонентов на используемых компьютерах должны быть открыты следующие порты:

Номера портов	Протоколы	Направление соединений	Назначение
2193	TCP	•входящие, исходящие для Сервера и Прокси-сервера •исходящие для Агента	Для связи антивирусных компонентов с Сервером и межсерверных связей. В том числе используется Прокси-сервером для установки соединения с клиентами.
	UDP	•входящие, исходящие	Для работы Сканера Сети.
139, 445	TCP	•входящие для Сервера •входящие, исходящие для Агента •исходящие для компьютера, на котором открывается Центр управления	Для работы Сетевого инсталлятора.
	UDP	входящие, исходящие	
9080	HTTP	•входящие для Сервера •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.
80	HTTP	•исходящие	Для получения обновлений с ВСО.
443	HTTPS		

Компьютер, на который будет установлен Сервер Dr.Web, должен соответствовать следующим требованиям:

Компонент	**Требования**
Процессор	CPU с поддержкой инструкций SSE2 и тактовой частотой 1,3 ГГц и выше.
Оперативная память	•Минимальные требования: 1 ГБ. •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). В зависимости от настроек Сервера, может потребоваться дополнительное место для хранения временных файлов, например для хранения персональных инсталляционных пакетов Агентов (примерно 17 МБ каждый) в подкаталоге var\installers-cache каталога установки Сервера Dr.Web. **Внимание!** При установке Сервера необходимо, чтобы на системном диске для ОС Windows или в /var/tmp для ОС семейства UNIX (или в другой директории для временных файлов, если она переопределена), вне зависимости от места установки самого Сервера, было не менее 4,3 ГБ для основного дистрибутива и 2,5 ГБ для дополнительного дистрибутива для запуска инсталлятора и распаковки временных файлов.
Операционная система	•Windows; •Linux; •FreeBSD. Полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А.
Прочее	При установке Сервера Dr.Web для ОС семейства UNIX требуется наличие библиотек: lsb версии 3 и старше, glibc версии 2.7 и старше. Для работы с БД **Oracle** требуется наличие библиотеки Linux kernel AIO access library (libaio). Дополнительно под ОС **FreeBSD** требуется наличие библиотеки compat-8x.

Использование внутренней БД допустимо при подключении к Серверу не более 200–300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен **Enterprise Сервер**, и нагрузка по прочим задачам, выполняемым на данном компьютере, — возможно подключение до 1000 станций. В противном случае необходимо использовать внешнюю БД.

При использовании внешней БД и подключении к Серверу более 10 000 станций рекомендуется выполнение следующих минимальных требований:

- процессор с частотой 3 ГГц,
- оперативная память — от 4 ГБ для **Enterprise Сервера**, от 8 ГБ — для сервера БД,
- ОС семейства UNIX.

Компьютеры, на которые устанавливается Прокси-сервер, должны удовлетворять следующим требованиям:

Компонент	**Требование**
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	•Windows; •Linux; •FreeBSD. Полный список поддерживаемых ОС приведен в документе **Приложения**, в Приложении А.
Прочее	При установке Прокси-сервера для ОС семейства UNIX требуется наличие библиотек: lsb версии 3 и старше. Дополнительно под ОС **FreeBSD** требуется наличие библиотеки compat-8x.

Для работы Центра управления безопасностью Dr.Web требуется:

a) Веб-браузер:

Веб-браузер	**Поддержка**
Windows Internet Explorer 11	Поддерживается.
Microsoft Edge 0.10 и выше	
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	

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 на компьютер, в названии которого присутствует символ "_" (подчеркивание), работа с Сервером 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 флажок **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.

b) Рекомендуемое разрешение экрана для работы с Центром управления 1280 × 1024 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® Apple® iPad®
Android	Android 4.0 и выше	–

Для работы NAP требуется:

Для сервера — ОС Microsoft® Windows Server® 2008

Для агентов — ОС Windows Vista, ОС Windows Server 2008

Компьютер, на который устанавливаются Dr.Web Agent и полный антивирусный пакет Enterprise Security Suite, должен удовлетворять следующим требованиям:

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.
Прочее	1. Для корректной работы контекстной справки **Агент Dr.Web для Windows** необходимо наличие Windows® Internet Explorer® 6.0 и выше. 2. Для подключаемого модуля Dr.Web для Outlook необходим установленный клиент Microsoft Outlook из состава Microsoft Office: •Outlook 2000; •Outlook 2002; •Outlook 2003; •Outlook 2007; •Outlook 2010 SP2; •Outlook 2013; •Outlook 2016.

- 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	Не менее 512 МБ.

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

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

На всех защищаемых объектах антивирусной сети Dr.Web не должно использоваться другое антивирусное ПО (в том числе другие версии ПО Dr.Web).

4.4. Комплект поставки

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

1. Для ОС семейства UNIX:

Название файла	Компонент
drweb-11.00.0-<*сборка*>-esuite-server-<*версия_ОС*>.run	Основной дистрибутив Сервера Dr.Web
drweb-11.00.0-<*сборка*>-esuite-extra-<*версия_ОС*>.run	Дополнительный дистрибутив Сервера Dr.Web
drweb-11.00.0-<*сборка*>-esuite-proxy-<*версия_ОС*>.run	Прокси-сервер Dr.Web
drweb-reploader-<*ОС*>-<*разрядность*>	Консольная версия Загрузчика репозитория Dr.Web

2. Для ОС Windows:

Название файла	Компонент
drweb-11.00.0-<*сборка*>-esuite-server-<*версия_ОС*>.exe	Основной дистрибутив Сервера Dr.Web
drweb-11.00.0-<*сборка*>-esuite-extra-<*версия_ОС*>.exe	Дополнительный дистрибутив Сервера Dr.Web
drweb-11.00.0-<*сборка*>-esuite-proxy-<*версия_ОС*>.exe	Прокси-сервер Dr.Web
drweb-11.00.0-<*сборка*>-esuite-agent-activedirectory.msi	Агент Dr.Web для Active Directory
drweb-11.00.0-<*сборка*>-esuite-modify-ad-schema-<*версия_ОС*>.exe	Утилита для модификации схемы Active Directory
drweb-11.00.0-<*сборка*>-esuite-aduac-<*версия_ОС*>.msi	Утилита для изменения атрибутов у объектов Active Directory
drweb-11.00.0-<*сборка*>-esuite-napshv-<*версия_ОС*>.msi	NAP Validator
drweb-11.05.0-<*сборка*>-esuite-agent-full-windows.exe	Полный инсталлятор Агента Dr.Web. Также входит в состав дополнительного дистрибутива Сервера Dr.Web.
drweb-reploader-windows-<*разрядность*>.exe	Консольная версия Загрузчика репозитория Dr.Web
drweb-reploader-gui-windows-<*разрядность*>.exe	Графическая версия Загрузчика репозитория Dr.Web

Дистрибутив Сервера Dr.Web состоит из двух пакетов:

1. Основной дистрибутив — базовый дистрибутив для установки Сервера Dr.Web. Состав аналогичен составу дистрибутива предыдущих версий Dr.Web Enterprise Security Suite.

Из основного дистрибутива осуществляется установка самого Сервера Dr.Web, включающего пакеты антивирусной защиты для станции только под ОС Windows.

2. Дополнительный дистрибутив (extra) — включает дистрибутивы всех корпоративных продуктов, предоставляемых для установки на защищаемые станции, управляемые всеми поддерживаемыми ОС.

Устанавливается как дополнение на компьютер с уже установленным основным дистрибутивом Сервера Dr.Web.

Внимание! Дополнительный дистрибутив должен устанавливаться из пакета того же типа, что и основной дистрибутив.

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.

Также в комплект поставки входят серийные номера, после регистрации которых вы получите файлы с лицензионными ключами.

4.5. Схема взаимодействия компонентов антивирусной сети

На рисунке ниже представлена общая схема фрагмента антивирусной сети.

Данная схема отображает антивирусную сеть, в состав которой входит только один Сервер. В крупных компаниях предпочтительно разворачивать антивирусную сеть с несколькими Серверами для распределения нагрузки между ними.

В данном примере антивирусная сеть развернута в пределах одной ЛВС, однако для установки и работы Dr.Web Enterprise Security Suite и антивирусных пакетов нахождение компьютеров в пределах какой-либо ЛВС необязательно, достаточно доступа в Интернет.

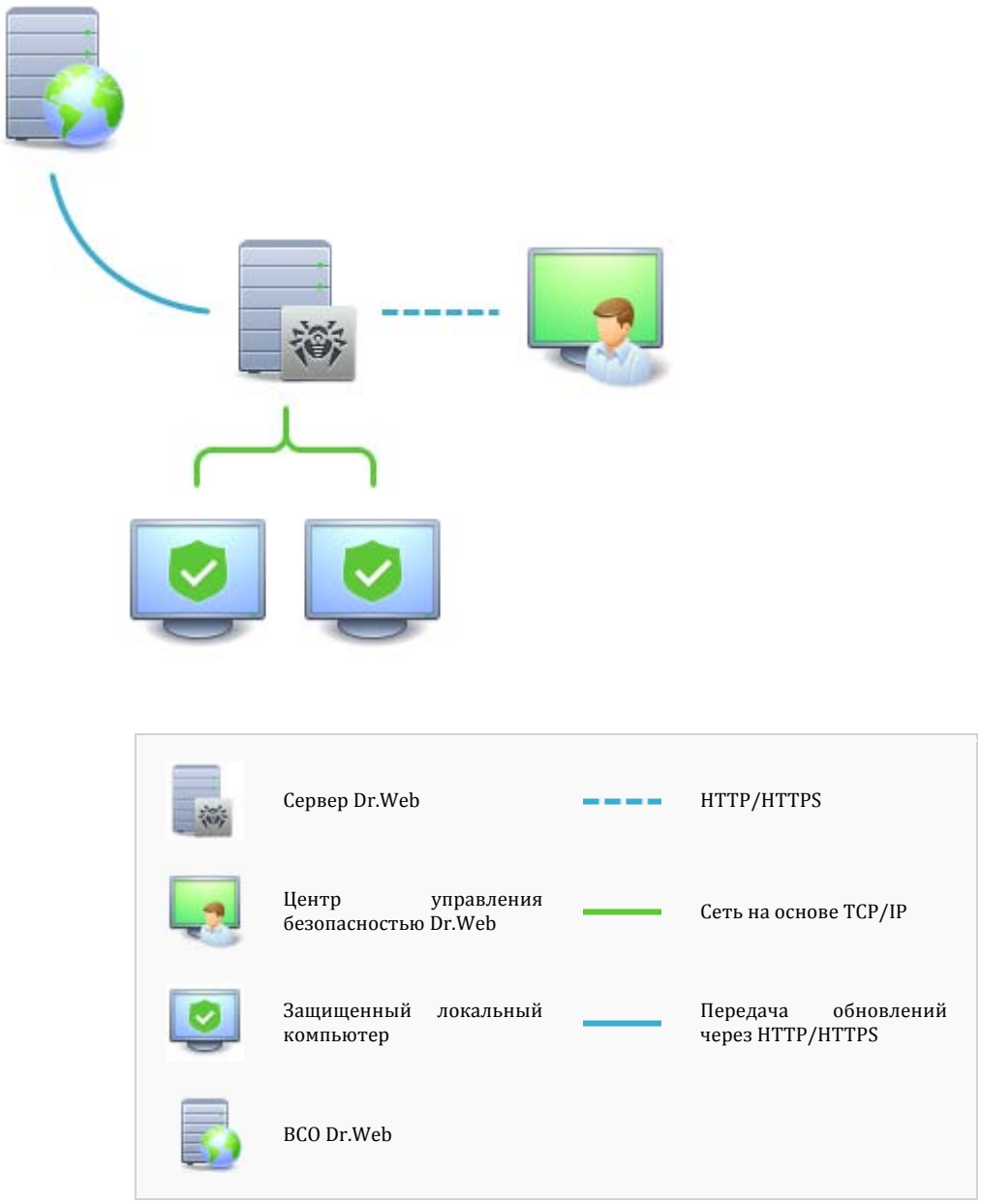
Структура антивирусной сети

При запуске Сервера Dr.Web выполняется следующая последовательность действий:

1. Загрузка файлов Сервера Dr.Web из каталога bin.
2. Загрузка Планировщика заданий Сервера.
3. Загрузка каталога централизованной установки и каталога обновления, инициализация системы сигнального информирования (системы оповещений).
4. Проверка целостности БД Сервера.
5. Выполнение заданий Планировщика заданий Сервера.
6. Ожидание информации от Агентов Dr.Web и команд от Центров управления.

Весь поток команд, данных и статистической информации в антивирусной сети в обязательном порядке проходит через Сервер Dr.Web. Центр управления также обменивается информацией только с Сервером; изменения в конфигурации рабочей станции и передача команд Агенту Dr.Web осуществляется Сервером на основе команд Центра управления.

Таким образом, логическая структура фрагмента антивирусной сети имеет вид, представленный на рисунке ниже.



Логическая структура антивирусной сети

Между Сервером и рабочими станциями (сплошная тонкая линия на рисунке выше) передаются:

- запросы Агента на получение централизованного расписания и централизованное расписание данной рабочей станции,
- настройки Агента и антивирусного пакета,
- запросы на очередные задания, подлежащие выполнению (сканирование, обновление вирусных баз и т. п.),
- файлы антивирусных пакетов — при получении Агентом задания на их установку,
- обновления ПО и вирусных баз — при выполнении задания на обновление,
- сообщения Агента о конфигурации рабочей станции,
- статистика работы Агента и антивирусных пакетов для включения в централизованный журнал,
- сообщения о вирусных событиях и других подлежащих фиксации событиях.

Объем трафика между рабочими станциями и Сервером, в зависимости от настроек рабочих станций и их количества, может быть весьма значительным. Поэтому антивирусная сеть Dr.Web Enterprise Security Suite предусматривает возможность компрессии трафика.

Описание использования этого факультативного режима см. ниже, п. Использование шифрования и сжатия трафика.

Трафик между Сервером и рабочей станцией можно зашифровать. Это позволяет избежать разглашения сведений, передаваемых по описываемому каналу, а также подмены ПО, загружаемого на рабочие станции. По умолчанию эта возможность включена. Описание использования этого режима см. ниже, п. Использование шифрования и сжатия трафика.

От веб-сервера обновлений к Серверу Dr.Web (сплошная толстая линия на рисунке выше) передаются, с использованием протокола HTTP, файлы, необходимые для репликации централизованных каталогов установки и обновления, и служебная информация о ходе этого процесса. Целостность передаваемой информации (файлов ПО Dr.Web Enterprise Security Suite и антивирусных пакетов) обеспечивается использованием механизма контрольных сумм: поврежденный при пересылке или подмененный файл не будет принят Сервером.

Между Сервером и Центром управления (пунктирная линия на рисунке выше) передаются сведения о конфигурации Сервера (включая информацию о топологии сети) и настройки рабочих станций. Эта информация визуализируется в Центре управления, и, в случае изменения пользователем (администратором антивирусной сети) каких-либо настроек, информация о внесенных изменениях передается на Сервер.

Установление соединения Центра управления с выбранным Сервером производится только после аутентификации администратора антивирусной сети посредством ввода его регистрационного имени и пароля на данном Сервере.

5. Изменения по сравнению с Dr.Web Enterprise Security Suite 10.0.

Изменения в серверной части:

- добавлена поддержка MySQL 8 и PostgreSQL версии 10 в качестве внешних баз данных;
- переработан принцип сканирования сети и удаленной установки Агентов (расширение для веб-браузеров более не используется);
- добавлена возможность восстановления поврежденной встроенной базы данных;
- передача групповых обновлений на защищаемые станции по multicast-протоколу теперь включена по умолчанию;
- добавлен механизм контроля лицензий, передаваемых соседним Серверам по межсерверным связям;
- переработана процедура сбора информации о программно-аппаратном обеспечении защищаемых станций, добавлен механизм передачи информации по межсерверным связям;
- добавлено ограничение по количеству одновременных установок Агентов с Сервера;
- добавлено ограничение по трафику для установок и обновлений Агентов с Сервера;
- установочные пакеты для Сервера под ОС семейства UNIX теперь поставляются только в универсальном формате;
- добавлена возможность возобновления сеансов TLS на основе мандатов сессий.

Изменения в Центре управления безопасностью:

- настройки межсерверных связей перемещены из раздела **Связи** в раздел **Антивирусная сеть**, связи с соседними Серверами теперь располагаются в дереве антивирусной сети;
- введена новая система комплексной настройки станций на основе политик, управление которыми доступно в дереве антивирусной сети;
- в главное меню добавлен новый раздел **Избранное**;

- переработаны технологии отображения таблиц и графиков;
- добавлена настройка веб-сервера, предоставляющая защиту против flood-атак при обращении к Центру управления;
- добавлена возможность просмотра журнала работы Сервера Dr.Web через Центр управления безопасностью Dr.Web в режиме реального времени;
- добавлена возможность управления настройками журнала работы Сервера Dr.Web через Центр управления безопасностью Dr.Web;
- возвращен метод отправки оповещений администратора через протокол Агента Dr.Web;
- переработана конфигурация оповещений администратора;
- добавлен журнал информационных сообщений, отправленных администратором на станции, и возможность создания шаблонов таких сообщений;
- расширен список утилит, доступных д ля скачивания через Центр управления безопасностью;
- в репозиторий Сервера добавлены новые продукты — Данные безопасности Сервера Dr.Web и Прокси-сервер Dr.Web;
- добавлен новый раздел **Резервные копии** для просмотра и сохранения содержимого резервных копий критичных данных Сервера;
- добавлено расширение Yandex.Locator для автоматического определения местоположения устройств под управлением ОС Android
- повышено удобство использования SQL-консоли: добавлены подсветка синтаксиса и автозавершение при вводе запроса;
- переработаны настройки для внешней аутентификации администраторов на Сервере: добавлен новый раздел с упрощенной настройкой аутентификации средствами LDAP;
- право администраторов **Запуск и прерывание компонентов** расширено за счет возможности управления карантином на станциях;
- для адресов Сервера и Агента теперь можно напрямую указать версию протокола IP;
- переработаны статусы защищаемых станций в дереве антивирусной сети, добавлена новая цветовая индикация в зависимости от состояния станций;
- добавлена сортировка клиентов (станций, Серверов, Прокси-серверов) в дереве антивирусной сети;
- добавлена возможность экспорта статистических отчетов сразу для нескольких объектов антивирусной сети;
- параметры подключения Агентов Dr.Web на компьютерах под управлением ОС Windows и UNIX вынесены в отдельный раздел конфигурации станций;
- добавлена возможность запуска антивирусных компонентов на станции через Центр управления безопасностью Dr.Web, разделы Антивирусной сети **Запущенные компоненты** и **Установленные компоненты** об ъединены в раздел **Компоненты защиты**;
- добавлена возможность дистанционной настройки Брандмауэра Dr.Web на станциях под управлением ОС Windows через Центр управления безопасностью Dr.Web, в настройках Брандмауэра Dr.Web в Центре управления по умолчанию отключено использование пакетного фильтра;
- добавлена возможность регулировать период, в течение которого вирусные базы на защищаемых станциях считаются актуальными;
- добавлен новый раздел Центра управления безопасностью Dr.Web с информацией об идентификаторах безопасности защищаемых станций;
- объединены разделы настроек SpIDer Gate и SpIDer Mail для станций под управлением ОС Windows, раздел исключений теперь един для обоих компонентов;
- расширена функциональность при задании исключений из сканирования компонентами SpIDer Gate и SpIDer Mail для станций под управлением ОС Windows;
- добавлен новый компонент **Монитор сетевых портов** для станций под управлением ОС Windows — он доступен только в Центре управления и не предоставляется пользователям защищаемых станций;

- добавлена возможность выбора существующей станции для размещения новичка при подтверждении доступа к Серверу;
- добавлена возможность управления настройками доступа к устройствам на защищаемых станциях;
- добавлена возможность управления настройками Офисного контроля отдельно для каждого пользователя станции;
- добавлена поддержка настроек компонентов новой версии для станций под управлением ОС семейства UNIX;
- добавлена возможность управления настройками и просмотра статистики работы продукта Dr.Web для Microsoft Exchange Server из Центра управления;
- расширены функции меню **Поддержка**: теперь со страниц Центра управления можно открыть соответствующую им страницу документации.

Новая утилита:

- добавлена утилита дистанционной диагностики Сервера Dr.Web для работы со скриптами (исполняемый файл drwcmd), которая позволяет удаленно подключаться к Серверу Dr.Web для базового управления и просмотра статистики работы.

Новые возможности Прокси-сервера:

- управление настройками через Центр управления безопасностью;
- установка и удаление через связанный с Прокси-сервером Агент;
- автоматическое обновление в процессе работы;
- кэширование для передаваемого шифрованного трафика;
- наполнение кэша вручную — в частности, из репозитория Сервера Dr.Web;
- накопление событий, передаваемых Агентами Dr.Web, и дальнейшая передача их на Сервер Dr.Web согласно расписанию.

Изменения в Агенте Dr.Web:

- для станций под управлением всех поддерживаемых ОС предоставляется групповой инсталлятор, позволяющий производить установку Агента Dr.Web на несколько станций при помощи одного установочного пакета;
- разрешена возможность «отката» Агента Dr.Web на предыдущую ревизию;
- «откат» Агента Dr.Web для Windows на предыдущую ревизию осуществляется с помощью полной переустановки продукта на станции;
- для станций под управлением ОС Windows добавлена возможность проверки скриптов по запросу от приложений через AMSI;
- в Офисном контроле полностью переработана опция для запрета доступа к данным на съемных носителях, новая редакция предоставляет возможность блокировки устройств по классам и шинам.

Более не поддерживаются:

- InitDB (SQLite 2) в качестве встроенной базы данных;
- Novell Netware в качестве ОС для защищаемых станций;
- Solaris Sparc в качестве ОС для установки Сервера Dr.Web.

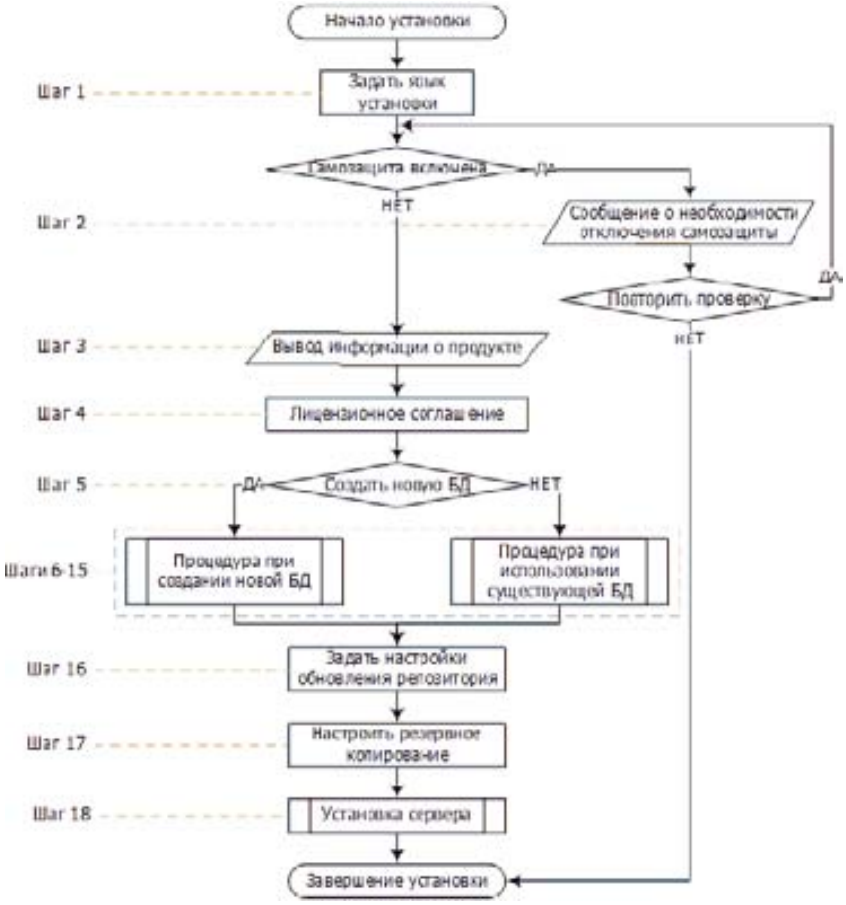
Также более не используются расширение Центра управления безопасностью Dr.Web для веб-браузеров, технология Adobe Flash в Центре управления безопасностью Dr.Web и Windows Messenger для отправки оповещений администратора.

Вместе с тем в рамках выпуска Dr.Web Enterprise Security Suite 11.0 исправлены выявленные ошибки.

6. Обеспечение антивирусной защиты сети предприятия с использованием Dr.Web Enterprise Security Suite

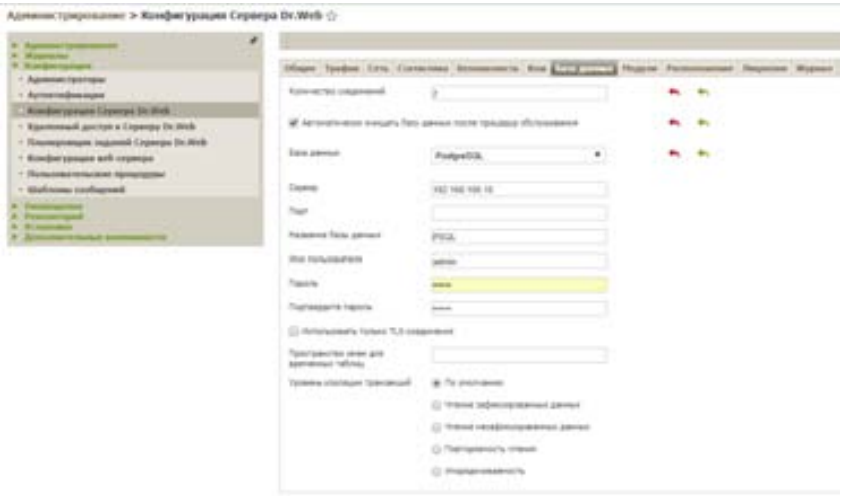
6.1. Процедура внедрения решения Dr.Web Enterprise Security Suite и анализ результатов тестирования системы

1. Назначение ответственного за проведение тестирования ПО Dr.Web.
2. Изучение возможностей ПО Dr.Web в ходе тестовых установок систем защиты рабочих станций, файловых серверов, почтовых серверов, а также серверов управления антивирусной защитой.
3. Проверка действия политик безопасности, сформированных в соответствии с политикой информационной безопасности компании.
4. Проверка совместимости ПО Dr.Web и ПО, используемого в компании.
5. Уточнение плана развертывания ПО Dr.Web по итогам тестовых установок в соответствии со структурой корпоративной сети компании и графиком работы сотрудников.
    a. Уточнение времени развертывания компонентов ПО Dr.Web в условиях локальной сети компании.
    b. Выбор типа развертывания ПО Dr.Web на локальных станциях и файловых серверах (политика AD, запуск дистрибутивов локально, сканирование сети на незащищенные станции и пр.).
    c. Выбор порядка и времени развертывания ПО Dr.Web в соответствии со структурой корпоративной сети компании и графиком работы сотрудников.
6. Обучение администраторов безопасности компании приемам работы с ПО Dr.Web.
7. Отработка процедур, связанных с удалением используемого антивирусного ПО и установкой ПО Dr.Web.
    a. Выработка мер защиты на период отсутствия антивирусного ПО на элементах сети компании.
8. Проверка локальной сети (защищаемых станций и серверов) на наличие сервисов, необходимых для развертывания ПО Dr.Web в сети компании, — в зависимости от выбранного типа развертывания. В случае необходимости корректировка правил файерволов, используемых в сети компании.
9. Утверждение плана-графика развертывания ПО Dr.Web в сети компании. Доведение плана-графика до сотрудников компании в части, их касающейся. Общая схема инсталляции антивируса в сети предприятия представлена на рис. 1.



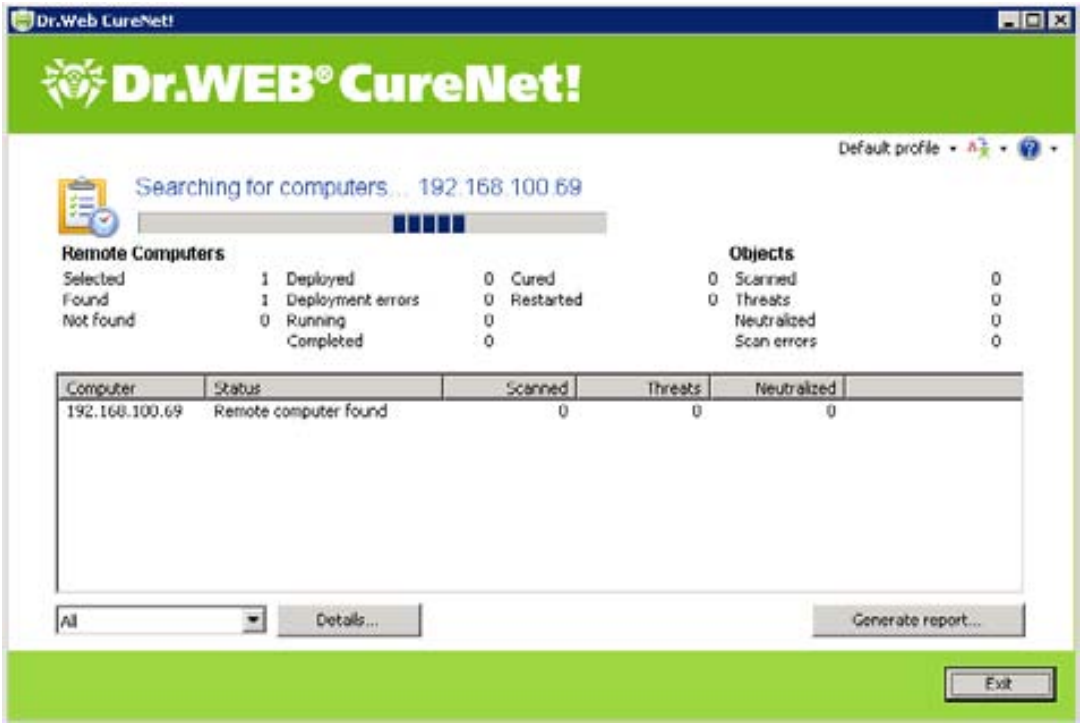
План-график развертывания ПО Dr.Web в сети компании

10. Замена антивирусного ПО в сети компании.
11. Подготовка ПО Dr.Web в зависимости от выбранного типа развертывания.
    a. Установка серверов иерархической сети Dr.Web, а также, в случае необходимости, настройка базы данных.

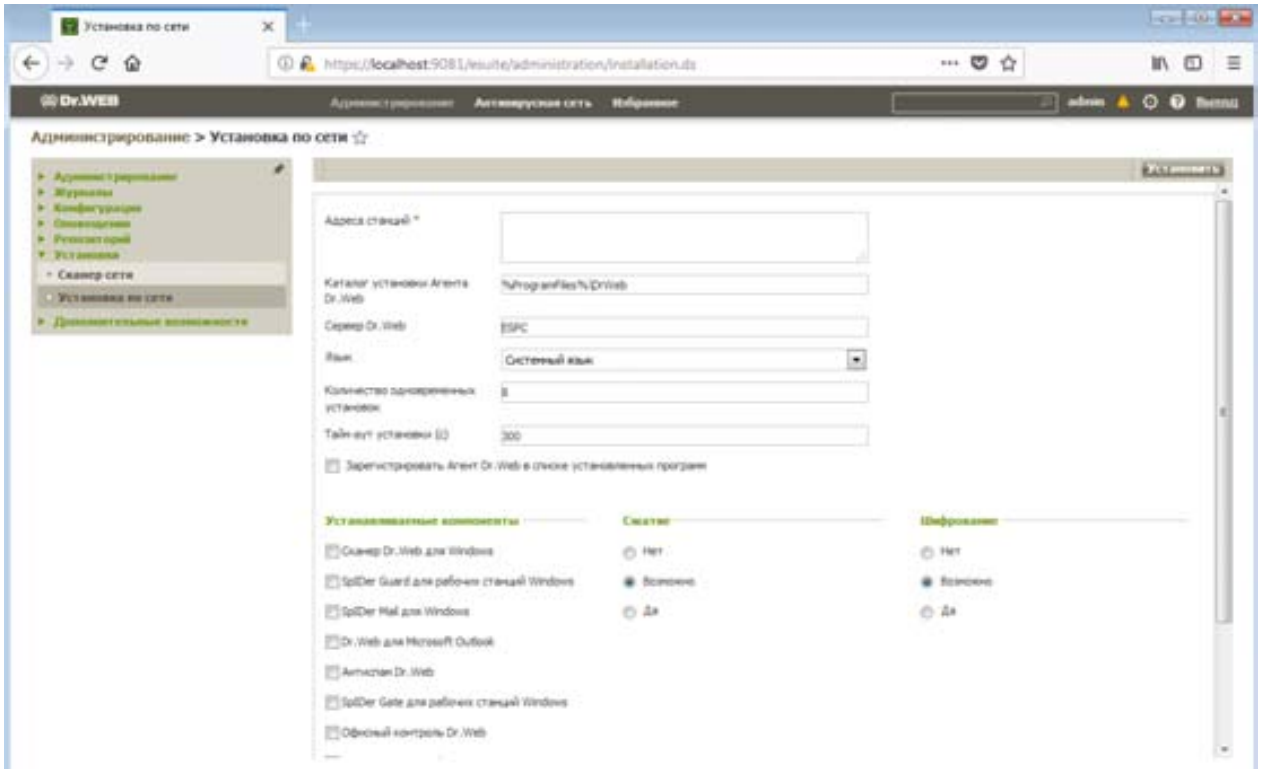


b. Развертывание системы резервирования серверов Dr.Web.
c. Настройка групп и политик.
d. В случае необходимости — назначение отдельных администраторов группы пользователей и ограничение прав данных администраторов в соответствии с политикой, действующей в компании.
e. В зависимости от выбранной политики развертывания — проведение иных мероприятий.

12. Сканирование сети компании сетевой утилитой Dr.Web CureNet! на наличие ранее неизвестных вредоносных программ.

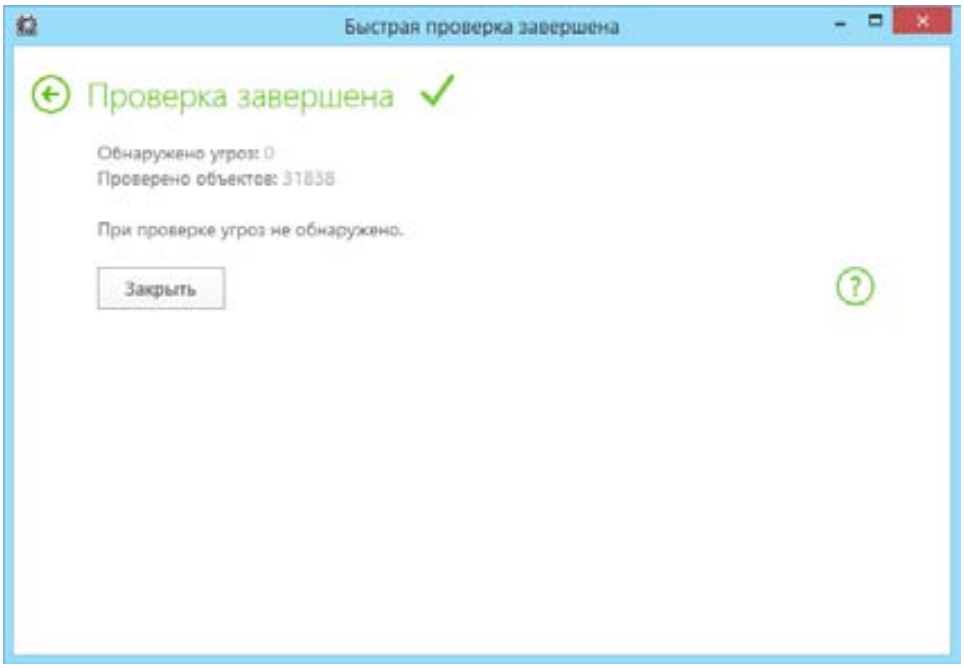


13. Деинсталляция используемых антивирусных продуктов.
14. Развертывание антивирусной сети Dr.Web Enterprise Security Suite, подробнее об этом написано в следующем разделе.



a. Установка системы защиты рабочих станций и файловых серверов в соответствии с настройками, сделанными на предыдущем этапе.
b. Установка системы защиты почтовых серверов.

15. Эксплуатация ПО Dr.Web в течение тестового периода.
16. Проведение обновлений ПО Dr.Web в соответствии с политикой, действующей в компании.
17. Проведение периодических проверок защищаемых рабочих станций, файловых и почтовых серверов.



18. Контроль действий ПО Dr.Web на тестовые воздействия вредоносного ПО.

19. Проверка процедуры взаимодействия с технической поддержкой ООО «Доктор Веб».
20. Подготовка отчета по результатам тестирования ПО Dr.Web в сети компании, согласование отчета с представителями ООО «Доктор Веб». Утверждение отчета.

Внимание! Существует бесконечное множество вариантов сетей — с разнообразной архитектурой, различными каналами связи, различным числом пользователей и всеми остальными параметрами. И продукты Dr.Web обеспечивают надежную защиту и стабильную работу в любых условиях и сетях. Тем не менее, нет предела совершенству, поэтому после развертывания антивирусной системы на основе Dr.Web ESS, будь то тестовое внедрение перед окончательным решением о приобретении или рабочее внедрение после покупки, рекомендуется запросить у поставщика продуктов Dr.Web и заполнить отчет о тестировании. Ваш поставщик передаст его в компанию «Доктор Веб», что в будущем поможет сделать антивирусную систему еще лучше и надежнее как в целом, так и для вашей сетевой инфраструктуры в частности!

6.2. Развертывание антивирусной сети Dr.Web Enterprise Security Suite

Для создания системы антивирусной защиты компании:

1. Составьте список актуальных для вашей компании ИТ-угроз.

   Внимание! Актуальные пути реализации современных вредоносных угроз, а также необходимые меры, позволяющие предотвратить реализацию данных угроз, описаны в курсе DWCERT-070-3 «Антивирусная система защиты предприятия».

2. Выберите меры защиты, необходимые для их нейтрализации.
3. Составьте план структуры антивирусной сети, включив в него все защищаемые рабочие станции, серверы, домашние компьютеры и устройства.
4. Определите, какие из защищаемых серверов будут выполнять функцию **Сервера**.
5. Установите ПО **Сервера** (вместе с ним установится Центр управления Dr.Web) на выбранный компьютер или компьютеры.
6. Используя Центр управления, произведите обновление репозитория.
7. При необходимости установите и настройте Прокси-сервер.
8. При необходимости установите и настройте компоненты реагирования на инциденты компьютерной безопасности.
9. Настройте ПО, предназначенное для установки на рабочие станции и серверы.
10. Установите ПО **Агента** на защищаемые узлы локальной сети, личные устройства.
11. Используя Центр управления, настройте и запустите необходимые модули защиты.

На этапе планирования структуры антивирусной сети прежде всего необходимо выбрать компьютер, который будет выполнять функции **Сервера**. **Сервер** можно установить на любом компьютере, а не только на компьютере, выполняющем функции сервера ЛВС. Основные требования к этому компьютеру приведены в разделе системных требований.

В состав антивирусной сети может входить несколько **Серверов**. Особенности такой конфигурации описаны в п. 8.6. Иерархия серверов.

Внимание! На время установки **Сервера** и **Агента** требуется доступ (физический или с использованием средств удаленного управления и запуска программ) к соответствующим компьютерам, для чего необходимо произвести настройки локальной сети, описанные в соответствующих разделах по установке. Все дальнейшие действия выполняются с рабочего места администратора антивирусной сети (в том числе, возможно, извне локальной сети) и не требуют доступа к **Серверам** или рабочим станциям.

Внимание! Настройка локальной сети в соответствии с системными требованиями к тестируемым продуктам описана в соответствующих разделах документации к используемым продуктам.

Внимание! Для нормального функционирования сервиса антивирусной защиты рекомендуется установить на сервер службу синхронизации времени NTP.

Все описанные выше шаги подробно рассмотрены далее в настоящем курсе.

6.3. Установка и настройка Сервера Dr.Web

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

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

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

Внимание! Язык названия папки, в которую ставится Сервер, должен совпадать с языком, указанным в языковых настройках ОС Windows для программ, не использующих unicode. В противном случае Сервер не будет установлен. Исключение — английский язык в названии папки для инсталляции.

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

По умолчанию **Enterprise Сервер** после установки запускается автоматически (для версии под ОС семейства UNIX это указывается в настройках инсталлятора).

6.3.1. Обновление существующего Сервера Dr.Web до версии 11 под ОС Windows

Важные замечания

- Перед началом обновления настоятельно рекомендуется проверить корректность настроек протокола TCP/IP для возможности доступа в Интернет. В частности, должна быть включена и должна содержать корректные настройки служба DNS.
- При многосерверной конфигурации антивирусной сети необходимо учитывать, что между Серверами версии 11.0 и Серверами версии 6 передача межсерверных обновлений не осуществляется, и межсерверная связь используется только для передачи статистики. Для обеспечения передачи межсерверных обновлений необходимо обновить все Серверы. Если необходимо оставить в составе антивирусной сети Серверы предыдущих версий для подключения Агентов, установленных на ОС, не поддерживаемых версией 11.0 , то Серверы версии 6 и Серверы версии 11.0 должны получать обновления независимо.
- Для антивирусной сети, в которой используется Прокси-сервер Dr.Web, при обновлении компонентов до версии 11.0 необходимо также произвести обновление Прокси-сервера до версии 11.0. В противном случае подключение Агентов,

поставляемых с версией 11.0, к Серверу версии 11.0 будет невозможно. Рекомендуется производить обновление в следующем порядке: Сервер Dr.Web → Прокси-сервер Dr.Web → Агент Dr.Web.

- При обновлении Сервера с версии 6 до версии 11.0 настройки работы Сервера через прокси-сервер не сохраняются. После установки версии 11.0 необходимо задать настройки подключения через прокси-сервер вручную (см. **Руководство администратора**, п. **Прокси**).
- При обновлении Сервера все настройки репозитория не переносятся в новую версию (сбрасываются в значения по умолчанию), однако осуществляется их резервное копирование. При необходимости задайте настройки репозитория вручную после обновления Сервера.

Обновление Сервера Dr.Web для ОС Windows

При обновлении Сервера Dr.Web под ОС Windows с предыдущих версий настройки из следующих разделов Центра управления не будут перенесены в версию 11.0:

- **Конфигурация Сервера Dr.Web → Сеть → Загрузка** (файл download.conf),
- **Удаленный доступ к Серверу Dr.Web** (файл frontdoor.conf),
- **Конфигурация веб-сервера** (файл webmin.conf).

Настройки в этих разделах будут сброшены в значения по умолчанию. Если вы хотите использовать настройки предыдущей версии, задайте их вручную после обновления Сервера в соответствующих разделах Центра управления на основе данных из резервных копий конфигурационных файлов.

Обновление Сервера с версий 6 и 10 до версии 11.0 и в пределах версии 11.0 осуществляется автоматически средствами инсталлятора.

Внимание! Перед обновлением Сервера необходимо вручную удалить дополнительный дистрибутив Сервера (extra).

Сохранение файлов конфигурации

При обновлении Сервера до версии 11.0 средствами инсталлятора конфигурационные файлы сохраняются в каталог, заданный для резервного копирования:

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

При обновлении Сервера с версии 6 сохраняются следующие конфигурационные файлы:

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

Файл	Описание
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
dbinternal.dbs	встроенная БД
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub	открытый ключ шифрования
enterprise.key (имя может отличаться)	лицензионный ключ Сервера
webmin.conf	конфигурационный файл Центра управления

При обновлении Сервера с версии 10 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ads.xml	конфигурационный файл внешней авторизации администраторов через Active Directory
auth-ldap.xml	конфигурационный файл внешней авторизации администраторов через LDAP
auth-radius.xml	конфигурационный файл внешней авторизации администраторов через RADIUS
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.conf.distr	шаблон конфигурационного файла Сервера с параметрами по умолчанию
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub	открытый ключ шифрования
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
webmin.conf	конфигурационный файл Центра управления
openssl.cnf	сертификат Сервера для HTTPS

При обновлении Сервера в пределах версии 11.0 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ads.conf	конфигурационный файл внешней авторизации администраторов через Active Directory
auth-radius.conf	конфигурационный файл внешней авторизации администраторов через RADIUS
auth-ldap.conf	конфигурационный файл внешней авторизации администраторов через LDAP
auth-ldap-rfc4515.conf	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме
auth-ldap-rfc4515-check-group.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory
auth-ldap-rfc4515-check-group-novar.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory с использованием переменных
auth-ldap-rfc4515-simple-login.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме
auth-pam.conf	конфигурационный файл внешней авторизации администраторов через PAM
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует
drwcsd-certificate.pem	сертификат Сервера
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.conf.distr	шаблон конфигурационного файла Сервера с параметрами по умолчанию
drwcsd.pri	закрытый ключ шифрования
dbexport.gz	экспорт базы данных
drwcsd.pub	открытый ключ шифрования
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
openssl.cnf	сертификат Сервера для HTTPS

Файл	Описание
webmin.conf	конфигурационный файл Центра управления
yalocator.apikey	API-ключ для расширения Yandex.Locator

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

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

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

Сохранение базы данных

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

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

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

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

Для обновления Сервера Dr.Web:

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

- По умолчанию в качестве языка инсталлятора выбирается язык операционной системы. При необходимости вы можете изменить язык установки на любом шаге, выбрав соответствующий пункт в правом верхнем углу окна инсталлятора.
- При использовании внешней базы данных Сервера в процессе обновления также выберите вариант **Использовать существующую базу данных**.
- Если вы планируете использовать в качестве внешней базы данных БД Oracle через ODBC-подключение, то при установке (обновлении) Сервера, в настройках инсталлятора отмените установку встроенного клиента для СУБД Oracle (в разделе **Поддержка баз данных → Драйвер базы данных Oracle**).

В противном случае работа с БД Oracle через ODBC будет невозможна из-за конфликта библиотек.

При обновлении с версии 6

1. Откроется окно, извещающее о наличии установленного ПО Сервера предыдущей версии и предоставляющее краткое описание процесса обновления до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Обновить**.
2. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флажок **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.
3. В последующих шагах осуществляется настройка Сервера аналогично процессу установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.
4. Для начала процесса удаления Сервера предыдущей версии и установки Сервера версии 11.0 нажмите кнопку **Установить**.

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

При обновлении с версии 10.0

1. Откроется окно, извещающее о наличии установленного ПО Сервера предыдущей версии и предоставляющее краткое описание процесса обновления до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Обновить**.
2. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флажок **Я принимаю ус ловия Лицензионного соглашения** и нажмите кнопку **Далее**.
3. В последующих шагах осуществляется настройка Сервера аналогично процессу установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.
4. Для начала процесса удаления Сервера предыдущей версии и установки Сервера версии 11.0 нажмите кнопку **Установить**.
5. В процессе обновления откроется окно с настройкой резервного копирования критичных данных перед удалением Сервера предыдущей версии. Рекомендуется установить флажок **Сохранить резервную копию критических данных Сервера Dr.Web**. При необходимости можете изменить каталог для резервного копирования, заданный по умолчанию (<*диск_установки*>:\DrWeb Backup).

При обновлении с версий 10.0.1, 10.1 и в пределах версии 11.0

1. Откроется окно, извещающее о наличии установленного ПО Сервера предыдущей версии и предоставляющее краткое описание процесса обновления до новой версии. Для начала настройки процедуры обновления нажмите кнопку **Обновить**.
2. Откроется окно с настройкой резервного копирования критичных данных перед удалением Сервера предыдущей версии. Рекомендуется установить флажок **Сохранить резервную копию критических данных Сервера Dr.Web**. При

необходимости можете изменить каталог для резервного копирования, заданный по умолчанию (<*диск_установки*>:\DrWeb Backup). Для начала процесса удаления предыдущей версии Сервера нажмите **Удалить**.

3. После завершения удаления предыдущей версии Сервера начнется установка новой версии. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флажок **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.
4. В последующих шагах осуществляется настройка Сервера аналогично процессу установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.
5. Для начала процесса установки Сервера версии 11.0 нажмите кнопку **Установить**.

После завершения обновлений Серверов антивирусной сети необходимо:

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

6.3.2. Обновление существующего Сервера Dr.Web до версии 11 под ОС Unix

При обновлении Сервера Dr.Web под ОС семейства UNIX с предыдущих версий настройки из раздела Центра управления **Конфигурация веб-сервера** (файл webmin.conf) не будут перенесены в версию 11.0.

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

Обновление Сервера до версии 11.0 зависит от исходной версии:

- Обновление с версии 6.0.4 на версию 11.0 осуществляется только вручную.
- Обновление с версии 10 на версию 11.0 автоматически поверх установленной версии возможно не для всех ОС семейства UNIX. Поэтому под ОС семейства UNIX, в которых невозможно произвести автоматическое обновление поверх уже установленного пакета, необходимо осуществить обновление вручную.
- Обновление Сервера в пределах версии 11.0 для одинаковых типов пакетов осуществляется автоматически для всех ОС семейства UNIX. При желании вы также можете осуществить обновление вручную.

Внимание! Все действия по обновлению необходимо выполнять от имени администратора **root**.

При удалении и автоматическом обновлении Сервера до версии 11.0 конфигурационные файлы сохраняются в каталог, заданный для резервного копирования по умолчанию: /var/tmp/drwcs/.

При удалении Сервера версии 6 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
certificate.pem	сертификат для SSL
common.conf	конфигурационный файл (для некоторых ОС семейства UNIX)
dbinternal.dbs	встроенная БД
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub	открытый ключ шифрования
enterprise.key (имя может отличаться)	лицензионный ключ Сервера
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления

При удалении Сервера версии 10 сохраняются следующие конфигурационные файлы:

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

Файл	Описание
drwcsd.pub	открытый ключ шифрования
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
local.conf	настройки журнала Сервера
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления
**.dbs* **.sqlite*	встроенная БД

При удалении Сервера версии 11.0 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ldap.conf	конфигурационный файл внешней авторизации администраторов через LDAP
auth-ldap-rfc4515.conf	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме
auth-pam.conf	конфигурационный файл внешней авторизации администраторов через PAM
auth-radius.conf	конфигурационный файл внешней авторизации администраторов через RADIUS
certificate.pem	сертификат для SSL
common.conf	конфигурационный файл (для некоторых ОС семейства UNIX)
dbexport.gz	экспорт базы данных (создается в процессе удаления Сервера командой drwcs.sh xmlexportdb)
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
drwcsd-certificate.pem	сертификат Сервера
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub	открытый ключ шифрования

Файл	Описание
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
local.conf	настройки журнала Сервера
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления
yalocator.apikey	API-ключ для расширения Yandex.Locator

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

Для Сервера версии 10:

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

Для Сервера версии 11.0:

Файл	Описание
auth-ldap.conf	конфигурационный файл внешней авторизации администраторов через LDAP
auth-ldap-rfc4515.conf	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме
auth-pam.conf	конфигурационный файл внешней авторизации администраторов через PAM
auth-radius.conf	конфигурационный файл внешней авторизации администраторов через RADIUS
db.backup.gz	экспорт базы данных (создается в процессе обновления Сервера командой drwcs.sh exportdb)

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

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

При необходимости сохраните другие важные для вас файлы.

Сохранение базы данных

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

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

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

Автоматическое обновление Сервера Dr.Web

При обновлении Сервера с версии 10 до версии 11.0 (кроме Серверов, установленных под ОС **Linux** из пакетов **.rpm.run и *.deb.run*) вместо удаления старой версии и установки новой версии Сервера возможно автоматическое пакетное обновление. Для этого запустите установку соответствующего пакета Сервера.

Обновление Сервера в пределах версии 11.0 для одинаковых типов пакетов осуществляется автоматически для всех ОС семейства UNIX.

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

Ручное обновление Сервера Dr.Web

В случае если невозможно произвести обновление Сервера версии 6.0.4 и старше поверх уже установленного пакета, необходимо удалить ПО Сервера более ранних версий, сохранив резервную копию, и установить ПО версии 11.0 на основе сохраненной резервной копии.

Для обновления Сервера Dr.Web выполните следующую процедуру:

1. Остановите Сервер.
2. Если вы хотите использовать в дальнейшем какие-либо файлы (помимо тех файлов, которые будут автоматически сохранены в процессе удаления Сервера на шаге **3**), создайте резервные копии этих файлов вручную, например копии шаблонов отчетов и т. п.
3. Удалите ПО Сервера (см. п. **Удаление Сервера Dr.Web для ОС семейства UNIX®** в **Руководстве по установке**). При этом будет автоматически предложено сохранить резервные копии файлов. Для этого достаточно ввести путь для сохранения или принять путь, предлагаемый по умолчанию.

4. Осуществите установку Сервера Dr.Web версии 11.0 согласно штатной процедуре установки (см. п. **Установка Сервера Dr.Web для ОС семейства UNIX®** в **Руководстве по установке**) на основе резервной копии из шага **3**. Все сохраненные конфигурационные файлы и встроенная база данных (в случае использования встроенной БД) будут автоматически конвертированы для использования Сервером версии 11.0. Без автоматической конвертации использование базы данных (в случае использования встроенной БД) и некоторых конфигурационных файлов Сервера предыдущих версий невозможно.

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

   Для всех сохраненных от предыдущей версии Сервера файлов (см. шаг **4**) необходимо установить в качестве владельца файлов пользователя, выбранного при установке новой версии Сервера (по умолчанию — **drwcs**).
5. Запустите Сервер.
6. Настройте обновление репозитория и обновите его полностью.

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

Примечание. Полностью наглядно процесс обновления с 10-й версии Сервера на 11-ю приведен в Инструкции по обновлению.

6.3.3. Установка сервера Dr.Web Enterprise Security Suite под ОС Windows 2003/Vista/2008/2012

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

Установка полного пакета Сервера Dr.Web состоит из двух этапов:

1. Установка *основного дистрибутива*. Из основного дистрибутива осуществляется установка самого Сервера Dr.Web, включающего пакеты антивирусной защиты для станции только под ОС Windows.
2. Установка *дополнительного дистрибутив (extra)*. Дополнительный дистрибутив включает дистрибутивы всех корпоративных продуктов, предоставляемых для установки на защищаемые станции, управляемые всеми поддерживаемыми ОС. Устанавливается как дополнение на компьютер с уже установленным основным дистрибутивом Сервера Dr.Web.

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

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

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

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

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

Исключение — английский язык в названии каталога установки.

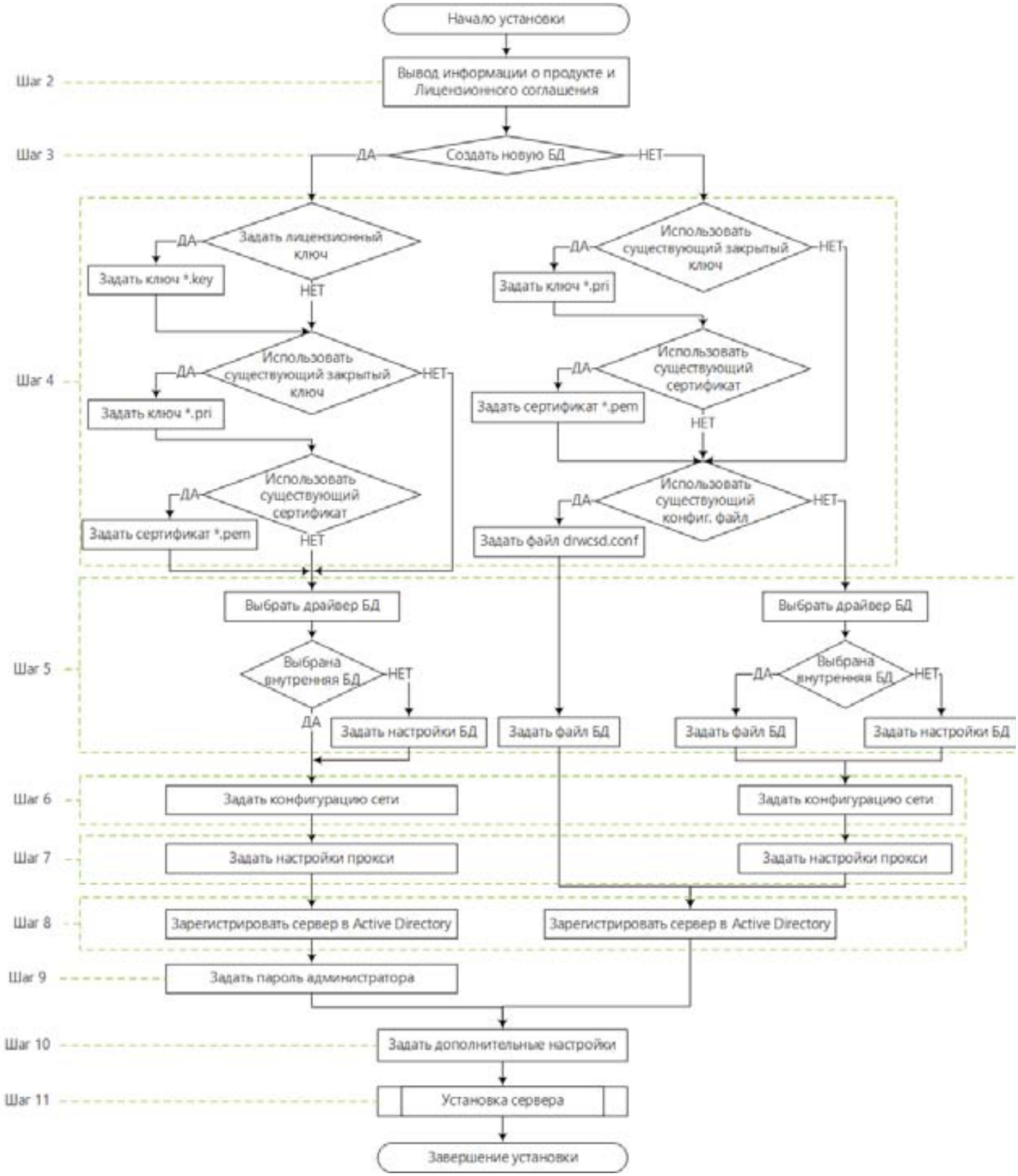
Вместе с Сервером Dr.Web автоматически устанавливается Центр управления безопасностью Dr.Web, который служит для управления антивирусной сетью и настройки Сервера.

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

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

- Файл д истрибутива и другие файлы, запрашиваемые в процессе установки программы, должны находиться на локальных дисках компьютера, на который устанавливается ПО Сервера. Права доступа должны быть настроены так, чтобы эти файлы были доступны для пользователя **LOCALSYSTEM**.
- Установка Сервера Dr.Web должна выполняться пользователем с правами администратора данного компьютера.
- После установки Сервера Dr.Web необходимо произвести обновление всех компонентов Dr.Web Enterprise Security Suite (см. **Руководство администратора**, п. Ручное обновление репозитория Сервера Dr.Web).
- При использовании внешней БД необходимо предварительно создать БД и настроить соответствующий драйвер (см. документ **Приложения**, п. Приложение В. Настройки для использования СУБД. Параметры драйверов СУБД).
- Инсталлятор Сервера поддерживает режим изменения продукта. Для добавления или удаления отдельных компонентов, например драйверов для управления базами данных, достаточно запустить инсталлятор Сервера и выбрать вариант **Изменить**.

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



В качестве примера рассмотрим установку антивирусного сервера с внутренней базой данных.

1. Запустите файл дистрибутива.

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

2. Откроется окно с информацией об устанавливаемом продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения установки установите флажок **Я прини маю условия Лицензионного соглашения** и нажмите кнопку **Далее**.

3. В следующем окне выберите, какую базу данных необходимо использовать для антивирусной сети:

- **Создать новую базу данных** — для создания новой антивирусной сети.
- **Использовать существующую базу данных** — чтобы сохранить базу данных Сервера от предыдущей установки. Файл базы данных вы сможете указать позднее (см. шаг **5**).

4. В следующем окне задайте настройки базы данных.

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

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

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

5. В окне **Драйвер базы данных** настраиваются параметры используемой базы данных, которые зависят от выбора типа базы данных на шаге **3** и от наличия конфигурационного файла Сервера, задаваемого на шаге **4**:

- Если на шаге **3** вы выбрали вариант **Создать новую базу данных** или для варианта **Использовать существующую базу данных** на шаге **4** вы не задали путь до конфигурационного файла Сервера, выберите драйвер, который следует использовать. При этом:
    - Вариант **SQLite (встроенная база данных)** предписывает использовать встроенные средства Сервера Dr.Web. Задание дополнительных параметров при этом не требуется.
    - Остальные варианты подразумевают использование соответствующей внешней БД. При этом необходимо указать соответствующие параметры для настройки доступа к БД. Настройки параметров СУБД подробно описаны в приложениях (см. документ **Приложения**, п. Приложение В. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД).
- Если на шаге **3** вы выбрали вариант **Использовать существующую базу данных** и на шаге **4** задали путь до конфигурационного файла Сервера, задайте путь до файла базы данных, которая будет использоваться согласно заданному конфигурационному файлу Сервера.

6. Если на шаге **3** вы выбрали вариант **Создать новую базу данных** или для варианта **Использовать существующую базу данных** на шаге **4** вы не задали путь до конфигурационного файла Сервера, откроется окно **Конфигурация сети**. В данном окне настраивается сетевой протокол для работы Сервера (разрешается задать только один сетевой протокол; дополнительные протоколы можно настроить в дальнейшем).

Чтобы задать настройки сети из предустановленного набора, выберите в выпадающем списке один из следующих вариантов:

- **Стандартная конфигурация** предписывает использование настроек по умолчанию на основе службы обнаружения Сервера.
- **Ограниченная конфигурация** предписывает ограничение работы Сервера только внутренним сетевым интерфейсом — 127.0.0.1. При этих настройках управление Сервером возможно только из Центра управления, открытого на том же компьютере, а также к Серверу может подключиться только Агент, запущенный на том же компьютере. В дальнейшем, после отладки настроек Сервера, настройки сети можно будет изменить.
- **Пользовательская конфигурация** означает изменение следующих предустановленных настроек:
    - В полях **Интерфейс** и **Порт** задайте соответствующие значения для обращения к Серверу. По умолчанию задан интерфейс 0.0.0.0, это означает, что к Серверу возможен доступ по всем интерфейсам.

По умолчанию используется порт 2193.

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

- Установите флажок **Ограничить доступ к Серверу Dr.Web**, чтобы ограничить локальный доступ к Серверу. Доступ Инсталляторам Агентов, Агентам и другим Серверам (в случае уже существующей антивирусной сети, построенной с помощью Dr.Web Enterprise Security Suite) будет запрещен. В дальнейшем эти настройки можно будет изменить через меню Центра

управления **Администрирование**, пункт **Конфигурация Сервера Dr.Web**, вкладка **Модули**.

- Установите флажок **Включить службу обнаружения Сервера Dr.Web**, если хотите, чтобы Сервер отвечал на широковещательные и многоадресные запросы других Серверов по IP-адресу и имени сервиса, заданным в соответствующих полях ниже.

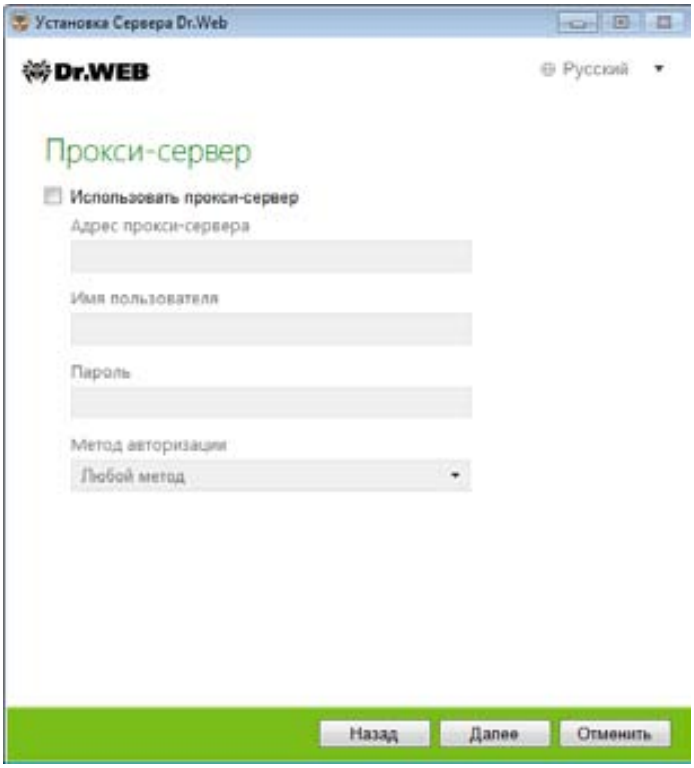
7. Если на шаге **3** вы выбрали вариант **Создать новую базу данных** или для варианта **Использовать существующую базу данных** на шаге **4** вы не задали путь до конфигурационного файла Сервера, откроется окно **Прокси-сервер** для настройки параметров использования прокси-сервера при подключении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

Чтобы п одключения к Серверу осуществлялись через прокси-сервер, установите флажок **Использовать прокси-сервер**.

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

Задайте следующие параметры подключения к прокси-серверу:

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



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

Для того чтобы агенты обращались к серверу с использованием SRV-записи, необходимо задать тип подключения через протокол srv. Например, запустив инсталлятор агента с явным указанием сервера: drwinst srv/drwcs. В дальнейшем агент прозрачно для пользователя использует функционал протокола SRV для обращения к антивирусному серверу.

Если при обращении антивирусный сервер явно не указан, по умолчанию в качестве имени сервиса используется drwcs.

Примечание. Подробнее о SRV-записях можно прочесть в Википедии: https://ru.wikipedia.org/wiki/SRV-запись

Для регистрации задайте следующие параметры:

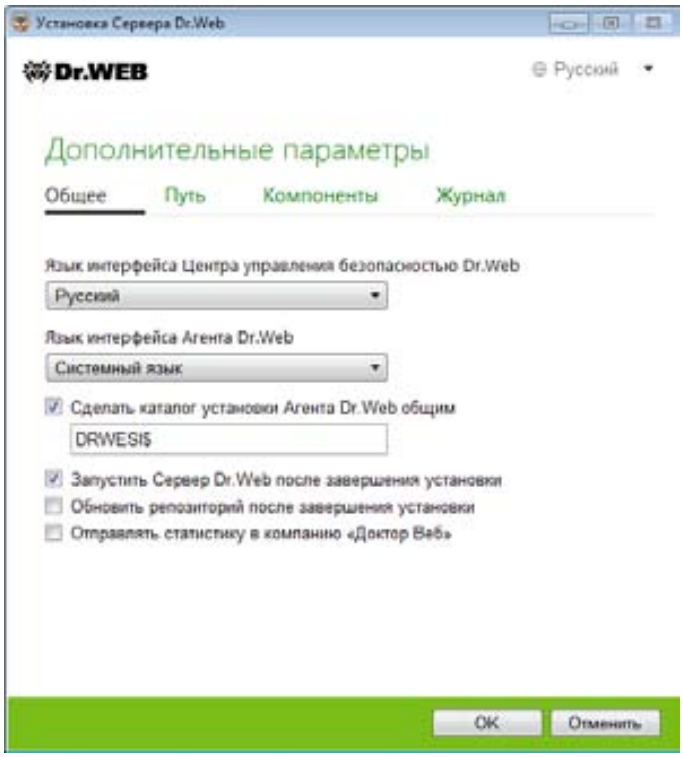
- Установите флажок **Зарегистрировать Сервер Dr.Web в Active Directory**.
- В поле **Домен** укажите название домена Active Directory, в котором будет зарегистрирован Сервер. Если домен не указан, используется домен, в котором зарегистрирован компьютер, на котором осуществляется установка.
- В полях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

9. Если на шаге **3** вы выбрали вариант **Создать новую базу данных**, откроется окно **Пароль администратора**. Задайте пароль администратора антивирусной сети, создаваемого по умолчанию с регистрационным именем **admin** и полным набором прав для управления антивирусной сетью.

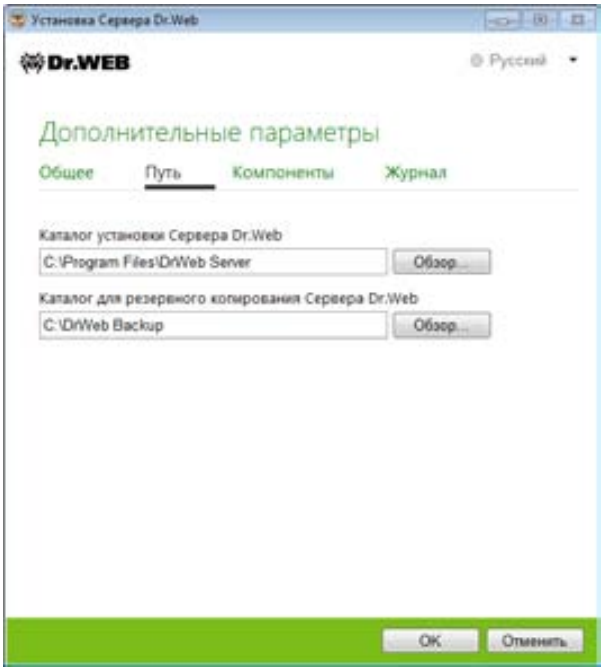
10. В следующем окне Мастер извещает о готовности к установке Сервера. При необходимости вы можете настроить дополнительные параметры установки. Для этого

нажмите пункт **Дополнительные параметры** в нижней части окна и задайте следующие настройки:

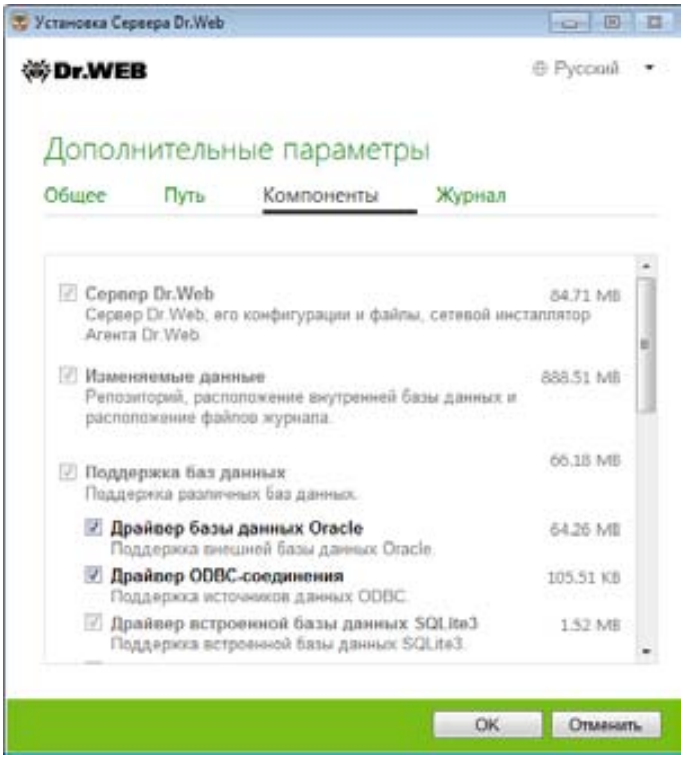
- На вкладке **Общее**:
  - В выпадающем списке **Язык интерфейса Центра управления безопасностью Dr.Web** выберите язык по умолчанию для интерфейса Центра управления безопасностью Dr.Web.
  - В выпадающем списке **Язык интерфейса Агента Dr.Web** выберите язык по умолчанию для интерфейса Агента Dr.Web и компонентов антивирусного пакета, устанавливаемых на станциях.
  - Установите флажок **Сделать каталог установки Агента Dr.Web общим**, чтобы изменить режим использования и наименование разделяемого ресурса для каталога установки Агента (по умолчанию задается скрытое имя разделяемого ресурса).
  - Установите флажок **Запустить Сервер Dr.Web после завершения установки**, чтобы автоматически запустить Сервер после установки.
  - Установите флажок **Обновить репозиторий после завершения установки**, чтобы автоматически обновить репозиторий Сервера сразу после завершения установки.
  - Установите флажок **Отправлять статистику в компанию «Доктор Веб»**, чтобы разрешить отправку статистики по вирусным событиям в компанию «Доктор Веб».



- На вкладке **Путь**:
  - В поле **Каталог установки Сервера Dr.Web** задается каталог, в который осуществляется установка Сервера. Для изменения каталога, задаваемого по умолчанию, нажмите кнопку **Обзор** и выберите требуемый каталог.
  - В поле **Каталог для резервного копирования Сервера Dr.Web** задается каталог, в который осуществляется резервное копирование критичных данных Сервера согласно расписанию заданий Сервера. Для изменения каталога, задаваемого по умолчанию, нажмите кнопку **Обзор** и выберите требуемый каталог.



- На вкладке **Компоненты** вы сможете выбрать компоненты, которые вы хотите установить.

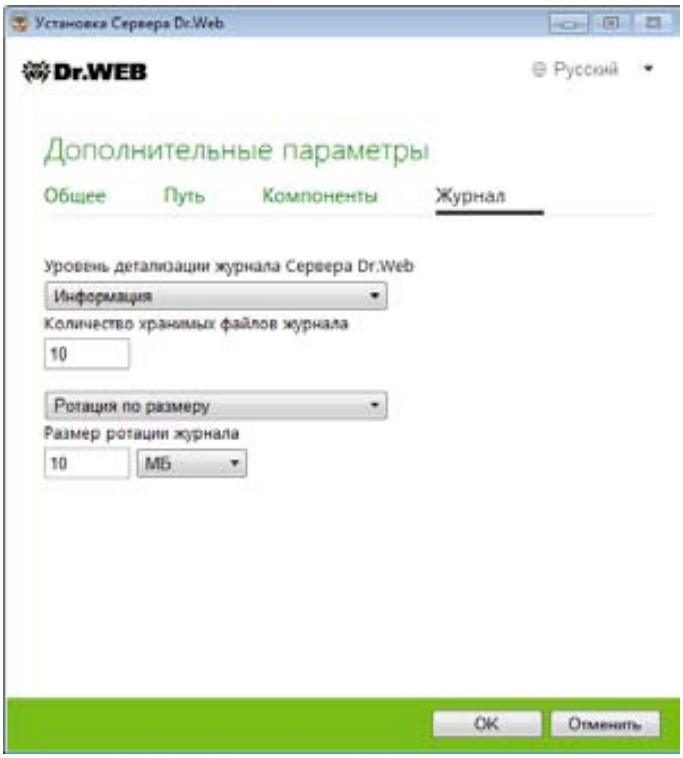


Внимание! Если вы планируете использовать в качестве внешней базы данных ODBC для Oracle, отмените установку встроенного клиента для СУБД Oracle (в разделе **Поддержка баз данных → Драйвер базы данных Oracle**).

В противном случае работа с БД Oracle будет невозможна из-за конфликта библиотек.

- На вкладке **Журнал** вы можете задать настройки ведения журнала установки и работы Сервера.

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



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

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

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

- Каталог **Управление сервером** содержит команды запуска, перезапуска и завершения работы Сервера, а также команды настройки ведения журнала и другие команды Сервера, подробнее описанные в документе **Приложения**, п. H4. Сервер Dr.Web.
- Пункт **Веб-интерфейс** — для открытия Центра управления и подключения к Серверу, установленному на данном компьютере (по адресу http://localhost:9080).
- Пункт **Документация** — для открытия документации администратора в формате HTML.

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

Внимание! В случае возникновения ошибок при установке антивирусного сервера на ОС Windows 2003 вида: «Данная установка запрещена политикой, выбранной системным администратором» (The system administrator has set polices to prevent this installation) необходимо установить обновление для ОС Windows (с учетом языка используемой ОС), которое можно скачать по адресу http://support.microsoft.com/kb/925336.

6.3.4. Установка дополнительных инсталляционных пакетов агентов защиты на серверы Dr.Web Enterprise Security Suite под ОС Windows

Дополнительный дистрибутив (extra) включает дистрибутивы инсталляционных пакетов антивирусных агентов, не входящие в состав основного дистрибутива. Его установка должна осуществляться на компьютер с уже установленным основным дистрибутивом Сервера Dr.Web. Описание установки основного дистрибутива Сервера приведено в разделах Установка Сервера Dr.Web для ОС Windows® и Установка Сервера Dr.Web для ОС семейства UNIX®.

Примечание. Дополнительный дистрибутив должен устанавливаться из пакета того же типа, что и основной дистрибутив.

Для установки дополнительного дистрибутива Сервера Dr.Web на компьютер с ОС Windows:

1. Запустите файл дистрибутива.
2. Откроется окно **Dr.Web ESuite Extra** с информацией об устанавливаемом продукте и текстом лицензионного соглашения. После ознакомления с условиями лицензионного договора, для продолжения установки выберите **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Установить**.
3. Начнется установка дополнительного дистрибутива. При отсутствии ошибок в процессе установки вмешательство пользователя не требуется.
4. После завершения установки нажмите кнопку **Готово**. Перезагрузка компьютера не требуется.

6.3.5. Установка Центра управления Dr.Web Enterprise Security Suite для ОС семейства UNIX

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

Чтобы установить Сервер Dr.Web для ОС семейства UNIX:

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

./ drweb-11.00.0-<*сборка*>-esuite-server-<*версия_ОС*>.run

Для запуска установочного пакета можете использовать ключи командной строки. Параметры команды запуска приведены в документе **Приложения**, п. H8. Инсталлятор Сервера Dr.Web для ОС семейства UNIX®.

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

2. Далее приводится текст лицензионного соглашения. Для продолжения установки вам необходимо принять лицензионное соглашение.

3. На запрос о каталоге для резервного копирования задайте путь до нужного каталога или подтвердите резервное копирование в каталог по умолчанию — /var/tmp/drwcs.

4. Если в системе был обнаружен дополнительный дистрибутив (extra), будет выведена информация об удалении дополнительного дистрибутива перед началом установки пакета Сервера. Возможность продолжить установку без удаления дополнительного дистрибутива не предоставляется.

5. Далее будет произведена установка ПО, в ходе которой инсталлятор может попросить подтверждения ваших действий от имени администратора.

6. В процессе установки генерируется случайный пароль для главного администратора. После завершения установки этот пароль выводится через консоль в результатах установки Сервера.

Созданный пароль администратора сохраняется в базе данных Сервера. При необходимости вы можете уточнить данный пароль с использованием средств управления базой данных в случае использования внешней базы или же при помощи утилиты **drwidbsh** для встроенной базы данных (для более подробной информации см. документ **Приложения**, п. Восстановление пароля администратора Dr.Web Enterprise Security Suite).

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

Используйте команды:

•*/usr/local/etc/rc.d/drwcsd.sh stop* — для ручной остановки Сервера;

•*/usr/local/etc/rc.d/drwcsd.sh start* — для ручного запуска Сервера.

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

Установку Сервера можно прервать в любой момент, отправив процессу установки любой из следующих сигналов: SIGHUP, SIGINT, SIGTERM, SIGQUIT и SIGWINCH (в операционной системе **FreeBSD** изменение размеров окна терминала влечет отправку сигнала SIGWINCH). При прерывании процесса установки производится полный откат изменений в файловой системе до начала установки. Установка rpm-пакета может быть прервана нажатием клавиш CTRL + C. Нажатие кнопки ESC в процессе инсталляции Сервера позволяет вернуться к предыдущему шагу установки. При этом на шаге 2 (первое окно инсталлятора с лицензионным соглашением) кнопка ESC прерывает работу инсталлятора.

После завершения процесса установки комплекса вам будет предложено запустить сервис. Для проверки успешности установки рекомендуется осуществить пробный запуск.

После того как сервис будет запущен, следует убедиться в наличии его процесса в списке процессов системы с помощью команды:

```
#ps aux | grep drwcsd
```

В случае успешного запуска сервера данная команда вернет строку, похожую на:

```
drwcs 85076 0.0 0.6 108888 51148 ?? Is Thu04PM 0:42.10 drwcsd: 4-17:51:39; 8
ttl, 3 max, 0 now; 0 agn, 0 con, 0 new, 0 ins, 0 srv;
```

Помимо наличия процесса, рекомендуется проверить лог сервера:

для FreeBSD: `/var/drwcs/log/drwcsd.log`
для GNU/Linux: `/var/opt/drwcs/log/drwcsd.log`

Также лог можно найти с помощью команды: `# find / -name 'drwcsd.log'`

6.3.6. Настройка сервера Samba

Если вы хотите производить развертывание антивирусной сети с использованием выложенных в общедоступной папке инсталляционных файлов, вам необходимо настроить сервер Samba. Для этого вам будет необходимо отредактировать файл конфигурации /etc/samba/smb.conf и перезапустить сервис smb. Например:

```
cd /etc/samba

vi /etc/samba/smb.conf

/etc/init.d/smb stop

/etc/init.d/smb start
```

```
[root@centos104 samba]# vi smb.conf
[root@centos104 samba]# /etc/init.d/smb start
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]
```

Пример файла smb.conf

```
[global]

        workgroup = DRWEB

        server string = ES

        netbios name = es

        security = share

        hosts allow =  192.168.100.  127.

        log file = /var/log/smb.log

        max log size = 1024

        interfaces = 192.168.100.66/28

        guest account = drwcs

        local master = NO

        display charset = utf-8

        unix charset = utf-8

        dos charset = cp866

[Public]

        comment = Public

        path = /opt/drwcs/Installer

        public = yes
```

```
browseable = yes

read only = yes

printable = no
```

6.3.7. Установка Центра управления в режиме командной строки для ОС Linux

Получив доступ к серверу Linux, перейдите к директории с дистрибутивами и выполните команду установки инсталляционного пакета.

Например:

```
sh ./ drweb-11.00.0-201805310-esuite-server-unix-linux-x86_64.tar.gz.run
```

Либо измените права на запуск дистрибутива и запустите его.

Внимание! Центр управления для своей работы требует наличия определенных библиотек, перечисленных в разделе системных требований. В случае их отсутствия необходимо их установить или создать соответствующие линки.

Например:

```
yum list all | grep curl

yum install libcurl.i686

ln -s /usr/lib/libcurl.so.4 /usr/lib/libcurl.so.3
```

Сразу после запуска необходимо ознакомиться с текстом лицензионного договора и принять его (набрав в командной строке **yes** и нажав **Enter**), выбрать группу и пользователя, от имени которого будет работать сервер (по умолчанию это drwcs). Если вы согласны на значение по умолчанию, то необходимо просто нажать **Enter**.

Далее будет произведена установка ПО, в ходе которой инсталлятор может попросить подтверждения ваших действий от имени администратора.

Установка сервера завершена. Имя администратора антивирусной сети по умолчанию **admin**. Пароль root

Аналогично установке через GUI, в процессе установки ПО для FreeBSD создается rc-скрипт `/usr/local/etc/rc.d/drwcsd.sh`.

Каталог установки Сервера Dr.Web имеет следующую структуру:

/opt/drwcs/ для ОС Linux и */usr/local/drwcs* для ОС FreeBSD:

- bin — исполняемые файлы Сервера Dr.Web.
- doc — файлы лицензионных соглашений.
- ds-modules — распакованные скриптовые модули.
- fonts — шрифты для PDF-документов.
- lib — набор библиотек для работы Сервера.

- vfs — запакованные скриптовые модули и языковые пакеты.
- webmin — элементы Центра управления.
- websockets — скрипты для работы с веб-сокетами.

/var/opt/drwcs/ для ОС Linux и */var/drwcs* для ОС FreeBSD:

- backup — резервные копии БД и других критичных данных.
- coredump — дампы падений Сервера. Создается при появлении дампов.
- etc — основные конфигурационные файлы компонентов антивирусной сети.
- extensions — скрипты пользовательских процедур, предназначенные для автоматизации выполнения определенных заданий.
- installers-cache — кэш для хранения персональных и групповых инсталляционных пакетов Агента при создании станций в Центре управления. Создается при создании инсталляционных пакетов.
- file-cache — файловый кэш.
- log — файлы журнала Сервера.
- plugins — временные объекты подключаемых модулей.
- objects — кэш объектов Центра управления.
- reports — временный каталог для генерации и хранения отчетов. Создается при необходимости.
- repository — каталог обновлений, в который помещаются актуальные обновления вирусных баз, файлов антивирусных пакетов и компонентов антивирусной сети. Каталог содержит подкаталоги для отдельных функциональных компонентов ПО, а внутри них — подкаталоги для отдельных ОС. Каталог должен быть доступен для записи пользователю, от имени которого запускается Сервер (как правило, пользователь **drwcs**).
- run — ID процесса Сервера.
- sessions — сессии Центра управления.
- tmp — временные файлы.
- twin-cache — распакованные вирусные базы для обратной совместимости с предыдущими версиями Агентов Dr.Web. Также может содержать другие распакованные файлы из репозитория, например инсталлятор Агента.
- upload — директория для загрузки временных файлов, которые задаются через Центр управления. Создается при загрузке файлов большого объема.

/etc/opt/drweb.com/ для ОС Linux и */usr/local/etc/drweb.com* для ОС FreeBSD:

- software/drweb-esuite.remove — скрипт для удаления Сервера.
- + возможно дополнительные файлы и каталоги.

/usr/local/etc/rc.d/ для ОС FreeBSD:

- drwcsd — скрипт для запуска и останова Сервера.

/var/tmp/drwcs — резервная копия после удаления Сервера.

Основные конфигурационные файлы

Файл	**Описание**	**Каталог по умолчанию**
agent.key (имя может	лицензионный ключ Агента	•для ОС Linux:

Файл	Описание	Каталог по умолчанию
отличаться)		
certificate.pem	сертификат для SSL	
common.conf	конфигурационный файл (для некоторых ОС семейства UNIX)	
database.conf	шаблон настроек базы данных с параметрами по умолчанию	
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента	
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера	
drwcsd.conf.distr	шаблон конфигурационного файла Сервера с параметрами по умолчанию	
drwcsd.pri	закрытый ключ шифрования	
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует	/var/opt/drwcs/etc
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера	•для ОС FreeBSD: /var/drwcs/etc
http-alerter-certs.pem	сертификаты для верификации хоста apple-notify.drweb.com при отправке push-уведомлений	
private-key.pem	закрытый ключ RSA	
yalocator.apikey	API-ключ для расширения Yandex.Locator	
webmin.conf	конфигурационный файл Центра управления	
auth-ldap.conf	конфигурационный файл внешней авторизации администраторов через LDAP	
auth-ldap-rfc4515.conf	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме	
auth-pam.conf	конфигурационный файл внешней авторизации администраторов через PAM	
auth-radius.conf	конфигурационный файл	

Файл	Описание	Каталог по умолчанию
	внешней авторизации администраторов через RADIUS	
database.sqlite	встроенная БД	•для ОС Linux: /var/opt/drwcs •для ОС FreeBSD: /var/drwcs
drwcsd.pub	открытый ключ шифрования	•для ОС Linux: /opt/drwcs/webmin/install •для ОС FreeBSD: /usr/local/drwcs/webmin/install

6.3.8. Установка дополнительных инсталляционных пакетов агентов защиты на сервера Dr.Web Enterprise Security Suite для ОС семейства UNIX

1. Запустите файл дистрибутива при помощи следующей команды:

./drweb-11.00.0-<*сборка*>-esuite-extra-<*версия_ОС*>.run

2. Далее приводится текст лицензионного соглашения. Для продолжения установки вам необходимо принять лицензионное соглашение.

3. Далее будет произведена установка ПО.

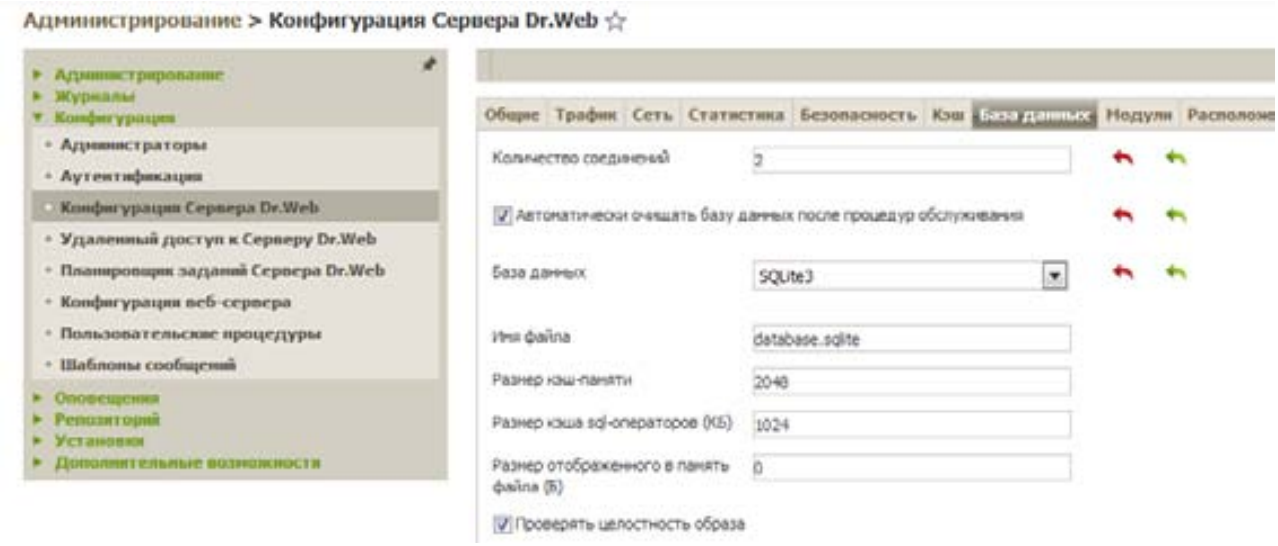
6.3.9. Установка внешней БД

Часто в ходе работы антивирусной сети возникает ситуация, когда возможностей внутренней базы данных становится недостаточно для обеспечения стабильной и бесперебойной работы антивирусной сети.

Для того чтобы настроить параметры работы с базой данных:

1. Выберите пункт **Администрирование** главного меню Центра управления.
2. В открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**.
3. Перейдите на вкладку **База данных** и выберите в выпадающем списке **База данных** тип базы данных:

   - SQLite3 — встроенная БД (компонент **Сервера Dr.Web**). Для встроенной БД при необходимости введите в поле **Файл** полный путь к файлу с базой данных и задайте размер кэш-памяти и режим записи данных.



- ODBC, MySQL или PostgreSQL — внешняя БД.
- Oracle — внешняя БД (для платформ, кроме FreeBSD).

  При использовании внешней СУБД Oracle необходимо установить последнюю версию ODBC-драйвера, поставляемую с данной СУБД. Использование ODBC-драйвера Oracle, поставляемого Microsoft, категорически не рекомендовано.

По умолчанию предусмотрено использование встроенной БД, но это создает значительную вычислительную нагрузку на Сервер Dr.Web, в результате при увеличении размера антивирусной сети удобным становится переход на внешнюю БД. Как было сказано ранее, в зависимости от мощности ПК, на котором установлен Сервер Dr.Web, и спользование внутренней БД эффективно при подключении к Серверу Dr.Web не более 1000 рабочих станций.

В качестве примера рассмотрим особенности установки Microsoft SQL Server 2017 Express Edition SP1, PostgreSQL, а также процедуру перехода с внутренней базы ES-сервера на внешнюю под эти СУБД.

Внимание! Для обеспечения необходимой производительности работы сервера настоятельно рекомендуется использовать внешнюю БД PostgreSQL версии не ниже **8.3.x** (самая ранняя поддерживаемая версия — 7.4). Дистрибутив PostgreSQL и драйвер ODBC можно скачать с сайта www.postgresql.org.

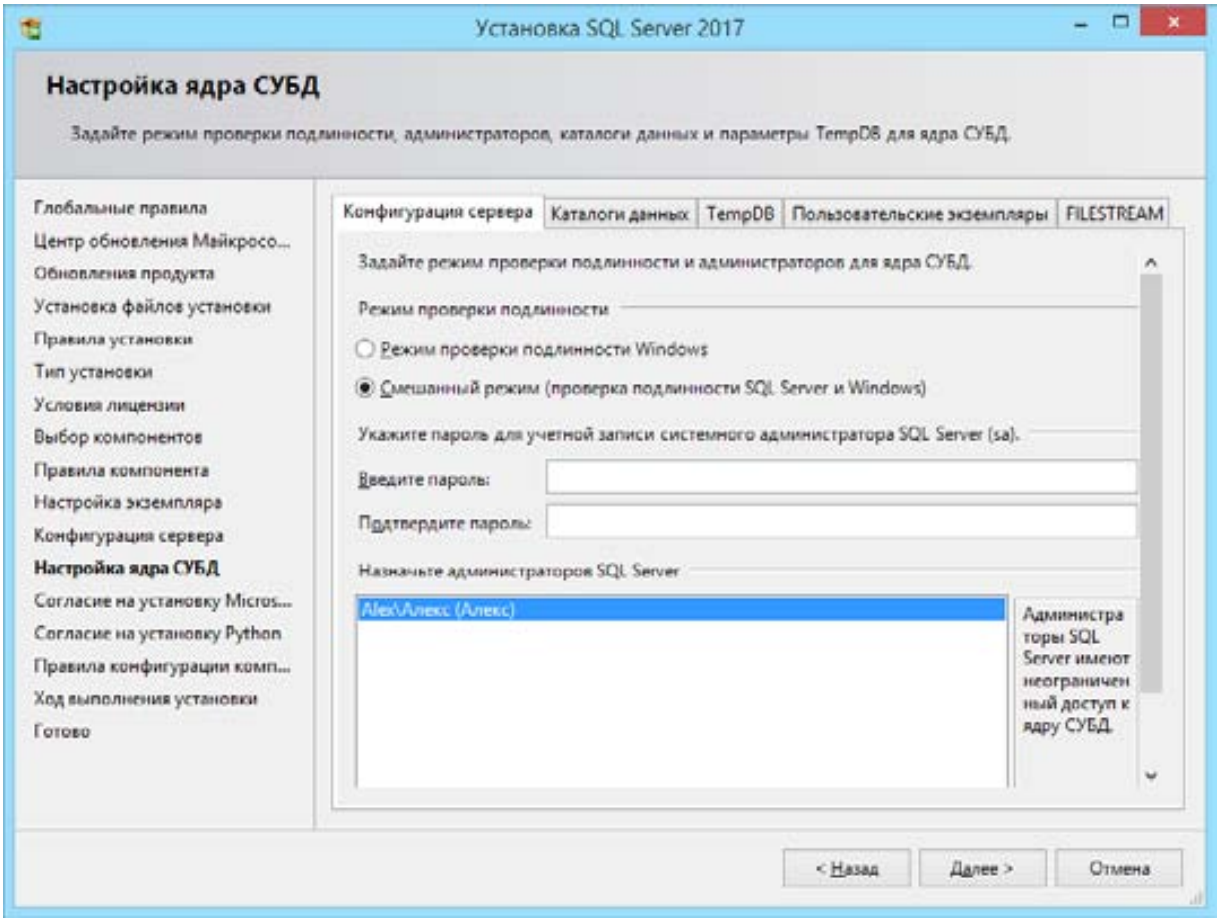
6.3.9.1. Установка Microsoft SQL Server 2017 SP1 Express и настройка параметров ODBC-драйвера

Загрузить актуальный дистрибутив Microsoft SQL Server 2017 Express SP1, а также компоненты, необходимые для использования данной СУБД, можно по ссылке: https://go.microsoft.com/fwlink/?linkid=853017. Данная СУБД совместима с о всеми поддерживаемыми версиями Windows, для е е работы необходимо компонент .Net Framework 4, который можно скачать по ссылке: https://www.microsoft.com/ru-ru/Download/details.aspx?id=17851.

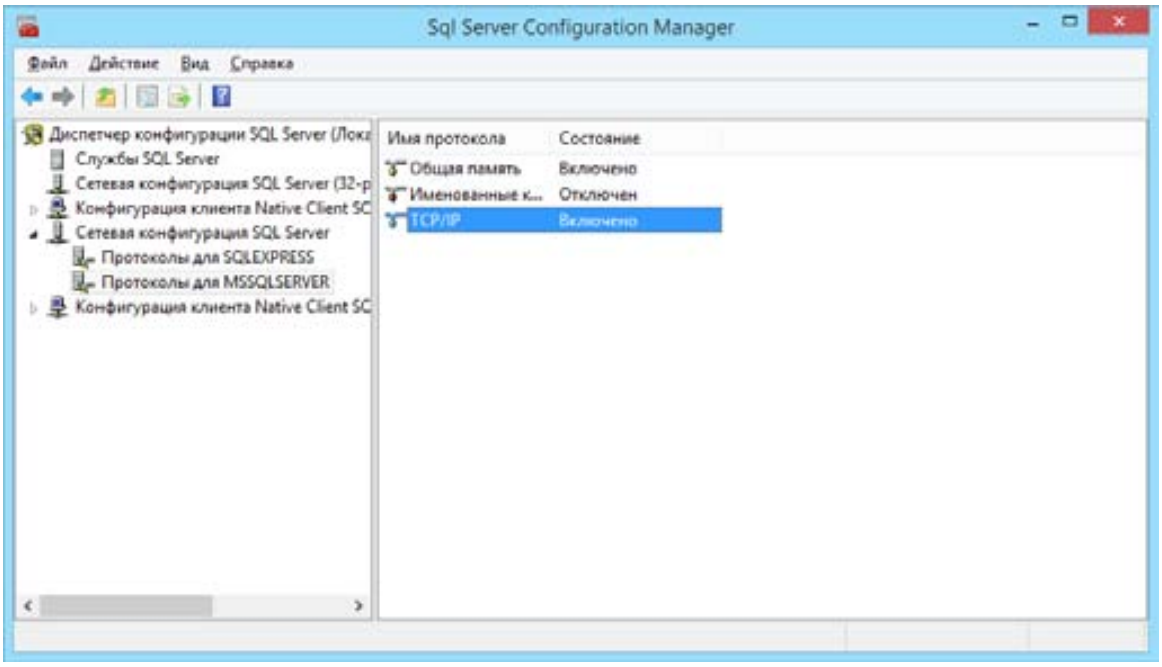
Ниже предполагается, что SQL Server и ES-сервер находятся на разных компьютерах локальной сети и между ними есть связь по протоколу TCP/IP.

При установке Microsoft SQL Server 2017 Express SP1 обратите внимание на следующие моменты.

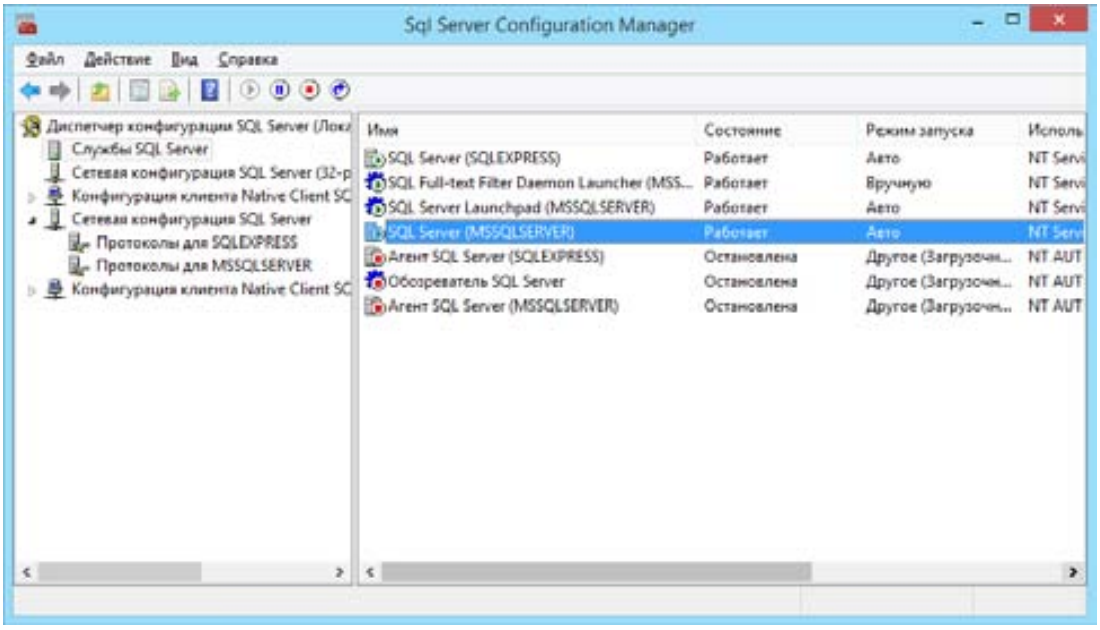
1. При установке пакета выберите тип **Пользовательский**.
2. На этапе установки **Настройка ядра СУБД** выберите пункт **Смешанный режим (проверка подлинности SQL Server и Windows)**. Введите также любой пароль для встроенной учетной записи системного администратора SQL Server. Этот пароль необходимо запомнить.



3. После установки Microsoft SQL Server необходимо открыть на компьютере с СУБД **SQL Server Configuration Manager** и включить протокол **TCP/IP**.



После этого для дальнейшей работы необходимо перезагрузить службу SQL-сервера.

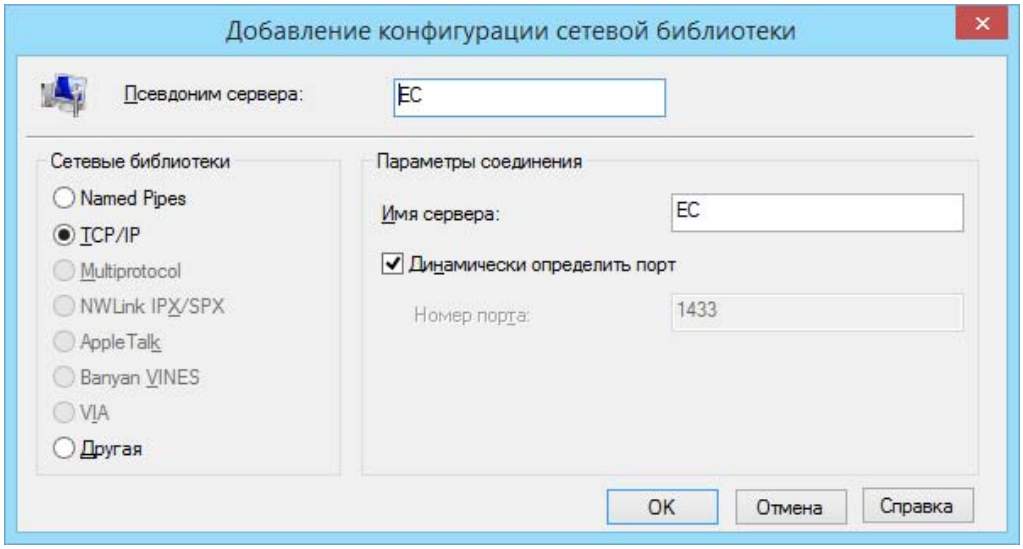


4. Для настройки ODBC-драйвера необходимо на компьютере с установленным ES-сервером произвести следующие действия (в примере рассматривается Windows 7 Максимальная):

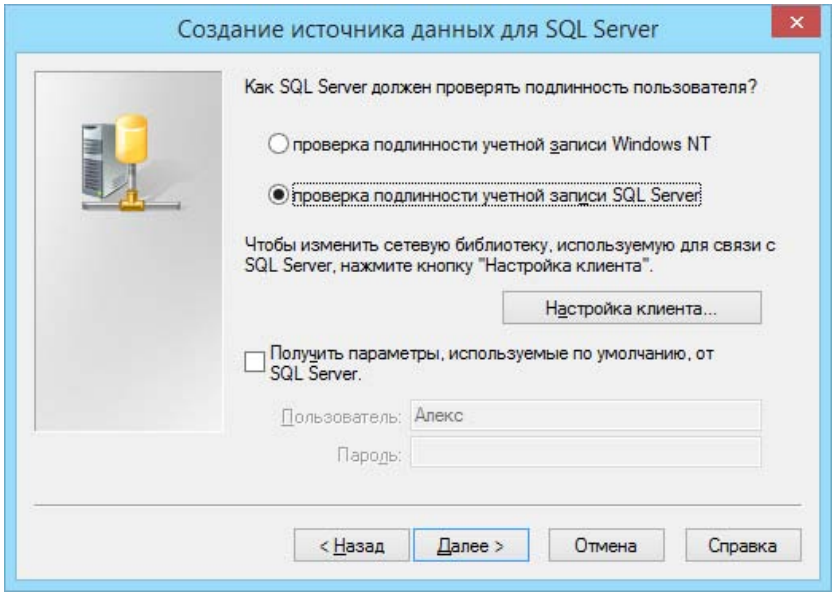
    1. В **Панели управления Windows** выберите пункт **Администрирование**, в открывшемся окне дважды щелкните по значку **Источники данных (ODBC)**. Откроется окно **Администратор источников данных ODBC**. Перейдите на вкладку **Системный DSN**.
    2. Нажмите на кнопку **Добавить**. Откроется окно выбора драйвера.
    3. Выберите в списке пункт **SQL Server** и нажмите на кнопку **Готово**. Откроется первое из окон настройки доступа к серверу баз данных.

        При использовании внешней СУБД необходимо установить последнюю версию ODBC-драйвера, поставляемую с данной СУБД. Использование ODBC-драйвера, поставляемого вместе с ОС Windows, не рекомендовано. Исключением являются БД, поставляемые Microsoft без ODBC-драйвера.

    4. Укажите параметры доступа к источнику данных, совпадающие с заданными в настройках антивирусного сервера. При этом в поле **Сервер** в выпадающем списке название сервера, на котором установлена СУБД, должно отобразиться автоматически. Нажмите на кнопку **Далее**. Откроется следующее окно настройки.
    5. Введите необходимые настройки доступа к БД в этом окне. Нажмите **Настройка клиента**. Откроется окно выбора и настройки сетевого протокола.



6. Выберите сетевую библиотеку для протокола **TCP/IP** или **Named pipes**. Нажмите **ОК**.
7. Убедитесь, что выбрана опция **Только при отключении** и установлены следующие флажки: **Заключенные в кавычки идентификаторы в формате ANSI**, **Значения null**, **Шаблоны и предупреждения в формате ANSI**. Нажмите кнопку **Далее**. Откроется последнее окно настройки доступа.
8. Выберите пункт **Проверка подлинности учетной записи SQL Server**. В поле **Пользователь** наберите sa, в поле **Пароль** введите тот же пароль администратора СУБД, который вы ввели при установке СУБД. Нажмите дважды на кнопку **Далее**.



9. Если при настройке ODBC-драйвера имеется возможность изменить язык системных сообщений SQL-сервера, необходимо установить английский язык. В этом случае на экране мастера выберите пункт **Изменить язык системных сообщений SQL-сервера на** и выберите **English**.
10. Нажмите на кнопку **Готово**, а затем **ОК**.

6.3.9.2. Настройка антивирусного сервера для работы с внешней БД MS SQL

Для того чтобы перейти с внутренней базы данных антивирусного сервера на внешнюю:

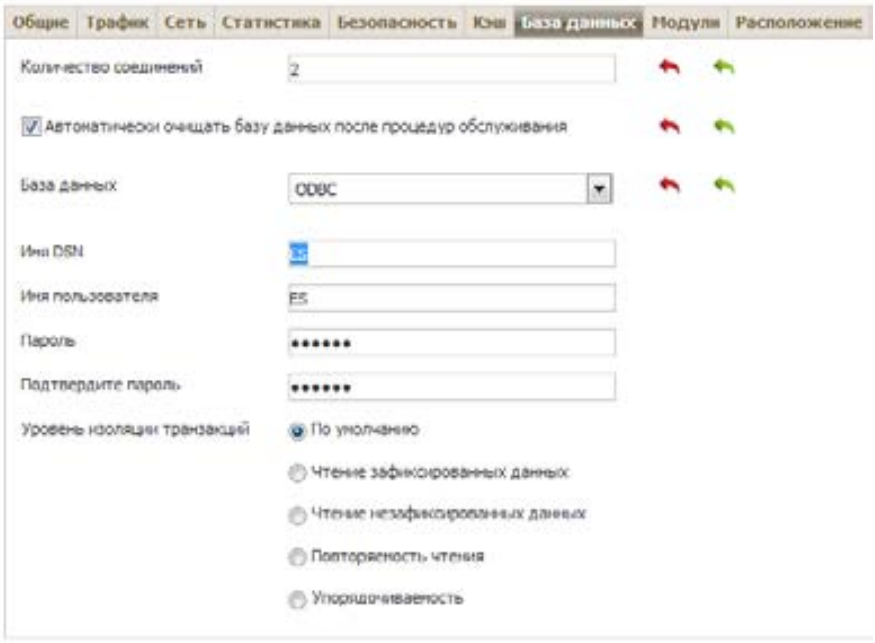
1. Остановите службу ES-сервера с помощью Центра управления — **Администрирование → Dr.Web Server**, нажмите на кнопку (**Остановить Dr.Web Server)**.

2. Выполните экспорт имеющейся внутренней базы данных. Для этого на компьютере с Сервером Dr.Web выполните следующую команду:

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

В результате действия этой команды внутренняя база данных будет экспортирована в файл C:\esbase.es.

3. Запустите службу Dr.Web Server с помощью средств управления службами Windows (**Панель управления → Администрирование → Службы**). Подключитесь к Серверу Dr.Web через Центр управления и настройте сервер на использование внешней базы данных: **Администрирование → Конфигурация Сервера Dr.Web → База данных**, после чего нажмите на кнопку **Сохранить**. Откажитесь от предложения перезапустить сервер.



4. Остановите службу Сервера Dr.Web с помощью Центра управления — **Администрирование → Dr.Web Server**, нажмите на кнопку **Остановить Dr.Web Server**.
5. Проинициализируйте новую базу данных Сервера Dr.Web. Для этого на компьютере с Сервером Dr.Web перепишите в корневую папку диска «C:\» ключ *agent.key*, относящийся к Серверу Dr.Web, и выполните следующую команду:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all initdb C:\agent.key - - root
```

Внимание! Согласно формату команды drwcsd пути к файлам init.sql и drweb32.ini могут быть опущены — вместо их указания достаточно оставить два дефиса. Если убрать два дефиса, то <пароль> будет рассматриваться как путь к init.sql, что приведет к выдаче ошибки.

6. Импортируйте базу данных, которую вы экспортировали на предыдущих этапах, в новую базу данных. Для этого на компьютере с Сервером Dr.Web выполните следующую команду:

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

7. Запустите службу Dr.Web Server с помощью средств управления службами Windows (**Панель управления → Администрирование → Службы**).

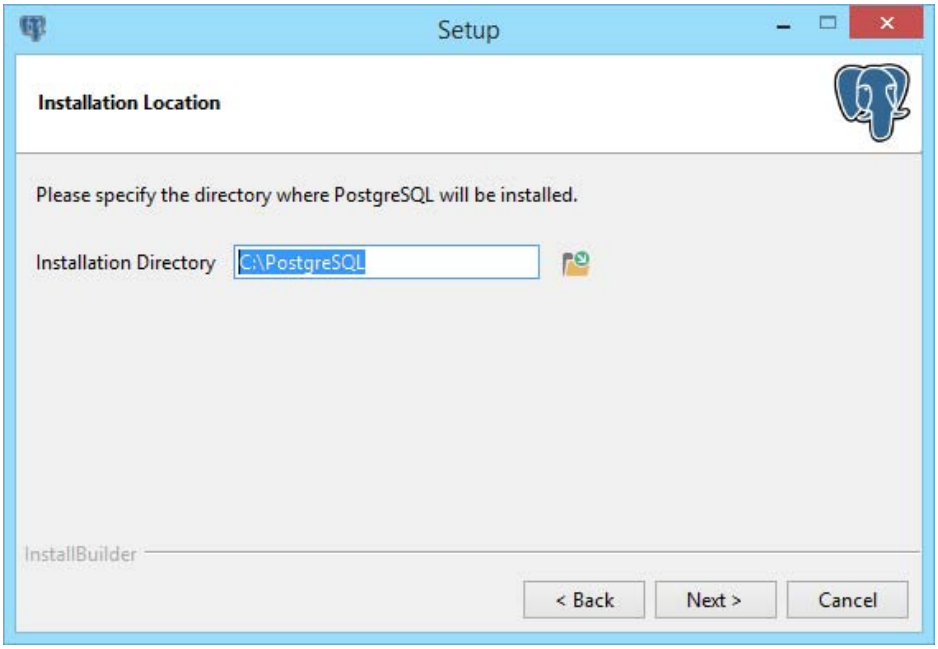
6.3.9.3. Установка PostgreSQL

Установка антивирусного комплекса для ОС Windows начинается с установки внешней БД. Как и в случае рекомендуемой установки на платформу Unix, наиболее предпочтительным является использование PostgreSQL в качестве внешней БД наряду с MS SQL. Также возможно использование БД Oracle.

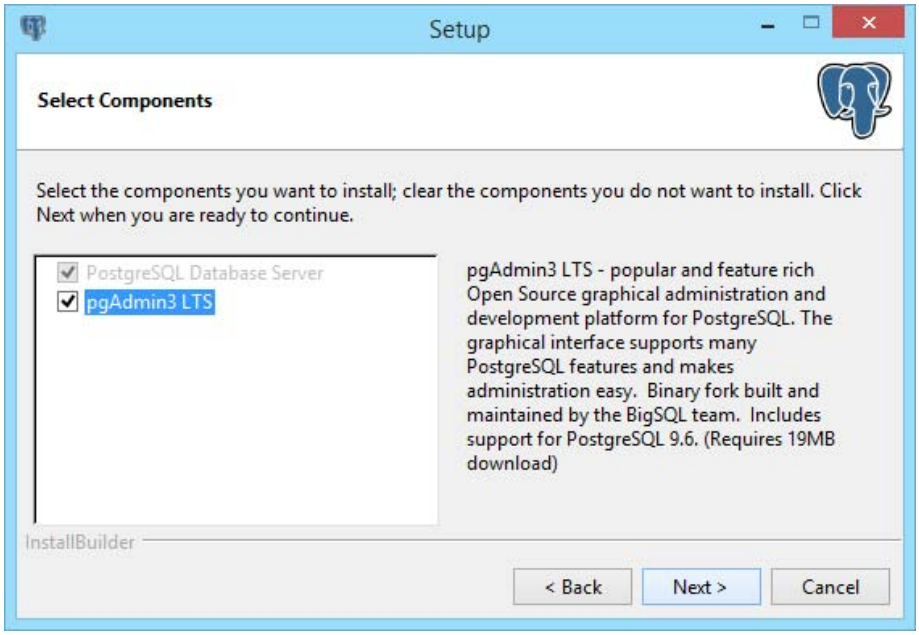
- для **Windows:**

  Актуальная версия PostgreSQL доступна по ссылке http://www.postgresql.org/download/windows.

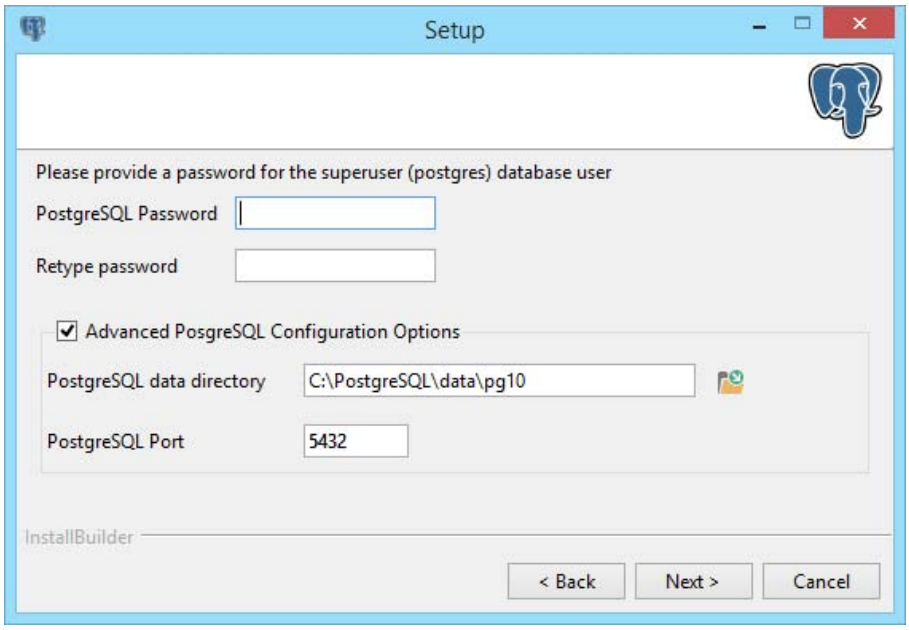
  Установка PostgreSQL начинается с запуска файла дистрибутива. В появившемся окне нажмите кнопку **Next**, затем выберите папку назначения исполняемых файлов, если это требуется, и нажмите **Next** еще раз.

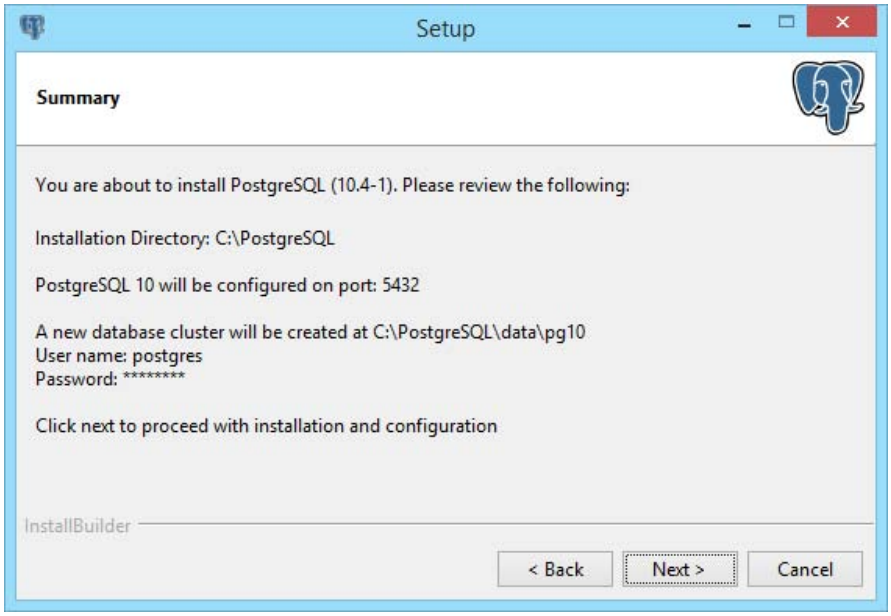


  В следующем окне будет предложено выбрать состав устанавливаемых компонентов. Компонент **pgAdmin3 LTS** — удобный графический интерфейс для работы с этой СУБД.



В следующем окне потребуется ввести пароль суперпользователя БД PostgreSQL (администратора), путь для расположения БД и порт для подключения к ней. Путь и порт можно оставить указанными по умолчанию, а пароль для доступа к БД должен быть длиной не менее 12 символов, чтобы обеспечить необходимую защиту. Нажмите **Next,** просмотрите суммарные сведения и нажмите **Next** для запуска процесса установки.





После завершения установки нажмите кнопку **Finish**.

- для **Debian Linux:** `# apt-get install postgresql`
- для **Linux** (для дистрибутивов, использующих менеджер пакетов yum):

```
# yum install postgres
```

- для **FreeBSD**:

  Перейти в каталог **/usr/ports/databases/postgresql104-server** и выполнить команду **make**, включив поддержку NLS, PAM, XML, INTDATA.

  После чего выполнить команду **make install clean** и дождаться окончания установки.

  Чтобы сервис PostgreSQL запускался автоматически при перезагрузке сервера, необходимо внести изменения в файл **/etc/rc.conf**, добавив в него строку `postgresql_enable="YES"`.

  Если используется **Jail**, нужно внести следующие изменения в конфигурационные файлы:

  /etc/sysctl.conf

  security.jail.sysvipc_allowed=1

  /etc/rc.conf

  jail_sysvipc_allow="YES"

После завершения установки необходимо проверить, что сервис PostgreSQL стартовал, и далее создать пользователя и базу для антивирусного сервера.

Внимание! Для корректной работы с антивирусным сервером желательно, чтобы сервер использовал UTF-8 локаль. Если это невозможно по каким-либо причинам, необходимо как минимум инициализировать БД PostgreSQL с данной локалью, что поможет избежать проблем с БД в будущем. Локаль сервера можно узнать, выполнив команду `locale` от имени суперпользователя.

Прежде всего необходимо инициализировать БД PostgreSQL командой:

- для FreeBSD: `# /usr/local/etc/rc.d/postgresql initdb`
- для Linux: `# /etc/init.d/postgresql initdb`

для Gentoo Linux, возможно, потребуется создать симлинки:

/usr/lib/libssl.so → /usr/lib/libssl.so.6

/usr/lib/libcrypto.so → /usr/lib/libcrypto.so.6

и собрать пакет mit-krb5.

В некоторых более новых версиях PostgreSQL инициализация БД происходит автоматически.

Теперь нужно запустить сервер БД командой

для FreeBSD: `# /usr/local/etc/rc.d/postgresql start`

для Linux: `# /etc/init.d/postgresql-10.4 start`

Следует убедиться, что БД инициализирована и запущена, для этого проверьте последние сообщения из системного лога. В общем случае системный лог находится в файле /var/log/messages:

```
# less /var/log/messages
```

После того как БД запущена, можно приступить к созданию пользователя, который будет владеть базой данных сервиса, так как политика безопасности PostgreSQL в большинстве случаев не позволит выполнять команды, адресованные БД от имени суперпользователя, для успешного продолжения необходимо изменить пользователя. В зависимости от типа ОС имя пользователя может отличаться.

- Для **Windows**:

  Зайдите в меню **Пуск → Все программы → PostgreSQL 10.4 → SQL Shell** (или запустите консоль управления PostgreSQL командой **Пуск → Программы → PostgreSQL 10.4 → Командная строка** и выполните команду *psql -U postgres*). В появившемся окне на вопросы Server [localhost], Database [postgres], Port [5432], Username [postgres] следует ответить нажатием на клавишу ENTER либо ввести актуальные данные, если они отличаются от предложенных по умолчанию, затем следует ввести пароль, который был задан при установке PostgreSQL. После успешной авторизации можно вводить команды:

  для создания пользователя drwcsd:

```
create user drwcs;
alter user drwcs password 'uHtd5aNE';
```

- Для **FreeBSD**:

```
# createuser –U pgsql -S -D -R -P drwcs или # su –l pgsql –c
‘createuser -S -D -R -P drwcs’
```

- Для **Linux**:

```
# createuser –U postgres -A -D -P drwcs или # su –l postgres –c
‘createuser -A -D -P drwcs’
```

В появившемся запросе введите пароль для нового пользователя.

Внимание! Для задания пароля *не используйте пароль из приведенного примера.* В целях безопасности для коммерческого использования рекомендуется создать более криптостойкий пароль длиной не менее восьми символов. Создать криптостойкий псевдослучайный пароль можно с помощью команды `makepasswd –chars=12`. Необходимо запомнить пароль, потому что в дальнейшем он будет использоваться для подключения к БД.

Теперь создадим саму базу данных:

- для **Windows**:

```
create database drwcs_db owner=drwcs encoding='UTF8';
```

Или

```
# su –l pgsql –c 'createdb -E UTF-8 -O drwcs drwcs_db’
```

- для Linux:

createdb –U postgres -E UTF-8 -O drwcs drwcs_db

Или

```
# su –l postgres –c 'createdb -E UTF-8 -O drwcs drwcs_db’
```

После того как процесс создания владельца и самой БД завершен, не следует использовать аккаунт суперпользователя, для этого покиньте оболочку, запущенную от имени владельца БД PostgreSQL, командой `exit` или нажмите `Ctrl-D`.

Настройка типа аутентификации осуществляется с помощью файла pg_hpa, расположенного в подкаталоге data каталога установки Postgres.

6.3.9.4. Примеры запросов во внешнюю БД PostgreSQL

Для осуществления запросов в БД PostgreSQL необходимо подключиться к ней, предварительно сменив учетную запись на используемую для данной БД:

для FreeBSD: `# su pgsql`
для Linux: `# su postgresql`
и выполнить команду: `$ psql drwcs_db`

6.3.9.5. Вывод таблицы администраторов

```
drwcs_db=# SELECT login,password FROM admins;
```

Ответом на данный запрос будет таблица пар login/possword всех учетных записей, зарегистрированных на сервере Enterprise Suite.

6.3.9.6. Вывод размеров таблиц БД антивирусного сервера

```
drwcs_db=# SELECT relname AS name, relfilenode AS oid, (relpages * 8192 / (1024*1024))::int as size_mb, reltuples as count FROM pg_class WHERE relname NOT LIKE 'pg%' ORDER BY relpages DESC;
```

Ответом на данный запрос будет список таблиц с указанием р азмера в мегабайтах и количеством записей в ней.

6.3.9.7. Настройка антивирусного сервера для работы с внешней БД PostgreSQL

Необходимо разрешить антивирусному серверу доступ к БД, для чего нужно отредактировать файл конфигурации БД PosgreSQL, который в зависимости от семейства ОС и настроек располагается:

во FreeBSD: `/usr/local/pgsql/data/pg_hba.conf`
в Linux: `/etc/postgresql/10.4/main/pg_hba.conf`
Также конфигурационный файл можно найти командой: `# find / -name 'pg_hba.conf'`

Откройте этот файл в текстовом редакторе и добавьте в него строку:

```
host drwcs_db drwcs 127.0.0.1/32 md5
```

Следует обратить особое внимание на режим доступа к серверу БД, он должен иметь вид:

```
# «local» is for Unix domain socket connections only
local all all trust
# IPv4 local connections:
host all all 127.0.0.1/32
```

В редких случаях бывает необходимо отредактировать основной конфигурационный файл PostgreSQL postgresql.conf, расположенный в зависимости от ОС:

во FreeBSD: `/usr/local/pgsql/data/postgresql.conf`
в Debian Linux: `/etc/postgresql/10.4/main/postgresql.conf`
который также можно найти командой: `# find / -name 'postgresql.conf'`

В файле следует раскомментировать строки, чтобы получилось:

```
listen_addresses = 'localhost'
port = 5432
```

После того как БД сконфигурирована, нужно перезапустить ее командой:

для FreeBSD: `# /usr/local/etc/rc.d/postgresql restart`

для Linux: `# /etc/init.d/postgresql restart`

Необходимо убедиться, что сервер БД запустился без ошибок, для чего проверим системный лог:

```
# less /var/log/messages
```

Для того чтобы сконфигурировать антивирусный сервер для работы с внешней БД вместо используемой по умолчанию внутренней, необходимо внести изменения в конфигурационный файл drwcsd.conf. В зависимости от используемой ОС он расположен:

во FreeBSD: `/var/drwcs/etc/drwcsd.conf`
в Linux: `/var/opt/drwcs/etc/drwcsd.conf`
также его можно найти командой: `# find / -name 'drwcsd.conf'`

После того как сервер Enterprise Suite был перенастроен на использование внешней БД, необходимо инициализировать ее командой:

для FreeBSD: `# /usr/local/etc/rc.d/drwcsd.sh initdb`
для Linux: `# /etc/init.d/drwcsd initdb`

Внимание! После инициализации БД пароль доступа администратора сбрасывается в значение по умолчанию, а именно root.

Для того чтобы убедиться, что все операции были выполнены верно, следует проверить лог антивирусного сервера. Код завершения процесса должен быть 0x00, что явно отображено в последних строках лога.

6.4. Развертывание антивирусной сети

Основные моменты и этапы подготовки к развертыванию антивирусной сети:

1) Перед первой установкой Агентов необходимо обязательно обновить репозиторий Сервера Dr.Web.
2) Установка Агента должна выполняться пользователем с правами администратора компьютера как при локальной, так и при удаленной установке.
3) Если на защищаемом объекте уже установлен Агент, то перед началом новой инсталляции необходимо удалить установленный Агент. Для этого удаленная установка должна запускаться с ключом **-uninstall**.

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

Установка при помощи Сетевого инсталлятора возможна в двух режимах: графическом и фоновом.

4) При установке Агентов на серверы ЛВС и компьютеры кластера также необходимо учесть:

- Для обеспечения работы Агентов на терминальных серверах Windows (т. е. в ОС Windows с установленными службами **Terminal Services**) в терминальных сессиях пользователей, их установка должна осуществляться только локально с помощью **Мастера установки и удаления программ Windows**.
- На серверы ЛВС, выполняющие важные сетевые функции (домен-контроллеры, серверы раздачи лицензий и т. д.), а также на узлы кластера не рекомендуется устанавливать компоненты **SpIDer Gate**, **SpIDer Mail** и **Брандмауэр** во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса Dr.Web.
- При необходимости защиты кластера — установка Агентов должна выполняться отдельно на каждый узел кластера.
- Если доступ к кворум-ресурсу кластера строго ограничен, рекомендуется исключить его из проверки сторожем **SpIDer Guard** и регулярно проверять с помощью **Сканера Dr.Web**, запускаемого по расписанию или вручную.

5) С помощью сетевого инсталлятора можно проводить установку Агентов только на операционные системы семейства Windows 2000 и новее, включая Windows Vista Starter,

Home Basic, Home Premium; Windows 7 Начальная, Домашняя, Домашняя расширенная. На ПК с другими ОС Агент может быть установлен только локально.

6) Для получения инсталляторов под операционными системами, отличными от ОС Windows, а также полного дистрибутива инсталлятора под ОС Windows необходима установка дополнительного дистрибутива (extra) Сервера Dr.Web.

Внимание! Состав и последовательность шагов установки могут несколько различаться в зависимости от версии дистрибутива.

6.4.1. Установка с использованием Центра управления Dr.Web Enterprise Security Suite

Центр управления предоставляет возможность выявлять компьютеры, на которые еще не установлена антивирусная защита **Dr.Web ES**, и удаленно устанавливать такую защиту.

Для того чтобы удаленно установить **Агент** на рабочие станции, вы должны иметь права администратора соответствующих рабочих станций. Такая установка не требует дополнительной настройки удаленной станции, если она входит в домен и используется доменная учетная запись администратора. В случае если удаленная машина не входит в домен или используется локальная учетная запись для установки, то для ряда версий ОС Windows необходима дополнительная настройка удаленной машины.

Внимание! Настройка для удаленной установки может снизить безопасность удаленной машины. Настоятельно рекомендуется ознакомиться с назначением указанных настроек перед внесением изменений в систему либо отказаться от использования удаленной установки и установить Агент вручную на рабочую станцию вне домена или с использованием локальной учетной записи.

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

- Для Windows 2000, Windows Server 2000, Windows Server 2003 дополнительная настройка не требуется.
- Для Windows Vista, Windows 7, Windows Server 2008:
  - Включить опцию Общий доступ к файлам: **Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Общий доступ и сетевое обнаружение → Общий доступ к файлам → Включить**.
  - Включить встроенную локальную учетную запись администратора и установить на нее пароль. При установке использовать эту учетную запись: **Панель управления → Система и ее обслуживание → Администрирование → Управление компьютером → Локальные пользователи и группы → Пользователи**. Щелчок левой кнопкой по записи **Администратор →** снять флажок **Заблокировать учетную запись → OK**. Щелчок правой кнопкой по записи **→ Задать пароль →** задайте пароль.
  - Создайте ключ **LocalAccountTokenFilterPolicy**:
    - В редакторе реестра откройте ветку HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Если записи **LocalAccountTokenFilterPolicy** не существует, в меню **Правка** выберите **Создать** и задайте значение **DWORD**. Введите значение **LocalAccountTokenFilterPolicy** и нажмите **ENTER**.
    - В контекстном меню пункта **LocalAccountTokenFilterPolicy** выберите **Изменить**.
    - В поле **Значение** задайте значение **1** и нажмите **OK**.

Перезагрузка не требуется.

В случае если учетная запись на удаленной машине имеет пустой пароль, нужно установить в локальных политиках политику доступа с пустым паролем: **Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Учетные записи: ограничить использование пустых паролей только для консольного входа → Отключить**.

В случае установки через обозреватель сети, как и при установке вручную, необходимо, чтобы на антивирусном сервере был открыт для общего доступа каталог %DrWeb_ES%\Installer (по умолчанию в ОС Windows это каталог C:\Program Files\DrWeb Server\Installer, его сетевое имя по умолчанию DRWESI$), содержащий два файла: drwcsd.pub и drwinst.exe. Данный каталог с указанными файлами создается автоматически в процессе инсталляции Сервера Dr.Web.

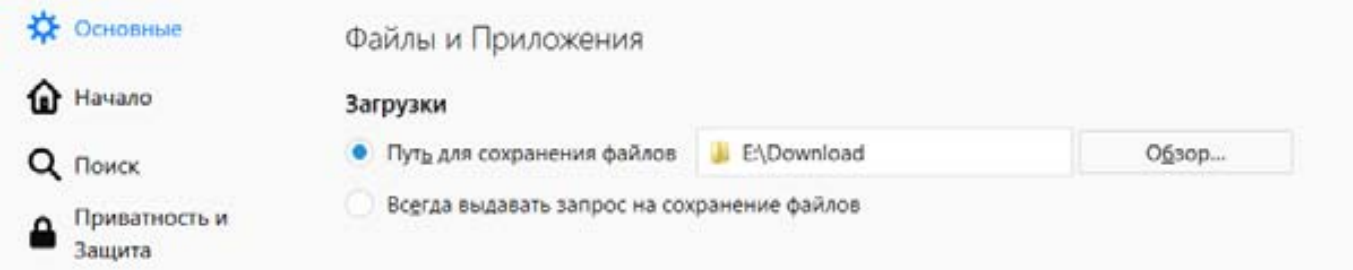
Внимание! Если Сервер Dr.Web установлен не на серверную операционную систему, общая папка может быть не видна по сети. В этом случае можно скопировать папку в какое-либо другое место и вручную организовать к ней доступ по сети.

Для того чтобы соединиться с помощью Центра управления с антивирусным сервером, необходимо в адресной строке браузера ввести имя или адрес антивирусного сервера и указать порт 9080 (9081 в случае использования протокола HTTPS).

Пример: http://192.168.100.66:9080. В нашем примере в качестве логина используется admin, в качестве пароля — пароль, указанный при установке ESS-сервера.

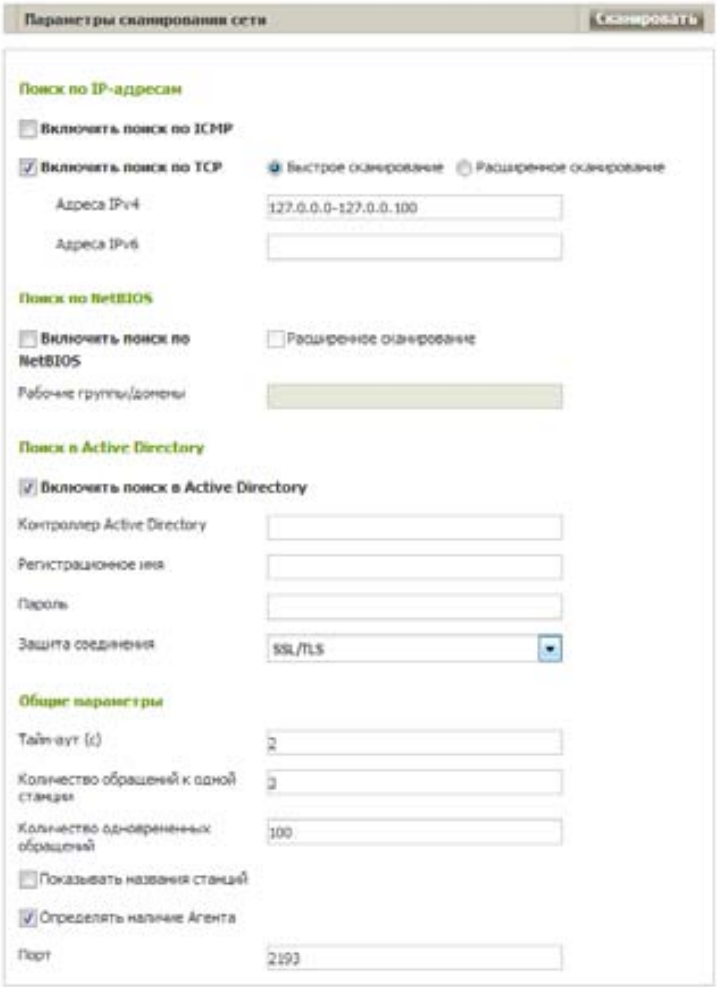
Прейдите в меню **Администрирование → Установка → Сканер сети**.

Внимание! При использовании неанглоязычного браузера типа Firefox на англоязычной операционной системе Windows необходимо убедиться, что в названии папки загрузки по умолчанию используются только символы латиницы. Настройка папки скачивания производится на странице **Основные → Файлы и Приложения → Загрузки** меню **Настройки** браузера Mozilla Firefox.



Сканер сети выполняет следующие действия:

- Сканирование (обзор) сети (по IP-адреса и NetBIOS) с целью обнаружения рабочих станций.
- Определение наличия **Агента** на станциях. Сканер сети способен определить наличие на станции Агента только версии **4.44** и старше, но не способен взаимодействовать с Агентами более ранних версии. Установленный на защищаемой станции Агент версии **4.44** и старше о существляют обработку соответствующих запросов Сканера сети, поступающих на определенный порт. По умолчанию используется порт udp/2193, ранее использовавшийся порт udp/2372 не поддерживается. Соответственно, эти же порты по умолчанию предлагается опрашивать и в Сканере сети. Сканер сети делает вывод о наличии или отсутствии Агента на станции исходя из возможности обмена информацией (запрос — ответ) через вышеуказанный порт.
- Поиск станций в Active Directory и LDAP, при этом поиск может осуществляться для станций, находящихся в разных доменах. При поиске в AD также возможна защита соединения.



Внимание! 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.

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

Работа Сканера сети гарантируется под ОС семейства UNIX или ОС Windows Vista и старше.

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.

Для ОС семейства UNIX: установите флажок **Поиск по LDAP**, чтобы осуществлять поиск станций по LDAP. При этом задайте следующие параметры:

- **Домены —** список доменов, в которых будет осуществляться поиск станций. В качестве разделителя для нескольких доменов используйте запятую.
- **Сервер LDAP —** сервер LDAP, например ldap://ldap.example.com.
- **Регистрационное имя —** регистрационное имя пользователя LDAP.
- **Пароль —** пароль пользователя LDAP.

Нажмите **Сканировать**.

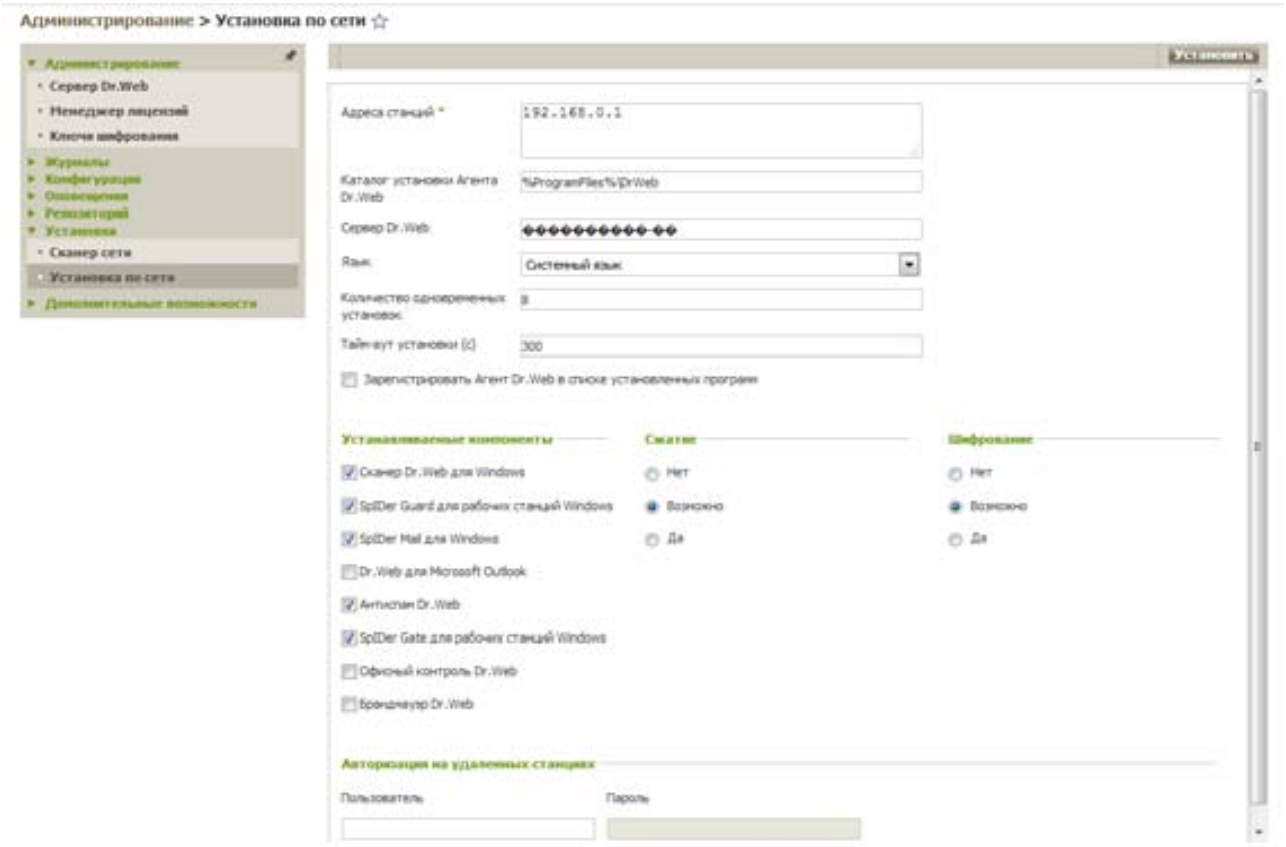
По завершении сканирования в окно будет выведен иерархический список компьютеров с указанием, на каких из них антивирусное ПО установлено, а на каких — нет. Все элементы каталога, соответствующие рабочим группам и отдельным станциям, помечаются различными значками, значение которых приведено в документации.

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)

Кроме того, вместо IP-адресов вы можете указать доменные имена компьютеров.

По умолчанию ПО Агента будет установлено в каталог C:\Program Files\DrWeb Enterprise Suite. При необходимости укажите другой путь в поле **Каталог установки**.

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.

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).

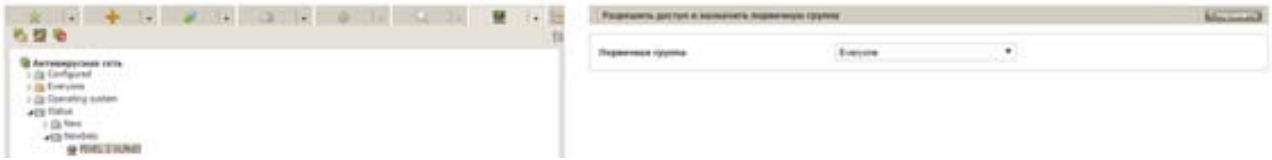
Внимание! После изменения уровня параметров управления учетными записями требуется перезагрузка станции для их применения.

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. 7.5.7. Политика подключения новых станций). При этом новые рабочие станции не подключаются автоматически, а помещаются Сервером в подгруппу **Newbies**, группы **Status**.

Выберите пункт **Администрирование** главного меню Центра управления. В иерархическом списке антивирусной сети выберите станции в подгруппе **Newbies** группы **Status**. Для задания доступа к **Серверу** на панели инструментов в разделе (**Неподтвержденные станции**) задайте действие, которое будет применено для выбранных станций:

- **Разрешить доступ выбранным станциям и назначить первичную группу** — подтвердить доступ станции к **Серверу** и задать для нее первичную группу из предложенного списка (**Everyone** или другую первичную группу). После подтверждения станции (если этого требуют настройки **Enterprise Сервера**) автоматически будут установлены антивирусные компоненты.
- **Отменить действие, заданное для выполнения при подключении** — отменить действие над неподтвержденной станцией, которое было ранее назначено для выполнения в момент, когда станция подключится к **Серверу**.
- **Отказать в доступе выбранным станциям** — запретить доступ станции к **Серверу**.

При нажатии на значок появится окно с выбором первичной группы.



Выберите группу и нажмите **Сохранить.**

Станция будет подключена к Серверу, а изображение значка станции в антивирусной сети изменится.

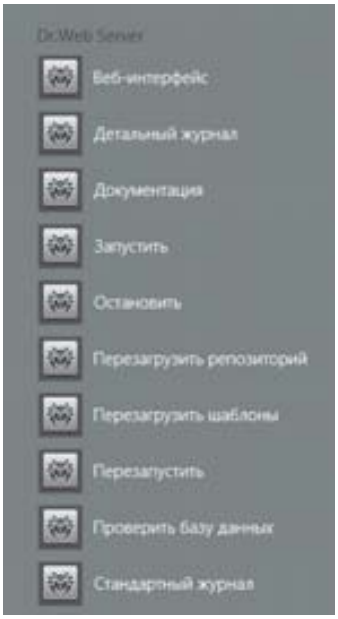
При этом рабочая станция помещается в предустановленные группы рабочих станций Everyone, Online, а также группы, соответствующие протоколу соединения, семейству ОС и конкретной ОС.

На станцию будут установлены компоненты антивирусного пакета, заданные в настройках первичной группы станции. В дальнейшем вы можете изменить состав компонентов в настройках первичной группы или задать соответствующие персональные настройки для конкретной станции.

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.

Внимание! В случае установки защиты станции, на которой установлено ПО антивирусного сервера, рекомендуется перед перезагрузкой или выключением сервера произвести его остановку во избежание повреждения базы данных антивирусного сервера. При наличии доступа к станции для этого можно воспользоваться командами управления сервером, расположенными в группе и доступными по нажатию кнопки **Пуск**.



Внимание! В ходе установки автоматически удаляются обнаруженные антивирусные продукты. Список антивирусных продуктов, удаление которых возможно в автоматическом режиме, приведен в документации.

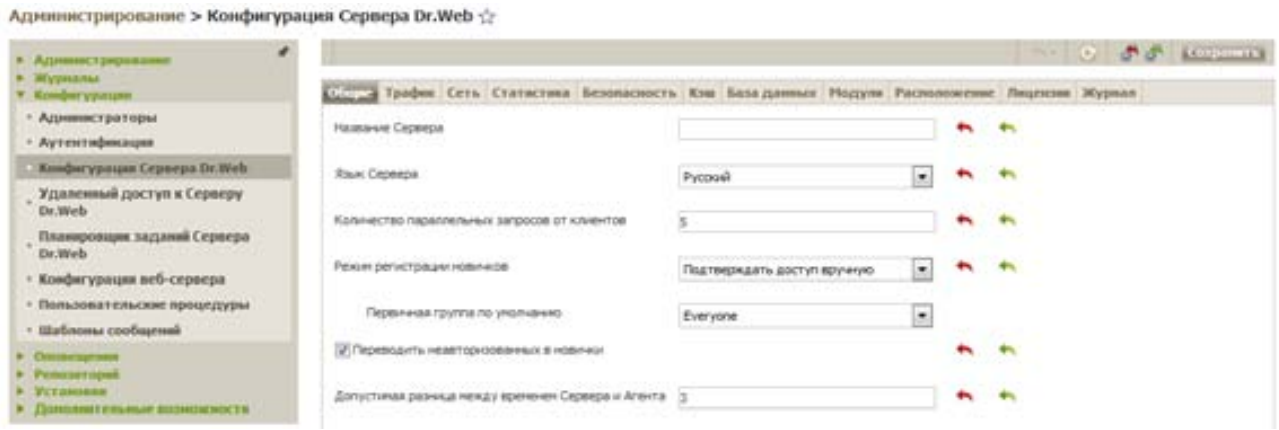
Внимание! В случае недоступности на ОС Windows Vista и Windows 2008 некоторых настроек компонентов через меню Агента после установки Dr.Web Firewall необходимо произвести перезагрузку станции.

Внимание! При получении ошибок при удаленной установке обратитесь к разделу «Диагностика проблем удаленной установки» документации.

6.4.2. Автоматическое подтверждение новых станций

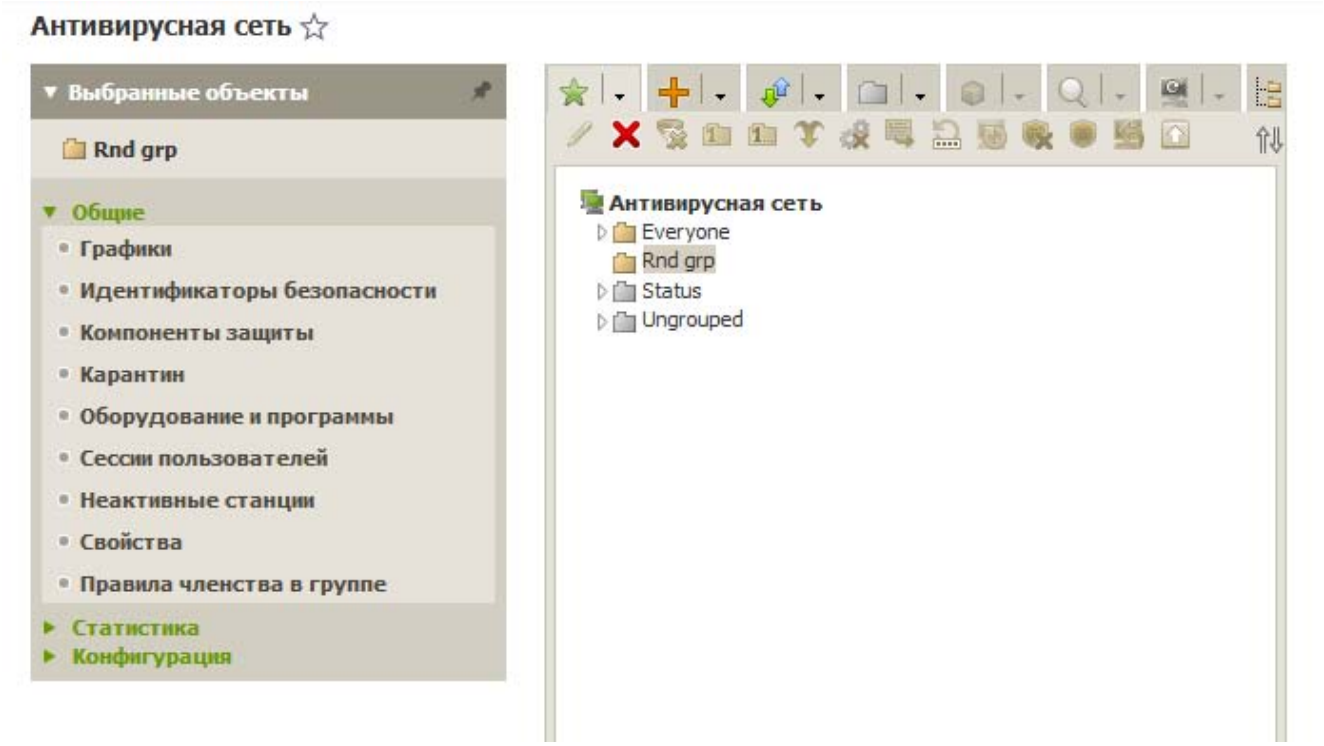
Администратор антивирусной сети может либо лично подтверждать подключение каждой новой станции к антивирусному серверу, либо настроить параметры автоматического подключения.

Для выбора типа подключения нужно перейти на страницу **Конфигурация Сервера Dr.Web**, вкладка **Общие**, и в выпадающем меню **Режим регистрации новичков** выбрать тип подключения. В поле **Первичная группа** нужно указать группу, в которую будут попадать станции при автоматическом подтверждении доступа станций к антивирусному серверу.

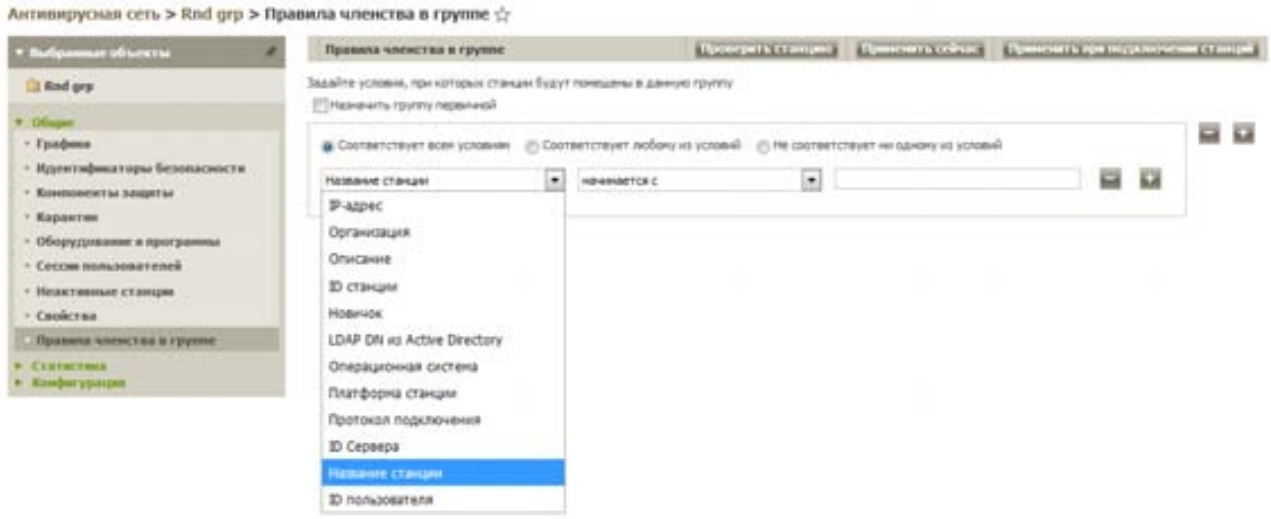


При наличии пользовательских групп администратор может настроить правила, по которым станции попадают в эти группы (правила членства в группе).

Для этого необходимо выбрать пользовательскую группу и в меню слева открыть пункт **Правила членства в группе**.



После настройки правил необходимо подтвердить, нажав кнопку **Применять при подключении станций**.



6.4.3. Рассылка инсталляционных файлов из Центра управления по электронной почте

При создании новой учетной записи станции в Центре управления генерируется инсталляционный пакет для установки Агента Dr.Web, который включает в себя инсталлятор Агента, набор параметров для подключения и авторизации на Сервере Dr.Web. Описание инсталляционного пакета и процесса установки Агента с его помощью приведено в документе Руководство по установке, в разделе Локальная установка Dr.Web Agent).

В случае необходимости администратор антивирусной сети имеет возможность рассылки инсталляционных файлов Агентов Dr.Web непосредственно из Центра управления по электронной почте.

При отправке инсталляционных пакетов содержимое письма формируется следующим образом:

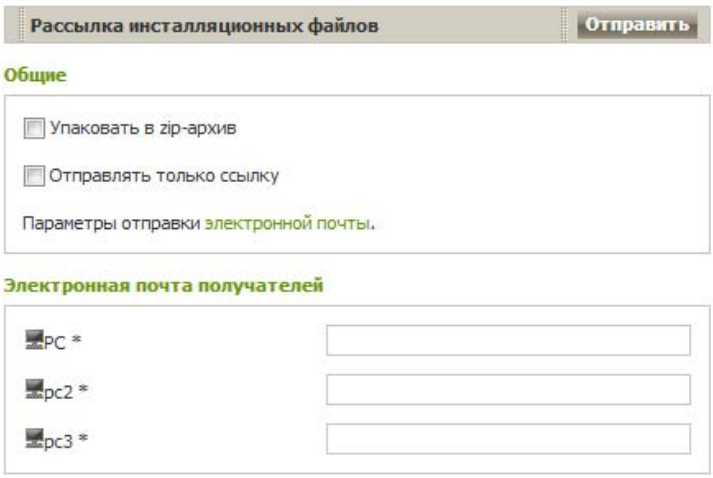
1. Операционная система станции известна:

   a. ОС Windows: к письму прикладывается инсталляционный пакет Агента для Windows.

   b. ОС Linux, macOS, ОС Android: к письму прикладывается инсталляционный файл Dr.Web Agent для соответствующей о перационной системы и конфигурационный файл с настройками подключения к Серверу Dr.Web.

2. Операционная система станции не известна (новая учетная запись станции, Агент еще не установлен):
   a. Если на Сервере нет пакетов для станций под ОС Linux, macOS, ОС Android (в частности, на Сервере не установлен дополнительный (extra) дистрибутив): к письму прикладывается инсталляционный пакет Dr.Web Agent для Windows, а также конфигурационный файл с настройками подключения к Dr.Web Серверу для станций под ОС Linux, macOS, ОС Android.
   b. Если на Сервере есть хотя бы один пакет, кроме пакета для станций под ОС Windows: к письму прикладываются инсталляционный пакет Dr.Web Agent для Windows, конфигурационный файл с настройками подключения к Dr.Web Серверу для станций под ОС Linux, macOS, ОС Android, а также ссылка на скачивание инсталляционных файлов для станций под ОС Linux, macOS, ОС Android.

Для рассылки инсталляционных файлов необходимо выбрать станцию или группу в иерархическом списке, доступном при выборе пункта **Антивирусная сеть** главного меню **Центра управления**, нажать кнопку и в открывшейся панели справа указать необходимые параметры.



При выборе станции на нее отправляется специально сгенерированный для нее пакет, при выборе группы — отправляются все инсталляционные пакеты, сгенерированные для станций данной группы.

Флажок **Упаковать в zip-архив** позволяет упаковать файлы инсталляционных пакетов в zip-архив. Упаковка в архив может быть полезна при наличии фильтров электронной почты на стороне пользователя, блокирующих передачу исполняемых файлов во вложениях электронных писем.

Флажок **Отправлять только ссылку** позволяет отправить в письме только ссылку на скачивание дистрибутива, при этом физически он останется на Сервере.

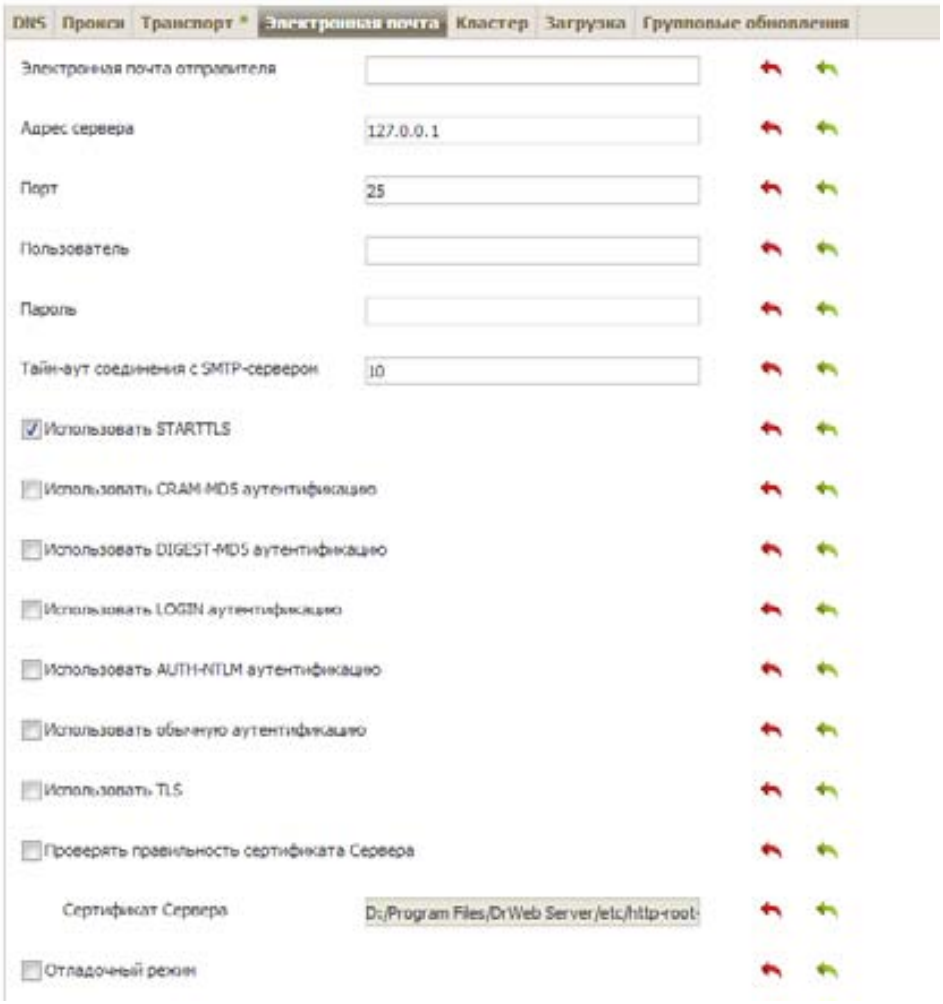
В разделе **Электронная почта получателей** необходимо задать адреса электронной почты, соответствующие каждой станции (например, электронные адреса сотрудников, работающих за этими компьютерами).

Параметры рассылки задаются в другом разделе Центра управления, куда можно перейти, щелкнув по ссылке **Параметры отправки электронной почты**. Она ведет на вкладку **Электронная почта** раздела **Администрирование → Конфигурация Сервера Dr.Web → Сеть**.

Здесь з адаются параметры SMTP-сервера, который будет использоваться для отправки электронной почты:

- **Электронная почта отправителя** — адрес ящика электронной почты, от имени которого будут отправляться электронные письма.
- **Адрес сервера** — адрес SMTP-сервера, который будет использоваться для отправки электронной почты.
- **Порт** — порт для подключения к SMTP-серверу. По умолчанию порт 465 при открытии отдельного защищенного TLS-соединения или порт 25 в противном случае.
- **Пользователь**, **Пароль** — при необходимости задайте имя пользователя и пароль пользователя SMTP-сервера, если SMTP-сервер требует авторизации.
- **Тайм-аут соединения с SMTP-сервером** — тайм-аут в секундах для установления соединения с SMTP-сервером. Значение — целое положительное число большее или равное 1.
- Установите флажок **Использовать STARTTLS** для шифрованного обмена данными. При этом переключение на за щищенное соединение осуществляется через команду STARTTLS. По умолчанию для соединения предусматривается использование 25-го порта.
- Установите флажок **Использовать CRAM-MD5 аутентификацию** для использования *CRAM-MD5* аутентификации на почтовом сервере.
- Установите флажок **Использовать DIGEST-MD5 аутентификацию** для использования *DIGEST-MD5* аутентификации на почтовом сервере.
- Установите флажок **Использовать LOGIN аутентификацию** для использования *LOGIN* аутентификации на почтовом сервере.
- Установите флажок **Использовать AUTH-NTLM аутентификацию** для использования *AUTH-NTLM* аутентификации на почтовом сервере.
- Установите флажок **Использовать обычную аутентификацию** для использования *plain text* аутентификации на почтовом сервере.
- Установите флажок **Использовать TLS** для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование 465-го порта.
- Установите флажок **Проверять правильность сертификата Сервера** чтобы проверять правильность TLS-сертификата почтового сервера. В поле **Сертификат Сервера** укажите путь к корневому TLS-сертификату Сервера Dr.Web.
- Установите флажок **Отладочный режим** для получения детального журнала SMTP-сессии.
- В поле **Электронная почта получателей** можете задать адреса ящиков электронной почты, чтобы проверить отправку электронной почты. Нажмите кнопку **Отправить тестовое сообщение**, чтобы отправить тестовое письмо (аналогичное оповещению

Сервера) по электронной почте в соответствии с заданными настройками в данном разделе.



В секции **Отправитель** указывается адрес электронной почты, который будет указан в качестве отправителя электронного письма с инсталляционными файлами.

После завершения всех настроек нажмите **Отправить** для рассылки писем.

6.4.4. Установка с использованием дистрибутивов компонентов Dr.Web Enterprise Security Suite

Установка с использованием дистрибутивов может производиться как администратором, так и пользователем. Для локальной установки Агента Dr.Web на станции под ОС Windows доступны следующие средства:

- Персональный инсталляционный пакет, созданный в Центре управления drweb_ess_<*ОС*>_<*станция*>.exe.
- Групповой инсталляционный пакет, созданный в Центре управления drweb_ess_<*ОС*>_<*группа*>.exe.
- Полный инсталлятор Агента Dr.Web drweb-11.05.0-<*сборка*>-esuite-agent-full-windows.exe.
- Сетевой инсталлятор Агента Dr.Web drwinst.exe.

Внимание! Установка **Агента** должна выполняться с правами администратора данного компьютера.

Для того чтобы задать список устанавливаемых компонентов при удаленной установке, используйте пункт **Устанавливаемые компоненты** меню **Администрирование Сервера Dr.Web**.

При установке через данные инсталляторы вы можете не задавать параметры подключения к **Серверу** и авторизации или задать их вручную. Для задания параметров авторизации вручную необходимо сначала создать новую учетную запись станции в **Центре управления**. При этом будет доступен инсталляционный пакет.

Если нет необходимости установки через полный дистрибутив или сетевой инсталлятор, рекомендуется использовать инсталляционный пакет вместо инсталлятора.

Возможны следующие варианты подключения к **Серверу** с соответствующими параметрами авторизации.

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

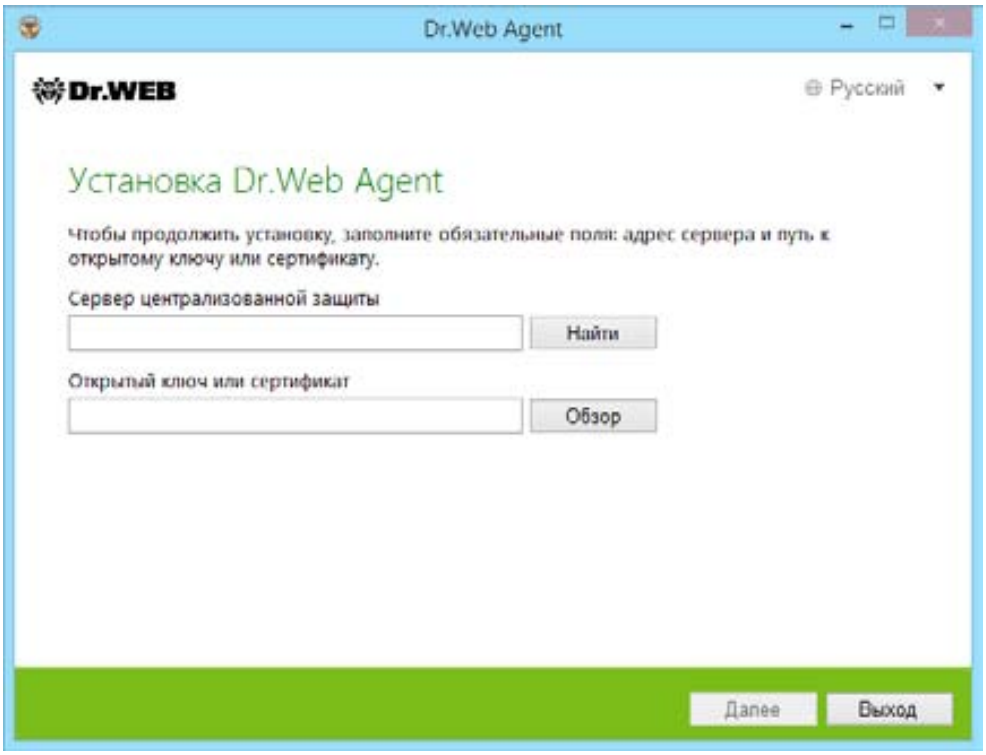
6.4.4.1. Локальная установка при помощи полного инсталляционного пакета для ОС Windows

Для установки Агента при помощи полного инсталляционного пакета необходимо на защищаемой станции запустить пакет `drweb-11.05.0-<сборка>-esuite-agent-full-windows.exe`.

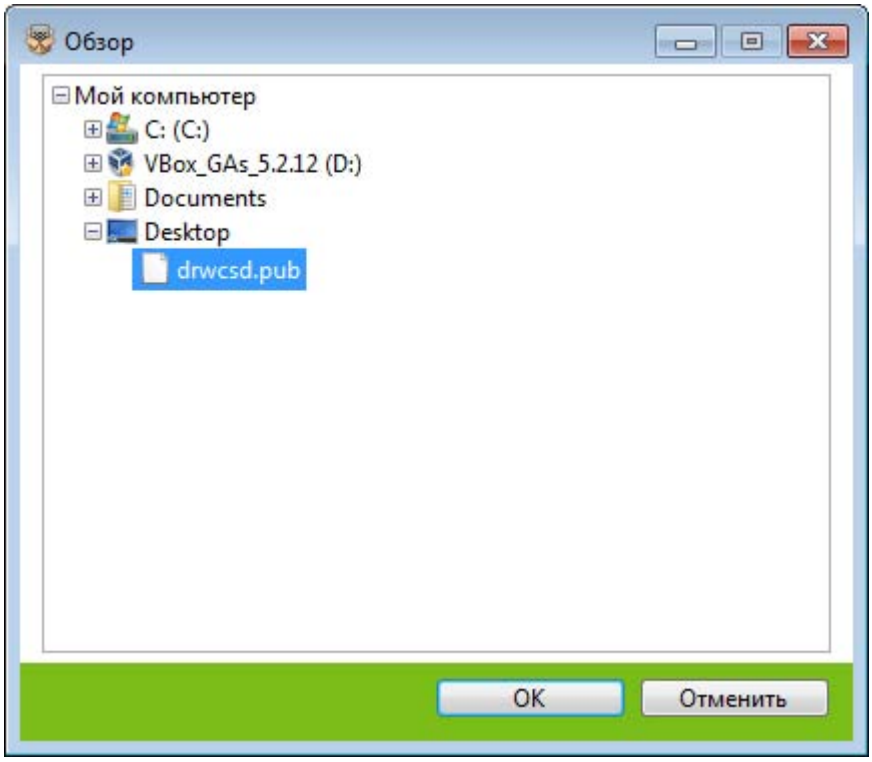
Внимание! Для успешной инсталляции на рабочую станцию должен быть помещен открытый ключ шифрования антивирусного сервера (по умолчанию файл drwcsd.pub).

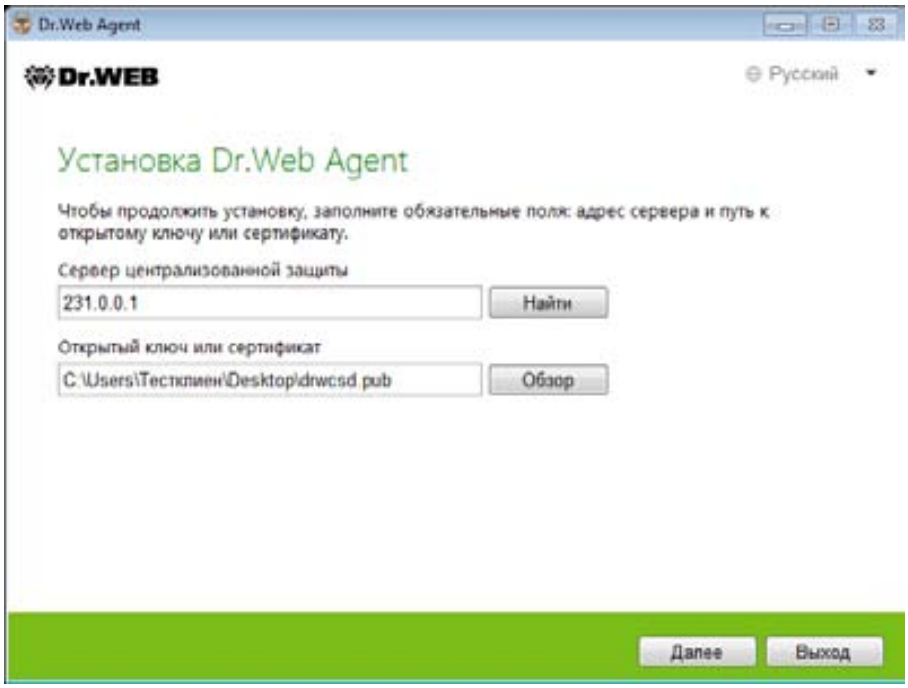
В случае обнаружения ранее установленного антивирусного решения будет выведено соответствующее предупреждение.

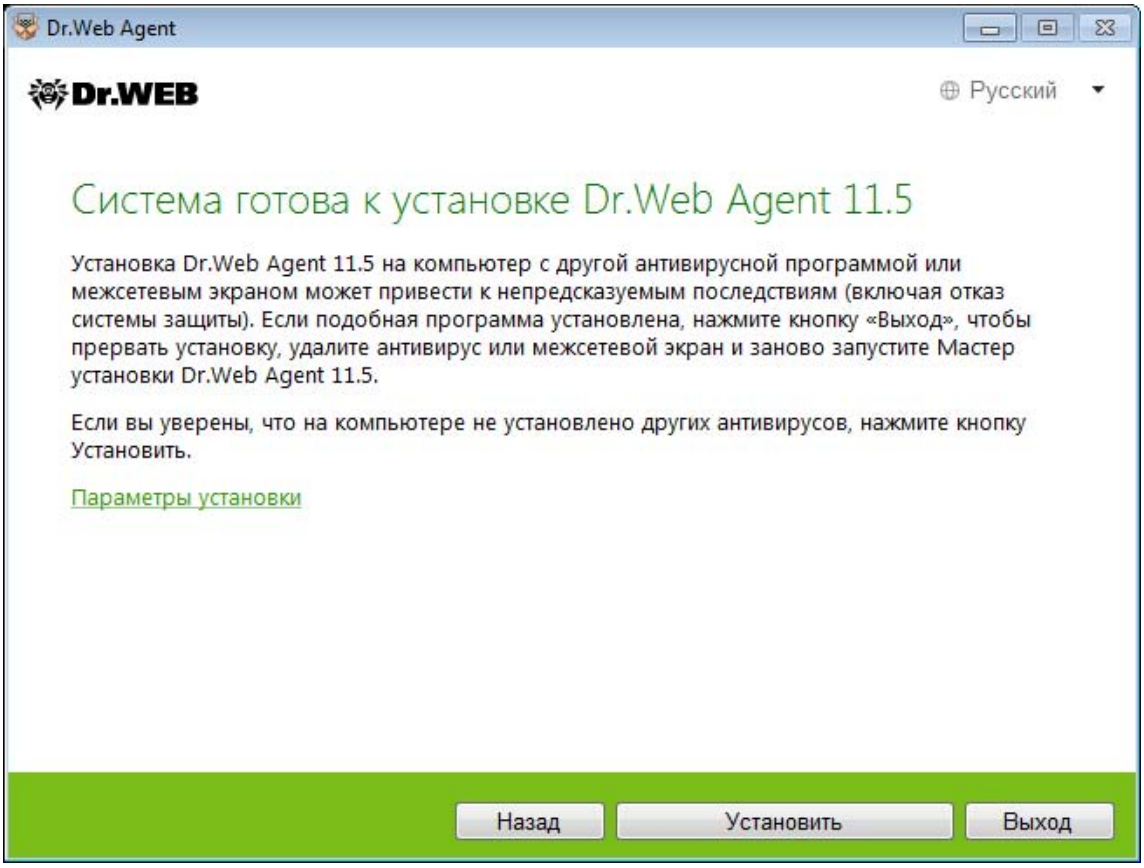
В появившемся окне необходимо указать адрес сервера и путь до открытого ключа шифрования.



Для поиска открытого ключа шифрования можно использовать кнопку **Обзор**.

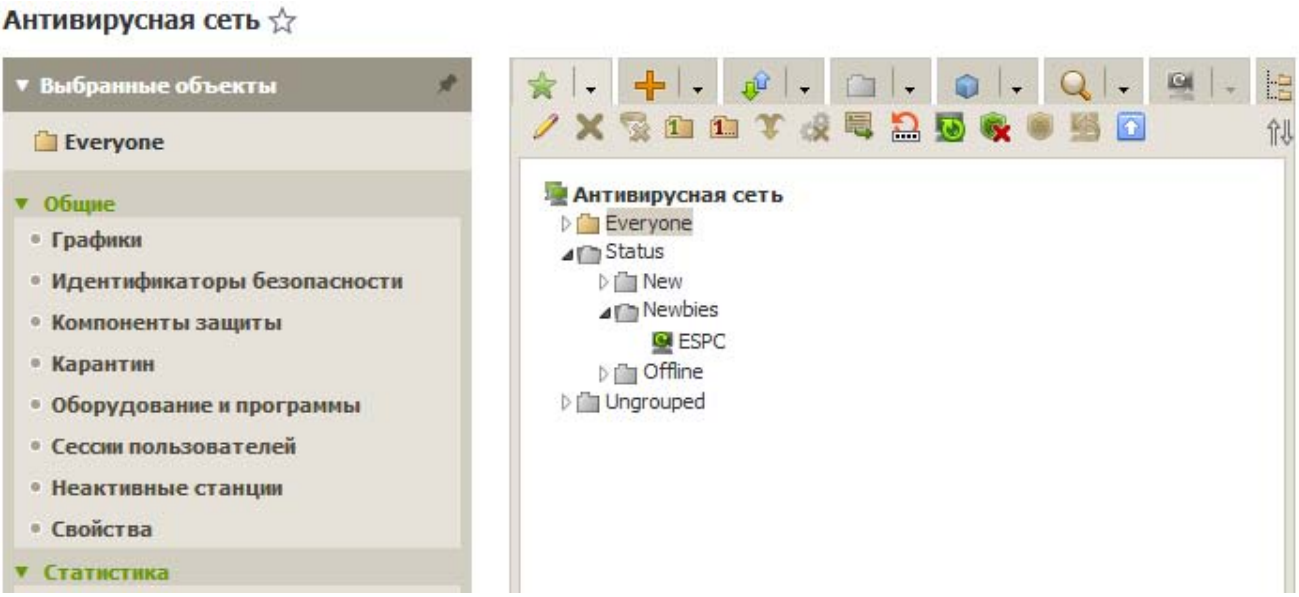

Обзор
Мой компьютер
C: (C:)
VBox_GAs_5.2.12 (D:)
Documents
Desktop
drwcsd.pub
OK
Отменить


Dr.Web Agent
Dr.WEB
Русский
Установка Dr.Web Agent
Чтобы продолжить установку, заполните обязательные поля: адрес сервера и путь к открытому ключу или сертификату.
Сервер централизованной защиты
231.0.0.1
Найти
Открытый ключ или сертификат
C:\Users\Тестклиен\Desktop\drwcsd.pub
Обзор
Далее
Выход

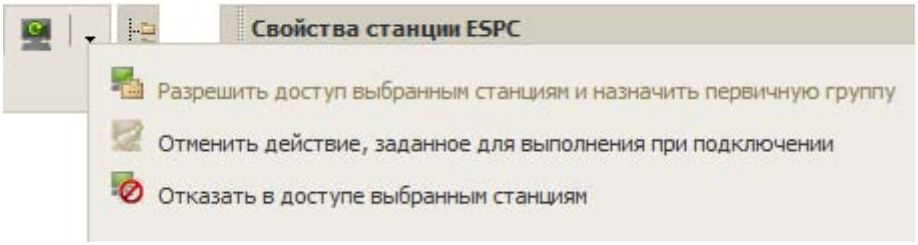


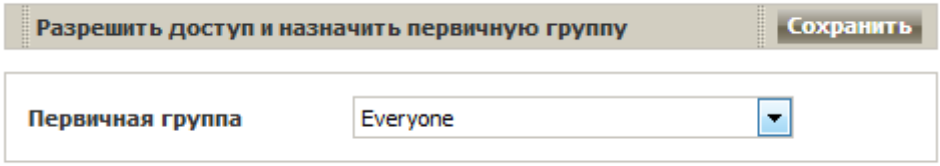
Проверьте правильность выбранных настроек и нажмите **Установить**.

После окончания установки в связи с установкой драйверов необходимо перезагрузить защищаемую станцию.



После установки, если не используется политика автоматического подтверждения новых станций, Агент находится в группе **Newbies**. Необходимо разрешить доступ станции в антивирусную сеть и назначить для нее группы. Нажмите кнопку  и выберите необходимое действие.





До окончания установки обновлений и формирования репозитория станция имеет статус **Ошибка обновления**.

Для завершения установки перезагрузите станцию еще раз.

6.4.4.2. Установка Dr.Web Agent при помощи инсталляционного пакета esinst

Инсталляционный пакет *drweb_ess_windows_<имя_станции>.exe* генерируется при создании новой учетной записи пользователя. Ссылка для скачивания файла для конкретной станции доступна:

1. Сразу после создания новой станции (подробнее в разделе **Создание новой учетной записи**).
2. В любое время после создания станции в разделе свойств станции или в разделе **Выбранные объекты** при выборе станции в иерархическом списке.

Созданная ссылка на инсталляционный пакет **Агента Dr.Web** соответствующей операционной системы компьютера или мобильного устройства может быть отправлена пользователю для самостоятельной установки. Если установка осуществляется на станцию под операционной системой, отличной от ОС Windows, необходимо также отправить пользователю конфигурационный файл с настройками подключения к антивирусному серверу.

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

Внимание! В ссылке для скачивания после адреса сервера должен быть указан порт 9080 (для http) или 9081 (для https). Например:

https://win2008pdc.drweb.test:9081/download/download.ds?os=windows&id=70ae56b9-910e-e411-38c7-f0bbb5985790

Внимание! Для антивирусного сервера тре буется использование DNS имени вместо IP-адреса. Данное требование связано с жесткой привязкой агентов к данной настройке и их невозможностью подключиться к серверу в случае изменения IP-адреса. Помимо этого, рекомендуется использование специального имени для антивирусного сервера, даже если сервер установлен на машине, уже имеющей DNS-имя и выполняющей другие функции. Использование отдельного DNS-имени исключит проблемы в случае изменения IP-адреса сервера или переноса сервера на другую машину.

Настройка адреса сервера осуществляется редактированием файла **webmin.conf**, расположение которого может варьироваться в зависимости от ОС:

- для FreeBSD:

  `/var/drwcs/etc/webmin.conf`

- для Linux:

  `/var/opt/drwcs/etc/webmin.conf`

- также его можно найти командой:

  `find / -name 'webmin.conf'`

- в ОС Windows он, как правило, расположен в папке `C:\Program Files\DrWeb Server\etc`

В связи с этим для получения файлов без указания порта необходимо задать параметр ServerName, хранящийся в файле webmin.conf, — указать имя (актуальный адрес) сервера, сохранив указание порта. Например: server-name value='win2003ad1.drweb.test:9080'.

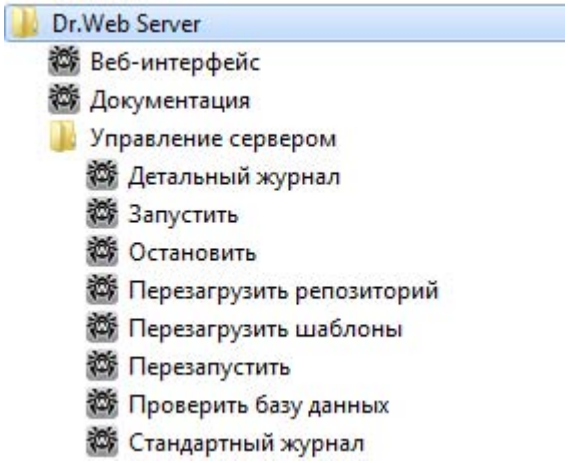
После изменения файла webmin.conf необходимо перезапустить сервер, чтобы настройки вступили в силу, и обновить страницу со ссылками, если она была открыта.

Сделать это можно командой:

для FreeBSD: `# /usr/local/etc/rc.d/drwcsd.sh restart`
для Linux: `# /etc/init.d/drwcsd restart`
для ОС Windows:

> **Панель управления → Администрирование → Службы** и, выбрав **Dr.Web Server**, нажать **Перезапустить**.

Также перезапустить антивирусный сервер можно из меню **Пуск**:



или с использованием Центра управления, нажав на кнопку 

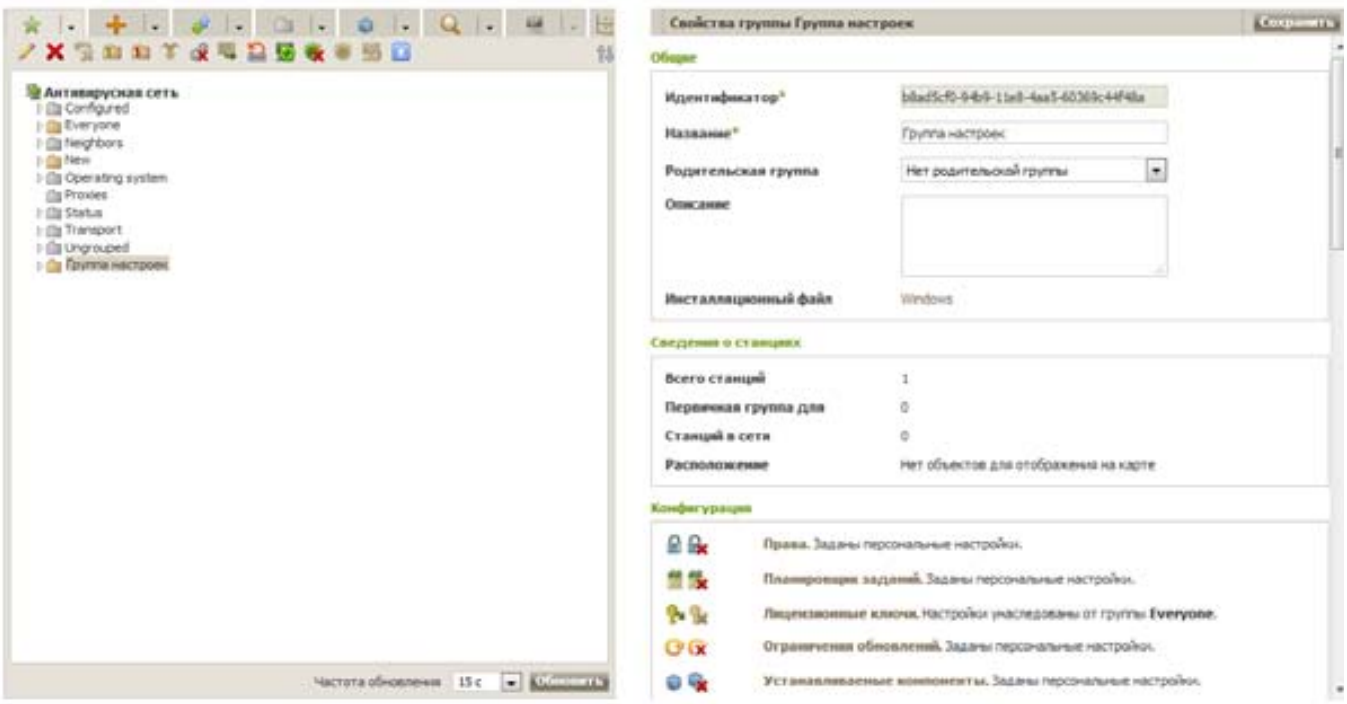
Для установки Агента Dr.Web через инсталляционный пакет *drweb_ess_windows_<имя_станции>.exe* при помощи Центра управления необходимо создать учетную запись новой станции на Сервере, получить ссылку для загрузки инсталлятора Агента и произвести установку Агента на рабочую станцию при помощи полученного файла. Авторизация новой антивирусной станции на Сервере по умолчанию осуществляется автоматически.

Установка Агента Dr.Web должна выполняться пользователем с правами администратора данного компьютера. Если на рабочей станции уже установлено антивирусное ПО, то перед началом установки инсталлятор предпримет попытку его удалить. В случае если такая попытка окажется неудачной, пользователю нужно будет самостоятельно удалить используемое на рабочей станции антивирусное ПО.

6.4.4.3. Установка Dr.Web Agent при помощи группового инсталляционного пакета

Процесс групповой установки в целом аналогичен установке с помощью персонального инсталляционного пакета. Отличие в том, что в данном случае инсталляционные пакеты для каждой ОС создаются не под конкретную станцию с её свойствами, а сразу под всю группу станций.

Соответсвенно, ссылка на скачивание группового дистрибутива располагается не в свойствах станции, а в свойствах группы в разделе **Инсталляционный файл**. Обратите внимание, что если в группу входят станции с различными ОС, то для каждой из них будет отдельная ссылкка.

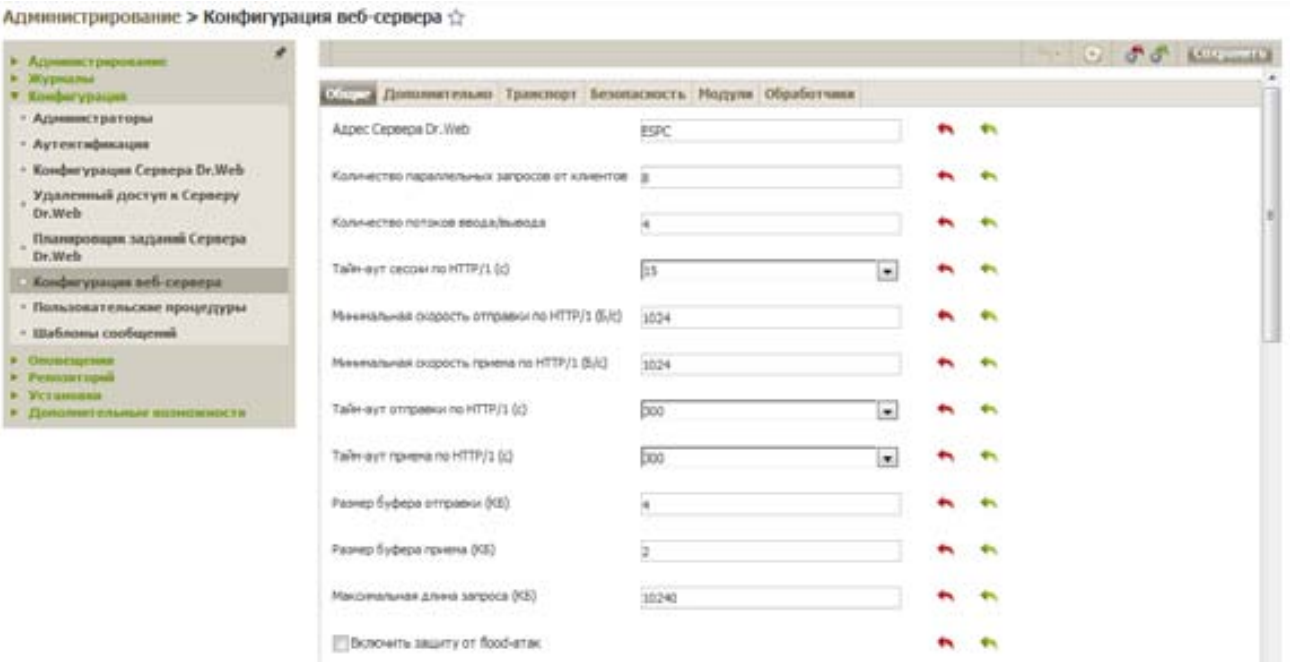


В остальном использование группового инсталлятора не отличается от персонального — сначала на Сервере создаются уч етные записи пользователей, затем формируется и настраивается группа, после чего пользователям отправляется ссылка на скачивание дистрибутива.

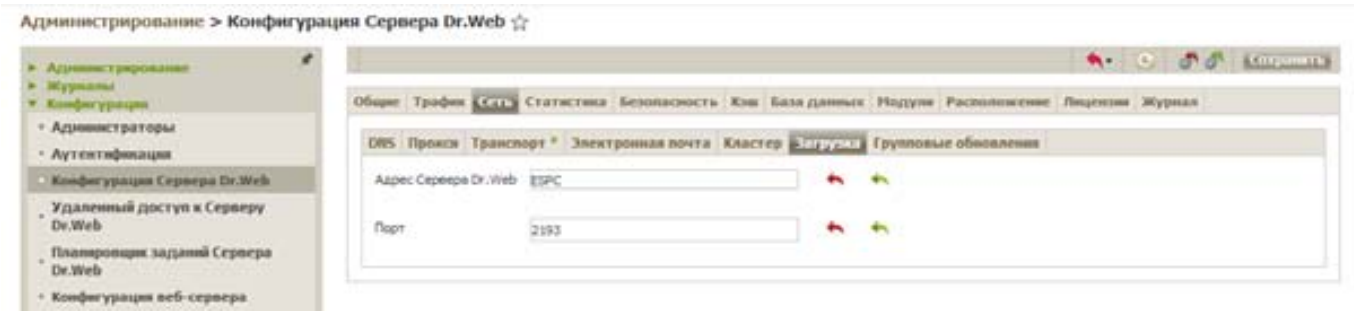
Подробно процесс использования группового инсталлятора описан в разделе Руководства по установке — Установка Агента Dr.Web при помощи группового инсталляционного пакета.

6.4.4.3.1. Создание записи для создаваемой станции (нового пользователя)

Убедитесь, что для параметра **server-name** в конфигурационном файле webmin.conf задано значение <*Адрес_Сервера*>:9080, где <*Адрес_Сервера*> — IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**. Параметр задается в поле **Сервер** страницы **Администрирование → Конфигурация веб-сервера**. Значение данного параметра подставляется при генерации ссылки на установочный пакет **Агента**. Если значение данного параметра нигде не задано, то в качестве имени **Сервера** для формирования ссылки на скачивание инсталлятора **Агента** задается DNS-имя (если доступно) или IP-адрес компьютера, на котором открыт Центр управления.



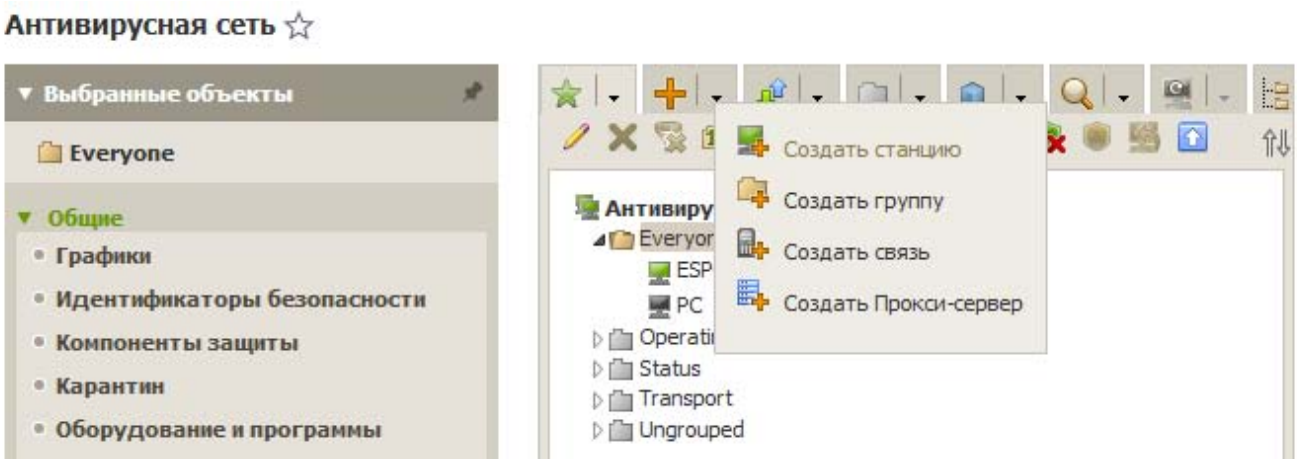
Также необходимо задать параметр, прописываемый в установочные пакеты **Агента** и определяющий, к какому **Серверу** будет подключаться **Агент** при установке. Параметр хранится в конфигурационном файле download.conf и задается в поле **Сервер** (**Администрирование → Конфигурация Сервера Dr.Web Server → Сеть → Загрузка)**. Если значение данного параметра нигде не задано, то при создании установочного пакета **Агента** в нем прописывается адрес **Сервера**, по которому подключен Центр управления. В этом случае подключение Центра управления к **Серверу** должно осуществляться по IP-адресу для домена, в котором создается учетная запись.



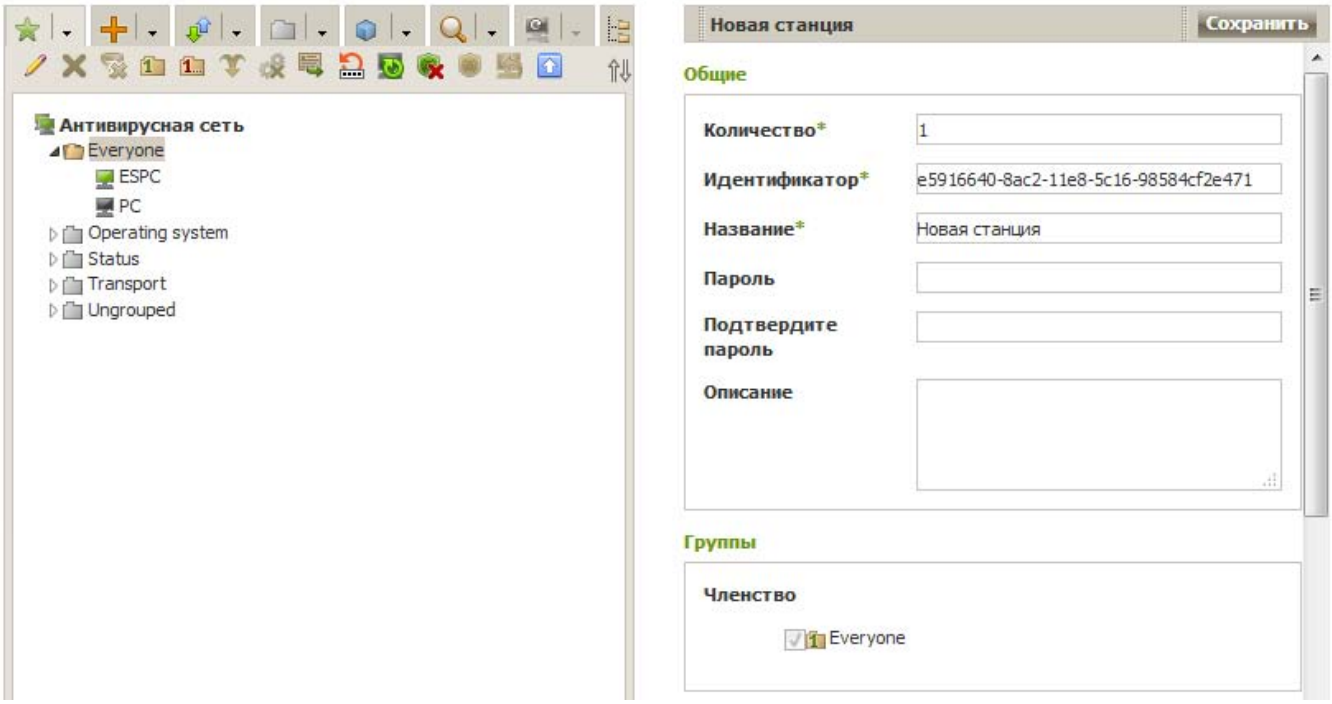
При подключении Центра управления к Серверу с локальной машины адрес Сервера не должен быть задан как loopback (127.0.0.1).

Для создания нового пользователя:

1. Выберите пункт **Антивирусная сеть** и нажмите на кнопку .



2. В открывшемся подменю выберите пункт **Создать станцию**. В правой части окна Центра управления откроется панель создания учетной записи пользователя.



3. В поле **Количество** укажите количество пользователей, которое вам нужно создать.
4. В поле **Идентификатор** автоматически генерируется уникальный идентификатор создаваемой станции. При необходимости вы можете его изменить.
5. В поле **Название** задайте имя станции, которое будет отображаться в иерархическом списке антивирусной сети. В дальнейшем после соединения станции с Сервером данное имя может быть автоматически заменено на название станции, заданное локально.
6. В полях **Пароль** и **Еще раз пароль** укажите пароль для доступа станции к Серверу.

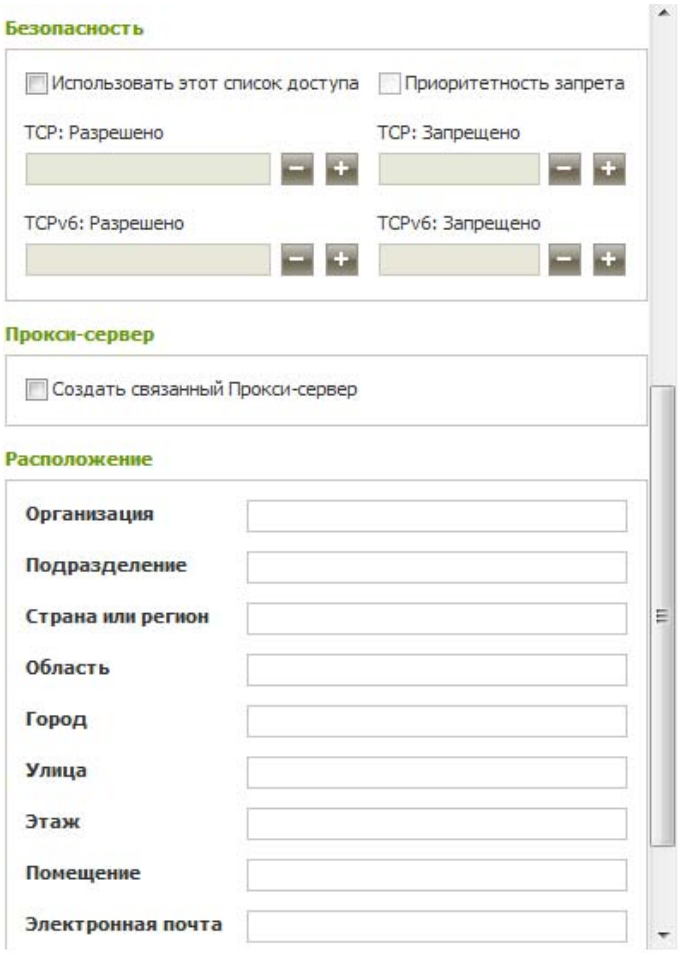
   При создании более одной учетной записи поля **Идентификатор**, **Название** и **Пароль** (**Еще раз пароль**) будут заданы автоматически и недоступны для изменений на этапе создания станций.

7. В поле **Описание** при необходимости введите дополнительную информацию о пользователе.
8. В разделе **Группа** выберите группы, в которые будет входить создаваемая антивирусная станция. По умолчанию станция входит в группу **Everyone**. В случае наличия пользовательских групп вы можете включить в них создаваемую станцию. Для

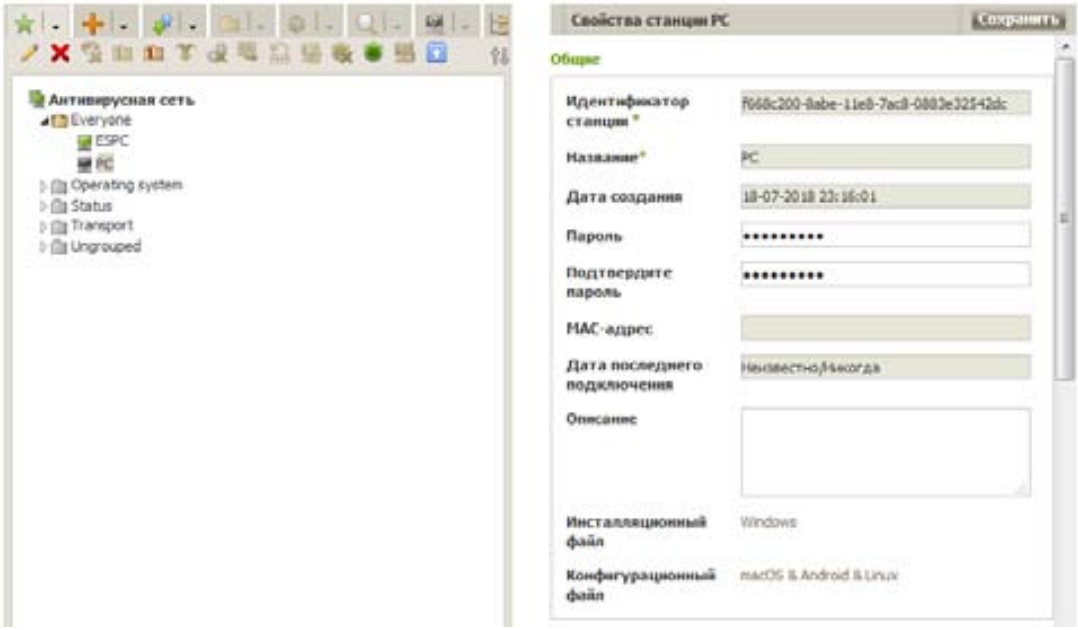
этого нажмите на название группы в разделе **Известные группы**. Для исключения станции из пользовательских групп, в которые она включена, нажмите на название группы в разделе **Членство в**.

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

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



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



Сразу после создания новой станции, до момента, когда будет задана операционная система станции, в разделе скачивания дистрибутива ссылки предоставляются отдельно для всех ОС, поддерживаемых **Dr.Web ES**. Ссылки для скачивания инсталлятора **Агента** и конфигурационного файла также доступны:

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

6.4.4.3.2. Настройки подключения к Серверу Dr.Web

Станции под ОС Windows

При установке **Агента Dr.Web** на станции под ОС Windows при помощи инсталляционного пакета дополнительная настройка не требуется. Параметры подключения к **Серверу** и параметры авторизации станции на **Сервере** включены в инсталляционный пакет непосредственно. После установки **Агента** станция автоматически подключится к **Серверу**.

Станции под ОС Android

1. На главном экране мобильного устройства вызовите меню приложения **Антивирус Dr.Web** и выберите пункт **Настройки**.
2. На экране **Dr.Web → Настройки** в разделе **Режим** установите флажок **Агент Dr.Web**.
3. Настройки подключения к **Серверу**, такие как IP-адрес и параметры авторизации на **Сервере**, автоматически задаются из конфигурационного файла.
4. Нажмите кнопку **Подключиться**.

Внимание! Антивирус Dr.Web для Android должен быть установлен с сайта «Доктор Веб» по ссылке: https://download.drweb.ru/android. **Версия из Google Play работать в режиме Агента не может!**

Станции под macOS

1. В меню приложения **Антивирус Dr.Web** нажмите пункт **Настройки** и выберите раздел **Режим**.
2. Установите флажок **Включить режим централизованной защиты**.

3. Настройки подключения к **Серверу**, такие как IP-адрес и параметры авторизации на **Сервере**, автоматически задаются из конфигурационного файла.

Станции под ОС семейства Linux

1. Откройте **Менеджер лицензий** и нажмите кнопку **Активировать лицензию** для начала процедуры регистрации.
2. Выберите опцию **Другие виды активации**.
3. В открывшемся поле укажите путь к конфигурационному файлу с настройками подключения и авторизации на **Dr.Web Сервере**.

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

Для станций под ОС Android, ОС Linux, macOS доступен инсталлятор для установки **Агента Dr.Web**, аналогичный инсталлятору автономной версии. Описание локальной установки **Агента Dr.Web** на рабочей станции приведено в руководстве пользователя для соответствующей операционной системы.

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

Параметры авторизации можете задать вручную или не задавать. При этом возможны следующие варианты подключения к **Серверу** и соответствующие им параметры авторизации:

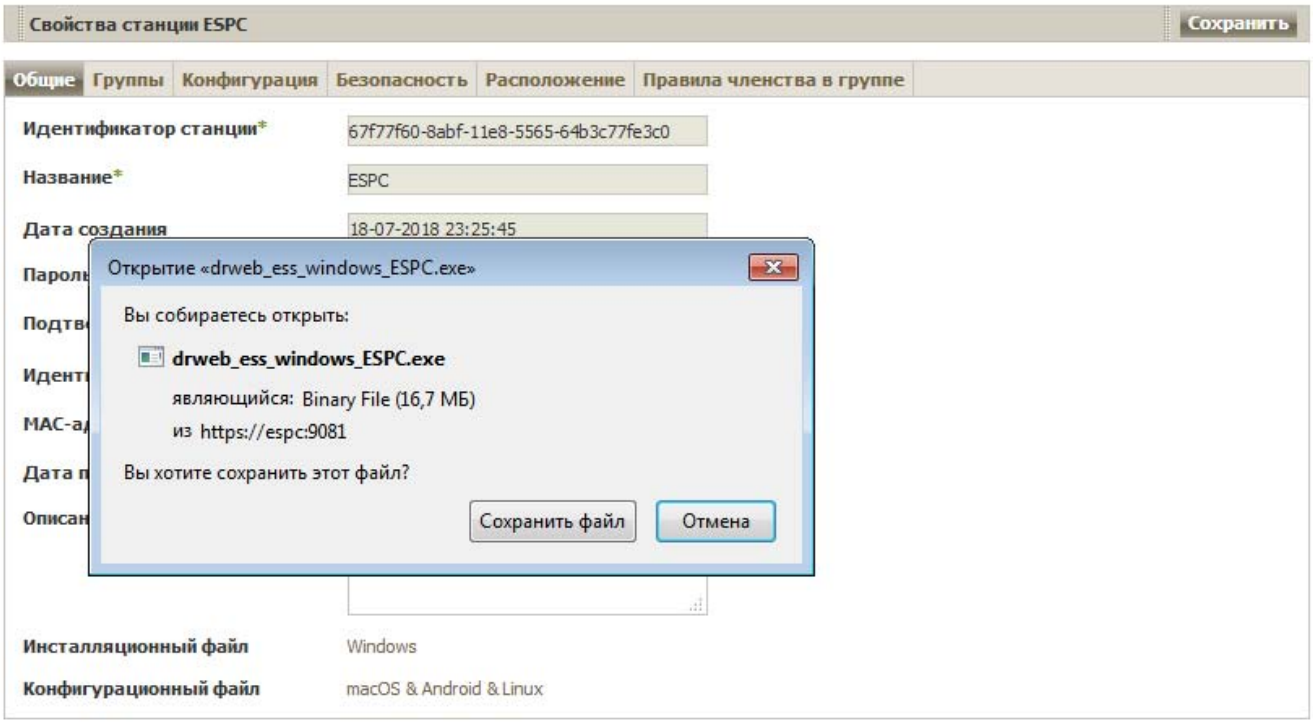
- Задается вручную — осуществляется попытка автоматической авторизации по заданным параметрам авторизации.
- Не задается — принцип авторизации на **Сервере** зависит от настроек **Сервера** для подключения новых станций (подробнее см. в Руководстве администратора, п. Политика подключения станций).

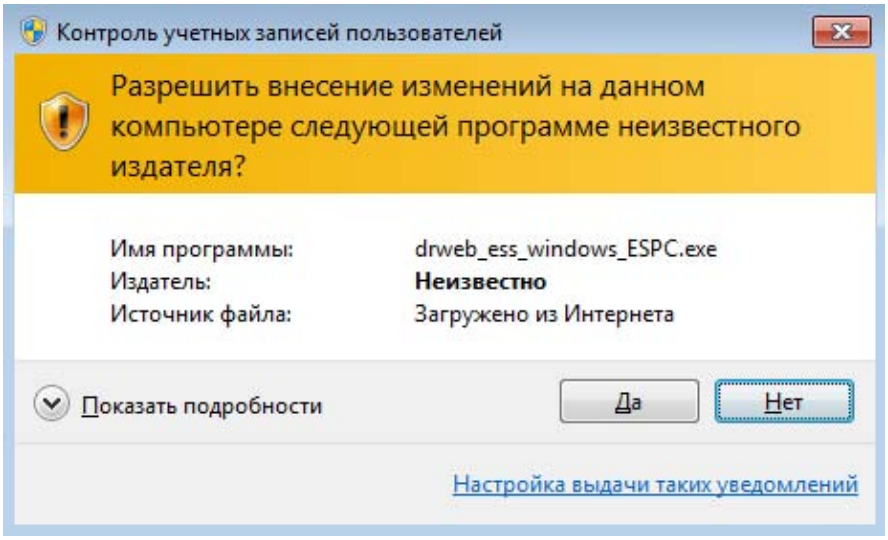
Для задания параметров авторизации вручную необходимо сначала создать новую учетную запись станции в Центре управления. При этом будет доступен инсталляционный пакет, содержащий конфигурационный файл с параметрами подключения и авторизации.

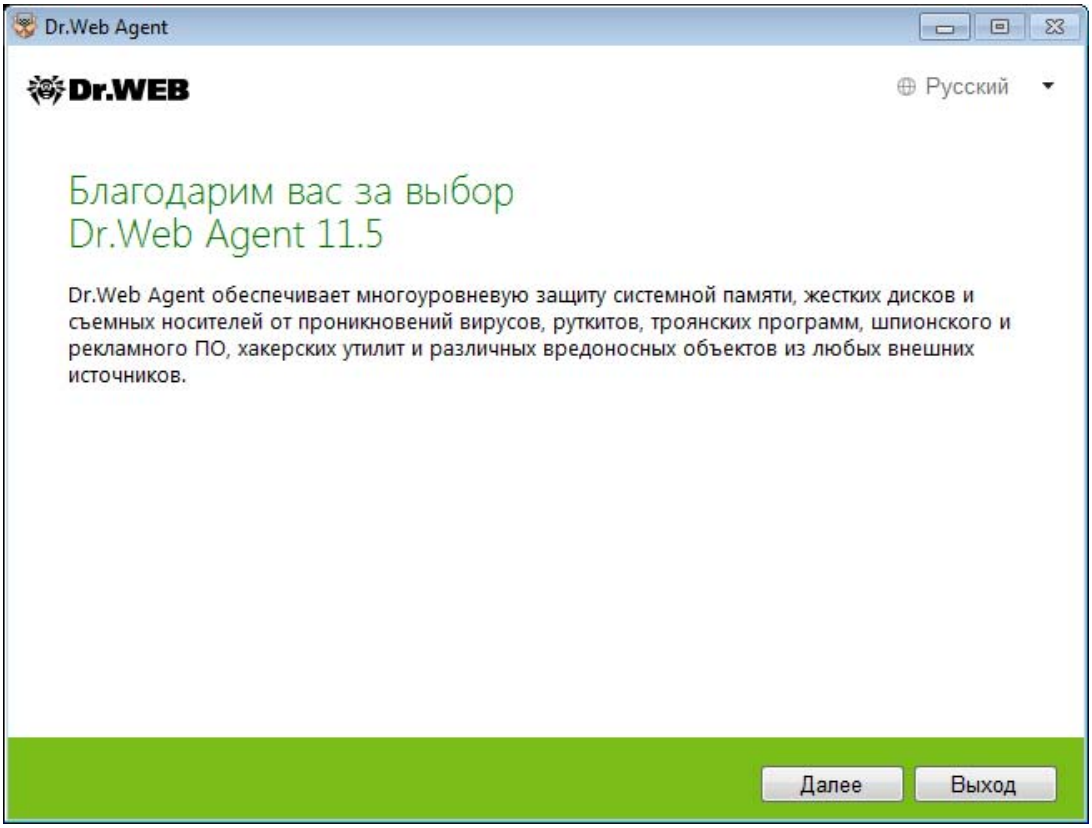
Рекомендуется использовать инсталляционный пакет вместо инсталлятора.

6.4.4.3.4. Локальная установка при помощи инсталляционного пакета для ОС Windows

1. Перейдя по ссылке, полученной при создании станции в Центре управления (ссылка **Windows** в разделе **Инсталляционный файл** в окне свойств станции), скачайте установочный файл *drweb_ess_windows_<имя_станции>.exe* и запустите его. Откроется окно мастера установки антивируса Dr.Web.

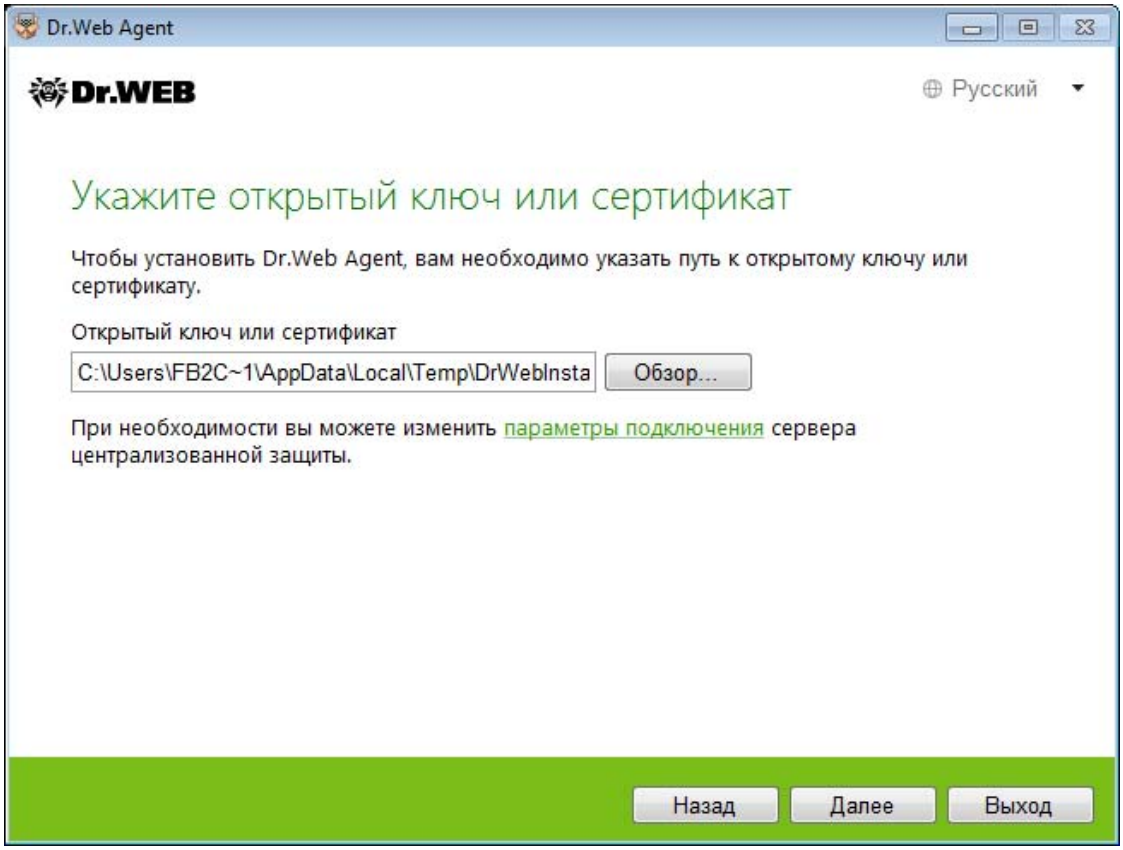

Свойства станции ESPC
Сохранить
Общие
Группы
Конфигурация
Безопасность
Расположение
Правила членства в группе
Идентификатор станции*
67f77f60-8abf-11e8-5565-64b3c77fe3c0
Название*
ESPC
Дата создания
18-07-2018 23:25:45
Открытие «drweb_ess_windows_ESPC.exe»
Вы собираетесь открыть:
drweb_ess_windows_ESPC.exe
являющийся: Binary File (16,7 МБ)
из https://espc:9081
Вы хотите сохранить этот файл?
Сохранить файл
Отмена
Инсталляционный файл
Windows
Конфигурационный файл
macOS & Android & Linux


Контроль учетных записей пользователей
Разрешить внесение изменений на данном компьютере следующей программе неизвестного издателя?
Имя программы:
drweb_ess_windows_ESPC.exe
Издатель:
Неизвестно
Источник файла:
Загружено из Интернета
Показать подробности
Да
Нет
Настройка выдачи таких уведомлений



В открывшемся окне проверьте правильность параметров установки и выберите язык установки.

В поле **Открытый ключ шифрования** задается полный путь к открытому ключу шифрования (drwcsd.pub), расположенному на компьютере пользователя (при запуске инсталлятора с Сервера по сети, ключ копируется во временные файлы ОС, а после перемещается в каталог установки).

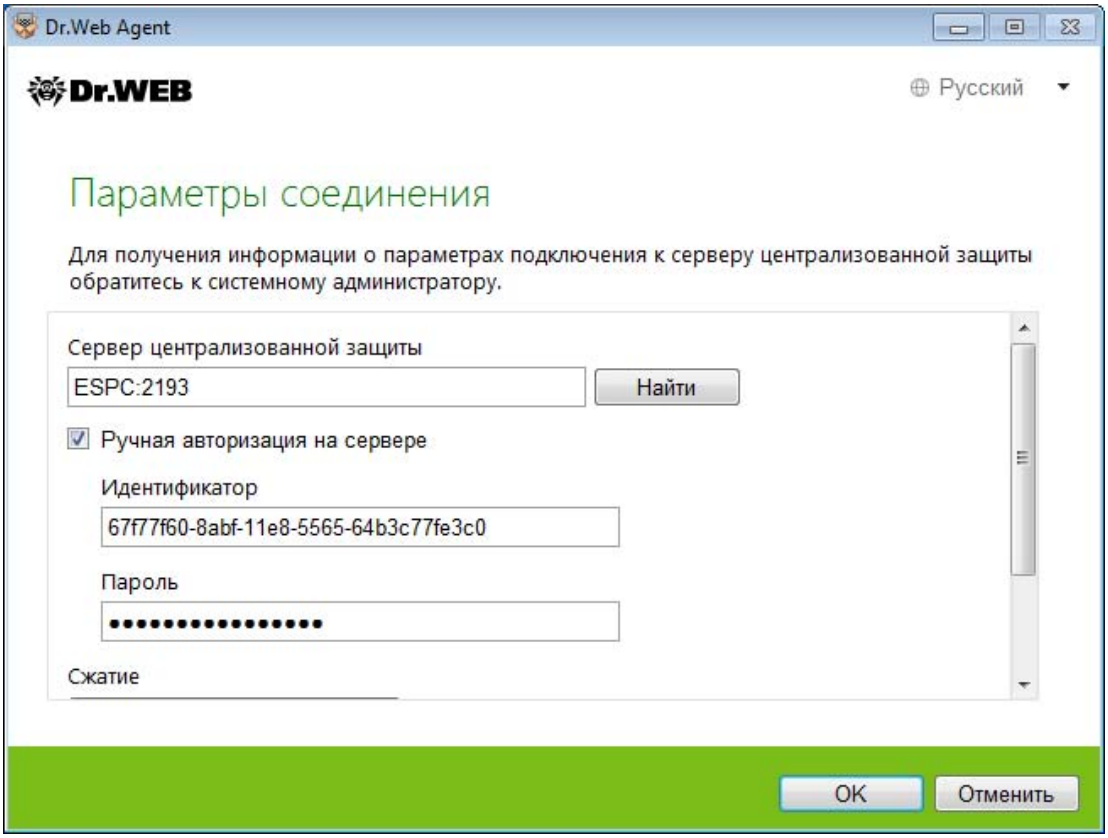


В случае возникновения ошибок доступа к серверу проверьте сетевые параметры.

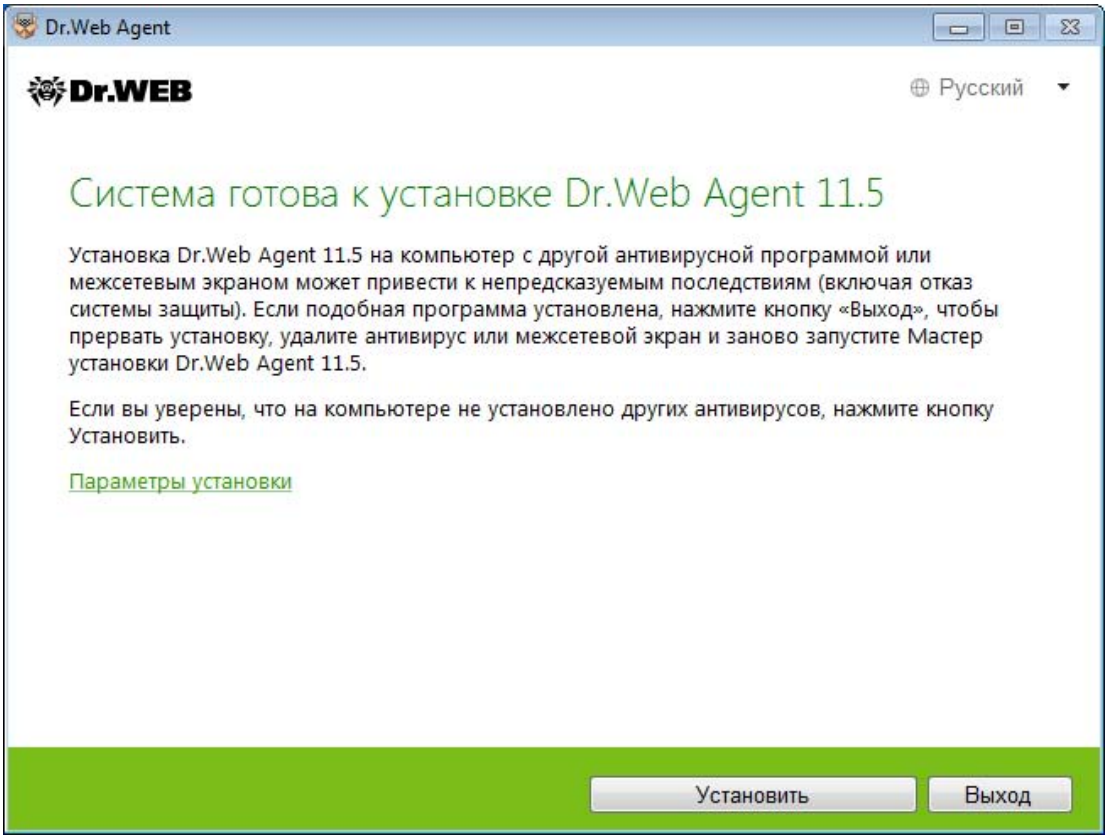
В поле **Сервер централизованной защиты** задается сетевой адрес антивирусного сервера, с которого будет производиться установка **Агента** и антивирусного пакета. Если при запуске инсталлятора вы задали адрес Сервера, то он будет автоматически занесен в данное поле. При установке **Агента** при помощи инсталлятора, созданного в Центре управления, поле заполняется автоматически.

Если вы не знаете адрес Сервера, нажмите на кнопку **Найти**. Будет выведено окно для поиска активных **Enterprise Серверов** сети. Задайте необходимые параметры (в формате *<имя_сервера>@<IP-адрес>/<префикс_сети>:<порт>*) и нажмите кнопку для начала поиска доступных серверов. В списке найденных серверов выберите тот, с которого будет устанавливаться антивирусное ПО, и нажмите на кнопку **ОК**.

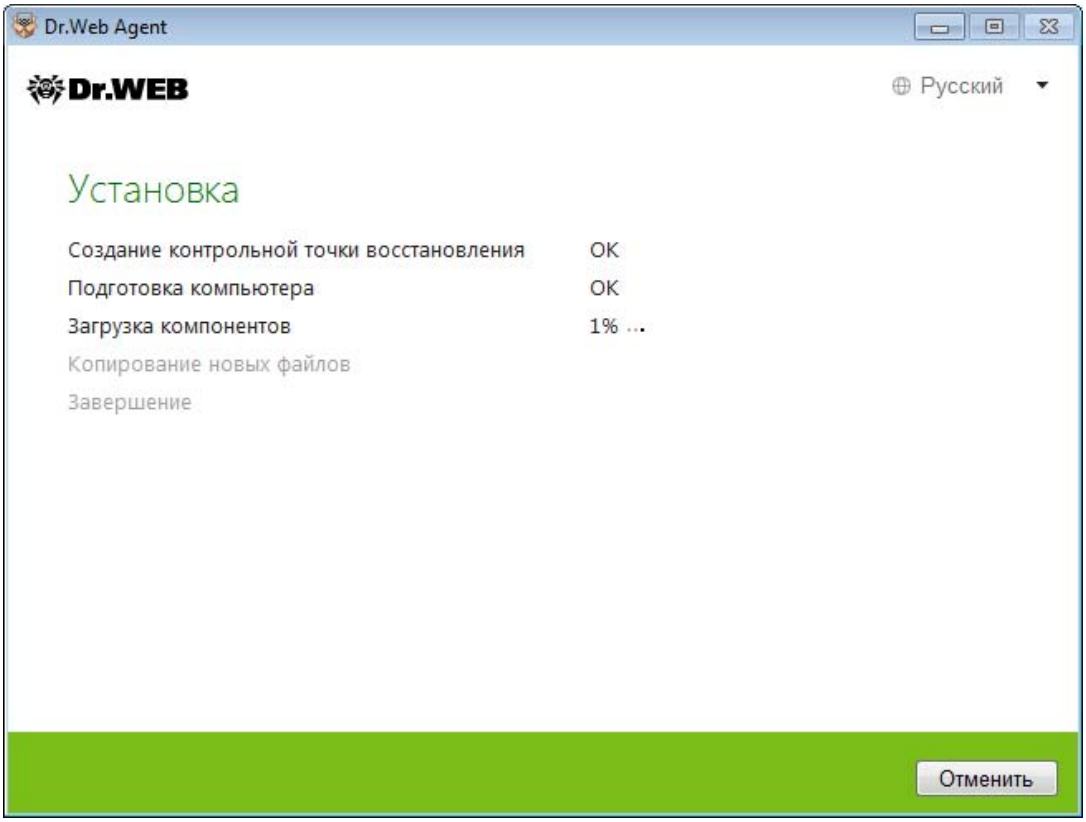
В разделе **Сжатие** выберите нужный для вас вариант компрессии трафика: **Да —** использовать сжатие, **Нет —** не использовать, **Возможно —** использование сжатия трафика зависит от настроек на Сервере.

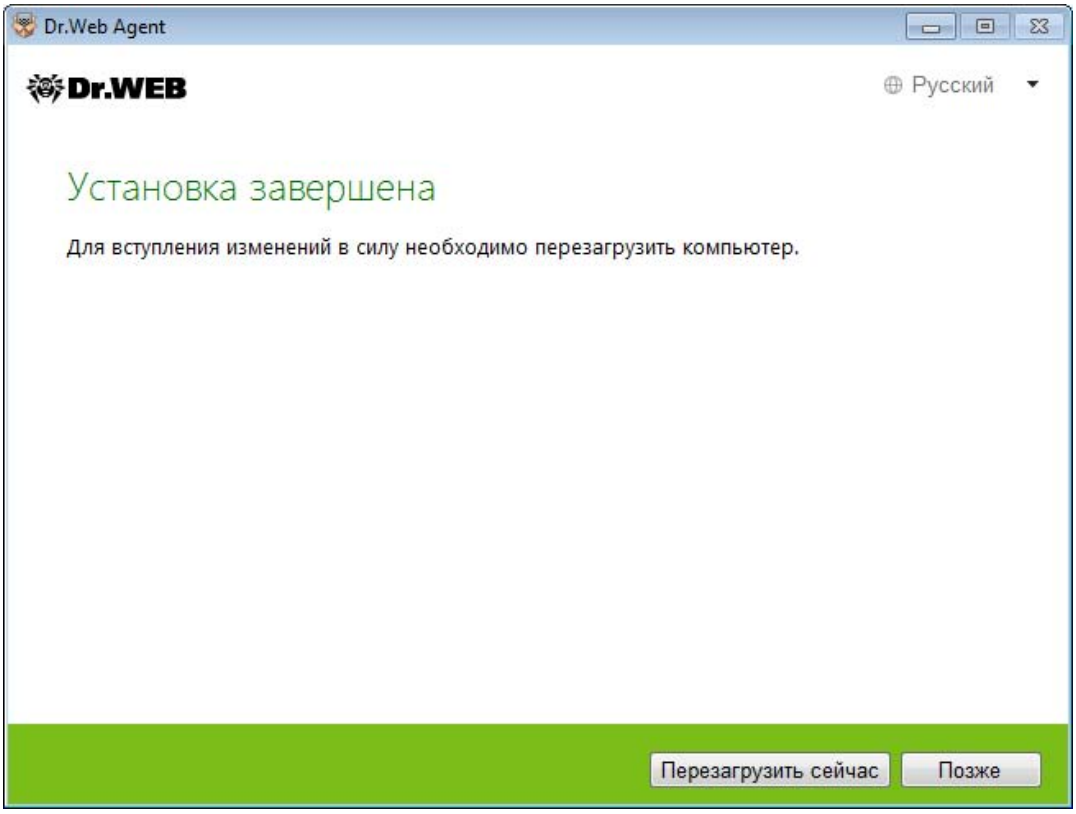


2. Подтвердите, что у вас не установлены антивирусные программы. Убедитесь, что на вашем компьютере не используется другое антивирусное ПО (в том числе ПО других версий антивирусных программ Dr.Web), после чего нажмите **Установить**.



Начнется установка Агента и антивирусных компонентов (не требует вмешательства пользователя).





3. После завершения инсталляции мастер установки сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Перезагрузить сейчас** для завершения работы мастера установки и перезагрузите компьютер.

Сразу после установки на компьютеры **Агенты** автоматически устанавливают соединение с Сервером. Как только Агент устанавливает связь с Сервером, в окне Центра управления появляется имя соответствующей рабочей станции.

6.4.4.3.5. Удаленная установка с использованием инсталляционного пакета с заданным ID на станцию с указанием IP-адреса вручную

Для установки Агента при помощи инсталляционного пакета необходимо:

1. При помощи Центра управления создать учетную запись нового пользователя на сервере и получить ссылку для загрузки инсталляционного пакета.
2. Произвести установку Агента на рабочую станцию.

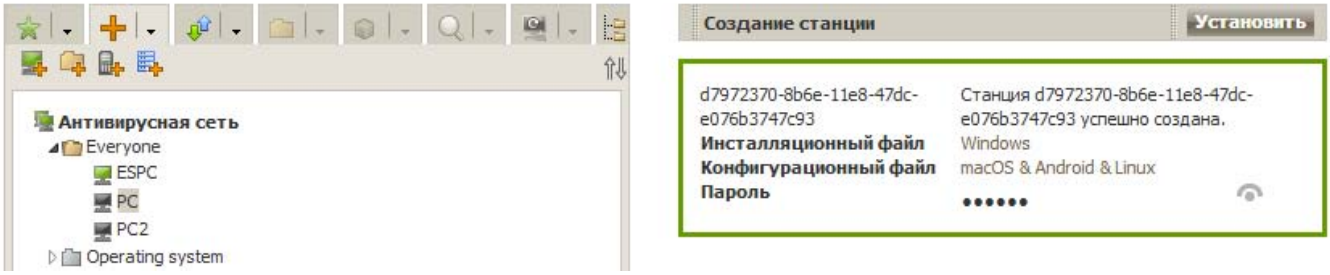
Авторизация новой антивирусной станции на Сервере по умолчанию осуществляется автоматически (подробная информация доступна в Руководстве администратора, п. Политика подключения новых станций).

6.4.4.3.6. Удаленная установка с использованием инсталляционного пакета с заданным ID на станцию с указанием IP-адреса средствами Центра управления

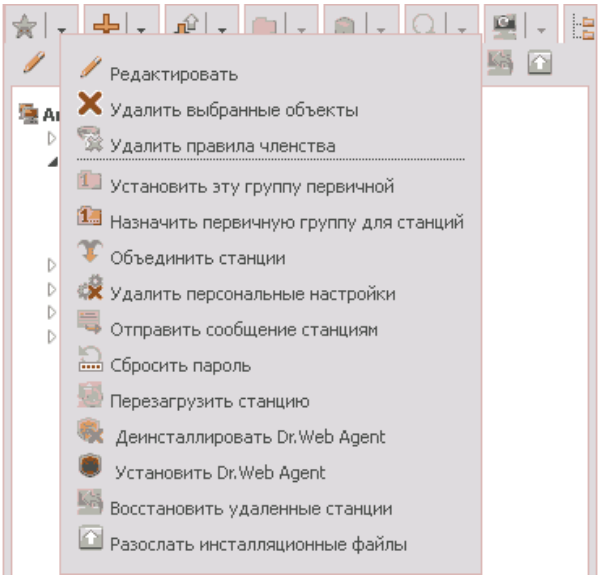
Для установки Агента при помощи инсталляционного пакета:

1. При помощи Центра управления создаем учетную запись нового пользователя на сервере и получаем ссылку для загрузки инсталляционного пакета — в иерархическом списке **Антивирусная сеть** выбираем иконку **Создать станцию**.

2. Сразу после создания учетной записи, в правой части главного окна откроется панель с заголовком **Создание станции**. В появившейся панели инструментов выбираем иконку **Установить**.

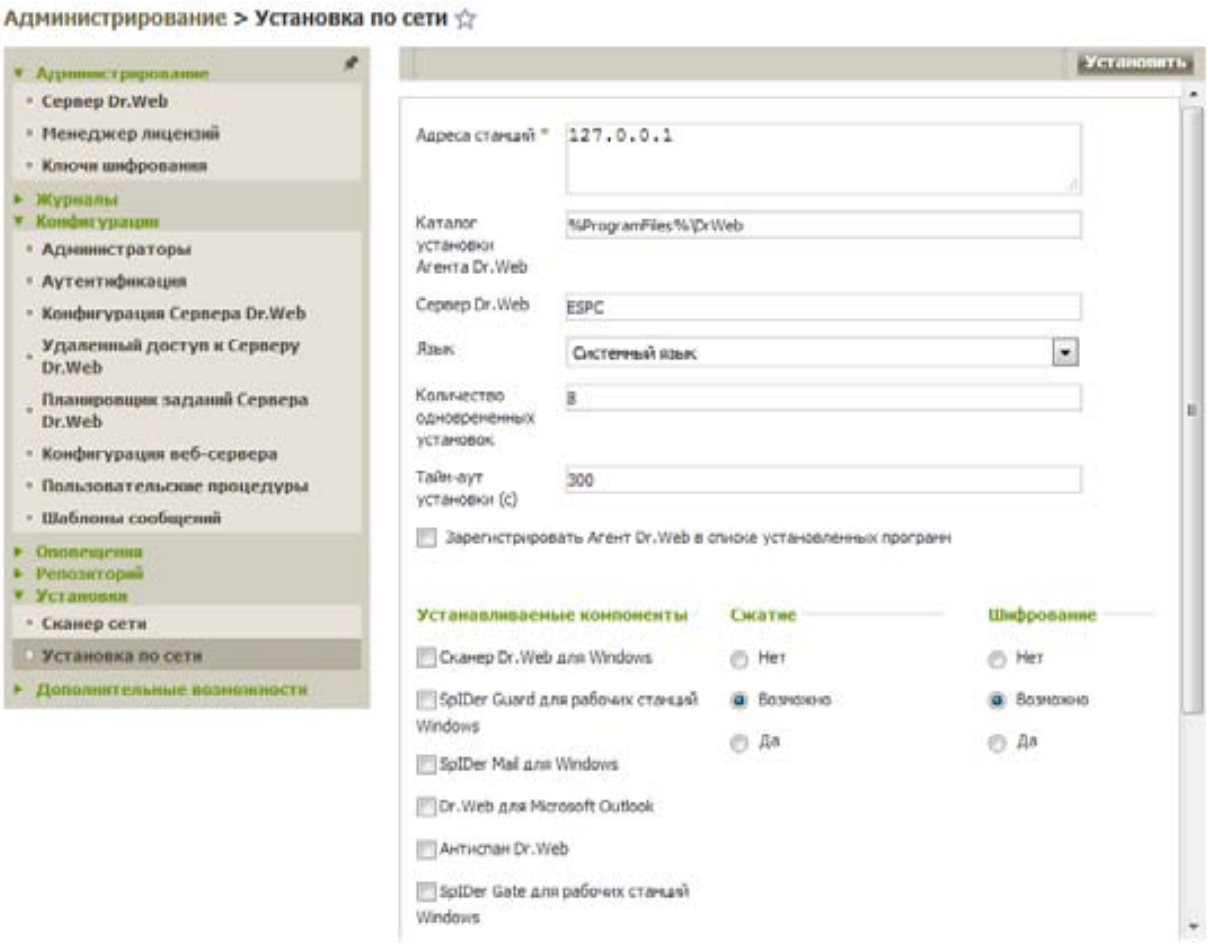


При использовании существующей учетной записи станции выберите **Установить Dr.Web Agent**.



3. Откроется окно **Сканера сети**. Проводим сканирование сети для подтверждения существования станции и выбираем ее.

4. После нажатия на значок процедура установки соответствует процедуре удаленной установки с помощью сканера сети.



После завершения установки проверьте, что в иерархическом списке у соответствующих станций изменились значки.

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

6.4.4.4. Установка Dr.Web Agent при помощи Сетевого инсталлятора

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

Установка при помощи **Сетевого инсталлятора** возможна в двух основных режимах:

1. В фоновом режиме — запускается, если задан ключ фонового режима.

2. В графическом режиме — режим по умолчанию. Запускается, если не задан ключ фонового режима.

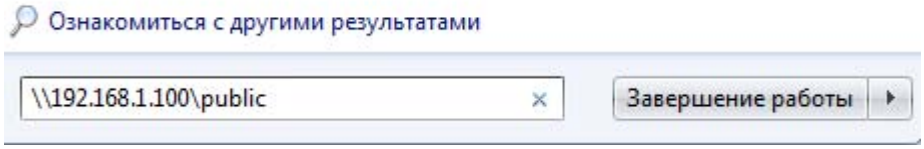
Если Сетевой инсталлятор запущен в режиме нормальной инсталляции (т. е. без ключа /instMode remove) на станции, на которой уже была проведена установка, это не приведет к выполнению каких-либо действий. Инсталлятор завершит работу и отобразит окно со списком допустимых ключей.

При помощи сетевого инсталлятора вы также можете установить **Агент Dr.Web** на рабочую станцию удаленно, с использованием **Центра управления**.

Внимание! Необходимо, чтобы на сервере был открыт для общего доступа каталог %DrWeb_ES%\Installer (по умолчанию в ОС Windows это каталог C:\Program Files\DrWeb Enterprise Server\Installer, его сетевое имя по умолчанию DRWESI$), содержащий два файла: drwcsd.pub и drwinst.exe. Данный каталог с указанными файлами создается автоматически в процессе инсталляции ES-сервера.

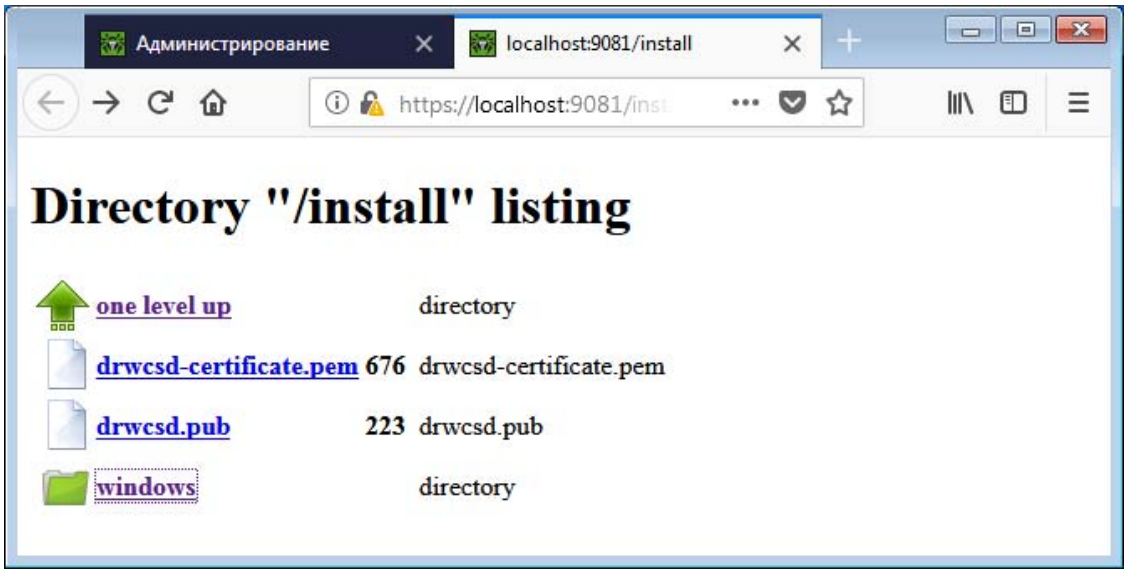
Необходимые для установки файлы можно получить двумя путями:

1) открыть папку на сервере Dr.Web Enterprise Security Suite (при установке Сервера это подкаталог Installer каталога установки Сервера, в дальнейшем его можно переместить), содержащую файлы, необходимые для установки компонентов Dr.Web Enterprise Security Suite. Обычно это папка Installer.



2) открыть страницу с инсталляторами агентов и файлами drwinst.exe и drwcsd.pub по ссылке http://<адрес_или_имя_сервера>:9080/install. Например, http://ES11:9080/install.

Из открывшейся папки необходимо скопировать на рабочий стол либо в иное место на локальном компьютере файлы drwinst.exe (из папки Windows) и drwcsd.pub.

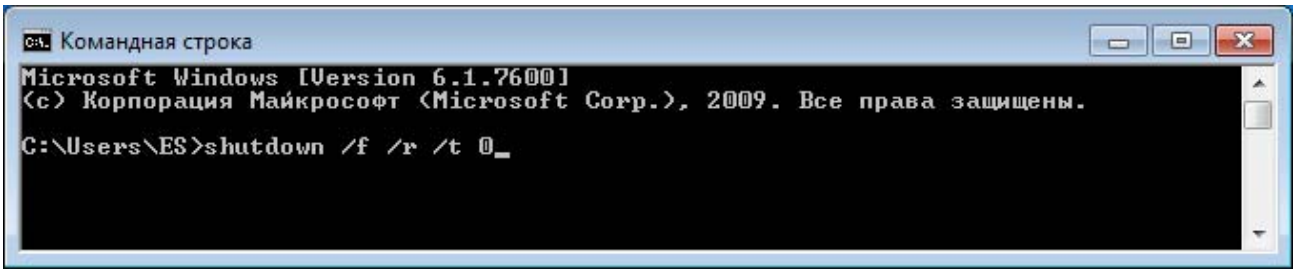


Внимание! После завершения работы инсталлятора на компьютер будет установлено только ПО Агента (но не компоненты антивирусной защиты). После подтверждения станции на Сервере (если этого требуют настройки Сервера) антивирусный пакет будет автоматически установлен.

Для завершения установки компонентов Dr.Web Enterprise Security Suite необходимо внести станцию, на которой была проведена установка, в число разрешенных. Выберите пункт **Администрирование** главного меню Центра управления. В иерархическом списке антивирусной сети выберите станции в подгруппе **Newbies** группы **Status**. Для задания доступа к **Серверу** на панели инструментов в разделе  **(Неподтвержденные станции)** задайте действие, которое будет применено.

2. Для завершения процесса установки необходимо перезагрузить станцию, на которой была проведена установка.

Внимание! В отличие от реальных машин, на виртуальных рекомендуется выполнять перезагрузку через выполнение команды shutdown.



По умолчанию команда drwinst, запущенная без параметров, использует режим **Multicast** для сканирования сети на наличие активных **Enterprise Серверов** и осуществляет попытку установки Агента с первого найденного Сервера в сети. При этом если имеющийся pub-ключ не соответствует ключу Сервера, установка завершится с ошибкой. В этом случае явно укажите адрес Сервера при запуске инсталлятора.

drwinst можно запускать с дополнительными параметрами:

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

  drwinst /silent yes <*DNS_имя_Сервера*>

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

Вы также можете использовать явное указание адреса Сервера, например

drwinst /silent yes 192.168.1.3

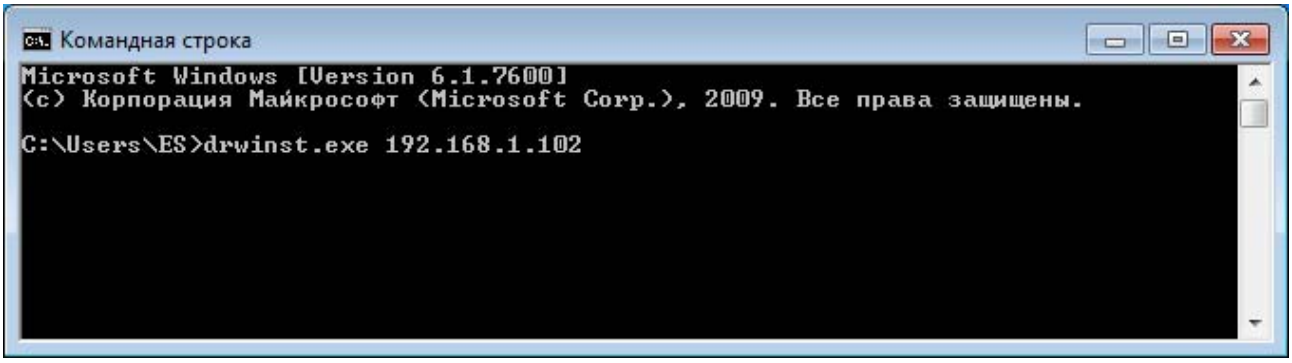
- Использование ключа /regagent позволяет при установке зарегистрировать Агент в списке **Установка и удаление программ** (**Add or Remove Programs**)
- Для запуска инсталлятора в графическом режиме используйте параметр -interactive.

Полный список параметров **Сетевого инсталлятора** приведен в документе Приложение, п. H2. Сетевой инсталлятор.

6.4.4.4.1. Установка Dr.Web Agent при помощи Сетевого инсталлятора в фоновом режиме инсталлятора

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

1. С компьютера, на который будет устанавливаться антивирусное ПО, войдите в сетевой каталог установки Агента (при установке Сервера это подкаталог Installer каталога установки Сервера, в дальнейшем его можно переместить) или скачайте с инсталляционной страницы Центра управления и запустите исполняемый файл drwinst.exe с ключом фонового режима /silent yes.



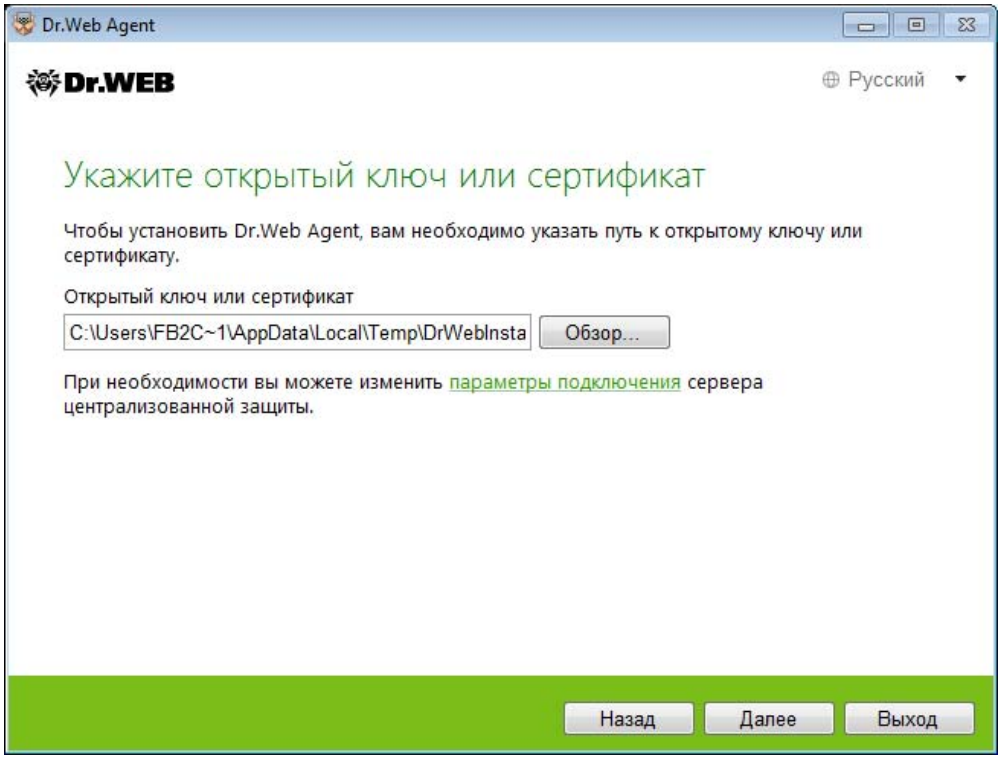
При использовании режима **Multicast** для поиска активных **Серверов**, установка **Агента** будет производиться с первого найденного **Сервера**. При этом, если имеющийся открытый ключ шифрования не соответствует ключу шифрования **Сервера**, установка завершится с ошибкой. В этом случае явно укажите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

2. После завершения работы инсталлятора на компьютер будет установлено ПО Агента (но не антивирусный пакет).
3. После подтверждения станции на Сервере (если этого требуют настройки Сервера) антивирусный пакет будет автоматически установлен.
4. Перезагрузите компьютер по требованию Агента.
5. Свидетельством удачного завершения установки является появление значка в трее.

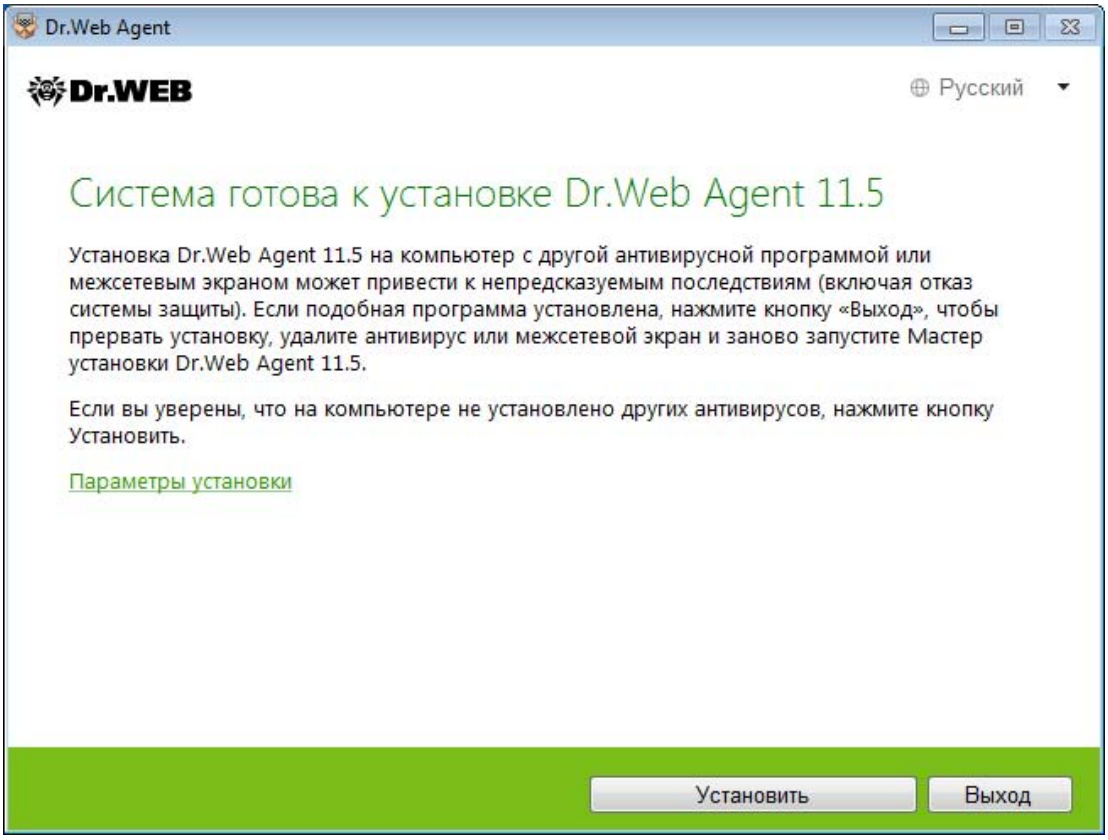
6.4.4.4.2. Установка Dr.Web Agent в графическом режиме инсталлятора

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

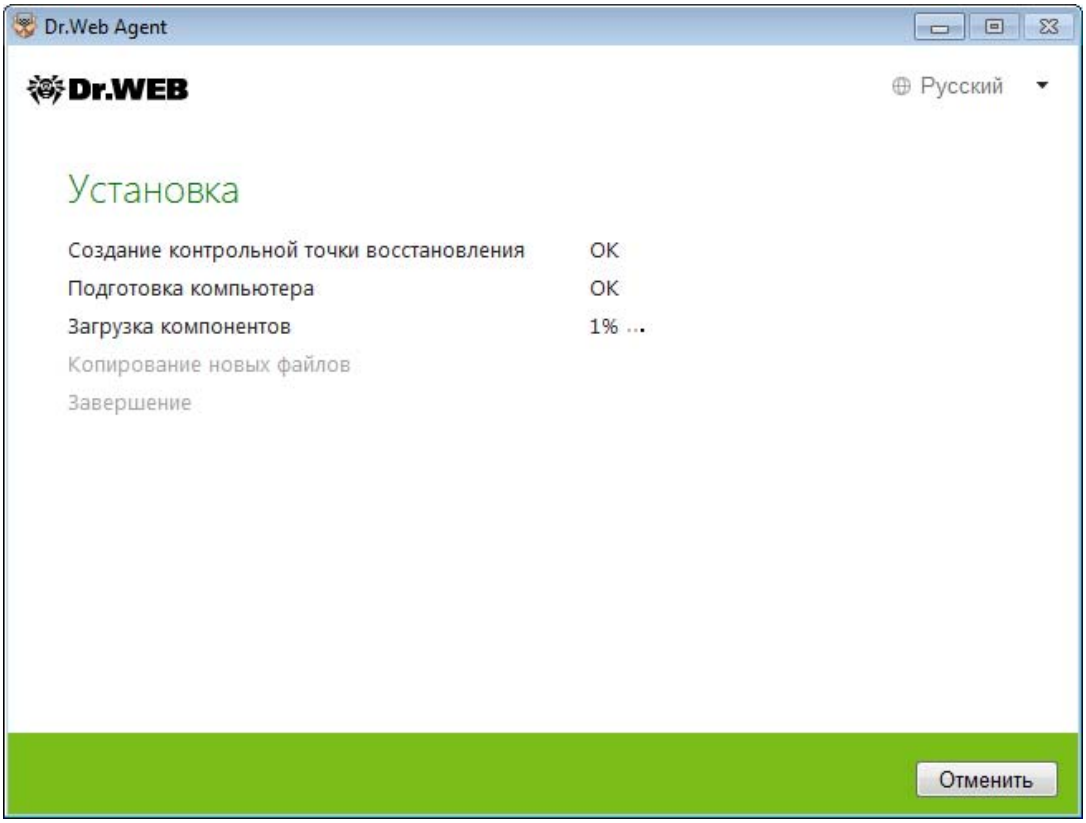
1. С компьютера, на который будет устанавливаться антивирусное ПО, войдите в сетевой каталог установки Агента (при установке Сервера это подкаталог **Installer** каталога установки Сервера, в дальнейшем его можно переместить) и запустите программу drwinst. Откроется окно мастера установки антивируса Dr.Web.
2. Действия по установке **Агента** на станцию при помощи графического режима сетевого инсталлятора аналогичны действиям при ус тановке при помощи инсталляционного пакета, но без н астроек подключения к **Серверу**, если они не были заданы в соответствующем ключе командной строки.
3. Укажите местоположение открытого ключа шифрования.

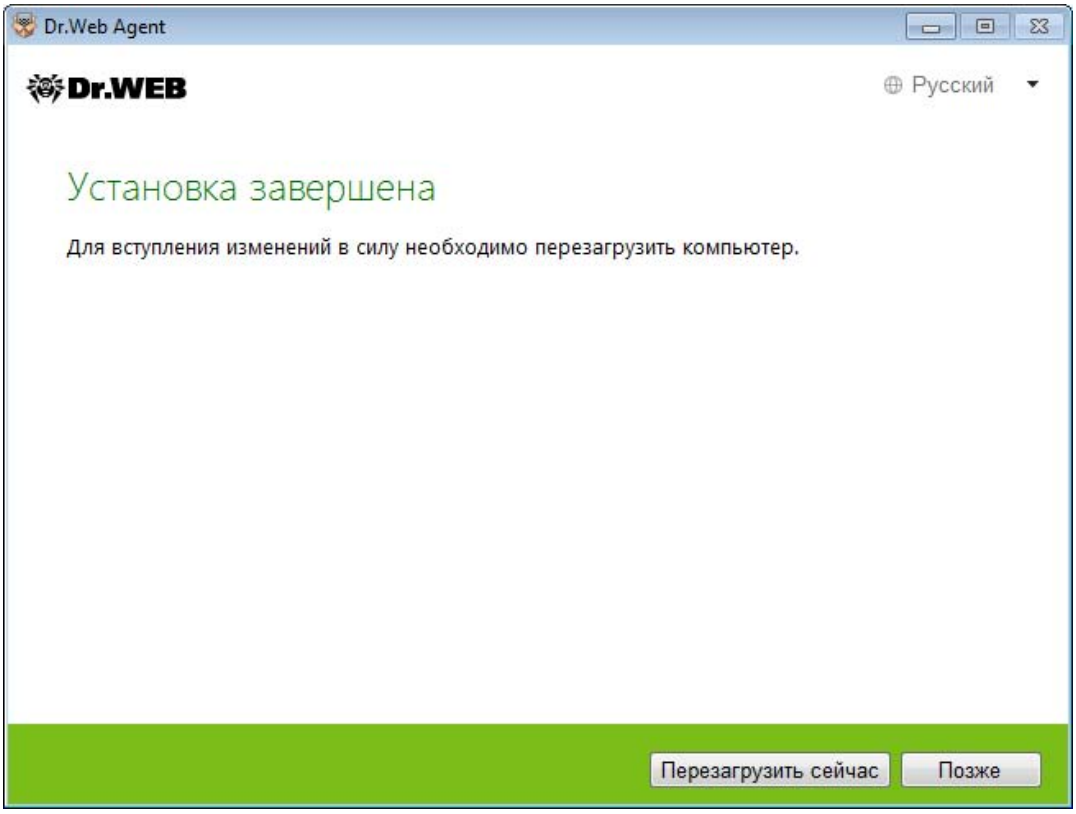


4. Перед началом инсталляции мастер установки попросит подтвердить, что на компьютере не установлены антивирусные программы. Убедитесь, что на компьютере не используется другое антивирусное ПО (в том числе ПО других версий антивирусных программ Dr.Web).



Нажмите на кнопку **Установить**.





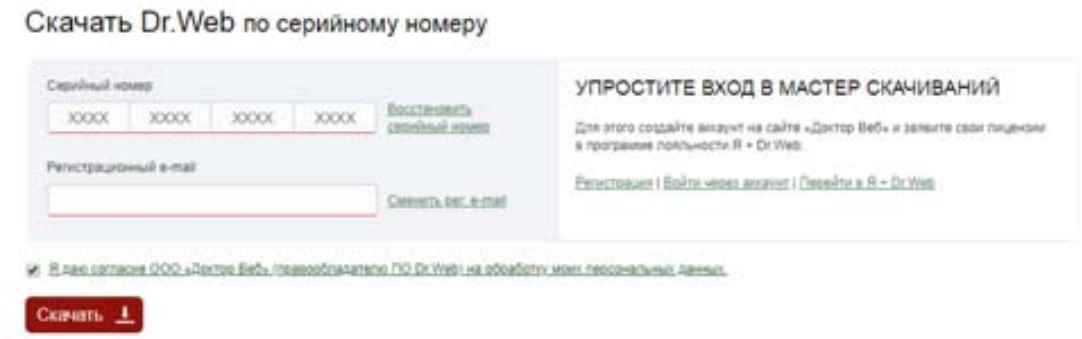
5. После завершения инсталляции мастер установки сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Перезагрузить сейчас** для завершения работы мастера установки и перезагрузите компьютер.

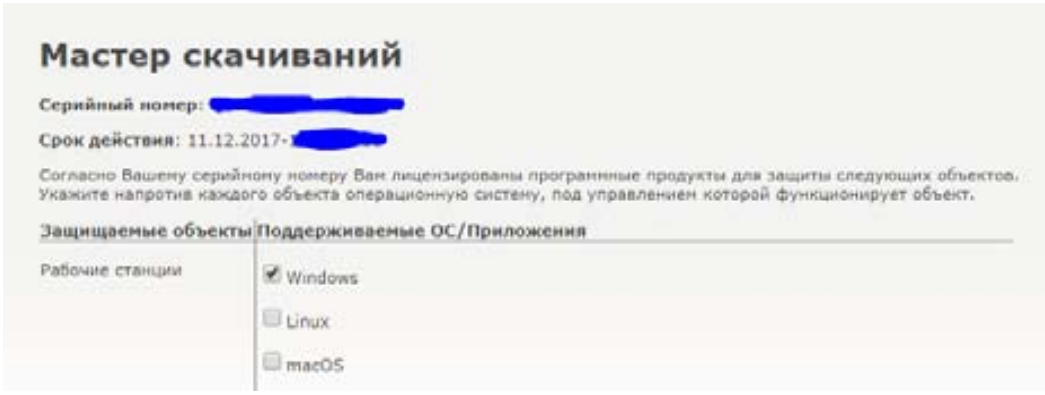
Сразу после установки на компьютеры **Агенты** автоматически устанавливают соединение с Сервером. Как только Агент устанавливает связь с Сервером, в окне Центра управления появляется имя соответствующей рабочей станции — имя ранее созданной станции заменяется именем машины, на которую осуществлена установка.

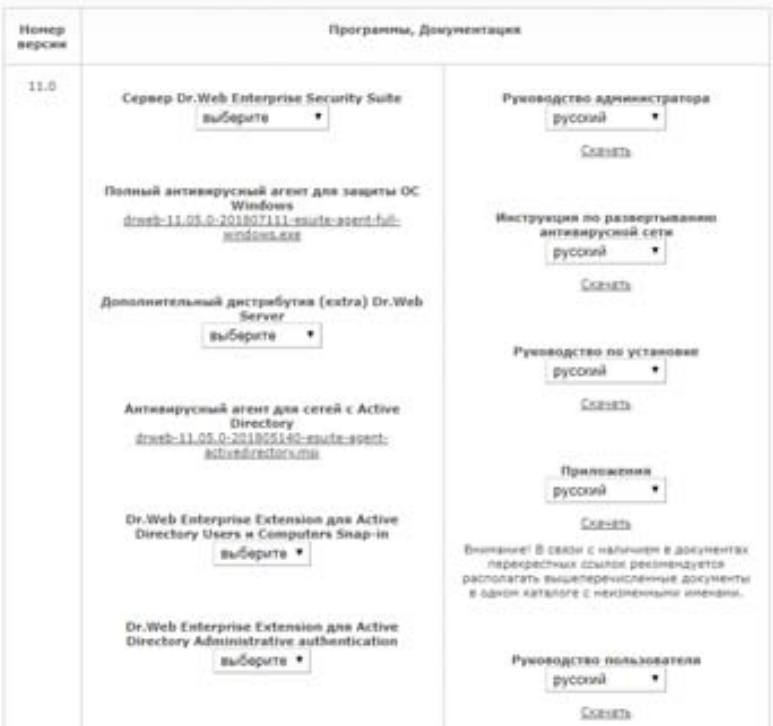
6.4.5. Удаленная установка с использованием службы Active Directory

Для установки Агента с использованием Active Directory загрузите с помощью Мастера скачиваний на сайте «Доктор Веб» (https://download.drweb.ru) инсталлятор **Агента** для сетей с Active Directory (файл вида: drweb-11.05.0-<номер_сборки>-esuite-agent-activedirectory.msi) и установите его с помощью команды *msiexec* на сервере локальной сети, поддерживающем службу Active Directory.

Внимание! Для скачивания вам потребуется указать серийный номер и электронную почту, на которую он зарегистрирован.



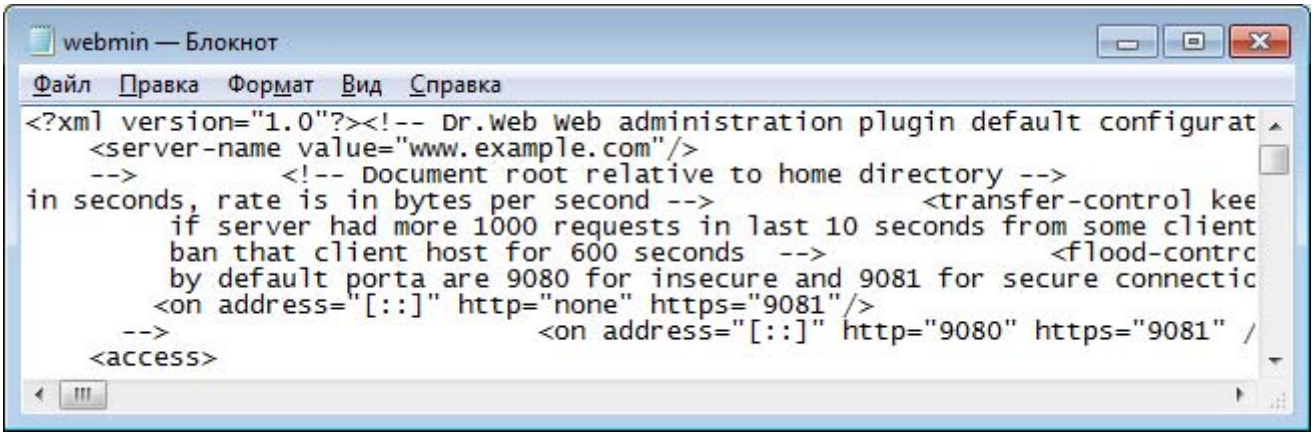




Установку можно производить как в режиме командной строки, так и в графическом режиме инсталлятора.

Перед установкой убедитесь, что целевой каталог для образа Агента не содержит в себе инсталлятор **Агента** для сетей с Active Directory.

Также перед инсталляцией рекомендуется задать параметр **ServerName**, хранящийся в файле webmin.conf.



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

6.4.5.1. Удаленная установка Dr.Web Agent для сетей с Active Directory в режиме командной строки

Выполните команду *msiexec* с необходимыми параметрами, указав параметр отключения графического режима.

Формат команды: msiexec /a <*название_пакета*>.msi /qn [<*параметры*>]

Формат ключей:

- /a запускает развертывание административного пакета.
- /qn — параметр отключения графического режима. При использовании этого ключа необходимо задать следующие обязательные параметры:
  - ESSERVERADDRESS=<*DNS_имя*> — указывает адрес **Enterprise Сервера**, к которому будет подключаться Агент. Подробное описание параметра содержится в Руководстве администратора, см. Приложение Е3.
  - ESSERVERPATH=<*путь_имя_файла*> — указывает полный доменный путь к открытому ключу шифрования **Enterprise Сервера** и имя файла (по умолчанию файл drwcsd.pub в подкаталоге Installer каталога установки **Enterprise Сервера**).
  - TARGETDIR — сетевой каталог для образа Агента (модифицированного установочного пакета Агента), который выбирается через редактор групповых политик для назначенной установки. Данный каталог должен иметь доступ на чтение и запись. Путь к каталогу следует указывать в формате сетевых адресов, даже если он доступен локально; каталог обязательно должен быть доступен с целевых станций.
  - Перед административной установкой целевой каталог для образа Агента (см. параметр ARGETDIR) не должен содержать в себе инсталлятор Агента для сетей с **Active Directory** (<*название_пакета*>.msi).

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

Примеры:

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net
ESSERVERPATH=\\win_serv\drwcs_inst\drwcsd.pub
TARGETDIR=\\comp\share

msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1
ESSERVERPATH="C:\Program Files\DrWeb
Server\Installer\drwcsd.pub" TARGETDIR=\\comp\share
```

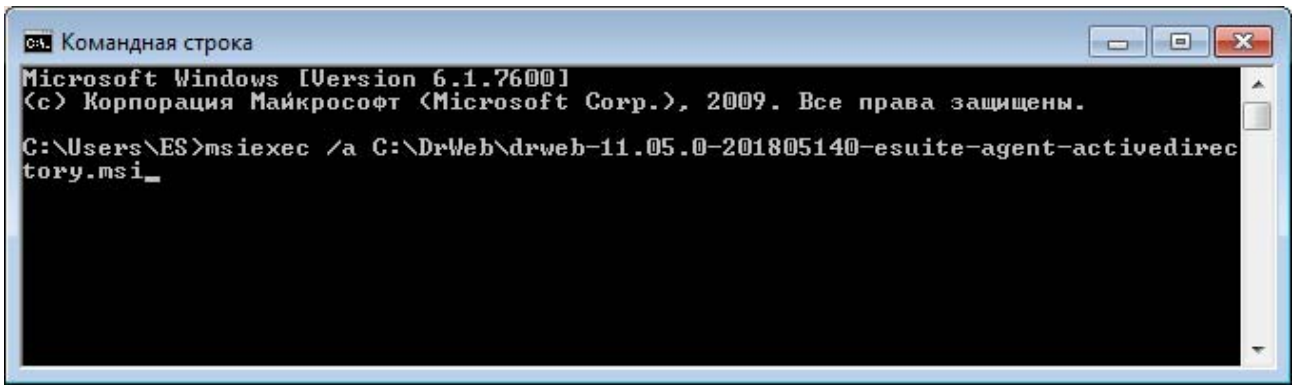
После окончания развертывания пакета необходимо на сервере локальной сети, где установлено ПО управления Active Directory, назначить установку пакета. Процедура описана далее в разделе 6.4.5.3.

6.4.5.2. Удаленная установка Dr.Web Agent для сетей с Active Directory в графическом режиме

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

1. Для запуска инсталлятора в графическом режиме выполните команду:

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

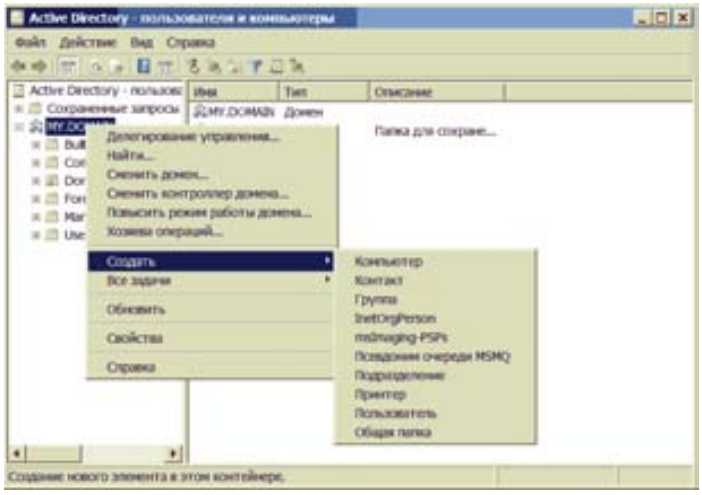


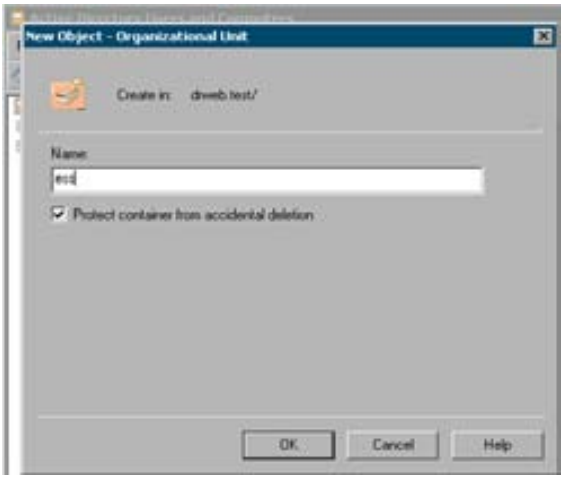
Внимание! Путь к инсталлятору должен быть полным — содержать не только имя, но и путь к файлу.

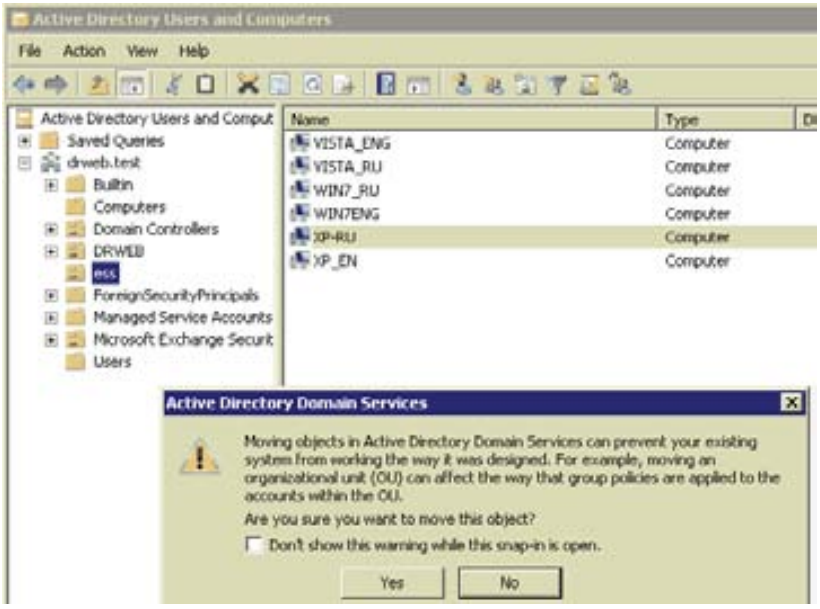
2. Откроется окно **InstallShield Wizard**, извещающее об устанавливаемом продукте. Язык установки будет соответствовать языку, указанному в языковых настройках компьютера. Нажмите на кнопку **Далее**.
3. В новом окне укажите DNS-имя или IP-адрес Сервера Dr.Web (см. в документе **Приложения**, п. Приложение Е2). Укажите местонахождение сертификата Сервера Dr.Web (drwcsd-certificate.pem). Нажмите кнопку **Далее**.
4. В следующем окне укажите сетевой каталог, в который будет записан образ Агента. Путь к образу следует указывать в формате сетевых адресов, даже если каталог доступен локально; каталог обязательно должен быть доступен с целевых станций. Нажмите кнопку **Установить**.
5. После завершения инсталляции будет автоматически вызвано окно настройки, с помощью которого вы сможете назначить установку пакетов на компьютеры сети.

6.4.5.3. Настройка параметров установки компонентов антивирусной защиты на выбранные станции

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







3. Откройте окно редактирования групповых политик. Для этого:

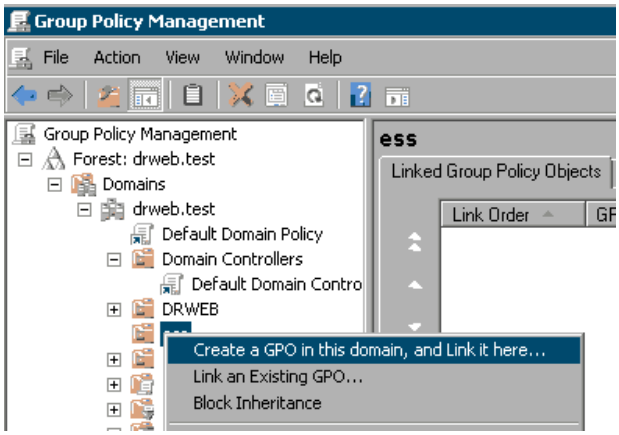
a) для ОС Windows 2000/2003 Server: в контекстном меню созданного подразделения **ESS** выберите пункт **Свойства**. В открывшемся окне свойств перейдите на вкладку **Групповая политика**.

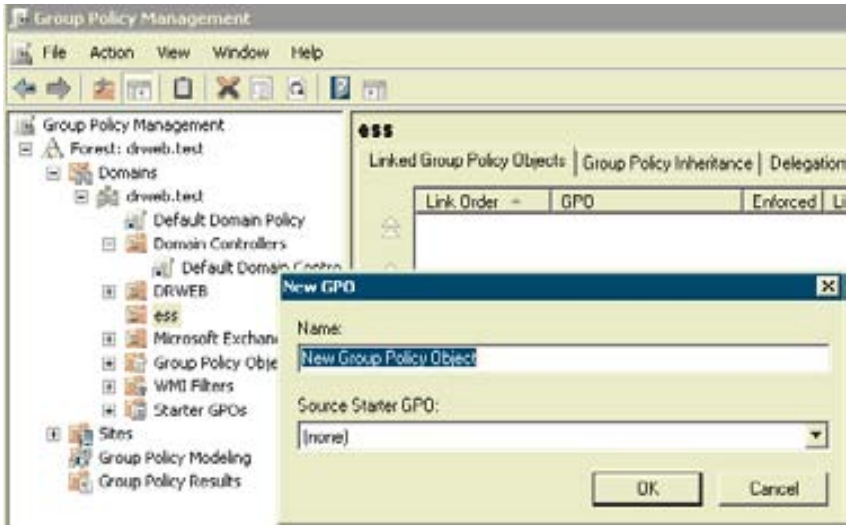
b) для ОС Windows 2008/2012/2012R2 Server: **Пуск → Администрирование → Управление групповой политикой**.

4. Для созданного подразделения задайте групповую политику. Для этого:

a) в ОС Windows 2000/2003 Server: нажмите кнопку **Добавить** и создайте элемент списка с именем политики **ESS**. Дважды щелкните по нему;

b) в ОС Windows 2008/2012/2012R2 Server: в контекстном меню созданного подразделения **ESS** выберите пункт **Создать объект GPO в этом домене и связать его**. В открывшемся окне задайте название нового объекта групповой политики и нажмите кнопку **ОК**. В контекстном меню новой групповой политики выберите пункт **Изменить**.



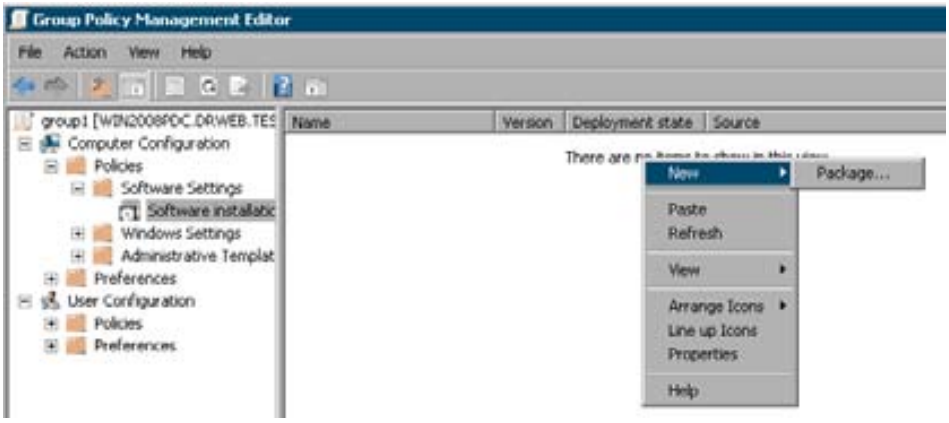


5. В открывшемся окне **Редактор управления групповыми политиками** внесите настройки для групповой политики, созданной в п. **4**. Для этого:

a) В ОС Windows 2000/2003 Server: в иерархическом списке выберите элемент **Конфигурация компьютера → Конфигурация программ → Установка программ**.

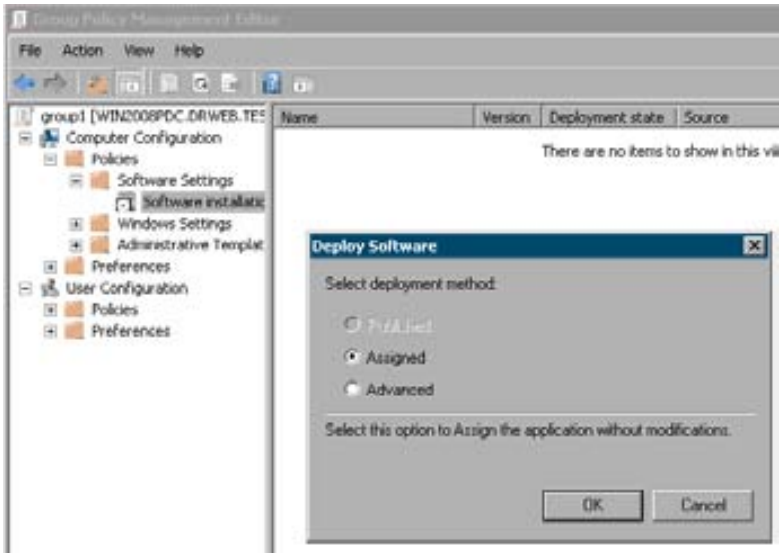
b) В ОС Windows 2008/2012/2012R2 Server: в иерархическом списке выберите элемент **Конфигурация компьютера → Политики → Конфигурация программ → Установка программ**.

6. В контекстном меню элемента **Установка программ** выберите пункт **Создать → Пакет**.



7. Далее задайте установочный пакет Агента. Для этого укажите адрес сетевого разделяемого ресурса (созданный при административной установке образ Агента). Путь к каталогу с пакетом следует указывать в формате сетевых адресов, даже если каталог доступен локально. В таблице в основной части окна необходимо выбрать строчку drweb-11.05.0-<номер_сборки>-esuite-agent-activedirectory и нажать на кнопку **Открыть**.

8. В окне **Развертывание программ** выберите опцию **Назначенные** и нажмите **ОК**.

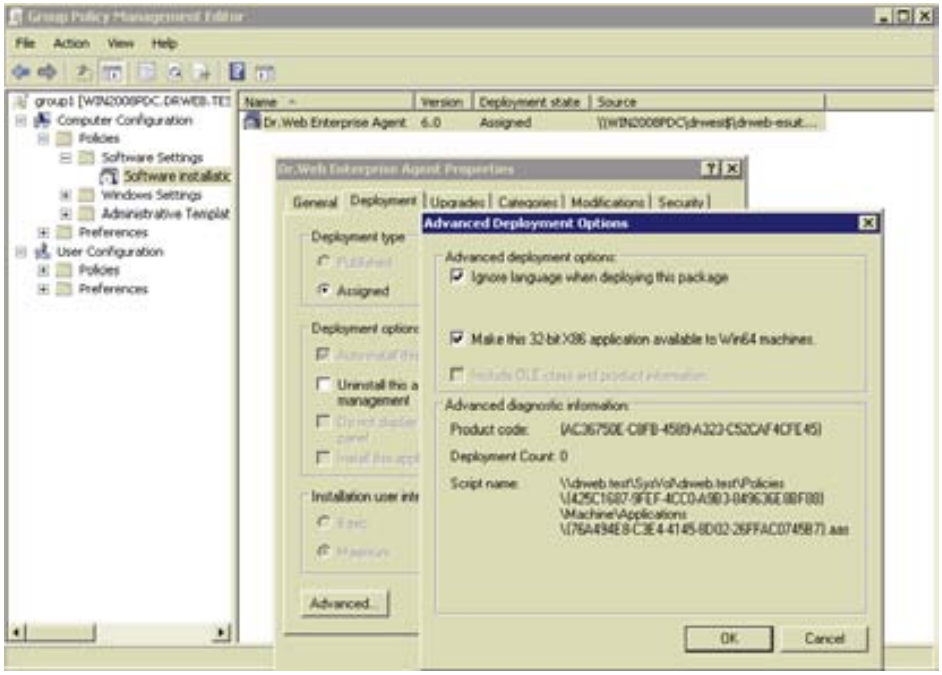


9. В окне редактора управления групповыми политиками появится пункт **Dr.Web Agent**. В контекстном меню этого пункта выберите **Свойства**.

10. В открывшемся окне свойств пакета перейдите на вкладку **Развертывание**. Нажмите кнопку **Дополнительно**.

11. Откроется окно **Дополнительные параметры развертывания**.

- Установите флажок **Не использовать языковые установки при развертывании**.
- Если вы планируете установку Агента Dr.Web при помощи настраиваемого msi-пакета на 64-битные ОС, установите флажок **Сделать доступным это 32-битное приложение для x64 машин**.



12. Нажмите дважды **ОК**.

Агент Dr.Web будет установлен на выбранные компьютеры при ближайшей регистрации их в домене.

6.4.5.4. Применение политик с учетом предыдущих установок Агента

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

1. **На станции нет Агента Dr.Web**.

После применения политик Агент будет установлен по общим правилам.

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

После применения политики Active Directory установленный Агент останется на станции.

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

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

3. На станции уже установлен Enterprise Агент с использованием службы Active Directory.

После применения политики:

1. Если для станции разрешены права на удаление Агента, то он будет удален со станции. Для установки Агента через Active Directory необходимо повторно назначить политики Active Directory для данной станции.

В данной ситуации необходимо повторное назначение политик для установки Агента, поскольку после первого назначения политик Агент на станции будет удален, но для службы Active Directory Агент считается установленным.

2. Если у станции нет прав на удаление Агента, назначение политик не приведет к изменению состояния антивирусного ПО на станции. Для дальнейших действий необходимо задать права на удаление Агента (см. п. 7.5.11.4. Установка или ограничение прав пользователей) и повторно назначить политики Active Directory для данной станции. Далее действия аналогичны предыдущему пункту.

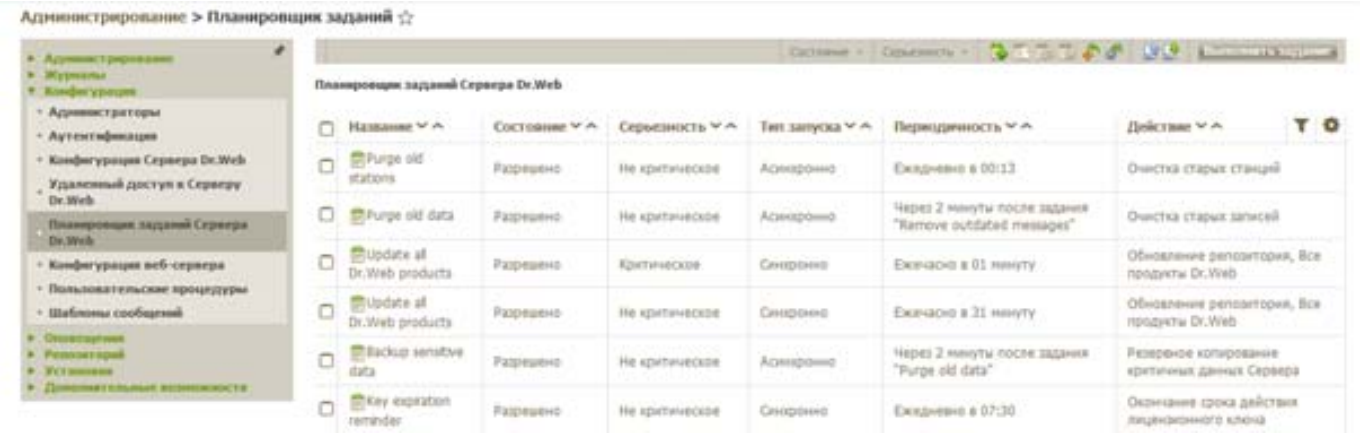
Повторное назначение политик Active Directory может осуществляться любым удобным способом.

6.4.6. Настройка параметров автоматического удаления станций

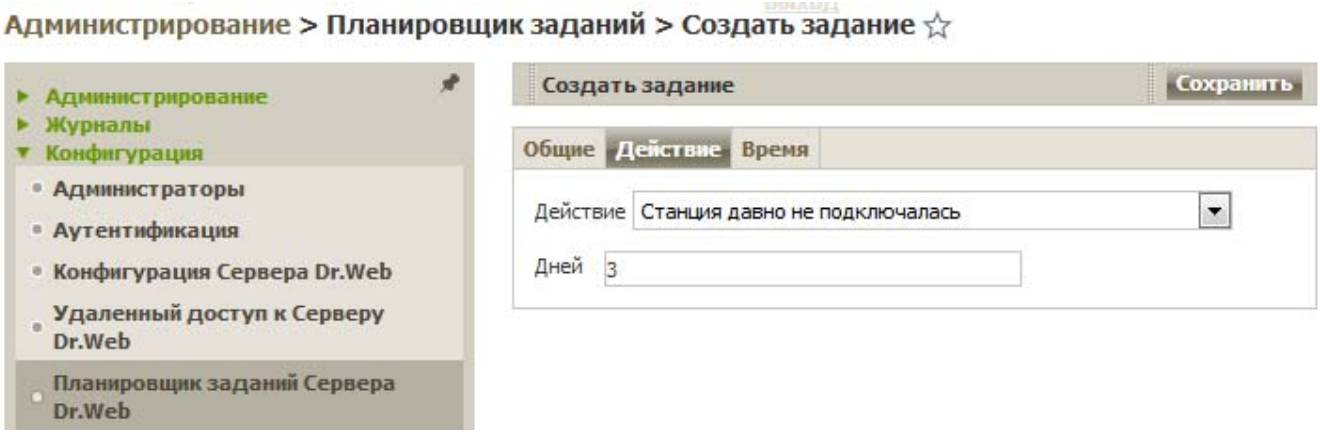
Станции, в течение указанного времени не подключавшиеся к антивирусному серверу, автоматически удаляются из репозитория с целью экономии дискового пространства. По умолчанию период для удаления старых станций составляет 90 дней.

Для изменения периода времени, в течение которого станция может быть недоступна:

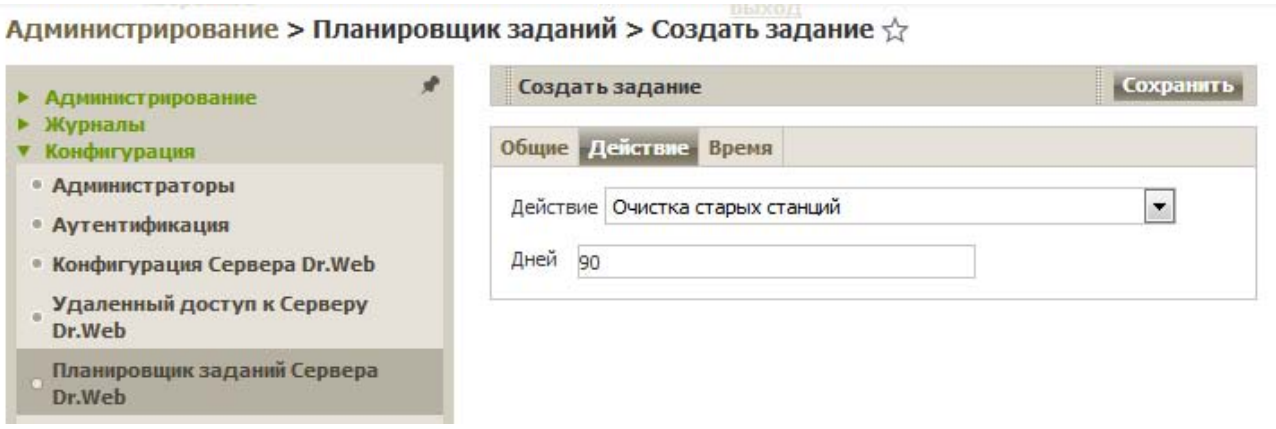
1. В меню **Администрирование** → **Конфигурация** выберите пункт **Планировщик заданий Сервера Dr.Web**.



2. Нажмите на значок  для создания нового задания, на вкладке **Общие** укажите название нового задания, после чего перейдите на вкладку **Действие** и в выпадающем списке выберите пункт **Станция давно не подключалась**.



3. Укажите период, по истечении которого должно выдаваться напоминание о том, что станция считается долго не посещавшей антивирусный сервер.
4. Нажмите **Сохранить** для сохранения задания.
5. Нажмите на значок  для создания нового задания.
6. Нажмите на значок  для создания нового задания, на вкладке **Общие** укажите название нового задания, после чего перейдите на вкладку **Действие** и в выпадающем списке выберите пункт **Очистка старых станций**.

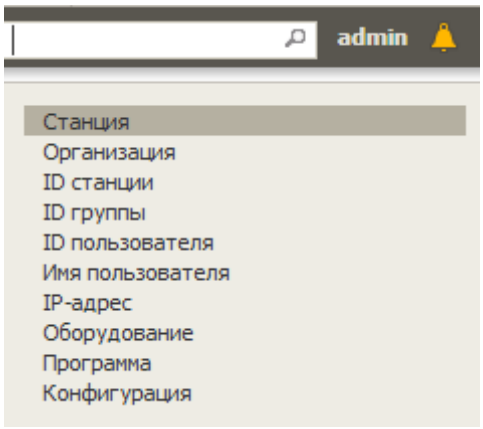


7. Укажите период (по умолчанию 90 дней), по истечении которого станция будет удалена из репозитория.
8. Нажмите **Сохранить** для сохранения задания.

6.4.7. Поиск станций в сети

Для поиска станций или группы станций:

1. В выпадающем списке панели поиска выберите критерий поиска:

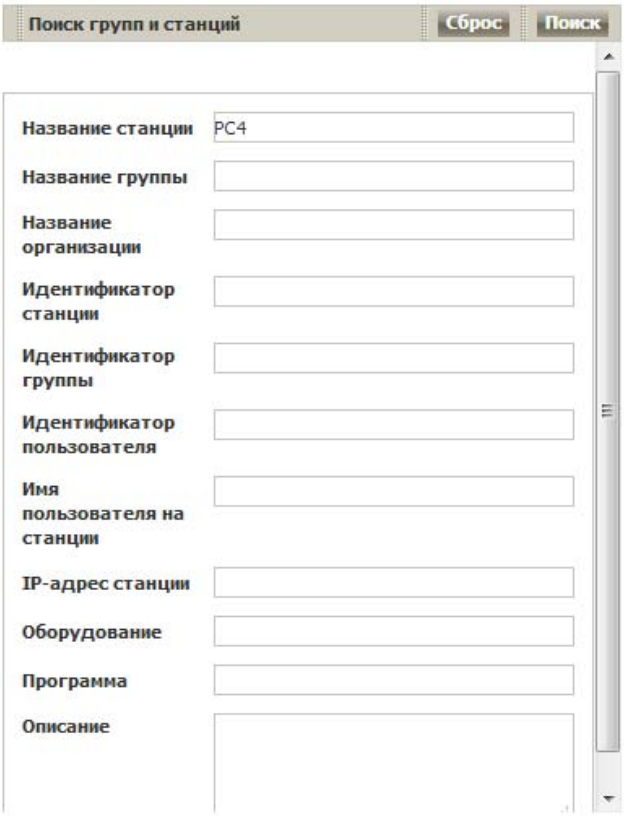


   - **Станция** — для поиска станций по названию,
   - **Организация** — для поиска станций по данным организации (фирмы, ЮЛ),
   - **ID ... —** для поиска групп, станций и пользователей по уникальным идентификаторам,
   - **Имя пользователя —** для поиска станций по имени пользователя,
   - **IP-адрес** — для поиска станций по IP-адресу,
   - **Оборудование —** для поиска станций по названию аппаратного обеспечения, установленного на станции,
   - **Программа —** для поиска станций по названию программного обеспечения, установленного на станции,
   - **Конфигурация —** для поиска станций по заданным параметрам их конфигурации.

2. Введите строку, в соответствии с которой будет производиться поиск. При этом необходимо задавать либо строку для полного совпадения с параметром поиска, либо использовать маски: допускаются символы «*» и «?».
3. Нажмите клавишу **ENTER** для начала поиска.
4. В иерархическом списке будут отображены все найденные элементы, в соответствии с параметрами поиска, при этом:

   - если осуществлялся поиск станции, то будут выведены вхождения станции во все группы,
   - если в результате поиска не найден ни один элемент, будет отображен пустой иерархический список с сообщением **Поиск не дал результатов**.

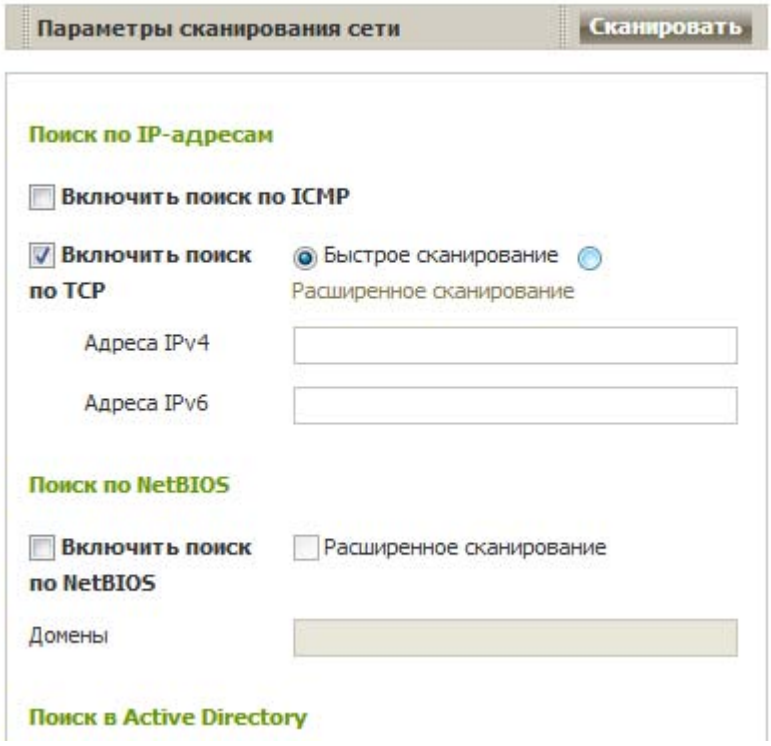
В открывшемся окне справа будет открыта панель **Поиск групп и станций**, где можно ввести название станции или его часть, а затем нажать **Поиск**.



Для уточнения условий поиска можно использовать также параметры **ID** (поиск по уникальным идентификаторам групп, станций и пользователей), **Описание**, **IP-адрес** (поиск по IP-адресам станций).

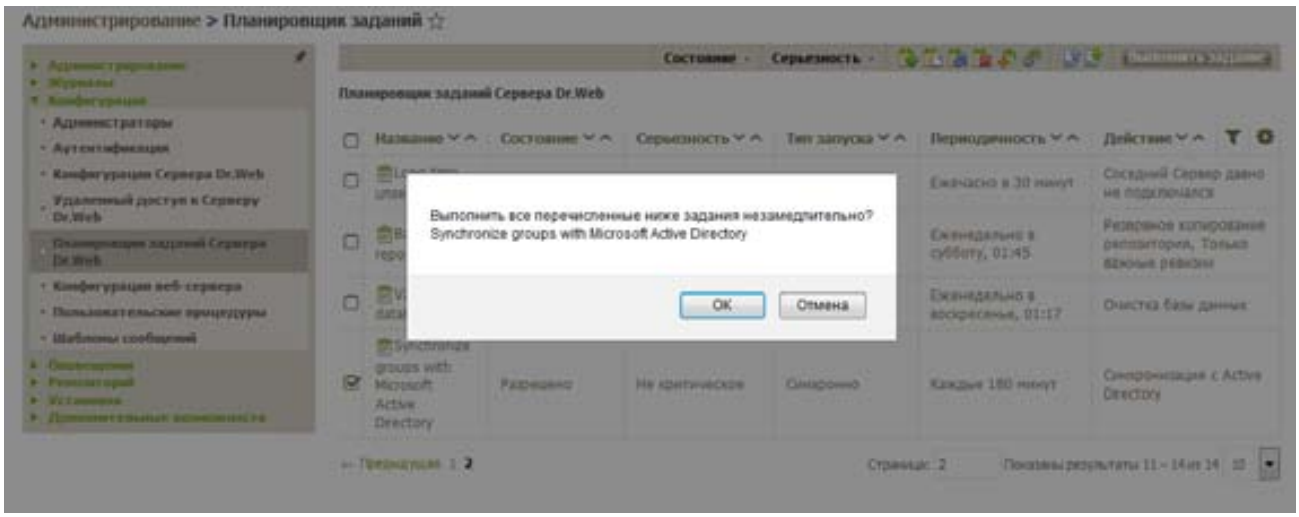
Вы можете задать значения для одного, нескольких или всех полей расширенного поиска. При этом если заполнены несколько полей, будет производиться поиск элементов, удовлетворяющих всем введенным параметрам. Например, при заполнении полей **Группа** и **Станция** од новременно, будут выведены станции, соответствующие полю **Станция** и входящие только в те группы, которые соответствуют значению в поле **Группа**.

Для поиска станций в сети можно также воспользоваться **Сканером сети**.

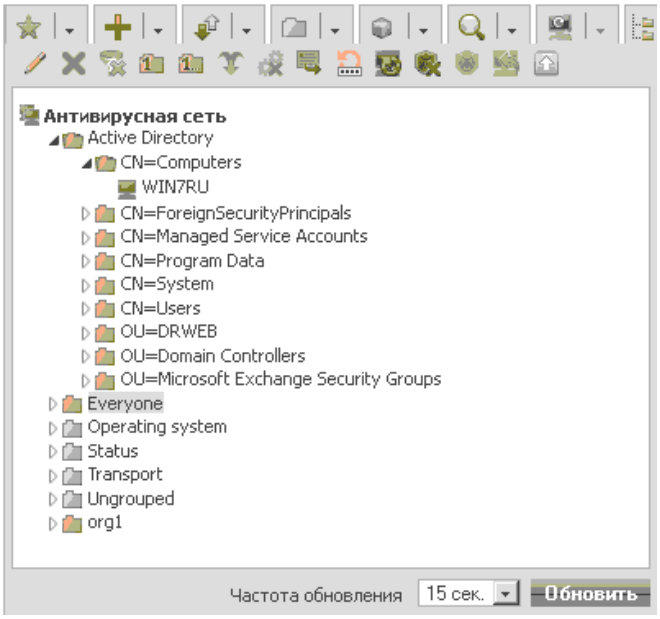


6.4.8. Отображение станций, зарегистрированных в Microsoft Active Directory

Для получения информации из Microsoft Active Directory служит задание сервера **Синхронизация с Active Directory**. По умолчанию синхронизация происходи каждые три часа. Для выполнения задания вручную нужно его отметить и нажать кнопку **Выполнить задание**.



Группы Microsoft Active Directory начинают отображаться в **Антивирусной сети** после первого же выполнения задания. До этого момента группы AD не отображаются.



6.4.9. Установка антивирусного прокси-сервера

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

Основная задача Прокси-сервера — обеспечение связи Сервера Dr.Web и Агентов Dr.Web в случае невозможности организации прямого доступа (например, если Сервер Dr.Web и Агенты Dr.Web расположены в различных сетях, м ежду которыми отсутствует маршрутизация пакетов).

Внимание! Для установки соединения между Сервером и клиентами через Прокси-сервер рекомендуется отключить шифрование трафика. Для этого достаточно установить значение **нет** для параметра **Шифрование** в разделе **Конфигурация Сервера Dr.Web → Общие**.

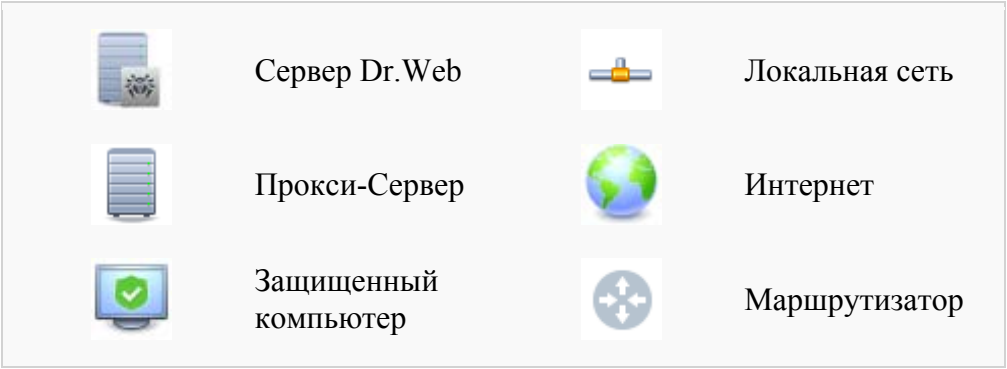
Основные функции

Прокси-сервер выполняет следующие функции:

1. Прослушивание сети и прием соединений в соответствии с заданным протоколом и портом.
2. Трансляция протоколов (поддерживаются протоколы TCP/IP).
3. Пересылка данных между Сервером Dr.Web и Агентами Dr.Web в соответствии с настройками Прокси-сервера.
4. Кэширование обновлений Агента и антивирусного пакета, передаваемых Сервером. В случае выдачи обновлений из кэша Прокси-сервера обеспечивается:
   - уменьшение сетевого трафика,
   - уменьшение времени получения обновлений Агентами.
5. Обеспечение шифрования трафика между Серверами и Агентами.

Примечание. Возможно создание иерархии Прокси-серверов.

Общая схема антивирусной сети при использовании Прокси-сервера приведена на рисунке ниже.



При использовании Прокси-сервера выполняется следующая последовательность действий:

1. Если на Агенте не прописан адрес Сервера, то Агент отправляет многоадресный запрос в соответствии с протоколом работы сети, в которой он находится.

2. В случае настройки Прокси-сервера на трансляцию соединений (параметр discovery="yes"), Агенту отправляется сообщение о наличии функционирующего Прокси-сервера.

3. Агент задает полученные параметры Прокси-сервера в качестве параметров Сервера Dr.Web. Дальнейшее взаимодействие осуществляется прозрачно для Агента.

4. В соответствии с параметрами конфигурационного файла Прокси-сервер прослушивает заданные порты на наличие входящих соединений по указанным протоколам.

5. Для каждого входящего соединения от Агента Прокси устанавливает соединение с Сервером Dr.Web.

Важные замечания

1. Сканер сети, запущенный на машине из внешней по отношению к Агентам сети, не сможет обнаружить установленных Агентов.

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

3. Управление настройками (редактирование конфигурационного файла) Прокси-сервера может выполняться только пользователем с правами администратора компьютера, на котором установлен Прокси-сервер.

Настройки

Прокси-сервер не имеет графического интерфейса. Задание настроек осуществляется одним из следующих способов:

1. Удаленно через Центр управления, если Прокси-сервер подключен к Серверу Dr.Web (см. п. Удаленная настройка Прокси-сервера).
2. Локально при помощи конфигурационного файла. Формат конфигурационного файла Прокси-сервера приведен в документе **Приложения**, п. Приложение G4.

Внимание! Управление настройками (редактирование конфигурационного файла) Прокси-сервера может осуществлять только пользователь с правами администратора данного компьютера.

Внимание! Для корректной работы Прокси-сервера под ОС семейства Linux после перезагрузки компьютера требуется системная настройка сети без использования Сетевого менеджера.

Запуск и останов

Под ОС Windows запуск и останов Прокси-сервера осуществляется штатными средствами при помощи элемента **Панель управления → Администрирование → Сервисы →** в списке сервисов дважды кликнуть по **drwcsd-proxy** и в открывшемся окне выбрать необходимое действие.

Под ОС семейства UNIX запуск и останов Прокси-сервера производится при помощи команд `start` и `stop` применительно скриптов, созданных в процессе установки Прокси-сервера (см. **Руководство по установке**, п. Установка прокси-сервера).

Также для запуска Прокси-сервера под ОС Windows и ОС семейства UNIX вы можете запустить исполняемый файл `drwcsd-proxy` с соответствующими параметрами (см. Приложение H7. Прокси-сервер).

6.4.9.1. Установка антивирусного прокси-сервера на компьютер с ОС Windows

1. С помощью лицензионного ключа скачайте установочный файл Прокси-сервера. Это файл вида drweb-<номер_версии>-<номер_сборки>-esuite-proxy-<ОС>-<разрядность>.exe, например: drweb-11.00.0-201805310-esuite-proxy-windows-nt-x64.exe) и создайте учетную запись Прокси-сервера при помощи Центра управления, как описано в разделе Создание учетной записи Прокси-сервера.

2. Скопируйте сертификат Сервера, к которому будет подключаться Прокси-сервер (см. Подключение Прокси-сервера к Серверу Dr.Web), и инсталлятор Прокси-сервера, поставляемый вместе с дистрибутивом Сервера, на станцию, на которой вы планируете осуществлять установку.

3. Запустите инсталлятор Прокси-сервера. Откроется окно **InstallShield Wizard**, извещающее об устанавливаемом продукте. Нажмите кнопку **Далее**.

4. В окне параметров Прокси-сервера на вкладке **Общее** задайте следующие основные параметры:

- В поле **Путь к данным программы** при необходимости измените путь для размещения файлов, используемых Прокси-сервером: журнала работы, конфигурационных файлов, кэша. По умолчанию используется путь %PROGRAMDATA%/Doctor Web/drwcs. Для выбора другого пути нажмите кнопку **Обзор**.
- В поле **Адрес для прослушивания** задайте IP-адрес, «прослушиваемый» Прокси-сервером. По умолчанию — any (0.0.0.0) — «прослушивать» все интерфейсы.

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

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

    - В поле **Multicast-группа** задайте IP-адрес многоадресной группы, в которую будет входить Прокси-сервер. Указанный интерфейс будет прослушиваться Прокси-сервером для взаимодействия с клиентами при поиске активных Серверов Dr.Web. Если поле оставить пустым, Прокси-сервер не будет входить ни в одну из многоадресных групп. По умолчанию многоадресная группа, в которую входит Сервер — 231.0.0.1.

- В разделе **Параметры соединения с клиентами**:

    - В выпадающем списке **Шифрование** выберите режим шифрования трафика для каналов между Прокси-сервером и обслуживаемыми клиентами: Агентами и инсталляторами Агентов.
    - В выпадающем списке **Сжатие** выберите режим сжатия трафика для каналов между Прокси-сервером и обслуживаемыми клиентами: Агентами и инсталляторами Агентов. В выпадающем списке **Уровень** выберите уровень сжатия (от 1 до 9).

5. На вкладке **Кэш** задайте следующие параметры кэширования Прокси-сервера:

Установите флажок **Включить кэширование**, чтобы кэшировать данные, передаваемые Прокси-сервером, и задайте следующие параметры:

- В поле **Период удаления ревизий (мин.)** задайте периодичность удаления старых ревизий из кэша в случае, если их количество превысило максимально допустимое количество сохраняемых ревизий. Значение задается в минутах. По умолчанию — 60 минут.

- В поле **Количество сохраняемых ревизий** задайте максимальное количество ревизий каждого продукта, которые останутся в кэше после очистки. По умолчанию хранятся 3 последние ревизии, более старые ревизии удаляются.

- В поле **Период выгрузки неиспользуемых файлов (мин.)** задайте временной интервал в минутах между выгрузками неиспользуемых файлов из оперативной памяти. По умолчанию — 10 минут.
- В выпадающем списке **Режим проверки целостности** выберите режим проверки целостности данных, хранящихся в кэше:

  - **На старте** — при запуске Прокси-сервера (может занять продолжительное время).
  - **При бездействии** — во время простоя Прокси-сервера.

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

6. Откроется окно настроек переадресации соединений:

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

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

- В выпадающем списке **Шифрование** выберите режим шифрования трафика для каналов связи между Прокси-сервером и заданным Сервером Dr.Web.
- В выпадающем списке **Сжатие** выберите режим сжатия трафика для каналов связи между Прокси-сервером и заданным Сервером Dr.Web. В выпадающем списке **Уровень** выберите уровень сжатия (от 1 до 9).

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

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

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

В случае если на Сервере задана конфигурация Прокси-сервера, все настройки, заданные в инсталляторе, будут переписаны на новую конфигурацию, полученную с Сервера.

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

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

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

- В поле **Сертификат Сервера** задайте файл сертификата, скопированного на станцию на шаге 2. Для выбора файла нажмите кнопку **Обзор**.

- В полях **Идентификатор** и **Пароль** задайте регистрационные данные учетной записи, созданной на Сервере на шаге 1.

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

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

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

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

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

6.4.9.2. Установка антивирусного прокси-сервера на компьютер с ОС семейства Unix

1. Выполните следующую команду:

`./<файл_дистрибутива>.run`

2. Для подключения к Серверу отредактируйте соответствующие конфигурационные файлы вручную

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

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

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

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

6.5. Установка Dr.Web NAP Validator, проверка соответствия рабочих станций установленным политикам и контроль доступа к сети

Для обеспечения непрерывной и качественной защиты рабочих станций и файловых серверов Windows от актуальных угроз безопасности, необходимо поддерживать антивирусное ПО в актуальном, исправном состоянии. Решение этой задачи возложено на Центр управления Dr.Web Enterprise Security Suite в сочетании с технологией Microsoft Network Access Protection (далее — NAP).

Dr.Web Enterprise Security Suite позволяет использовать технологию NAP для проверки работоспособности антивирусного ПО защищаемых рабочих станций по критерию соответствия политикам и управлять доступом подключающихся рабочих станций к ресурсам сети, используя результаты этой проверки.

При использовании технологии NAP возможно создание пользовательских политик работоспособности для оценки состояния компьютера. Полученные оценки анализируются в следующих случаях:

- перед тем, как разрешить доступ или взаимодействие,
- для автоматического обновления соответствующих требованиям компьютеров с целью обеспечения их постоянной совместимости,
- для адаптации не соответствующих требованиям компьютеров таким образом, чтобы они удовлетворяли установленным требованиям.

Подробное описание технологии NAP можно найти по ссылке https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730902(v=ws.10) (англ.) и https://ru.wikipedia.org/wiki/Защита_доступа_к_сети (рус.)

NAP Validator устанавливается на сервер, обладающий ролью **Службы политики сети и доступа** (Windows Server 2008 и более поздние), при этом на сервере должны работать такие службы ролей, как **Сервер политики сети** и **Протокол организации учетных данных узла**. В качестве клиентов технологии NAP могут выступать компьютеры, работающие под управлением ОС Windows Vista и более новых.

Dr.Web Enterprise Security Suite позволяет использовать технологию NAP для проверки работоспособности антивирусного ПО защищаемых рабочих станций. Для этого служит компонент Dr.Web NAP Validator.

При проверке работоспособности используются следующие средства:

- Установленный и настроенный сервер проверки работоспособности NAP.
- Dr.Web NAP Validator представляет собой средство оценки работоспособности антивирусного ПО защищаемой системы (System Health Validator — SHV) за счет подключаемых пользовательских политик Dr.Web. Устанавливается на компьютер с сервером NAP.
- Агент работоспособности системы (System Health Agent — SHA). Автоматически устанавливается вместе с ПО Агента Dr.Web на рабочую станцию.
- Сервер Dr.Web служит в качестве сервера исправлений, обеспечивающего работоспособность антивирусного ПО рабочих станций.

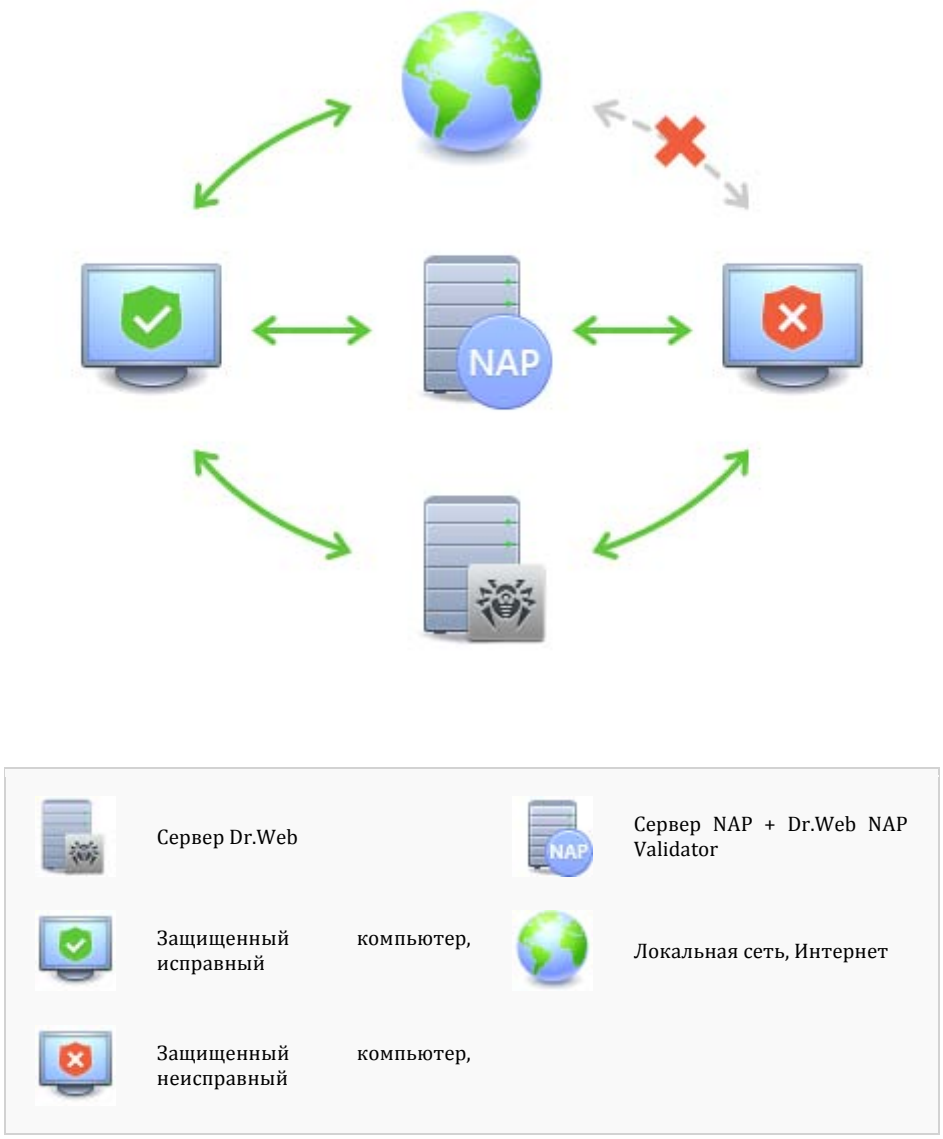


Схема антивирусной сети при использовании NAP

Процедура проверки осуществляется следующим образом:

1. Активация процесса проверки производится при установке соответствующих настроек Агента.
2. SHA на рабочей станции связывается с компонентом Dr.Web NAP Validator, установленном на сервере NAP.
3. Dr.Web NAP Validator осуществляет проверку политик работоспособности. Проверка политик представляет собой процесс, в котором NAP Validator выполняет оценку антивирусных средств с точки зрения выполнения заданных им правил и определяет категорию текущего состояния системы:

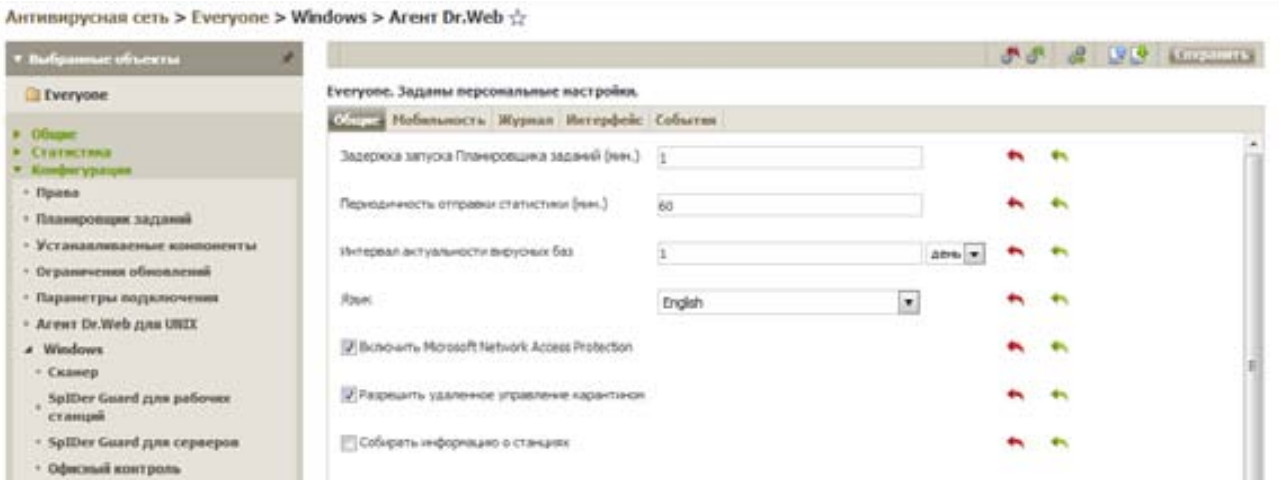
- станции, прошедшие проверку на соответствие элементам политики, считаются работоспособными и допускаются к полнофункциональной работе в сети;
- станции, не удовлетворяющие хотя бы одному из элементов политики, признаются неработоспособными. Доступ таких станций разрешен только к Серверу Dr.Web, от остальной сети они изолируются. Работоспособность станции восстанавливается при помощи Сервера, после чего станция проходит повторную процедуру проверки.

Требования к работоспособности:

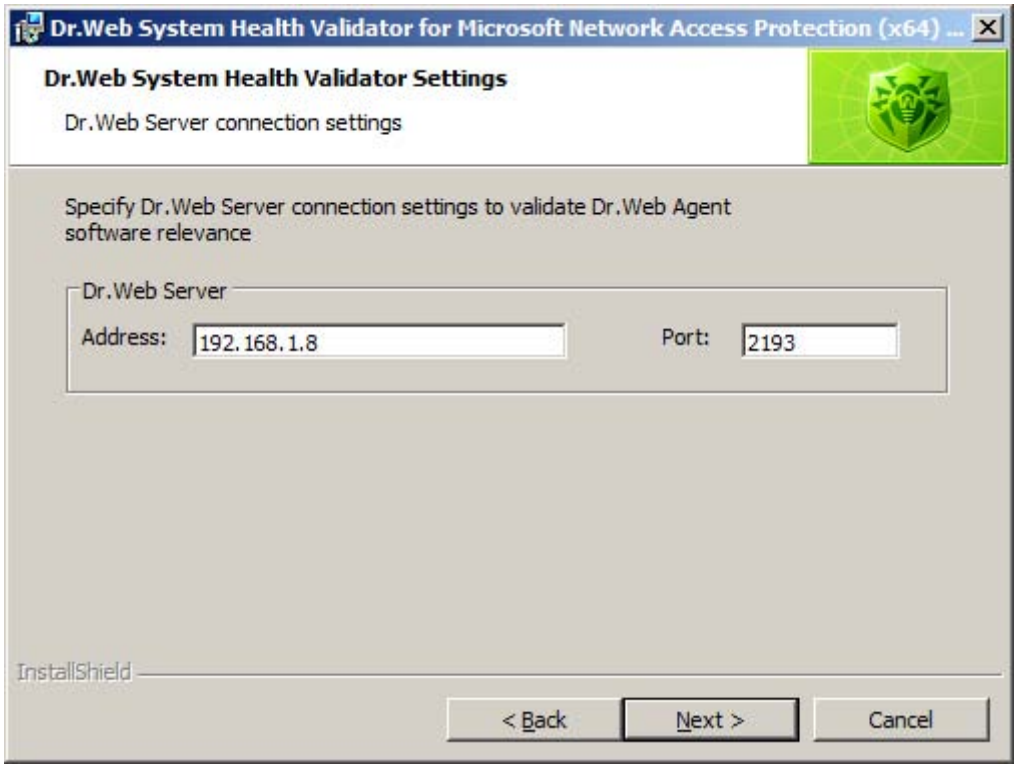
1. Рабочее состояние агента (запущен и функционирует).
2. Актуальность вирусных баз (базы совпадают с базами на сервере).

Для установки NAP Validator выполните следующие действия:

1. Выбрав для интересующих станций или групп пункт **Dr.Web® Agent для Windows** (меню **Антивирусная сеть → Конфигурация → Windows**), необходимо отметить пункт **Включить Microsoft Network Access Protection** для включения поддержки технологии Microsoft® Network Access Protection, использующейся для мониторинга состояния станций.



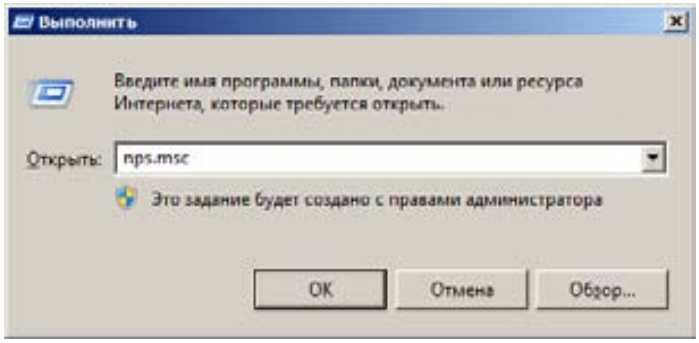
2. Перейдите в раздел Мастер скачиваний сайта https://www.drweb.ru и с помощью лицензионного ключа скачайте установочный файл **Dr.Web System Health Validator для Microsoft Network Access Protection**. Это файл вида drweb-<номер_версии>-<номер_сборки>-esuite-napshv-windows-nt-<разрядность>.msi, например: drweb-11.00.0-201805310-esuite-napshv-windows-nt-x64.msi.
3. Запустите файл дистрибутива. Откроется окно выбора языка, на котором будет производиться дальнейшая установка продукта. Выберите Русский и нажмите кнопку **Далее**.
4. Откроется окно InstallShield Wizard, извещающее об устанавливаемом продукте. Нажмите кнопку **Далее**.
5. Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора в группе кнопок выбора укажите **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Далее**.
6. В открывшемся окне в полях **Адрес** и **Порт** задайте, соответственно, IP-адрес и порт Сервера Dr.Web. Нажмите кнопку **Далее**.



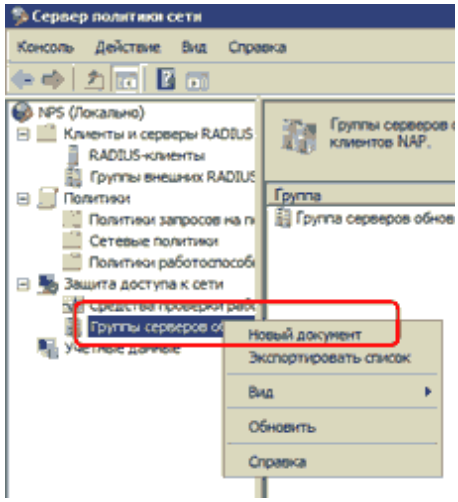
7. Нажмите на кнопку **Установить**. Дальнейшие действия программы установки не требуют вмешательства пользователя. По окончании установки нажмите на кнопку **Готово**.

После установки Dr.Web NAP Validator необходимо внести Enterprise Сервер в группу доверенных серверов NAP. На компьютере с установленным NAP-сервером:

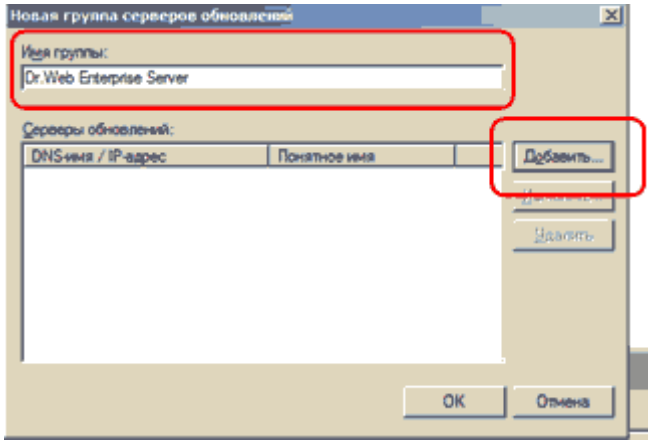
- Введите команду ***nps.msc***



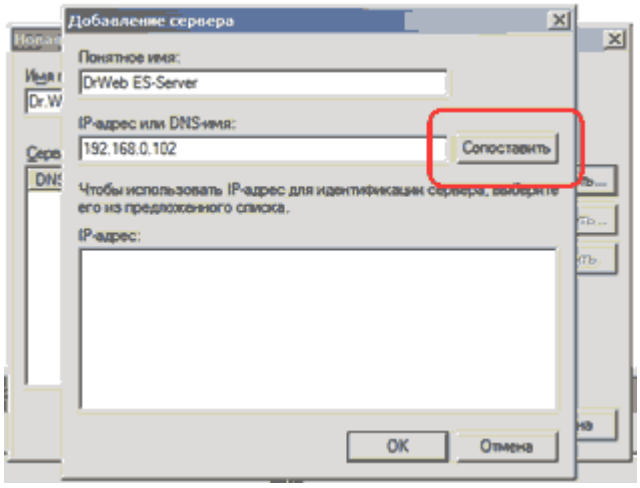
- Наведите курсор мыши на **Группы серверов обновлений**, нажмите правую клавишу мыши и выберите пункт меню **Новый документ**.



- Введите имя группы, например Dr.Web Enterprise Server. Нажмите кнопку **Добавить**.

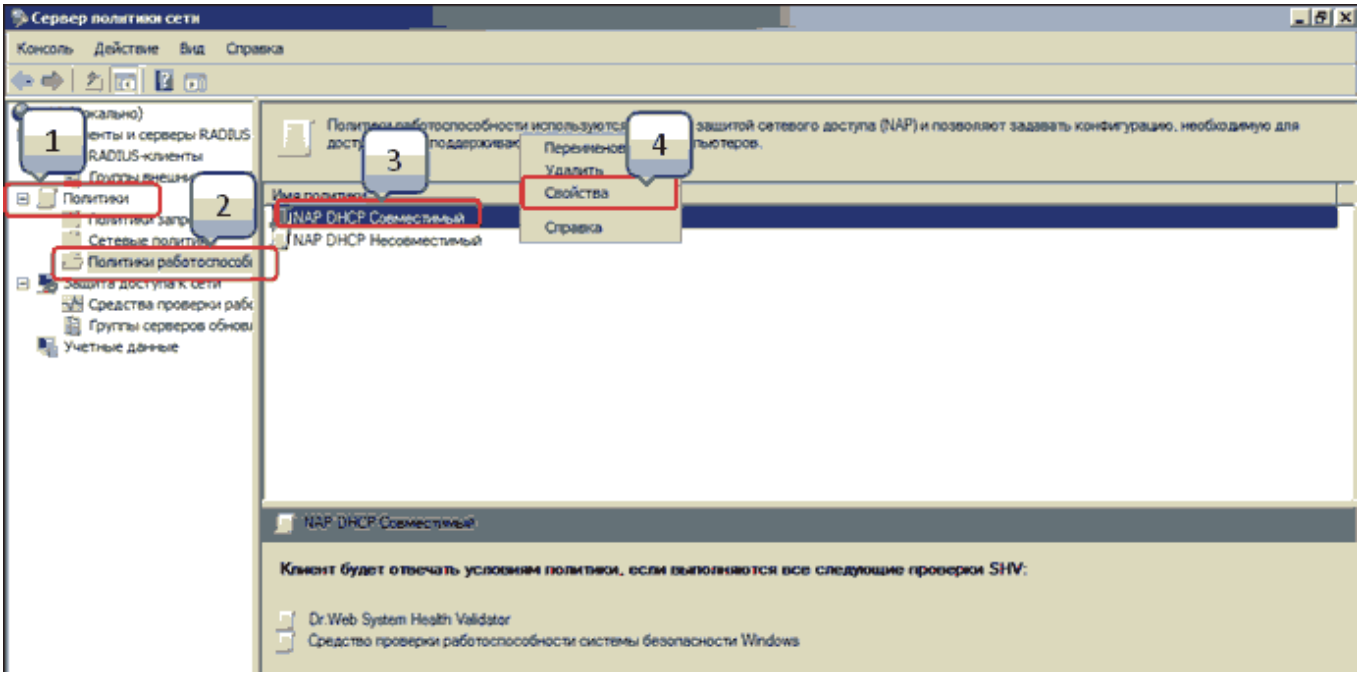


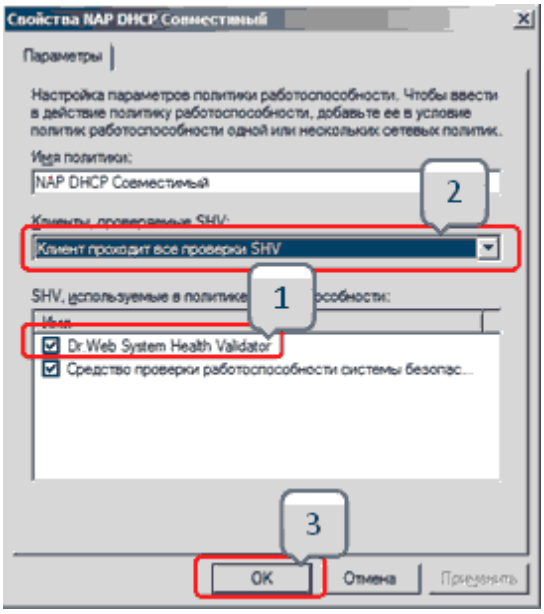
- Введите понятное имя сервера, например DrWeb ES-Server. В поле IP-адрес или DNS-имя в ведите IP-адрес или доменное имя Dr.Web Enterprise Server. Нажмите **Сопоставить**.



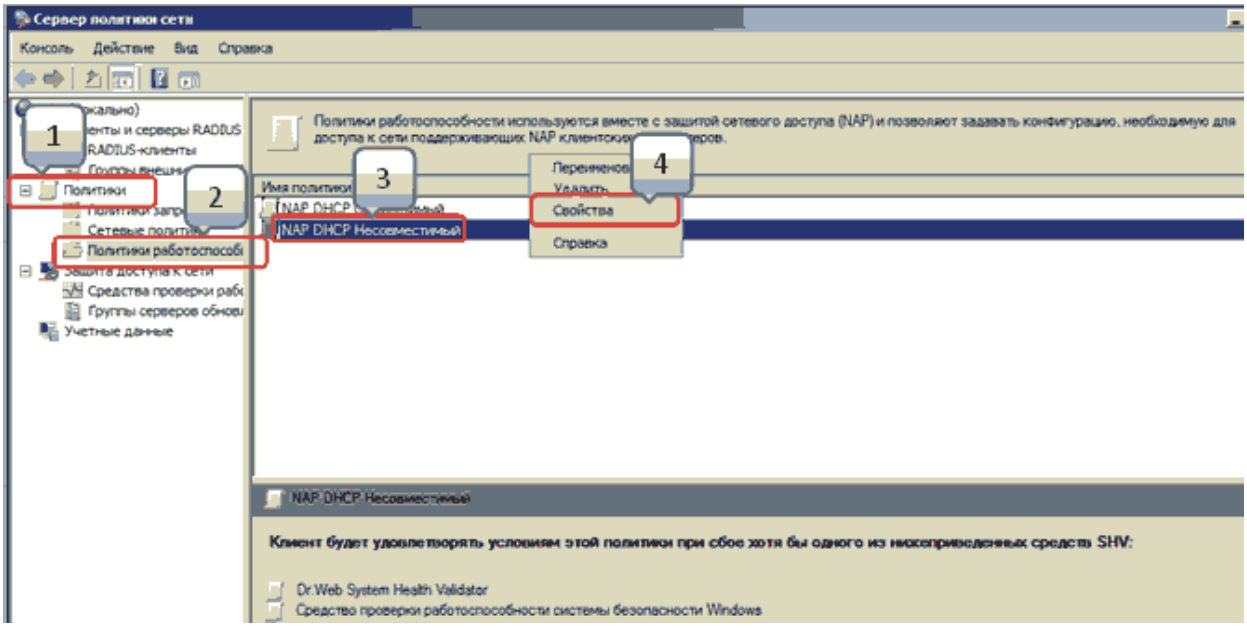
- Нажмите **ОК**.
- Закройте окно **Новая группа серверов обновлений**, нажмите **ОК**. Сервер Dr.Web добавлен в группу доверенных серверов NAP.
- В разделе **Политики** (Policies) выберите подпункт **Политики работоспособности** (Health Policies) и в открывшемся окне свойств элементов:
  - Наведите курсор мыши на элемент **NAP DHCP Совместимый** (NAP DHCP Compliant), нажмите правую клавишу мыши и выберите пункт **Свойства**. В окне

настроек установите флажок **Dr.Web System Health Validator**, задающий использование политик компонента Dr.Web NAP Validator. В выпадающем списке типа проверок укажите пункт **Клиент проходит все проверки SHV** (Client passed all SHV checks). Согласно данной опции станция будет объявлена работоспособной, если она соответствует всем элементам заданной политики. Нажмите **ОК**.

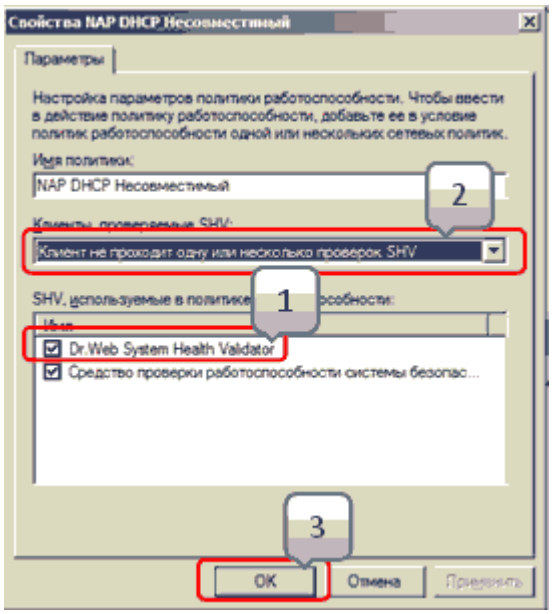




- Наведите курсор мыши на элемент **NAP DHCP Несовместимый** (NAP DHCP Noncompliant), нажмите правую клавишу мыши и выберите пункт **Свойства**.



- В окне настроек установите флажок **Dr.Web System Health Validator**, задающий использование политик компонента Dr.Web NAP Validator. В выпадающем списке типа проверок укажите пункт **Клиент не проходит одну или несколько проверок SHV** (Client fail one or more SHV checks). Согласно данной опции станция будет объявлена неработоспособной, если она не соответствует хотя бы одному из элементов заданной политики.



- Нажмите **ОК**.

7. Управление системой антивирусной защиты локальной сети

7.1. Центр управления Dr.Web

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

Центр управления может быть открыт на любом компьютере, имеющем сетевой доступ к Серверу. Возможно использование Центра управления под управлением практически любой

операционной системы, с полнофункциональным использованием на следующих веб-браузерах:

- Windows® Internet Explorer®,
- Microsoft Edge®,
- Mozilla® Firefox®,
- Google Chrome®.

Список возможных вариантов использования приведен в п. Системные требования.

Для того чтобы соединиться с помощью Центра управления с антивирусным сервером и производить описываемые ниже действия, необходимо на любом компьютере, имеющем сетевой доступ к **Серверу Dr.Web**, в адресной строке браузера ввести: http(s)://*<IP_адрес(или DNS_имя)антивирусного сервера>:<номер_порта>,* где в качестве *<IP адрес(или DNS_имя)>* укажите IP-адрес или доменное имя компьютера, на котором установлен Сервер **Dr.Web**. В качестве *<номер_порта>* укажите порт номер 9080 (или 9081 для https). В диалоговом окне запроса на авторизацию введите имя и пароль администратора (имя администратора по умолчанию — **admin**, пароль — пароль, который вы задавали при установке Сервера).

Пример: *http://192.168.100.66:9080*

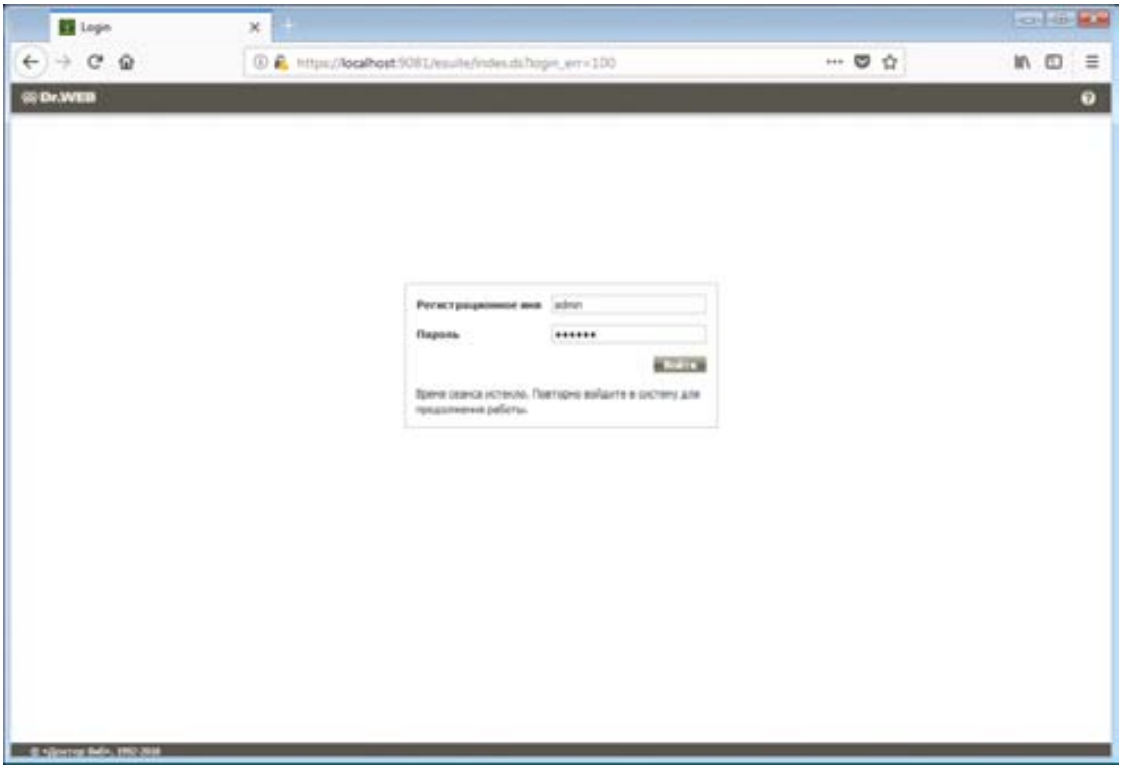
Для корректной работы Центра управления необходимо, чтобы в настройках веб-браузера было включено выполнение Java-скриптов.

1. Нажмите **Сервис → Свойства браузера**.
2. Перейдите на вкладку **Безопасность** и нажмите **Другой**.
3. В разделе **Сценарии → Активные сценарии** выберите **Включить**.
4. В разделе **Сценарии → Выполнять сценарии приложений Java** выберите **Включить**.
5. Чтобы сохранить настройки, нажмите **OK**.

Для корректной работы Центра управления под веб-браузером Microsoft Internet Explorer необходимо в настройках веб-браузера добавить адрес Центра управления в доверенную зону. Для этого перейдите **Сервис → Свойства обозревателя → Безопасность → Надежные сайты**, нажмите кнопку **Сайты** и укажите адрес сервера (как в примере выше).

При загрузке по https (защищенное соединение с использованием SSL) браузер запросит подтверждение сертификата, используемого Сервером Dr.Web. При этом запрос подтверждения может сопровождаться выражением недоверия к сертификату и информацией о подозрениях на его ошибочность. Данная информация выдается пользователю, поскольку сертификат неизвестен браузеру. Для возможности загрузки Центра управления следует принять предлагаемый сертификат.

В некоторых версиях браузеров при загрузке по https будет получена ошибка, и Центр управления не будет загружен. В таком случае на странице об ошибке следует выбрать пункт **Добавить сайт в список исключений** (под сообщением об ошибке). После этого будет разрешен доступ к Центру управления.

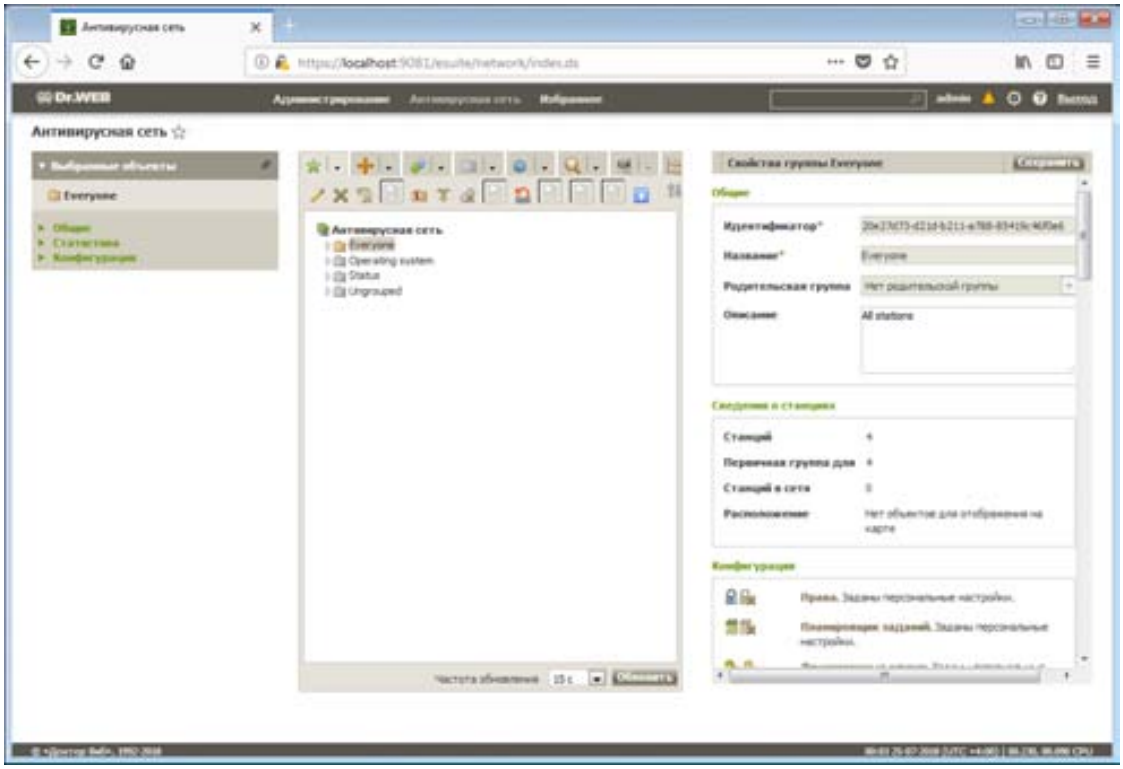


Аутентификация администратора для подключения к **Серверу Dr.Web** возможна следующими способами:

1. С хранением данных об администраторах в базе данных Сервера.
2. С помощью Active Directory (в версиях Сервера для ОС Windows).
3. С использованием LDAP-протокола.
4. С использованием RADIUS-протокола.

Изменение порядка использования типов авторизации осуществляется с помощью раздела **Авторизация** меню **Администрирование**.

После ввода пароля администратор получает доступ к Центру управления и в дальнейшем может управлять защитой с помощью функций, размещенных в разделах **Администрирование, Антивирусная сеть**, **Связи**.



Окно Центра управления делится на *заголовок* и *рабочую область*.

Заголовок содержит:

- логотип продукта **Dr.Web ESS**, нажатие на который соответствует выбору пункта **Антивирусная сеть** главного меню;
- главное меню.

Рабочая область отвечает за основной функционал Центра управления. Она состоит из двух или трех панелей, в зависимости от осуществляемых действий. При этом реализуется вложенность функционала панелей слева направо:

- *управляющее меню* всегда расположено в левой части окна;
- в зависимости от пункта, выбранного в управляющем меню, отображается одна или две дополнительные панели. В последнем случае в правой части выводятся свойства или поля настройки элементов центральной панели.

Язык интерфейса задается отдельно для каждой учетной записи администратора (см. п. 7.2. Смена языка отображения Центра управления).

В главном меню Центра управления доступны следующие разделы:

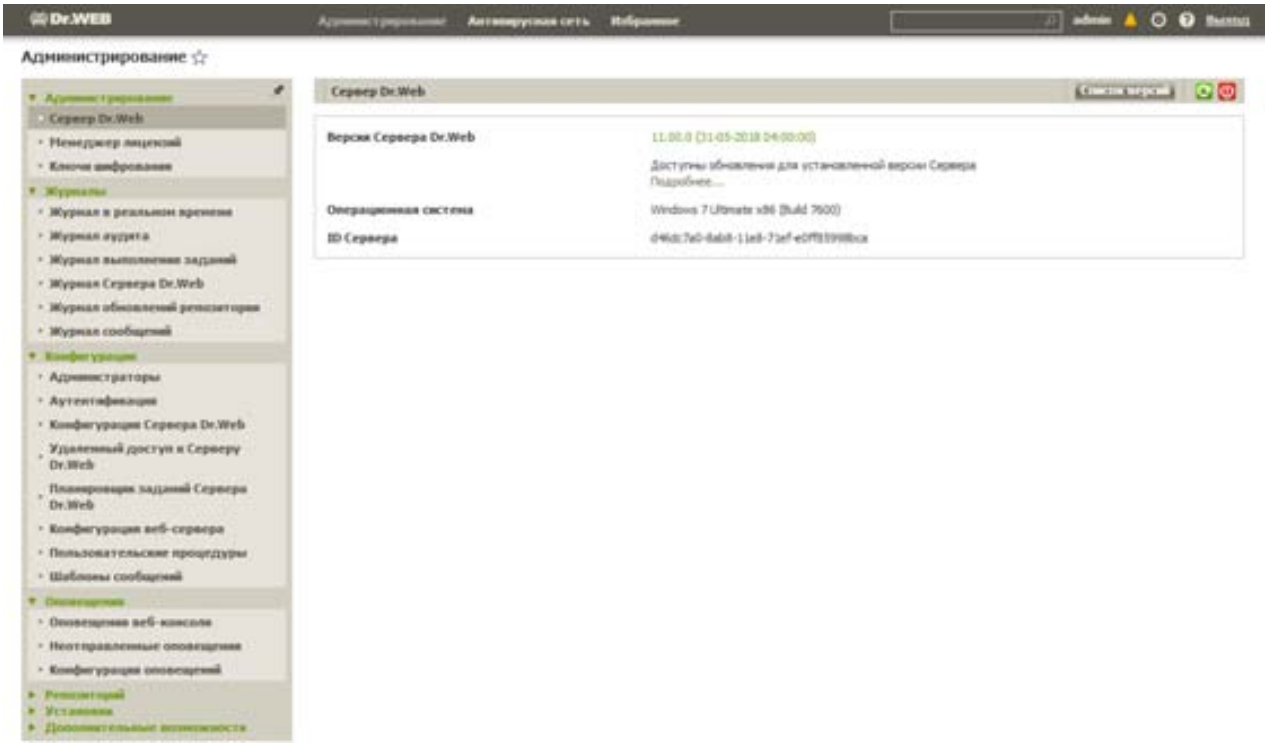
- Администрирование,
- Антивирусная сеть,
- Избранное,
- Панель поиска,
- Имя учетной записи администратора, под которой был осуществлен вход в Центр управления,
- Уведомления,
- раздел **Настройки (** **)**,

- раздел **Помощь (**  **)**,
- кнопка **Выход** для завершения текущего сеанса работы с Центром управления.

Если в Центре управления включена автоматическая авторизация, то при нажатии кнопки **Выход** информация об имени и пароле администратора удаляется.

Для облегчения поиска нужного элемента служит панель поиска, расположенная на правой границе главного меню Центра управления. Панель позволяет производить поиск как групп, так и отдельных станций в соответствии с указанными параметрами.

Меню **Администрирование**



Для просмотра и редактирования информации служит управляющее меню, расположенное в левой части окна. Управляющее меню содержит следующие пункты:

1. Администрирование

- Сервер **Dr.Web —** открывает панель, с помощью которой вы можете просмотреть основную информацию о Сервере, а также перезапустить или остановить его при помощи кнопок, расположенных в правой верхней части панели.
- Менеджер **лицензий** — позволяет управлять лицензионными ключевыми файлами Сервера и Агентов (см. п. 9.2.1. Менеджер лицензий).
- **Ключи шифрования —** позволяет экспортировать (сохранить локально) открытый и закрытый ключи шифрования.

2. Журналы

- Журнал **в реальном времени —** позволяет просмотреть список событий и изменений, связанных с работой Сервера, выводимых сразу в момент появления события.
- Журнал **аудита** — позволяет просмотреть журнал событий и изменений, осуществленных при помощи Центра управления.

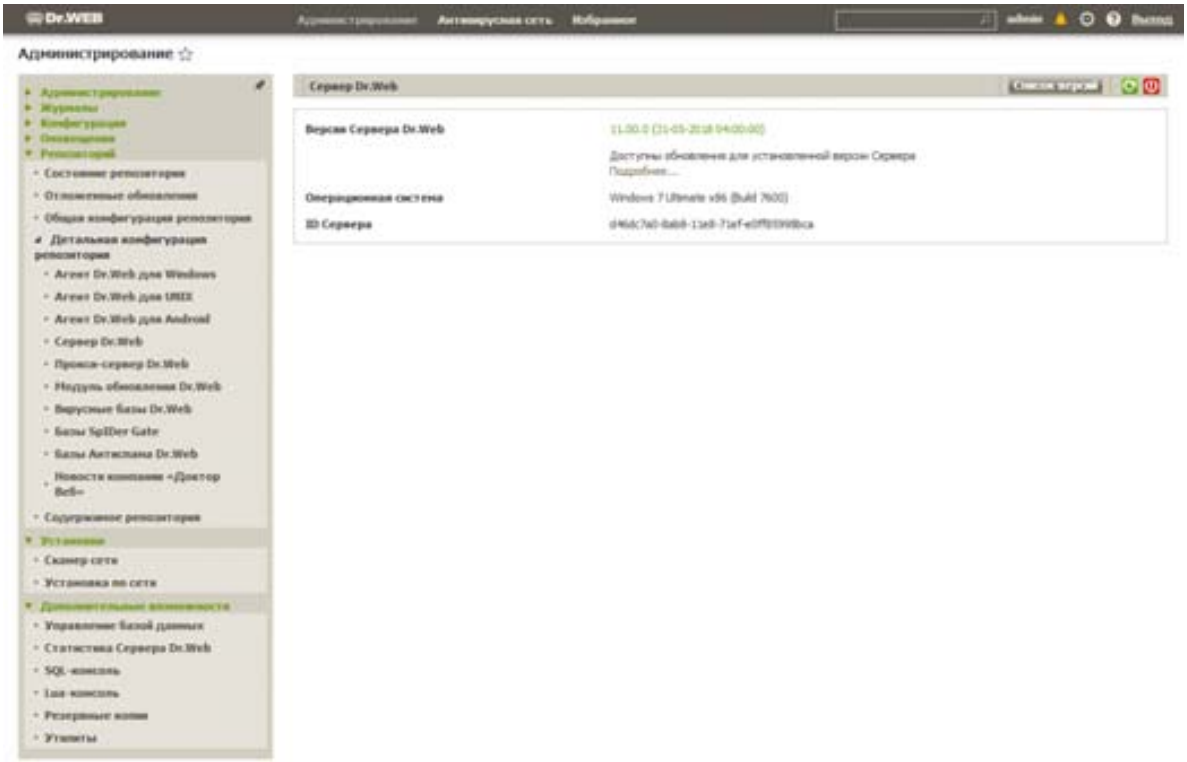
- **Журнал выполнения заданий** — содержит список назначенных заданий на **Сервере** с пометкой о выполнении и комментариями.
- **Журнал Сервера Dr.Web —** содержит список журналов событий, связанных с работой Сервера.
- **Журнал обновлений** репозитория **—** содержит список обновлений с ВСО, включающий подробную информацию об обновленных ревизиях продуктов.
- **Журнал сообщений —** содержит все текстовые сообщения, которые были отправлены администратором на станции антивирусной сети (см. Отправка сообщений станциям).

3. Конфигурация

- **Администраторы** — открывает панель управления учетными записями администраторов антивирусной сети (подробная информация доступна в Руководстве администратора, п. Управление учетными записями администраторов).
- **Аутентификация** — открывает панель управления аутентификацией администраторов в Центре управления.
- **Конфигурация Сервера Dr.Web** — открывает панель основных настроек Сервера.
- **Удаленный доступ к Серверу Dr.Web —** позволяет настроить удаленный доступ к Серверу.
- **Планировщик заданий Сервера Dr.Web —** позволяет задать расписание действий, которые Сервер должен автоматически выполнять в плановом порядке.
- **Конфигурация веб-сервера** — открывает панель основных настроек Веб-сервера.
- **Пользовательские процедуры —** в этом разделе можно как редактировать существующие процедуры, так и добавлять новые процедуры в виде LUA-скриптов, написанных администратором Сервера.
- **Шаблоны сообщений —** здесь приведен список шаблонов произвольных текстовых сообщений, отправляемых администратором на станции антивирусной сети (см. Отправка сообщений станциям).

4. Оповещения

- **Оповещения веб-консоли —** позволяет просматривать и управлять оповещениями, полученными от веб-консоли.
- **Неотправленные оповещения —** позволяет отслеживать и управлять оповещениями администратора, которые не удалось отправить согласно настройкам раздела Конфигурация оповещений.
- **Конфигурация оповещений —** позволяет настроить все параметры оповещений антивирусной сети.



5. Репозиторий

- **Состояние репозитория** — позволяет проверить состояние репозитория: дату последнего обновления компонентов репозитория и их состояние.
- **Отложенные обновления** — содержит список продуктов, для которых были временно запрещены обновления продуктов в разделе **Детальная конфигурация репозитория**.
- **Общая конфигурация репозитория** — открывает окно настроек подключения к **ВСО** и обновления репозитория для всех продуктов.
- **Детальная конфигурация репозитория** — позволяет настроить конфигурацию ревизий для каждого компонента репозитория в отдельности. Состав компонентов репозитория совпадает с составом компонентов антивируса.
- **Содержимое репозитория** — позволяет просмотреть список файлов, ревизий и всех остальных компонентов репозитория, а также получить полную информацию о его состоянии.

6. Установка

- **Сканер сети** — позволяет проводить сканирование сетей с целью обнаружения рабочих станций и определения наличия или отсутствия на них Агентов.
- **Установка по сети** — позволяет упростить установку ПО Агента на конкретные рабочие станции (см. **Руководство по установке**, п. Установка Агента Dr.Web с использованием Центра управления безопасностью Dr.Web).

7**.** Дополнительные возможности

- **Управление базой данных** — позволяет провести обслуживание БД Сервера Dr.Web.
- **Статистика Сервера Dr.Web** — содержит статистику работы данного **Сервера**.
- **SQL-консоль** — позволяет вручную отправлять SQL-запросы в БД Сервера Dr.Web.
- **Lua-консоль** — позволяет вручную отправлять LUA-скрипты на выполнение Сервером Dr.Web.
- **Резервные копии** — позволяет просматривать на уровне каталогов и файлов, а также сохранять локально содержимое резервных копий критичных данных Сервера.

- **Утилиты** — содержит ссылки для скачивания всех утилит, которые могут потребоваться в ходе работы с антивирусной сетью.

Меню **Антивирусная сеть**

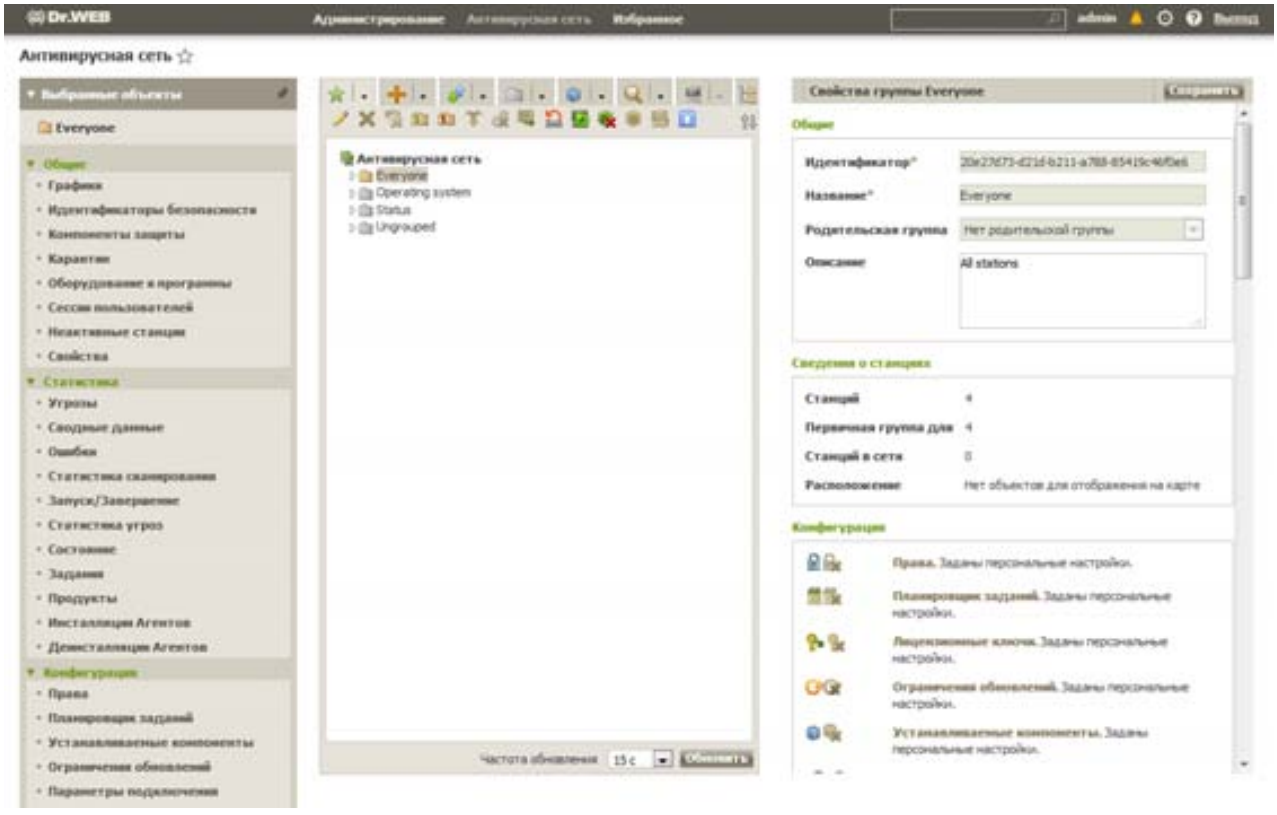
Для просмотра и редактирования информации в открывшемся окне служит управляющее меню, расположенное в левой части окна.

В центральной части окна расположен иерархический список антивирусной сети. Иерархический список (каталог) антивирусной сети отображает древовидную структуру элементов антивирусной сети. Узлами данной структуры являются группы и входящие в них станции.

В состав главного окна, отображающего информацию о защищаемой сети, входят следующие элементы:

- иерархический список (каталог) антивирусной сети (центральная часть окна);
- меню действий, которые можно предпринять по отношению к станциям и группам станций (левая часть окна);
- информация о количестве групп станций, количестве станций онлайн (правая часть окна).

Над каталогом антивирусной сети находится панель инструментов.



Вы можете выполнять следующие действия над элементами списка:

- нажмите левой кнопкой мыши на название группы или станции для о тображения управляющего меню (в левой части окна) соответствующего элемента;
- нажмите левой кнопкой мыши на значок группы для отображения содержимого группы;
- нажмите левой кнопкой мыши на значок станции для отображения раздела свойств этой станции.

Для выбора нескольких станций и групп иерархического списка используйте выделение мышью при нажатых клавишах **CTRL** или **SHIFT**.

Вид значка элемента списка зависит от типа или состояния этого элемента.

Значок	Описание
Группы. Основные значки	
	Группы, всегда отображаемые в иерархическом списке.
	Группы не будут отображаться в иерархическом списке если: • для групп было применено действие **Настроить видимость группы** → **Скрывать, если пустая** и в данный момент группы не содержат станций, • для групп было применено действие **Настроить видимость группы** → **Скрывать** и в данный момент в разделе **Настройки вида дерева** снят флаг **Показывать скрытые группы**.

Рабочие станции. Основные значки	
	Доступная рабочая станция с установленным антивирусным ПО.
	Доступная рабочая станция с установленным антивирусным ПО. Серьезность состояния станции **Средняя**. Для определения действий, необходимых со стороны администратора, уточните ситуацию на данной станции в разделе Состояние. Для отображения значка выберите на панели инструментов  **Настройки вида дерева → Показывать серьезность состояния станций**.
	Доступная рабочая станция с установленным антивирусным ПО. Серьезность состояния станции **Максимальная** или **Высокая**. Для определения действий, необходимых со стороны администратора, уточните ситуацию на данной станции в разделе Состояние. Для отображения значка выберите на панели инструментов  **Настройки вида дерева → Показывать серьезность состояния станций**.
	Станция недоступна.
	Антивирусное ПО на станции деинсталлировано.
	Состояние станции при удаленной установке Агента по сети. Станция находится в данном состоянии с момента удачной установки Агента на станции до момента первого подключения станции к Серверу.
Дополнительные значки	
	Значок персональных настроек отображается на основных значках станций и групп, для которых заданы персональные настройки (для групп в том числе, если в группе есть станции с персональными настройками). Для отображения значка выберите на панели инструментов  **Настройки вида дерева → Показывать значок персональных настроек**. Например, если персональные настройки заданы для рабочей станции с установленным антивирусным ПО, находящейся в данный момент в сети, то ее значок будет выглядеть следующим образом:  .
	Значок правил членства отображается рядом со основными значками групп, для которых установлены правила автоматического размещения станций. Для отображения значка выберите на панели инструментов  **Настройки вида дерева → Показывать значок правил членства**. Например, если для группы, которая всегда отображается в иерархическом списке, заданы правила членства, то ее значок будет выглядеть следующим образом: .

Управление элементами каталога антивирусной сети осуществляется при помощи панели инструментов иерархического списка.

Панель инструментов иерархического списка содержит следующие элементы:

 **Общие** — позволяет управлять общими параметрами иерархического списка. Выберите соответствующий пункт в выпадающем списке:

 **Редактировать** — открыть панель свойств станции или группы в правой части окна Центра управления.

 **Удалить выбранные объекты** — удалить объекты иерархического списка. Для этого выберите в списке объект или несколько объектов и нажмите **Удалить выбранные объекты**.

Удалить правила членства — удалить правила для автоматического включения станций в группы.

Установить эту группу первичной — установить выбранную в иерархическом списке группу в качестве первичной для всех входящих в нее станций.

Назначить первичную группу для станций — назначить для выделенных в иерархическом списке станций первичную группу. При этом если в иерархическом списке выделена группа, то для всех входящих в нее станций будет назначена выбранная первичная группа.

Объединить станции — объединять станции под единой учетной записью в иерархическом списке. Может использоваться в случае, когда одна и та же станция была зарегистрирована под разными учетными записями.

Удалить персональные настройки — удалить персональные настройки выбранного в списке объекта. В этом случае настройки будут унаследованы от первичной группы. Если в иерархическом списке выделена группа, то настройки будут также удалены у всех входящих в нее станций.

Отправить сообщение станциям — отправить пользователям сообщение произвольного содержания.

Сбросить пароль — удалить пользовательский пароль для доступа к настройкам антивирусных компонентов на выбранных станциях. Опция доступна только для станций под ОС Windows.

Перезагрузить станцию — удаленно запустить процесс перезагрузки станции.

Деинсталлировать Агент Dr.Web — удалить Агента и антивирусное ПО с выбранной станции или группы станций.

Установить Агент Dr.Web — открыть Сканер сети для установки Агента на выбранные станции. Данный пункт активен только при выборе новых подтвержденных станций или станций с деинсталлированным Агентом.

Восстановить удаленные станции — восстановить ранее удаленные станции. Данный пункт активен только при выборе станций из подгруппы **Deleted** в группе **Status**.

Разослать инсталляционные файлы — разослать инсталляционный файлы для выбранных в списке станций на адреса электронной почты, задаваемые в настройках данного раздела.

Открыть Центр управления безопасностью Dr.Web для выбранного соседнего сервера в другом окне. Данный пункт активен при выборе соседнего Сервера в дереве антивирусной сети.

Добавить объект сети — создать новый элемент антивирусной сети. Для этого выберите соответствующий пункт в выпадающем списке:

Создать станцию — создать новую станцию (см. **Руководство по установке**, п. Создание новой учетной записи).

Создать группу — создать новую группу станций.

Создать связь — создать связь с соседним Сервером Dr.Web.

Создать политику — создать новую политику для задания настроек станций.

Создать Прокси-сервер — создать новую учетную запись для подключения Прокси-сервера (см. **Руководство по установке**, п. Создание учетной записи Прокси-сервера).

Экспортировать данные:

Сохранить данные в CSV-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата CSV.

Сохранить данные в HTML-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата HTML.

Сохранить данные в XML-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата XML.

Сохранить данные в PDF-файл — записать общие данные о выбранных станциях антивирусной сети в файл формата PDF.

> При выборе перечисленных выше опций из раздела **Экспортировать данные** будет экспортирована информация только о выбранных станциях и станциях, входящих в выбранные группы.

Экспортировать конфигурацию — сохранить в файл конфигурацию выбранного объекта антивирусной сети. Для данной опции будет предложено выбрать сохраняемые разделы конфигурации.

Импортировать конфигурацию — загрузить из файла конфигурацию выбранного объекта антивирусной сети. Для данной опции будет предложено выбрать файл, из которого будет загружена конфигурация, а также загружаемые разделы конфигурации.

Распространить конфигурацию — распространить конфигурацию выбранного объекта на другие объекты антивирусной сети. Для данной опции будет предложено выбрать объекты, на которые будет распространена конфигурация, а также распространяемые разделы конфигурации.

Настроить видимость группы. Позволяет изменять параметры отображения групп. Для этого выберите группу в иерархическом списке и укажите в выпадающем списке один из следующих вариантов (при этом будет изменяться значок группы, см. таблицу выше):

Скрывать — означает, что отображение группы в иерархическом списке будет всегда отключено.

Скрывать, если пустая — означает, что отображение группы в иерархическом списке будет отключено, если эта группа пустая (не содержит станций).

Показывать — означает, что группа всегда будет отображаться в иерархическом списке.

Управление компонентами — позволяет управлять антивирусными компонентами на рабочих станциях. Для этого выберите в выпадающем списке один из следующих вариантов:

Восстановить сбойные компоненты — принудительно восстановить состояние компонентов, работающих с ошибкой. Восстанавливается та ревизия продукта, которая в данный момент установлена на станции.

Прервать запущенные компоненты — остановить работу запущенных на станции антивирусных компонентов.

Сканировать — позволяет провести сканирование станции в одном из режимов, выбираемых в выпадающем списке:

Сканер Dr.Web. Быстрое сканирование. В данном режиме производится сканирование при помощи Dr.Web Agent Сканера следующих объектов:

- оперативная память,
- загрузочные секторы всех дисков,
- объекты автозапуска,
- корневой каталог загрузочного диска,
- корневой каталог диска установки ОС Windows,
- системный каталог ОС Windows,
- папка Мои документы,
- временный каталог системы,
- временный каталог пользователя.

Сканер Dr.Web. Полное сканирование. В данном режиме производится полное сканирование всех жестких дисков и сменных носителей (включая загрузочные секторы) при помощи Dr.Web Agent Сканера.

Сканер Dr.Web. Выборочное сканирование. Данный режим предоставляет возможность выбрать любые папки и файлы для последующего сканирования при помощи Dr.Web Agent Сканера.

Неподтвержденные станции — позволяет управлять списком новичков — станций, регистрация которых не подтверждена (подробнее см. раздел Политика подключения станций). Данный пункт активен только при выборе станций из подгруппы **Newbies** в группе **Status**. При подтверждении регистрации на Сервере станции будут автоматически удалены из предустановленной подгруппы **Newbies**. Для управления регистрацией станций выберите в выпадающем списке один из следующих вариантов:

Разрешить доступ выбранным станциям и назначить первичную группу — подтвердить доступ станции к Серверу и задать для нее первичную группу из предложенного списка.

Отменить действие, заданное для выполнения при подключении — отменить действие над неподтвержденной станцией, которое было ранее назначено для выполнения в момент, когда станция подключится к Серверу.

Отказать в доступе выбранным станциям — запретить доступ станции к Серверу.

Настройки вида дерева — изменить внешний вид дерева антивирусной сети. Для включения параметра установите соответствующие флажки в выпадающем меню:

- для групп:

  - **Членство во всех группах** — дублировать отображение станции в списке, если она входит в несколько групп одновременно (только для групп, идущих под значком белой папки — см. таблицу выше). Если флажок установлен, будут показаны все вхождения станции. Если снят — станция будет отображена в списке единожды.
  - **Показывать скрытые группы** — отображать все группы, входящие в антивирусную сеть. При снятии данного флажка пустые группы (не содержащие станции) будут скрыты. Это может быть удобно для исключения излишней информации, например, при наличии большого количества пустых групп.

- для клиентов Сервера (станций, Прокси-серверов и соседних Серверов):

  - **Показывать идентификаторы клиентов** — отображать уникальные идентификаторы клиентов Сервера.
  - **Показывать названия клиентов** — отображать названия клиентов Сервера при наличии.

Внимание! Нельзя отключить отображение идентификаторов и названий клиентов одновременно. Один из параметров **Показывать идентификаторы клиентов** и **Показывать названия клиентов** всегда будет выбран.

  - **Показывать адреса клиентов** — отображать IP-адреса клиентов Сервера.
  - **Показывать серверы станций** — отображать имена или IP-адреса Серверов Dr.Web, к которым подключены станции. Актуально для станций, входящих в кластер Серверов Dr.Web.
  - **Показывать серьезность состояния станций** — отображать серьезность статуса для активных станций. При этом добавится цветовая градация для станций в зависимости от их статуса (см. таблицу выше). Если опция отключена, то для станции со статусами, которым соответствуют значки и , будет отображаться общий значок .

- для всех элементов:

  - **Показывать значок персональных настроек** — отображать маркер, обозначающий наличие персональных настроек, на значках групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов.
  - **Показывать описания** — отображать описания групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов (описания задаются в свойствах элемента).
  - **Показывать количество клиентов** — отображать количество клиентов Сервера: станций, Прокси-серверов и соседних Серверов для всех групп антивирусной сети, в которые эти клиенты входят.
  - **Показывать значок правил членства** — отображать маркер на значках станций, которые были добавлены в группу автоматически согласно правилам членства, а также на значках групп, в которые станции были добавлены автоматически.

Настройки сортировки клиентов — изменить параметр, по которому осуществляется сортировка, и порядок сортировки клиентов Сервера: станций, Прокси-серверов и соседних Серверов в дереве антивирусной сети.

- Для выбора параметра, по которому будет производиться сортировка, установите один из следующих флажков (допускается выбор только одного параметра):

- **Идентификатор** — сортировать по уникальным идентификаторам клиентов.
- **Название** — сортировать по именам клиентов.
- **Адрес** — сортировать по сетевым адресам клиентов. Те клиенты, у которых нет сетевого адреса, будут выводиться в произвольном порядке без сортировки.
- **Дата создания** — сортировать по дате создания учетной записи клиента на Сервере.
- **Дата последнего подключения** — сортировать по дате последнего подключения к Серверу.

- Для выбора порядка сортировки установите один из следующих флажков:

  - **Сортировать по возрастанию**.
  - **Сортировать по убыванию**.

Разделы **Настройки вида дерева** и **Настройки сортировки клиентов** взаимозависимы:

- Если вы выбираете параметр сортировки в разделе **Настройки сортировки клиентов**, отображение этого параметра автоматически включается в разделе **Настройки вида дерева**, если оно было отключено.
- Если в разделе **Настройки вида дерева** вы отключаете отображение параметра, выбранного для сортировки в разделе **Настройки сортировки клиентов**, то сортировка по этому параметру автоматически переключается на сортировку по названию клиента. Если отображение названий клиентов при этом отключено, то сортировка переключается на идентификатор клиента (название и идентификатор одновременно не могут быть отключены).

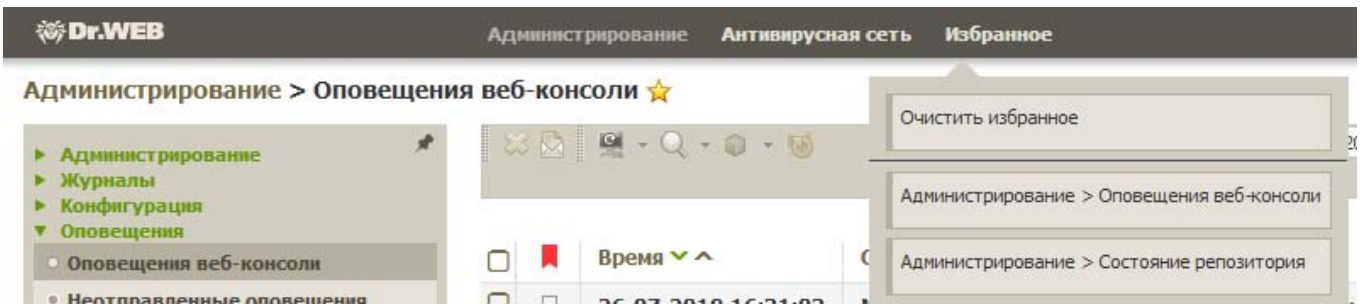
Панель свойств

Панель свойств служит для отображения свойств и настроек рабочих станций и групп.

Для отображения панели свойств в иерархическом списке выделите станцию или группу и нажмите **Общие** — **Редактировать** на панели инструментов. В правой части окна Центра управления откроется панель со свойствами рабочей станции. Данная панель содержит следующие группы настроек: **Общие**, **Группы**, **Безопасность, Расположение**. Подробное описание данных настроек приведено в п. 7.5.11.4 Установка или ограничение прав пользователей.

Меню **Избранное**

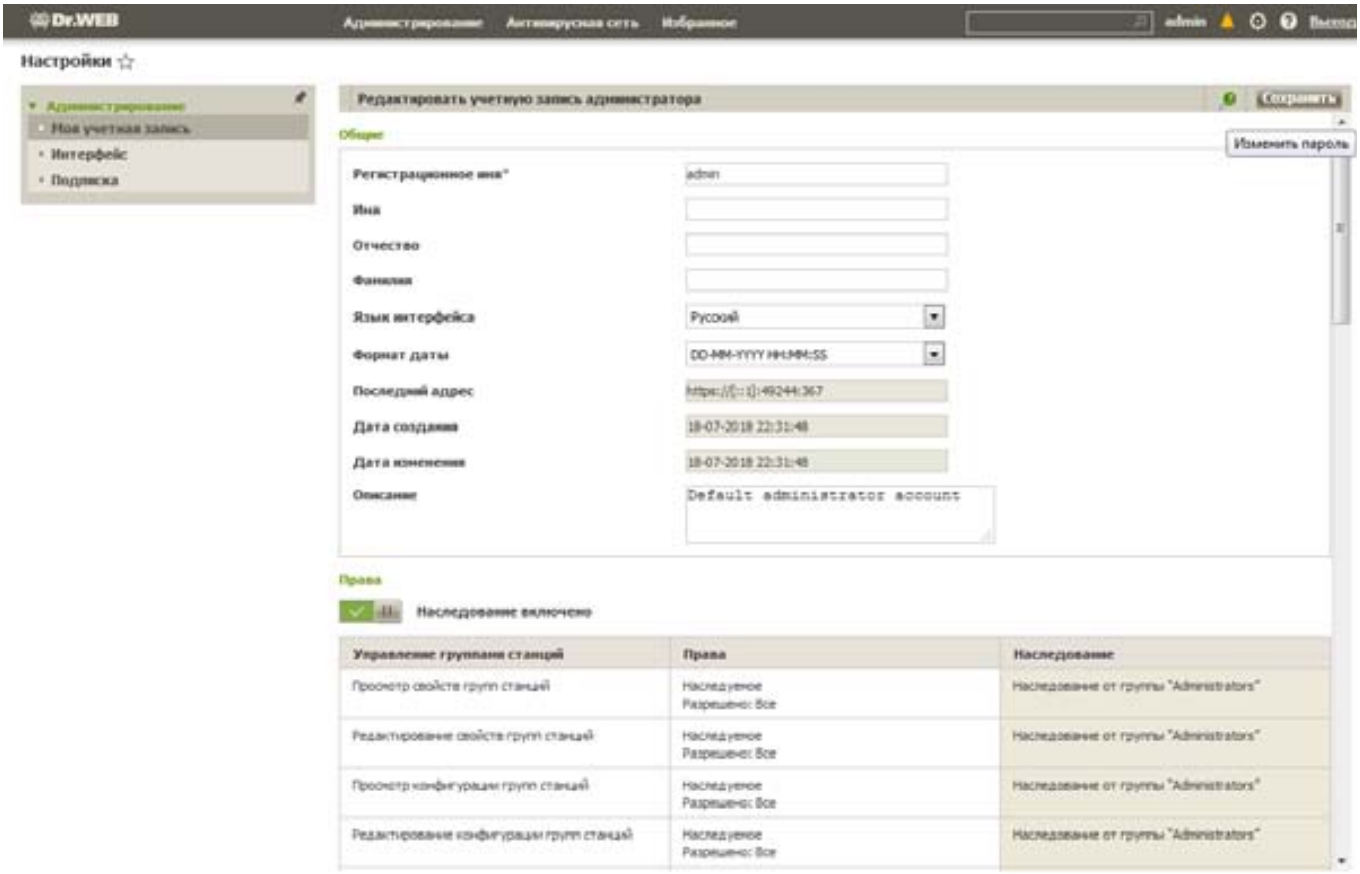
Сюда можно добавить те настройки и разделы, которые чаще всего используются в работе. Для этого нужно нажать на значок (☆) рядом с именем настройки, и она появится в быстром доступе меню **Избранное**.



Меню **Настройки**

Для перехода в раздел настроек Центра управления нажмите в главном меню кнопку .

Внимание! Все настройки данного раздела будут действительны только для текущей учетной записи администратора.



Управляющее меню, расположенное в левой части окна, содержит следующие элементы:

Моя учетная запись

При помощи данного раздела осуществляется управление текущей учетной записью администратора антивирусной сети (см. также п. Администраторы и административные группы).

Общие

Внимание! Значения полей, отмеченных знаком *, должны быть обязательно заданы.

При необходимости отредактируйте следующие параметры:

- **Регистрационное имя** администратора — логин для доступа к Центру управления.
- **Ф. И. О.** администратора.
- **Язык интерфейса**, используемый данным администратором.
- **Формат даты**, используемый данным администратором при редактировании настроек, содержащих даты. Доступны следующие форматы:
    - европейский: DD-MM-YYYY HH:MM:SS
    - американский: MM/DD/YYYY HH:MM:SS

- **Описание** учетной записи.
- Для смены пароля нажмите кнопку **Изменить пароль** на панели инструментов.

Следующие параметры доступны только для чтения:

- Даты создания учетной записи и последнего изменения ее параметров,
- **Последний адрес** — отображает сетевой адрес последнего подключения под данной учетной записью.

Права

Описание прав администраторов и их редактирование приведено в разделе Редактирование администраторов.

После изменения параметров нажмите кнопку **Сохранить**.

Для учетных записей с правами только на чтение для редактирования доступны только следующие поля:

- **Язык интерфейса**
- **Описание**
- **Интерфейс**

Настройки вида дерева

Параметры данного подраздела позволяют изменять внешний вид списка и аналогичны настройкам, расположенным на панели инструментов пункта **Настройки вида дерева** в разделе главного меню **Антивирусная сеть**:

- для групп:

▫**Членство во всех группах** — дублировать отображение станции в списке, если она входит в несколько групп одновременно (только для групп, идущих под значком белой папки — см. таблицу выше). Если флажок установлен, будут показаны все вхождения станции. Если снят — станция будет отображена в списке единожды.

▫**Показывать скрытые группы** — отображать все группы, входящие в антивирусную сеть. При снятии данного флажка пустые группы (не содержащие станции) будут скрыты. Это может быть удобно для исключения излишней информации — например, при наличии большого количества пустых групп.

- для клиентов Сервера (станций, Прокси-серверов и соседних Серверов):
    - **Показывать идентификаторы клиентов** — отображать уникальные идентификаторы клиентов Сервера.
    - **Показывать названия клиентов** — отображать названия клиентов Сервера.

Внимание! Нельзя отключить отображение идентификаторов и названий клиентов одновременно. Один из параметров **Показывать идентификаторы клиентов** и **Показывать названия клиентов** всегда будет выбран.

    - **Показывать адреса клиентов** — отображать IP-адреса клиентов Сервера.
    - **Показывать серверы станций** — отображать имена или IP-адреса Серверов Dr.Web, к которым подключены станции. Актуально для станций, входящих в кластер Серверов Dr.Web.
    - **Показывать серьезность состояния станций** — отображать серьезность статуса для активных станций. При этом добавится цветовая градация для

станций в зависимости от их статуса (см. таблицу выше). Если опция отключена, то для станции со статусами, которым соответствуют значки  и  , будет отображаться общий значок  .

- для всех элементов:
  - **Показывать значок персональных настроек** — отображать маркер, обозначающий наличие персональных настроек, на значках групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов.
  - **Показывать описания** — отображать описания групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов (описания задаются в свойствах элемента).
  - **Показывать количество клиентов** — отображать количество клиентов Сервера: станций, Прокси-серверов и соседних Серверов для всех групп антивирусной сети, в которые эти клиенты входят.
  - **Показывать значок правил членства** — отображать маркер на значках станций, которые были добавлены в группу автоматически согласно правилам членства, а также на значках групп, в которые станции были добавлены автоматически.

Настройки вида дерева

Параметры данного подраздела позволяют изменять внешний вид списка и аналогичны настройкам, расположенным на панели инструментов пункта **Настройки вида дерева** в разделе главного меню **Антивирусная сеть**:

- для групп:
  - **Членство во всех группах** — дублировать отображение станции в списке, если она входит в несколько групп одновременно (только для групп, идущих под значком белой папки — см. таблицу выше). Если флажок установлен, будут показаны все вхождения станции. Если снят — станция будет отображена в списке единожды.
  - **Показывать скрытые группы** — отображать все группы, входящие в антивирусную сеть. При снятии данного фла жка пустые группы (не содержащие станции) будут скрыты. Это может быть удобно для исключения излишней информации, например, при наличии большого количества пустых групп.
- для клиентов Сервера (станций, Прокси-серверов и соседних Серверов):
  - **Показывать идентификаторы клиентов** — отображать уникальные идентификаторы клиентов Сервера.
  - **Показывать названия клиентов** — отображать названия клиентов Сервера.

Нельзя отключить отображение идентификаторов и названий клиентов одновременно. Один из параметров **Показывать идентификаторы клиентов** и **Показывать названия клиентов** всегда будет выбран.

  - **Показывать адреса клиентов** — отображать IP-адреса клиентов Сервера.
  - **Показывать серверы станций** — отображать имена или IP-адреса Серверов Dr.Web, к которым подключены станции. Актуально для станций, входящих в кластер Серверов Dr.Web.
  - **Показывать серьезность состояния станций** — отображать серьезность статуса для активных станций. При этом добавится цветовая градация для станций в зависимости от их статуса (см. таблицу выше). Если опция отключена, то для станции со статусами, которым соответствуют значки  и  , будет отображаться общий значок .

- для всех элементов:

- **Показывать значок персональных настроек** — отображать маркер, обозначающий наличие персональных настроек, на значках групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов.
- **Показывать описания** — отображать описания групп и клиентов Сервера: станций, Прокси-серверов и соседних Серверов (описания задаются в свойствах элемента).
- **Показывать количество клиентов** — отображать количество клиентов Сервера: станций, Прокси-серверов и соседних Серверов для всех групп антивирусной сети, в которые эти клиенты входят.
- **Показывать значок правил членства** — отображать маркер на значках станций, которые были добавлены в группу автоматически согласно правилам членства, а также на значках групп, в которые станции были добавлены автоматически.

Временной интервал

В данном подразделе задаются настройки временного интервала, в пределах которого отображаются статистические данные (см. п. Просмотр статистики по рабочей станции):

- В выпадающем списке **Интервал по умолчанию для просмотра статистики** задается временной интервал, который будет установлен по умолчанию для всех разделов статистических данных.
- При первом открытии страницы статистика будет отображаться за данный временной интервал. При необходимости можно изменить временной интервал непосредственно в самих разделах статистики.
- Для того чтобы в разделах статистики сохранялся последний заданный для них интервал, установите флажок **Сохранять последний интервал просмотра статистики**.
- Если флажок установлен, то при первом открытии страницы отображается статистика за последний период, который был выбран в Веб-браузере.
- Если флажок снят, то при первом открытии страницы отображается статистика за период, заданный в списке **Интервал по умолчанию для просмотра статистики**.

Авторизация

В выпадающем списке **Длительность сессии** выберите период времени, по истечении которого сессия работы с Центром управления в веб-браузере автоматически прерывается.

Экспорт в PDF

В данном подразделе задаются настройки текста при экспорте статистических данных в формат PDF:

- В выпадающем списке **Шрифт отчетов** вы можете выбрать шрифт текста, используемый при экспорте отчетов в формат PDF.
- В поле **Размер шрифта отчетов** задается размер шрифта основного текста статистических таблиц, используемый при экспорте отчетов в формат PDF.

Отчеты

В данном подразделе задаются настройки отображения статистических данных в разделе **Отчеты** Центра управления:

- В поле **Количество строк на странице** задается максимальное количество строк на одной странице отчета при постраничном отображении статистики.
- Установите флажок **Показывать графики**, чтобы отображать графические данные на страницах статистических отчетов. Если флажок снят, отображение графических данных отключается.

Подписка

В данном подразделе настраивается подписка на новости компании «Доктор Веб».

Установите флажок **Автоматическая подписка на новые разделы** для автоматического добавления новых разделов в разделе новостей в Центре управления.

Меню **Помощь**

Для получения помощи в процессе работы с Dr.Web Enterprise Security Suite нажмите в главном меню кнопку **Поддержка**. Откроется контекстное меню, содержащее следующие пункты:

- **Справка** — открыть раздел документации администратора, соответствующий разделу Центра управления, в котором вы находитесь в данный момент. Если для текущего раздела Центра управления нет соответствующего раздела в документации, пункт **Справка** не будет отображаться в контекстном меню значка .
- **Поддержка** — открыть раздел **Поддержка** Центра управления (см. ниже).

Поддержка

Управляющее меню раздела **Поддержка** содержит следующие элементы:

1. **Общие**

- **Форум** — перейти на форум компании «Доктор Веб».
- **Новости** — перейти на страницу новостей компании «Доктор Веб».
- **Обратиться в службу технической поддержки** — перейти на страницу технической поддержки «Доктор Веб».
- **Прислать подозрительный файл** — открыть форму для отправки вируса в лабораторию «Доктор Веб».
- **Википедия «Доктор Веб»** — перейти на страницу Википедии — базы знаний, посвященной продуктам компании «Доктор Веб».
- **Сообщить о ложном срабатывании в Офисном контроле** — открыть форму для отправки сообщения о ложном срабатывании или пропуске вредных ссылок в модуле Офисного контроля.

2. **Документация администратора**

- **Руководство администратора** — открыть документацию администратора в формате HTML.
- **Руководство по установке** — открыть документацию по установке Dr.Web Enterprise Security Suite в формате HTML.
- **Инструкция по развертыванию антивирусной сети** — открыть краткую инструкцию по развертыванию антивирусной сети в формате HTML. Рекомендуется ознакомиться с данной инструкцией перед началом развертывания антивирусной сети, установкой и настройкой компонентов.
- **Приложения** — открыть приложения к руководству администратора в формате HTML.

- **Руководство по Web API** — открыть документацию администратора по Web API (см. также документ **Приложения**, п. Приложение L. Интеграция Web API и Dr.Web Enterprise Security Suite) в формате HTML.
- **Примечания к выпуску** — открыть раздел примечаний к выпуску Dr.Web Enterprise Security Suite для установленной у вас версии.
- **Руководства администратора по управлению станциями** — открыть документацию администратора в формате HTML по управлению станциями для соответствующей операционной системы, представленной в списке.
  В данных руководствах приведена информация о централизованной настройке антивирусного ПО рабочих станций, осуществляемой администратором антивирусной сети через Центр управления безопасностью Dr.Web. Руководства описывают настройки соответствующего антивирусного решения и особенности централизованного управления данным ПО.

3. Документация пользователя — открыть документацию пользователя в формате HTML для соответствующей операционной системы, представленной в списке.

7.2. Смена языка отображения Центра управления

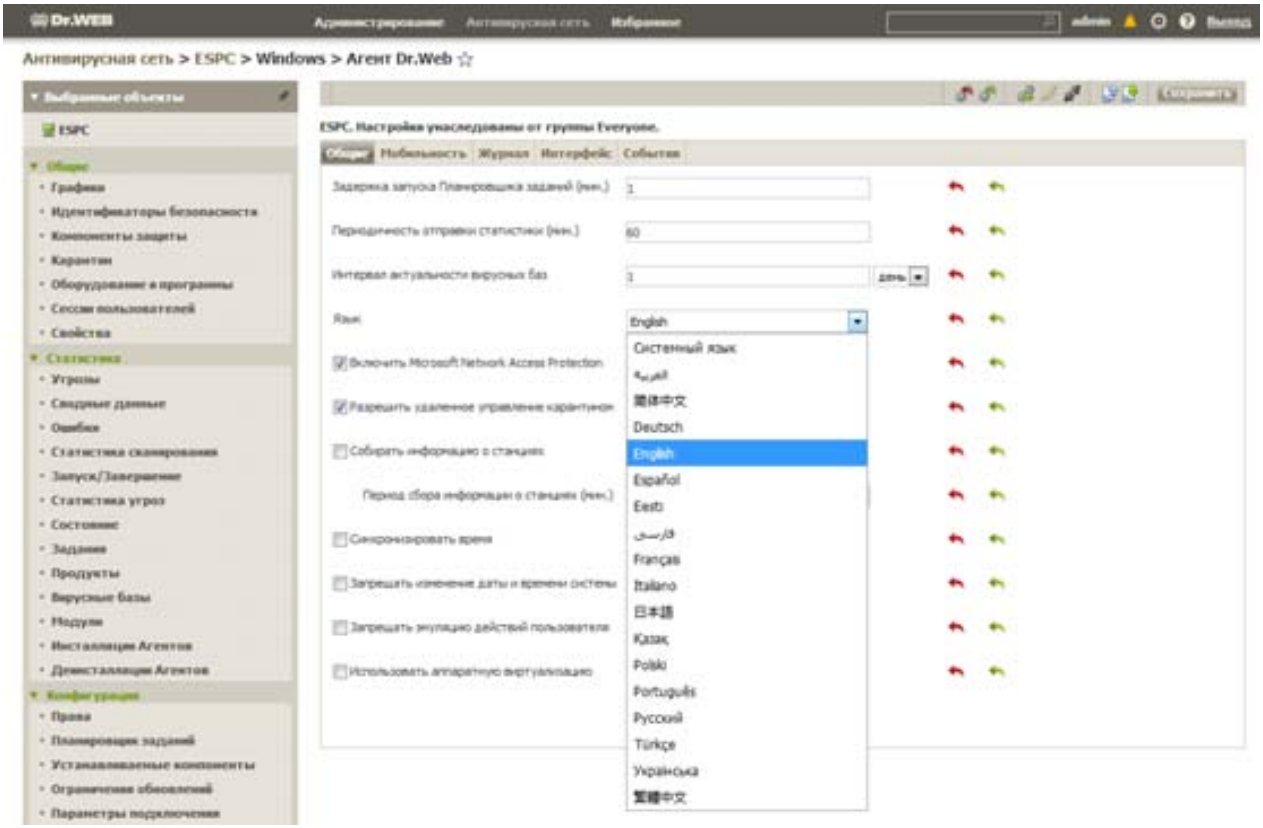
В связи с тем, что Центр управления позволяет использовать для управления системой более одного системного администратора, каждый из которых может иметь свой предпочтительный язык отображения, этот параметр задается в профиле администратора. Для выбора язы ка перейдите в раздел **Администрирование** (Administration) → **Конфигурация** (Configuration) → **Администраторы** (Administrator accounts), в списке выберите необходимого администратора и на панели справа в выпадающем списке **Язык интерфейса** (Interface language) укажите нужный язык. Для сохранения выбора нужно нажать на кнопку **Сохранить** (Save) и обновить страницу браузера.

Аналогичные параметры также доступны в разделе **Настройки** ( ) главного меню Центра управления, в разделе **Моя учетная запись** (My account).

7.3. Настройка языка интерфейса антивирусных компонентов на рабочих станциях под управлением ОС Windows®

Чтобы установить язык интерфейса компонентов Антивируса Dr.Web на рабочей станции или на группе рабочих станций под управлением ОС Windows:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления.
2. В открывшемся окне в иерархическом списке нажмите на название станции или группы.
3. В открывшемся управляющем меню (панель слева) выберите пункт **Агент Dr.Web** для Windows вкладка **Общие**.
4. В поле **Язык** выберите из выпадающего списка необходимый язык.



5. Нажмите на кнопку **Сохранить**.

7.4. Просмотр новостей компании «Доктор Веб» из Центра управления

Для того чтобы настроить параметры подписки на новости информационной безопасности компании «Доктор Веб», п ерейдите на вкладку **Администрирование → Репозиторий → Общая конфигурация репозитория → Сервер Dr.Web → Новости компании «Доктор Веб»** и в открывшемся окне задайте список языков, на которых будет скачиваться новостная лента.

Выбор разделов новостей, которые будут автоматически скачиваться из BCO и отображаться на странице новостей, осуществляется в разделе **Настройки → Подписки**.

С новостями компании **«Доктор Веб»** вы можете ознакомиться в разделе **События** главного меню **Центра управления**.

7.5. Группы станций и их использование. Предустановленные группы

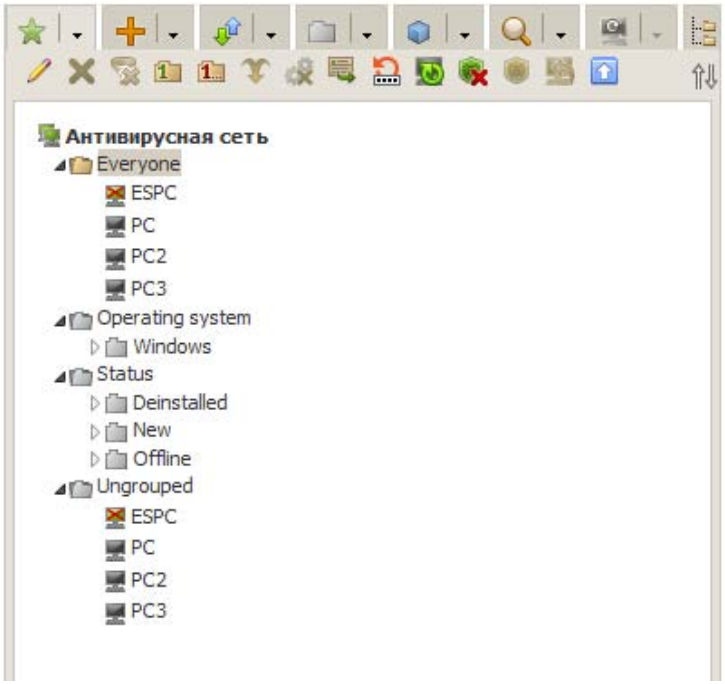
Для удобства управления антивирусной сетью администратор может удобным для себя образом распределять защищаемые компьютеры по группам. Объединение станций в группы позволяет с помощью одной команды задавать параметры, а также инициировать выполнение определенных заданий для всех входящих в группу рабочих станций. Группы могут использоваться также для создания и структурирования списка защищаемых объектов.

Во время установки Сервера Dr.Web создается базовый набор системных групп, которые не могут быть изменены или удалены, но при необходимости администратор может скрыть их отображение. Предустановленные группы:

Everyone — сюда входят все рабочие станции. Для группы **Everyone** отображается список всех компонентов всех активных ключей.

Online и **Offline** — станции антивирусной сети автоматически переносятся в одну из этих групп во время работы сервера в зависимости от того, активны на них Агенты или нет. Первая включает все активные рабочие станции (реагирующие на запросы сервера), вторая — все не активные. Данные группы полностью виртуальны и не могут содержать никаких настроек, также они не могут являться первичными группами.

Подробнее о предустановленных группах рассказано в документации.



Это группы, создаваемые администратором антивирусной сети для его собственных нужд. Администратор может создавать собственные группы, а также вложенные группы и включать в их рабочие станции. Ни на состав, ни на название данных групп Dr.Web Enterprise Security Suite не накладывает никаких ограничений.

Для удобства в таблице ниже сведены все возможные группы и типы групп, а также характерные параметры, которые поддерживаются (+) или не поддерживаются (–) данными группами.

При этом рассматриваются следующие параметры:

- **Автоматическое членство**. Параметр определяет возможность автоматического включения станций в группу (поддержка автоматического членства), а также автоматического изменения состава группы в процессе работы Сервера.
- **Управление членством**. Параметр определяет возможность управления администратором членством в группе: добавлением или удалением станций из группы.
- **Первичная группа**. Параметр определяет, может ли данная группа являться первичной для станции.
- **Содержание настроек**. Параметр определяет, может ли группа содержать настройки антивирусных компонентов (для возможности наследования их станциями).

Группы и поддерживаемые параметры

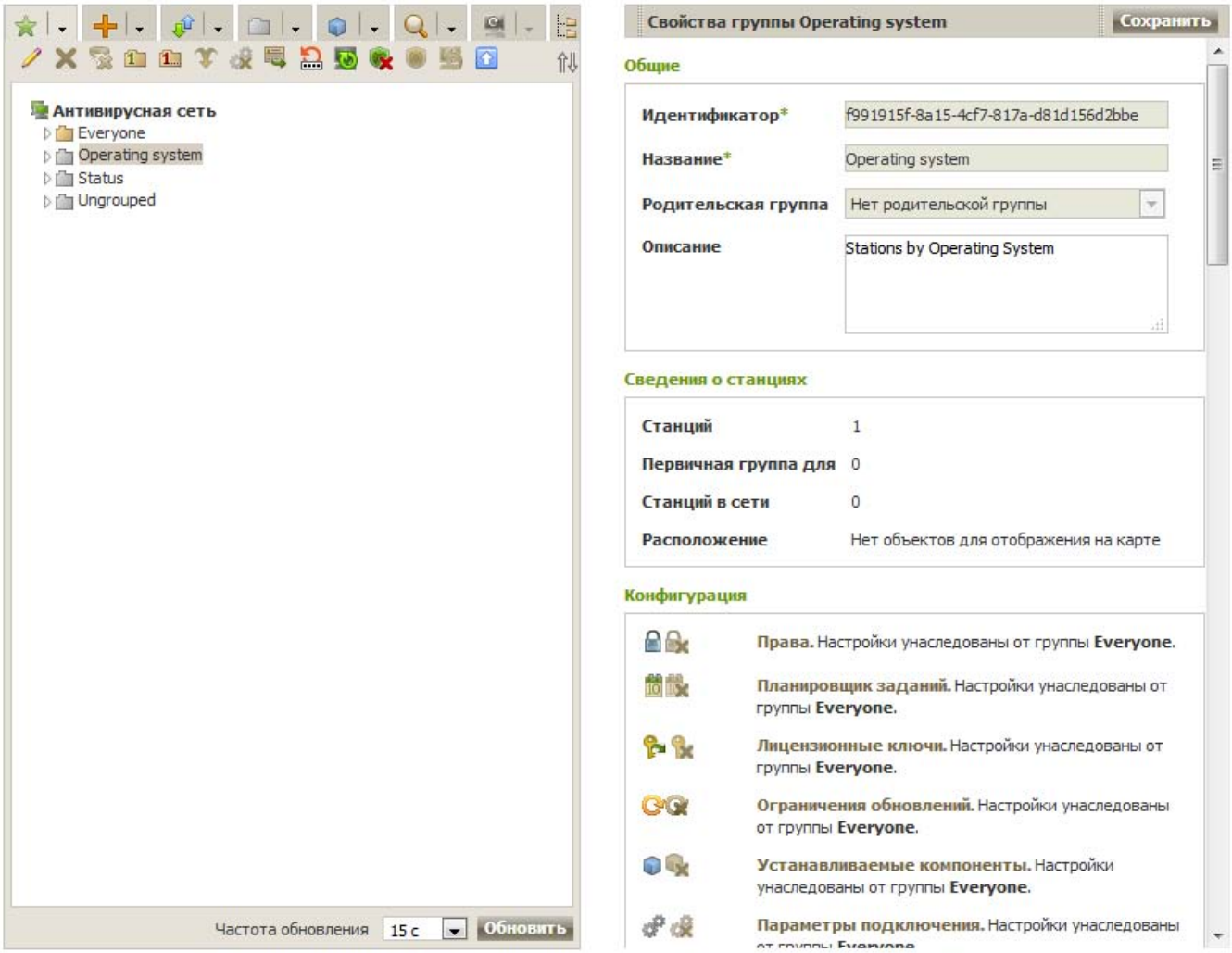
Группа / тип групп	**Параметр**			
	Автоматическое членство	**Управление членством**	**Первичная группа**	**Содержание настроек**
Everyone	+	–	+	+
Configured	+	–	–	–
Operating System	+	–	+	+
Status	+	–	–	–

Группа / тип групп	Параметр			
	Автоматическое членство	Управление членством	Первичная группа	Содержание настроек
Transport	+	–	–	–
Ungrouped	+	–	–	–
Пользовательские группы	–	+	+	+

Под учетной записью *администратора группы* пользовательская группа, которой он управляет, будет отображаться в корне иерархического дерева, даже если фактически у нее есть родительская группа. При этом будут доступны все дочерние от управляемой группы.

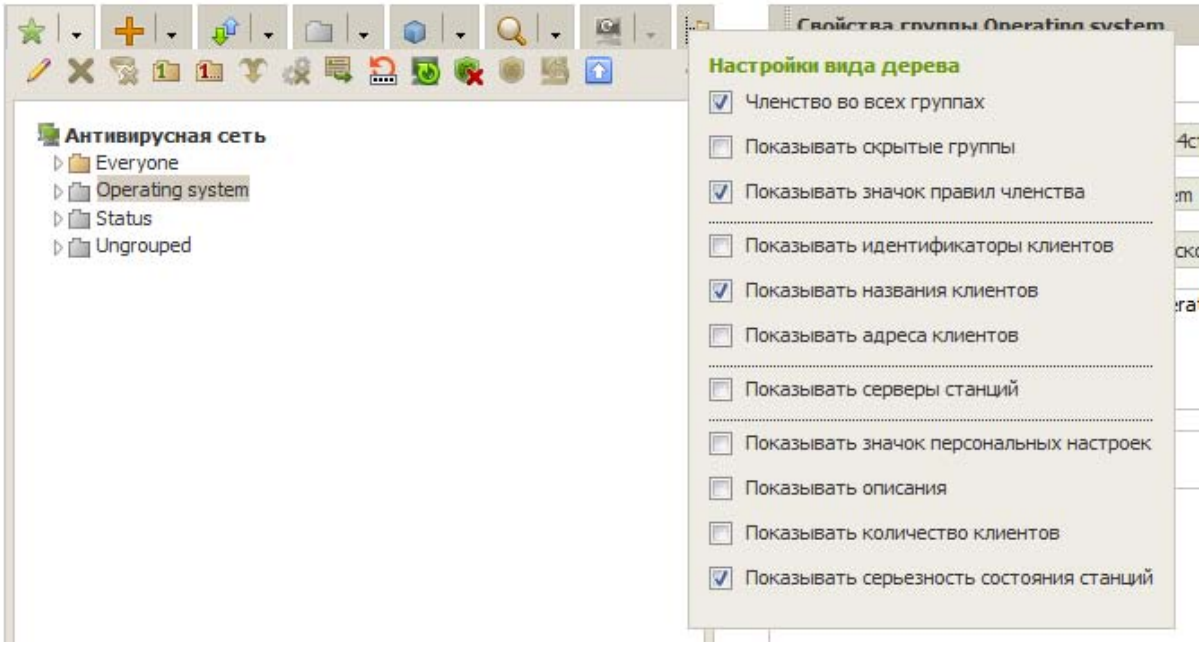
7.5.1. Просмотр параметров групп

Просмотреть свойства групп и станций можно, однократно нажав левой кнопкой мыши на их значок в дереве групп.

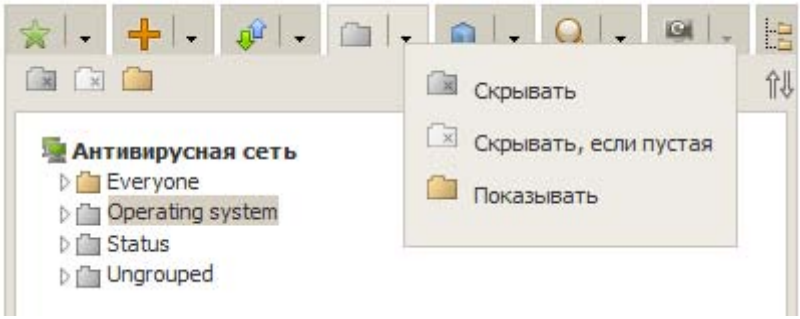


7.5.2. Настройка отображения групп

Используя значок , можно настроить представление дерева групп в удобном виде.



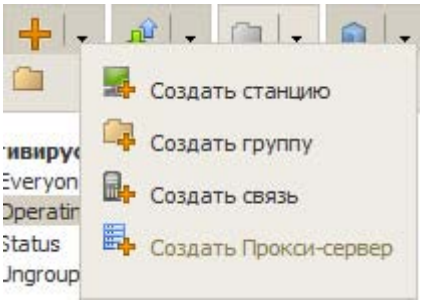
Дополнительно, используя значок , можно определить режим показа группы.



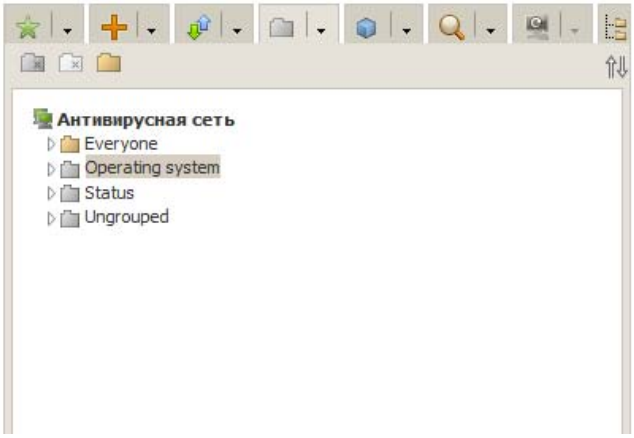
7.5.3. Создание и удаление группы

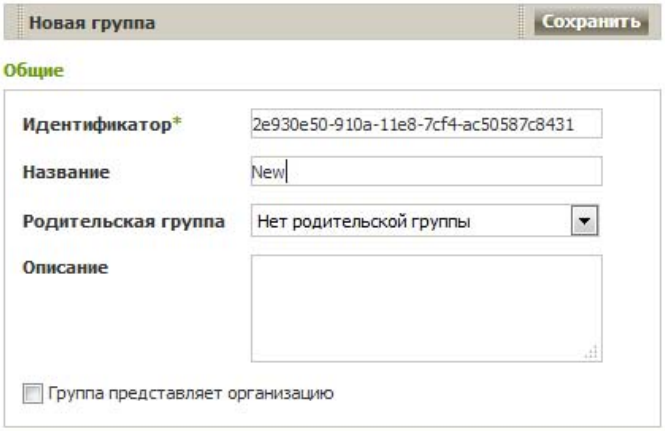
Для создания группы и включения в нее рабочих станций сделайте следующее:

1. В меню **Антивирусная сеть** нажмите кнопку (**Добавить объект сети**) и в появившемся списке выберите **Создать группу** или **Создать станцию**.

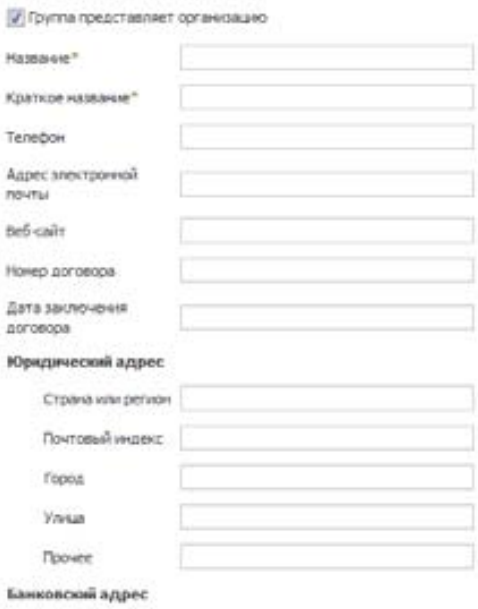


Если вы выбрали **Создать группу**, то появится форма **Новая группа**.

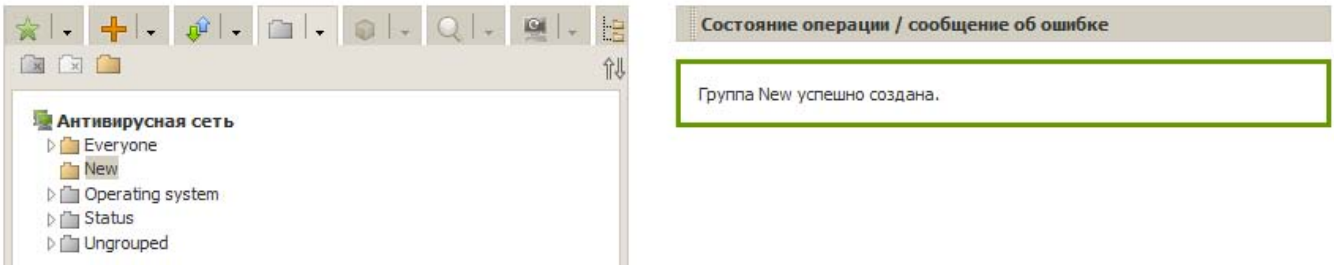




2. Поле ввода **Идентификатор** заполняется автоматически, но при необходимости его можно отредактировать. Идентификатор не должен включать пробелы. Рекомендуется использовать уникальные идентификаторы, как-либо связанные со структурой сети или оставлять значения по умолчанию.
3. Введите в поле **Название** наименование группы.
4. Для вложенных групп в поле **Родительская группа** выберите из выпадающего списка группу, которая будет назначена родительской группой, от которой наследуется конфигурация, если не заданы персональные настройки. Для корневой группы (не имеющей родителя) оставьте это поле пустым, группа будет добавлена в корень иерархического списка. В этом случае настройки будут наследоваться от группы **Everyone**.
5. Введите произвольный комментарий в поле **Описание**.
6. Если в группу планируется внести рабочие станции, относящиеся к одной организации, отметьте флажком пункт **Группа представляет организацию** и заполните данные организации.



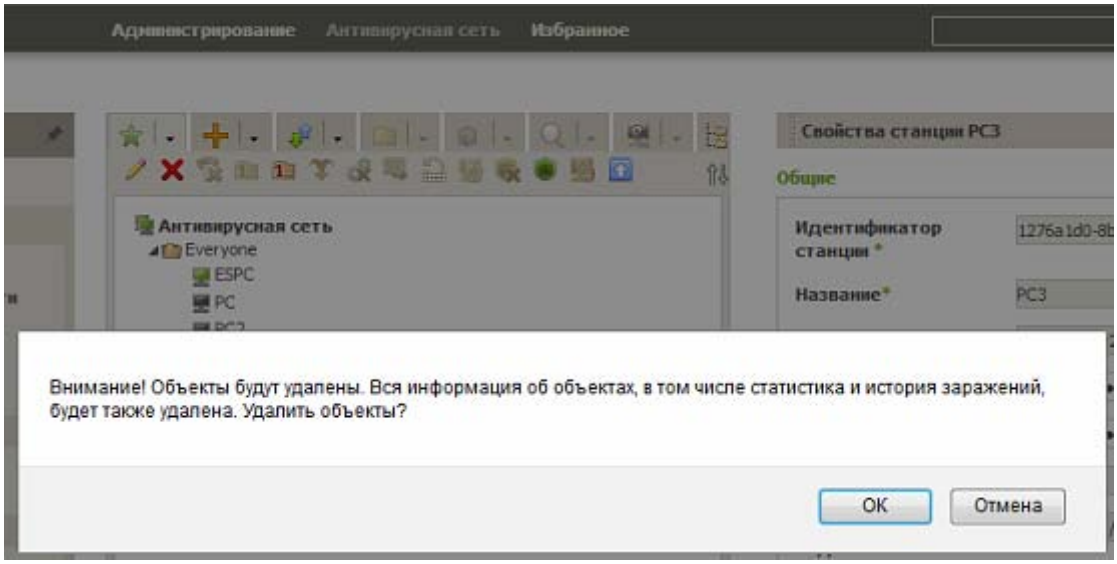
7. Нажмите на кнопку **Сохранить**.

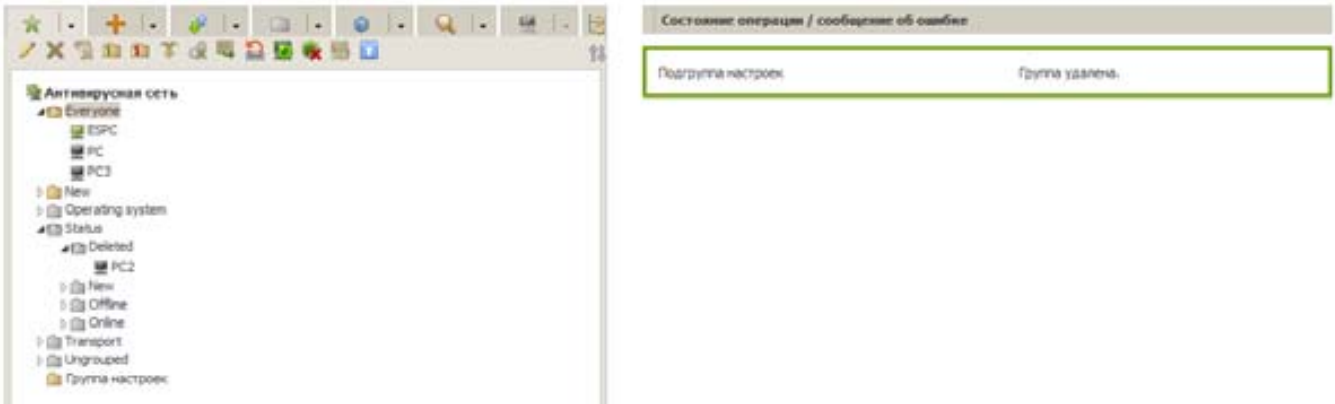


Созданные группы первоначально пусты. Процедура включения рабочих станций в группы описана ниже.

При создании станции администратор дополнительно указывает членство в группах, а также месторасположение станции, что может облегчить процесс работы в крупных компаниях с большим парком машин.

Вы также можете удалять созданные вами станции или группы (за исключением предустановленных групп). Для этого выберите станцию или группу, после чего нажмите кнопку **Удалить выбранные объекты (** **)**.



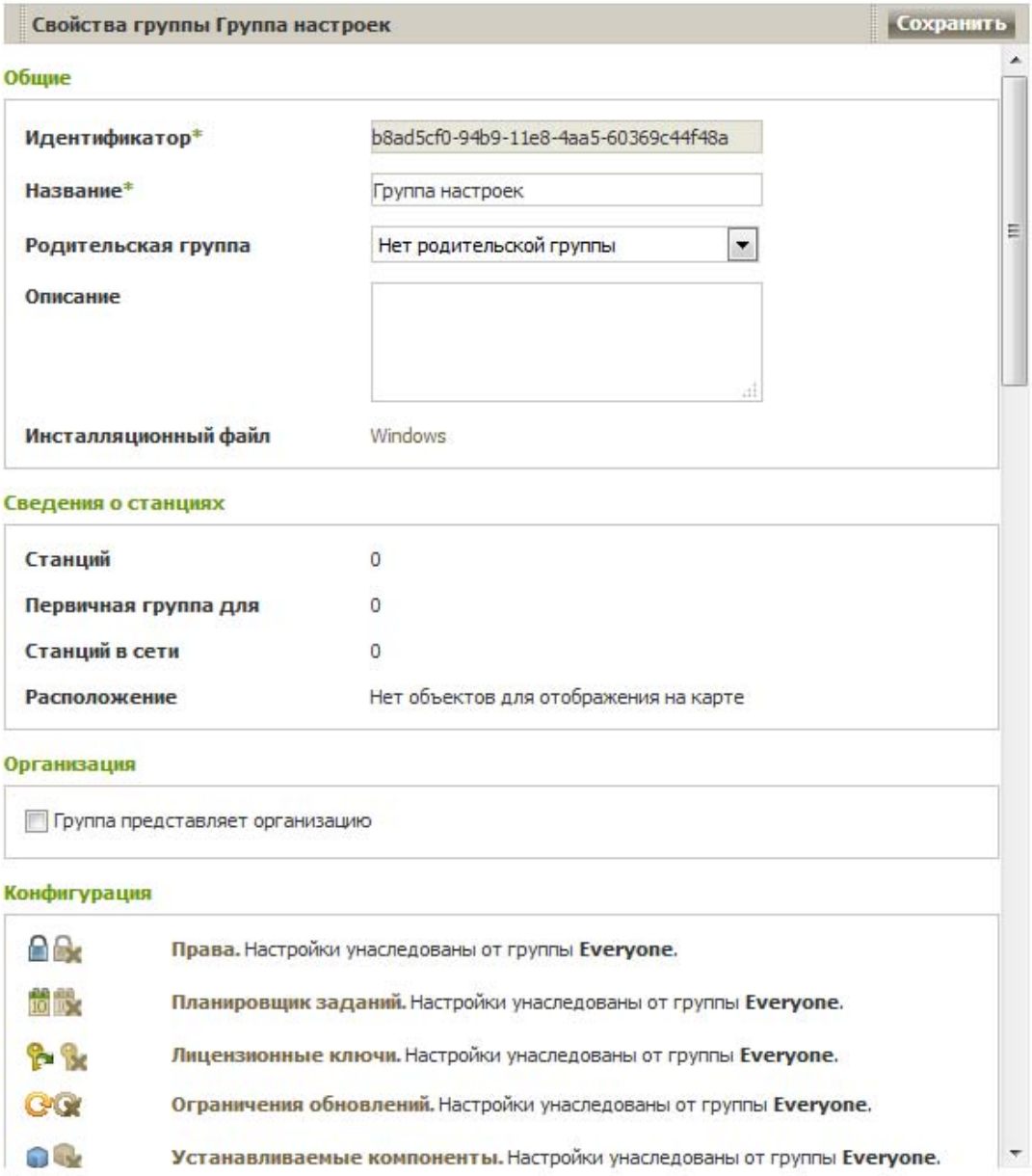


7.5.4. Настройки группы. Использование групп для настройки рабочих станций. Настройки полномочий пользователей

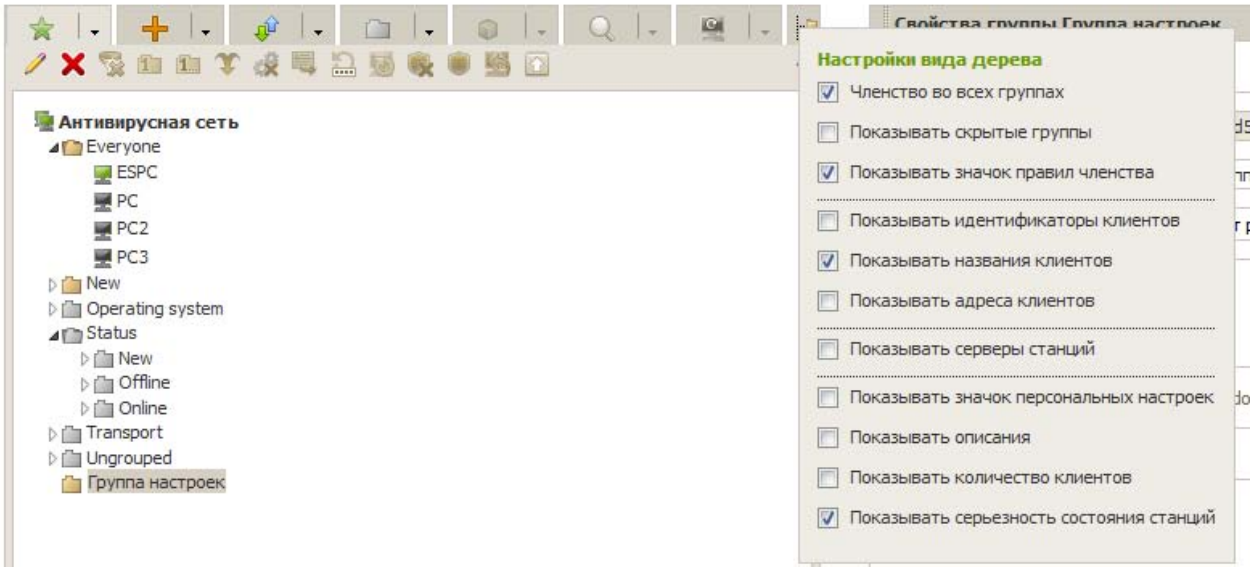
Сразу после установки все группы и рабочие станции имеют единые настройки, заданные по умолчанию (наследуются от группы **Everyone**). В дальнейшем вы можете установить

отдельные настройки для разных ОС, изменив настройки соответствующих групп. Вы также можете изменять параметры вновь создаваемых групп.

Настраивая группу, вы тем самым создаете набор параметров, которые будут автоматически присваиваться рабочим станциям при переносе их в данную группу. Для изменения параметров группы в разделе **Антивирусная сеть** Центра управления выделите имя группы, которую необходимо настроить, и нажмите на кнопку **Редактировать**. В правой части окна откроется форма **Свойства группы <имя группы>**.

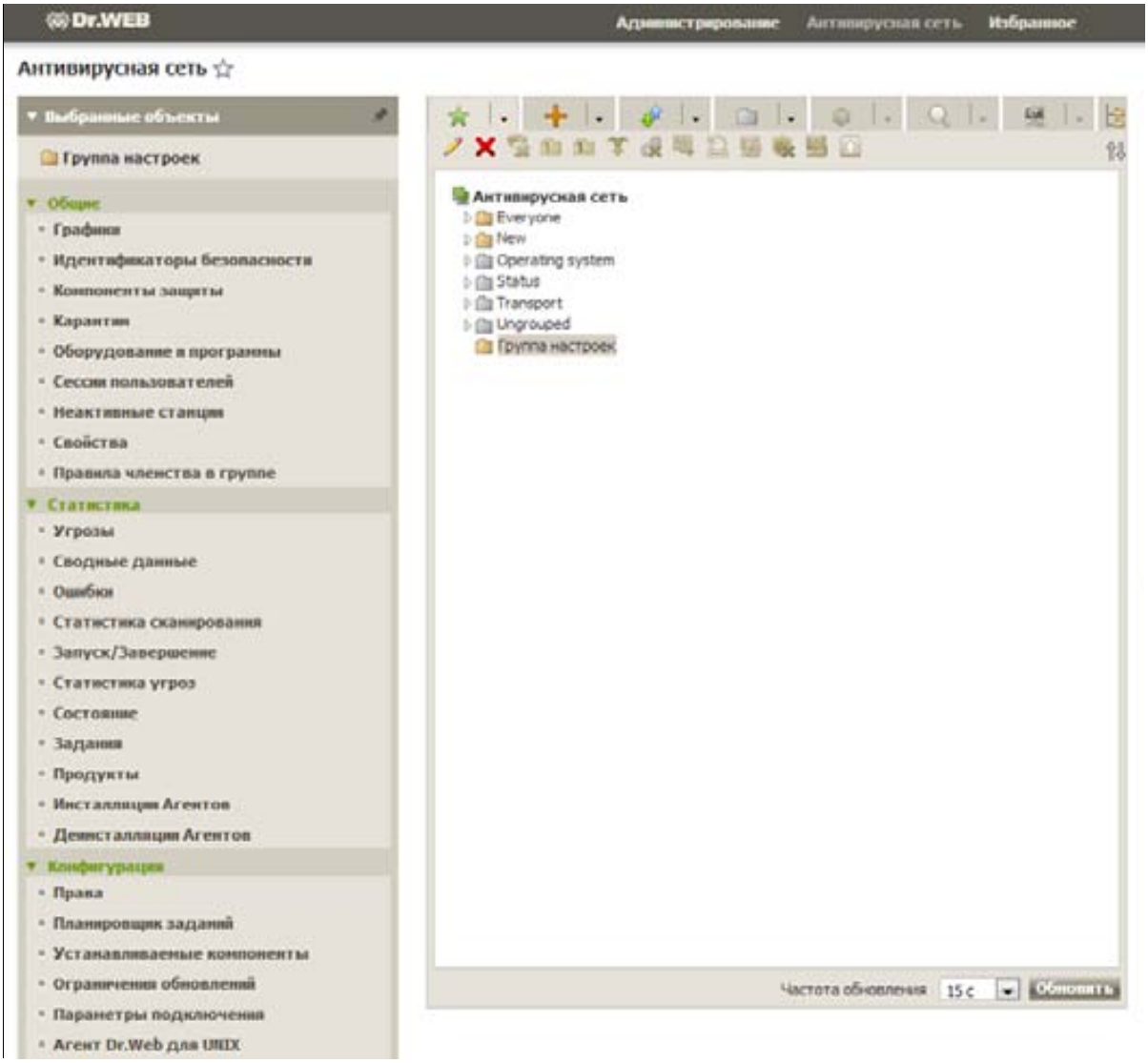


По умолчанию структура сети представлена таким образом, чтобы продемонстрировать вхождения станций только в первичных группах. Если вы хотите отображать в каталоге сети членство станций во всех группах, куда входит станция, нажмите кнопку **Настройки вида дерева** и установите флажок **Членство во всех группах**.



Настройки группы включают конфигурацию антивирусных средств, расписание и определение прав пользователей.

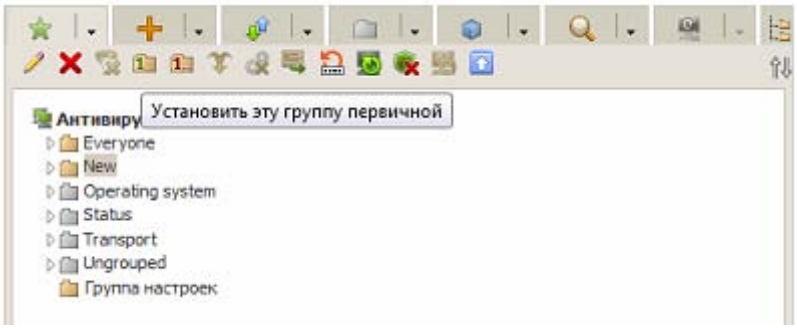
Используя пункты меню справа, вы можете запускать, просматривать и прекращать задания на сканирование как для отдельной группы, так и для нескольких выбранных групп. Точно так же вы можете просматривать статистику (в т ом числе вирусы, запуск/завершение, ошибки сканирования и установки) и суммарную статистику для всех рабочих станций группы или нескольких групп.



7.5.5. Наследование элементов конфигурации рабочей станции из конфигурации группы. Первичные группы

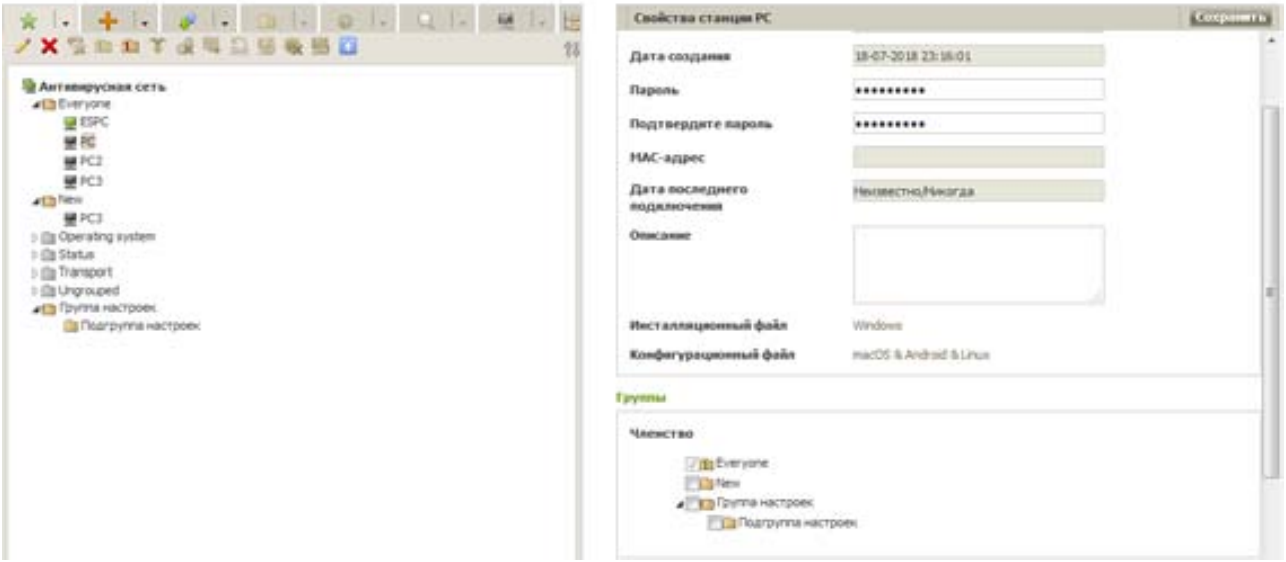
При подключении новой рабочей станции элементы ее конфигурации заимствуются (наследуются) от одной из групп, в которую она входит (первичной группы). При изменениях в настройках этой группы они автоматически наследуются входящими в группу станциями. При создании станции вы можете указать, какая из групп будет считаться первичной. По умолчанию это группа **Everyone**. Если первичная группа — не **Everyone**, и у указанной первичной группы нет персональных настроек, то наследуются настройки группы **Everyone**.

Для того чтобы установить в качестве первичной группы группу, отличную от **Everyone** (сделать группу первичной для всех входящих в нее рабочих станций), необходимо выделить соответствующую группу и нажать кнопку **Установить эту группу первичной**.



7.5.6. Добавление рабочих станций в группу. Удаление рабочих станций из группы. Восстановление станции

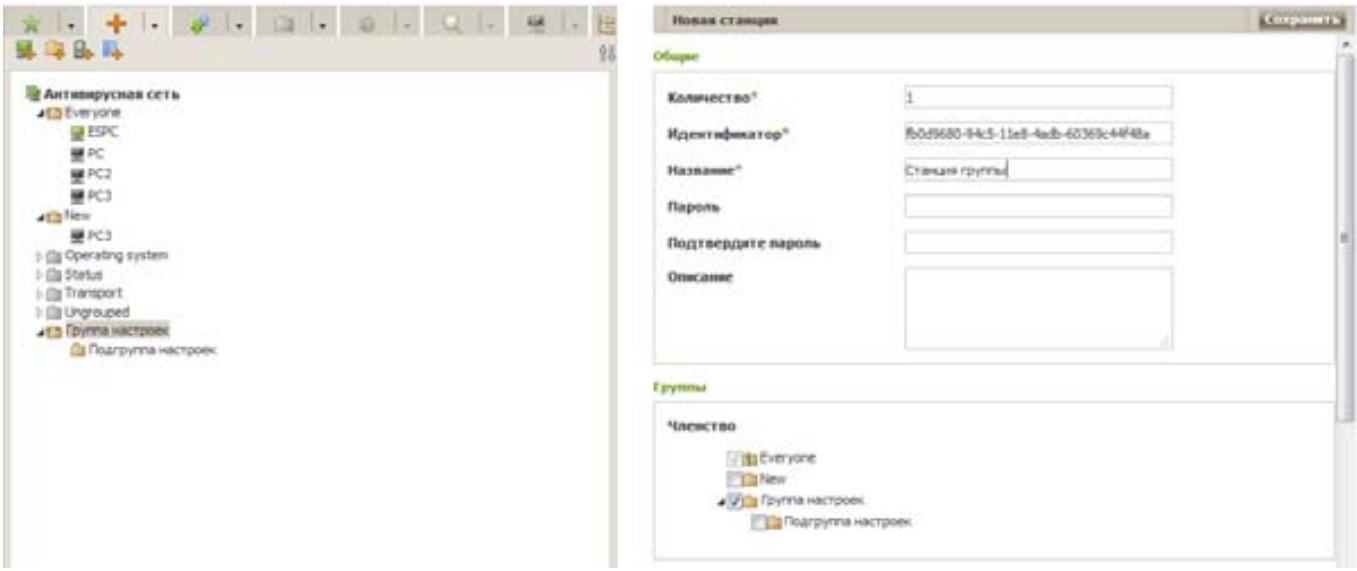
Создаваемые группы первоначально всегда пусты. Чтобы добавить станцию в группу, в разделе **Антивирусная сеть** укажите добавляемую станцию, выделив ее в дереве групп и станций, после чего в разделе **Свойства станции → Группы → Членство** отметьте флажками те группы, к которым нужно отнести данную станцию.



Для сохранения внесенных изменений нажмите **Сохранить**.

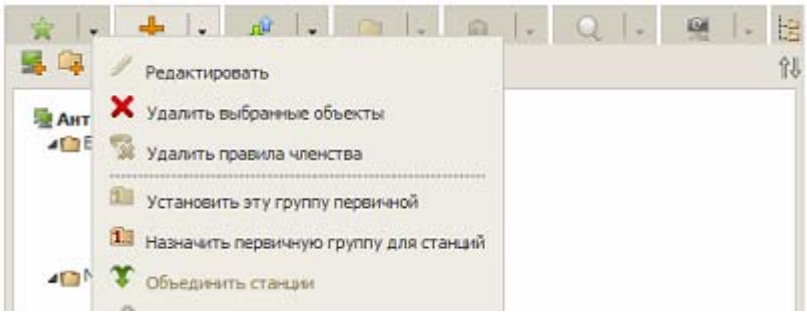
Вы также можете включить рабочую станцию в группу, устанавливая новую группу первичной (подробнее см. п. 7.5.11.3 Наследование элементов конфигурации рабочей станции. Первичные группы).

Для создания записи о новой станции выберите пункт **Антивирусная сеть**, в открывшемся окне на панели инструментов нажмите кнопку  (**Добавить объект сети**), в выпадающем меню выберите **Создать станцию**. Откроется окно создания новой станции.



Заполните необходимые поля (подробнее — в разделе 6.4.4.2.1. Создание записи для создаваемой станции (нового пользователя) и нажмите **Сохранить**.

Внимание! В результате операций с базой данных или при переустановке ПО антивирусных станций в иерархическом списке антивирусной сети может появиться несколько станций с одинаковым названием. При этом только одно из них будет соотнесено с соответствующей антивирусной станцией. Для того чтобы убрать повторяющие имена станции, выделите (с помощью клавиши CTRL) все имена такой станции и на панели инструментов выберите **Объединить станции**. По умолчанию будет предложено использовать то имя, которое было присвоено антивирусной станции в самый последний раз при регистрации на Сервере.

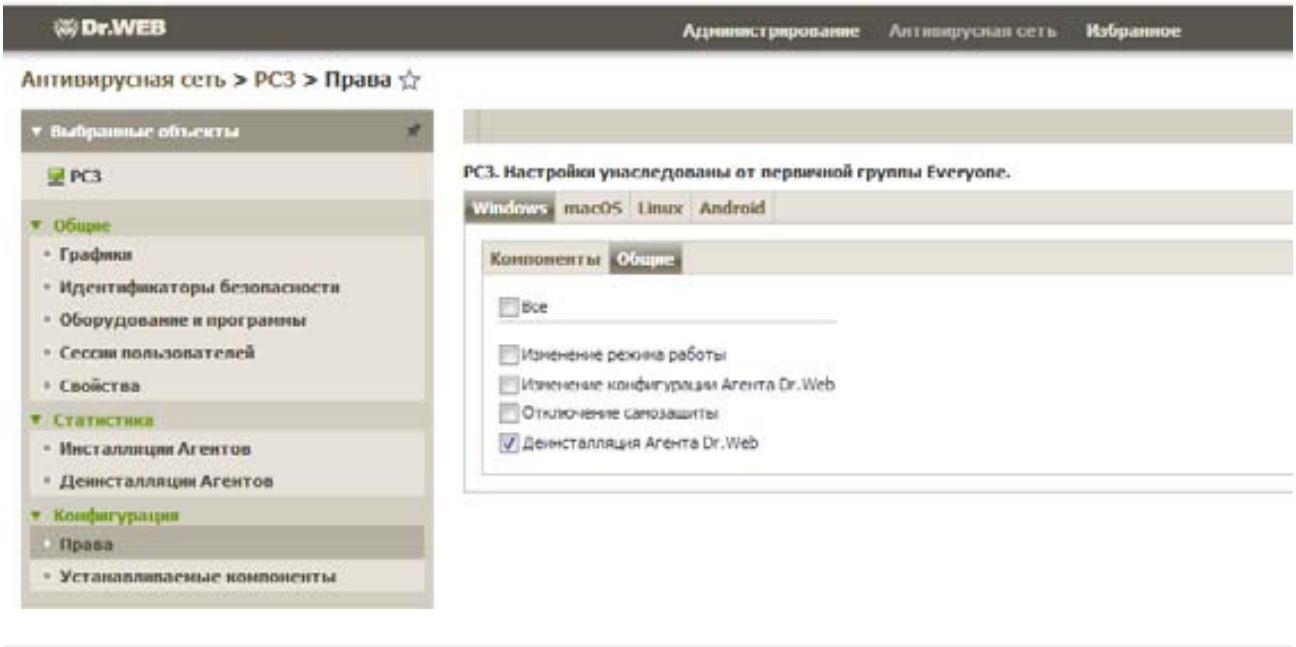


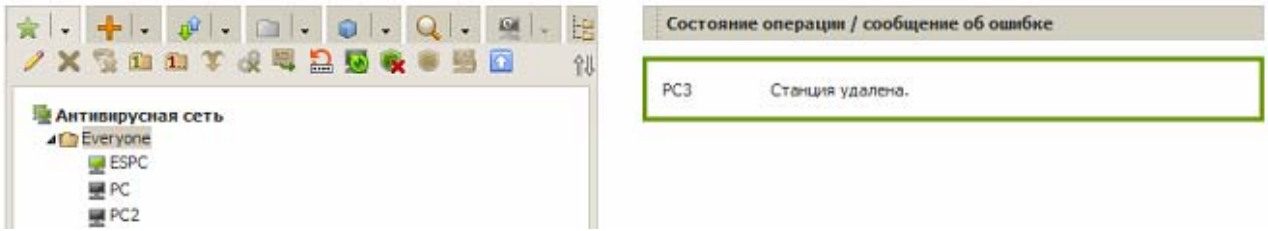
Аналогично для удаления станции из группы щелкните в группе настроек **Группы** по названию группы, в которую входит станция, отметьте название группы в списке **Членство**, и станция будет исключена из этой группы. Для применения настроек нажмите **Сохранить**.

Ручное удаление станций из предустановленных групп невозможно.

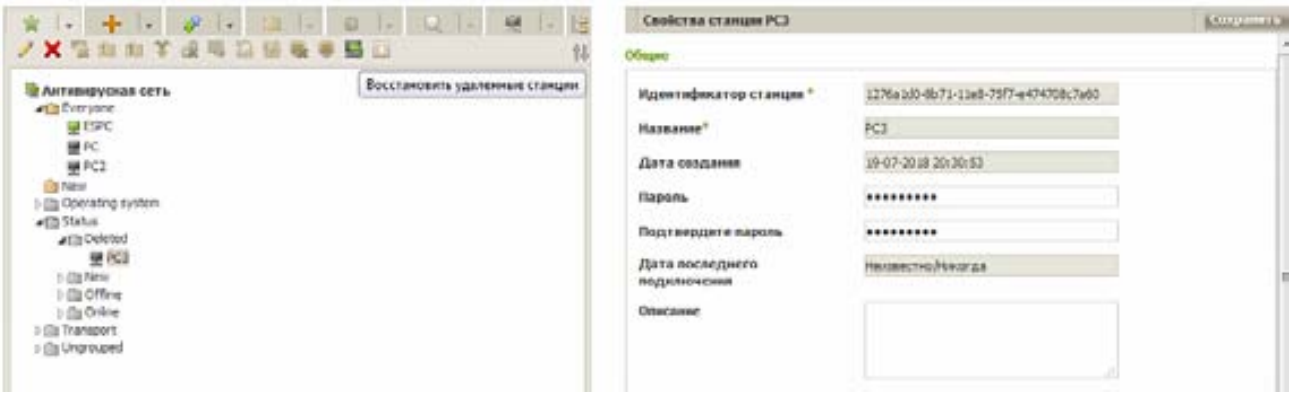
Чтобы удалить запись о рабочей станции, выделите ее в списке станций и групп, после чего в меню **Общие** нажмите на значок ✖ (**Удалить выбранные объекты**). Для подтверждения нажмите **ОК**.

Внимание! Перед удалением станции убедитесь в том, что у выбранной вами станции присутствуют права на ее удаление. Для этого выберите станцию в дереве станций и групп меню **Антивирусная сеть** и в свойствах станции **Конфигурация → Права → Общие**, отметьте пункт **Деинсталляция Агента Dr.Web** и нажмите **Сохранить**.

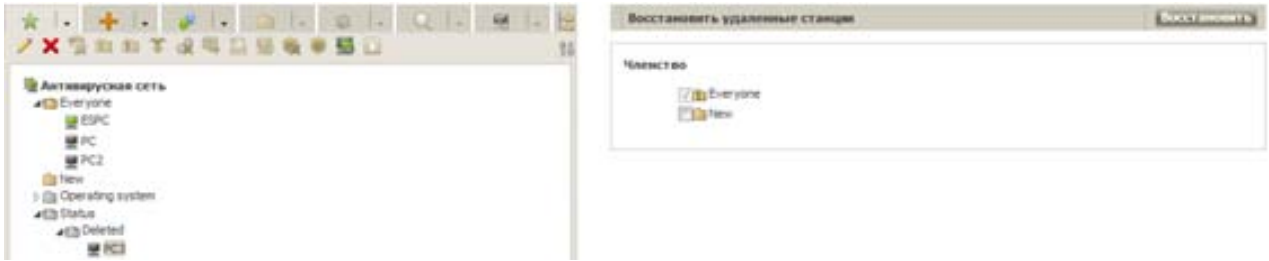




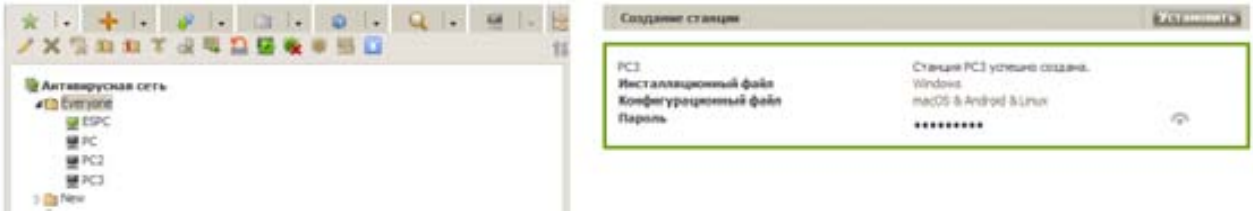
Удаленные станции помещаются в подгруппу **Deleted**, находящуюся в группе **Status**. При этом с удаленными станциями можно работать непосредственно в дереве антивирусной сети — так же, как и с обычными станциями. В число доступных операций входит возможность восстановить удаленные ранее станции (**Восстановить удаленные станции**). Удаленные группы не восстанавливаются, но их можно создать заново.



При восстановлении станции можно указать для нее членство в группах.



Для подтверждения восстановления нажмите кнопку **Восстановить**.



7.5.7. Политика подключения новых станций

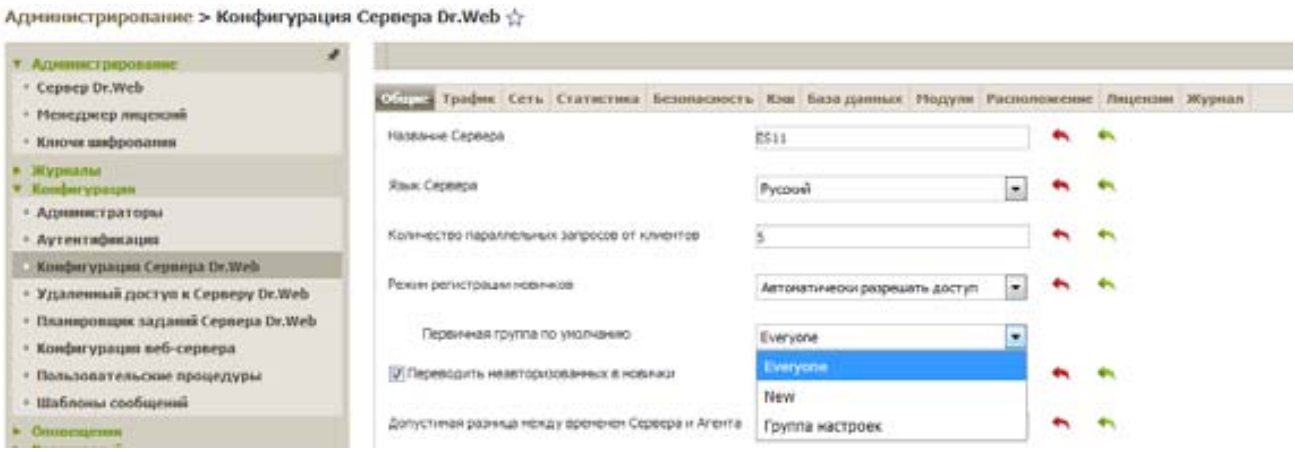
В зависимости от выбранной политики новые станции могут подключаться автоматически или вручную. Во втором случае администратор должен подтверждать подключение каждой новой станции к антивирусной сети. При этом:

- Если при установке **Агента** на станции был выбран вариант авторизации **Автоматически**, то режим доступа станций к **Серверу** будет определяться в соответствии с настройками, заданными на **Сервере** (используется по умолчанию).
- Если при установке **Агента** на станции был выбран вариант авторизации **Ручная** и заданы параметры **Идентификатор** и **Пароль**, то при подключении к **Серверу** станция будет авторизована автоматически вне зависимости от настроек **Сервера** (вариант используется по умолчанию при установке **Агента** через инсталляционный пакет *esinst* — см. п. 6.4.4.2. Установка Dr.Web Agent при помощи инсталляционного пакета esinst).

Задание типа авторизации **Агента** при его установке описано в разделе 6.4.4. Установка с использованием дистрибутивов компонентов Dr.Web Enterprise Security Suite.

Вы можете настроить политику подключения, изменив режим доступа станций к **Серверу Dr.Web,** для этого:

1. Откройте настройки конфигурации Сервера. Для этого выберите пункт **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**.



2. На вкладке **Общие** в выпадающем списке **Регистрация новичков** выберите одно из трех значений:
   - **Подтверждать доступ вручную** (по умолчанию). В этом режиме новые станции помещаются в список неподтвержденных станций до их непосредственного одобрения администратором.

Для доступа к списку неподтвержденных станций в разделе **Антивирусная сеть** в дереве групп и станций откройте группу **Status → Newbies**. На панели инструментов в разделе **Неподтвержденные станции** задайте действие, которое будет применено для выбранных станций:

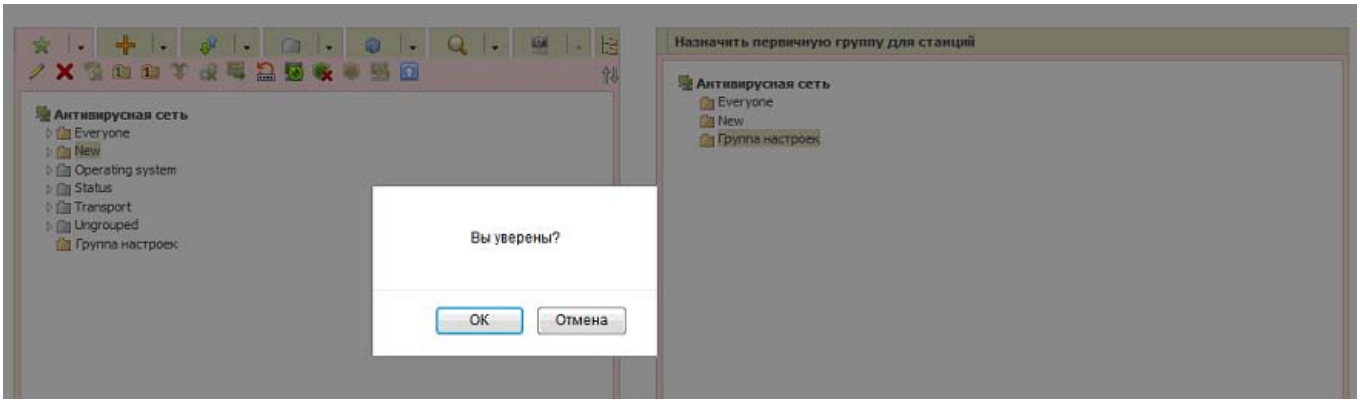
Список неподтвержденных станций позволяет:

- разрешить доступ выбранным станциям и назначить первичную группу — разрешить станции (или всем станциям) доступ к Серверу Dr.Web и назначить для них первичную группу из списка доступных;
- отменить действие, заданное для выполнения при подключении — отменить действие над неподтвержденной станцией, которое было ранее назначено для выполнения в момент, когда станция подключится к Серверу;
- отказать в доступе выбранным станциям — запретить станции (или всем станциям) доступ к Серверу.

- **Автоматически разрешать доступ**. В этом режиме все станции, которые запрашивают доступ к **Серверу**, подключаются автоматически без дальнейших запросов администратору. При этом в качестве первичной группы назначается группа, указанная в поле **Первичная группа** по умолчанию.
- **Всегда отказывать в доступе**. В этом режиме отказывается в доступе при получении запросов от новых станций. Администратор должен вручную создавать записи о станциях и присваивать им пароли доступа.

7.5.8. Перемещение в новую группу

Для перемещения станции в новую или существующую группу необходимо в разделе **Группы → Членство** свойств станции отметить выбрать пункт меню  (**Назначить первичную группу для станций**), в появившемся окне выбрать необходимую группу и подтвердить изменения.

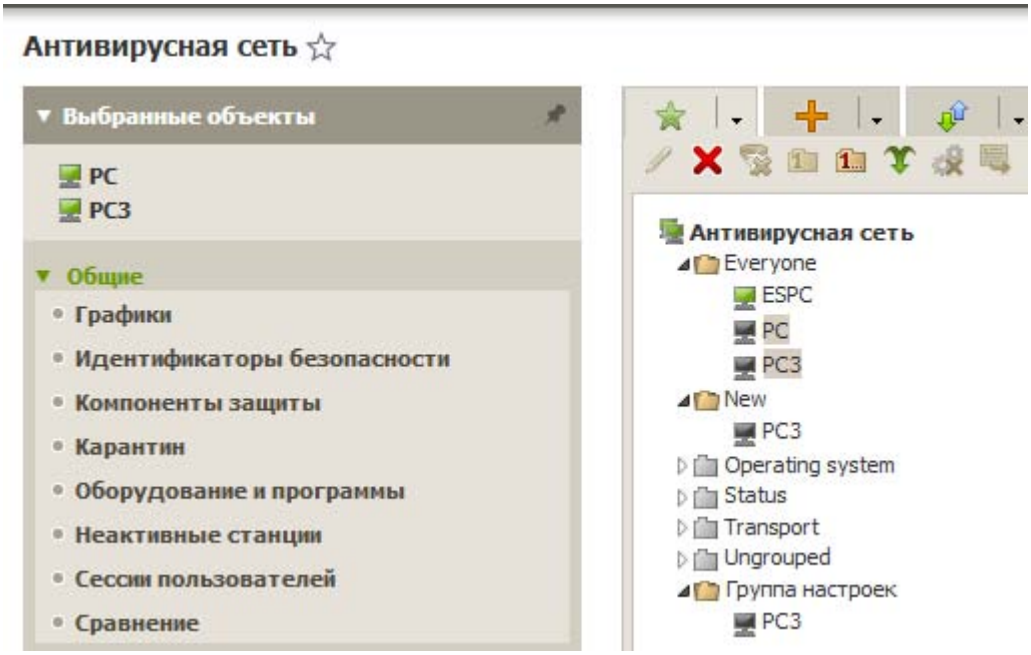


7.5.9. Сравнение станций и групп

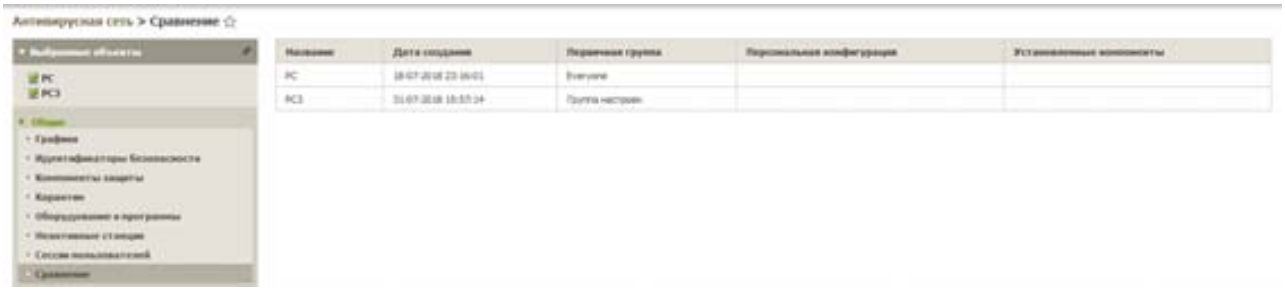
Для сравнения нескольких объектов антивирусной сети:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке выберите объекты, которые вы хотите сравнить. Используйте для этого клавиши CTRL и SHIFT. Возможны следующие варианты:

- выбор нескольких станций — для сравнения выбранных станций;
- выбор нескольких групп — для сравнения выбранных групп и всех вложенных групп;
- выбор нескольких станций и групп — для сравнения всех станций: как выбранных непосредственно в иерархическом списке, так и входящих во все выбранные группы и их вложенные группы.



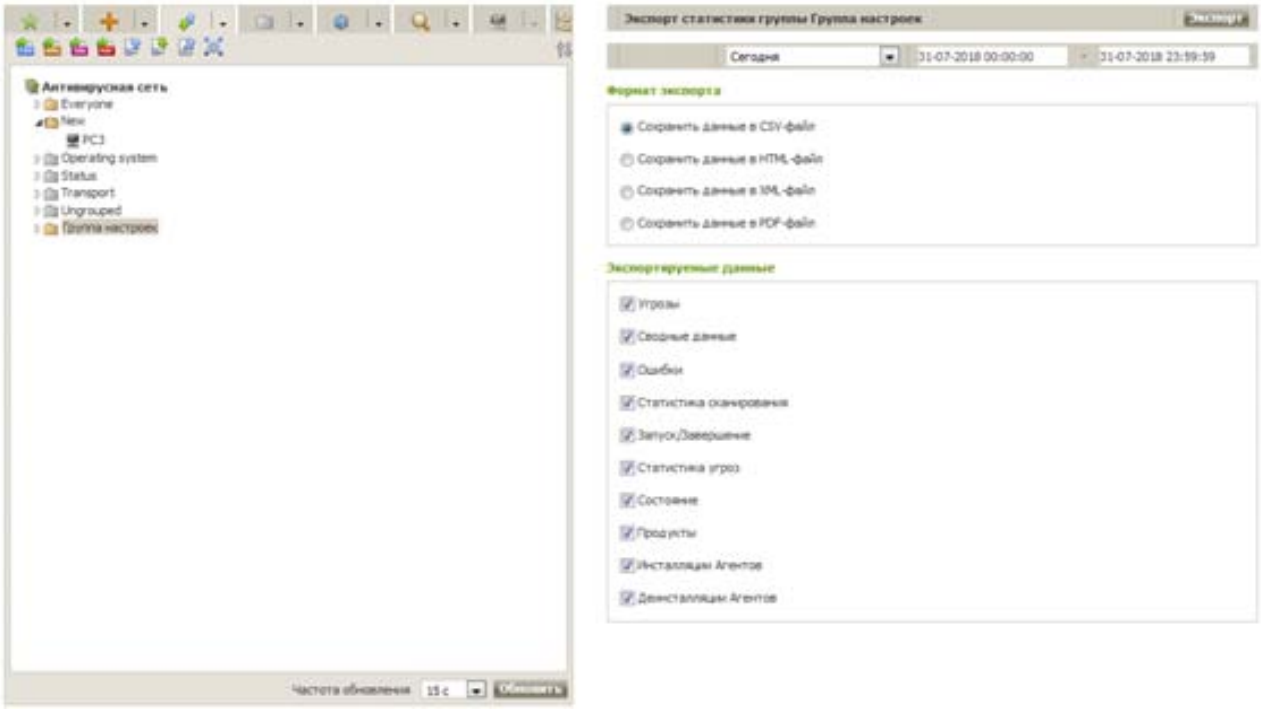
2. В управляющем меню (панель слева) нажмите пункт **Сравнение** — откроется сравнительная таблица для выбранных объектов.



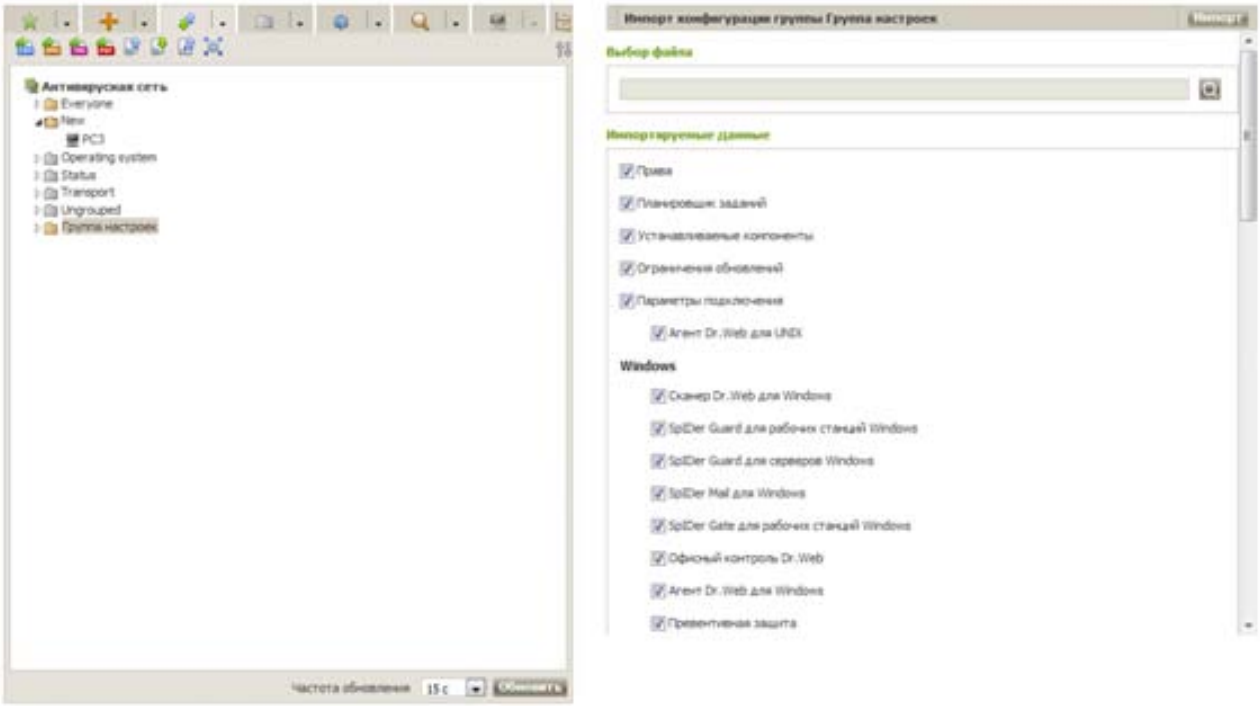
- Параметры сравнения для групп:
  - **Станций** — общее количество станций, входящих в данную группу.
  - **Станций в сети** — количество станций, активных на данных момент.
  - **Первичная группа для** — количество станций, для которых выбранная группа является первичной.
  - **Персональная конфигурация** — список компонентов, для которых назначены персональные настройки, не унаследованные от родительской группы.
- Параметры сравнения для станций:
  - **Дата создания**
  - **Первичная группа**
  - **Персональная конфигурация** — список компонентов, для которых назначены персональные настройки, не унаследованные от первичной группы.
  - **Установленные компоненты** — список антивирусных компонентов, установленных на данной станции.

7.5.10. Экспорт, импорт и распространение конфигураций

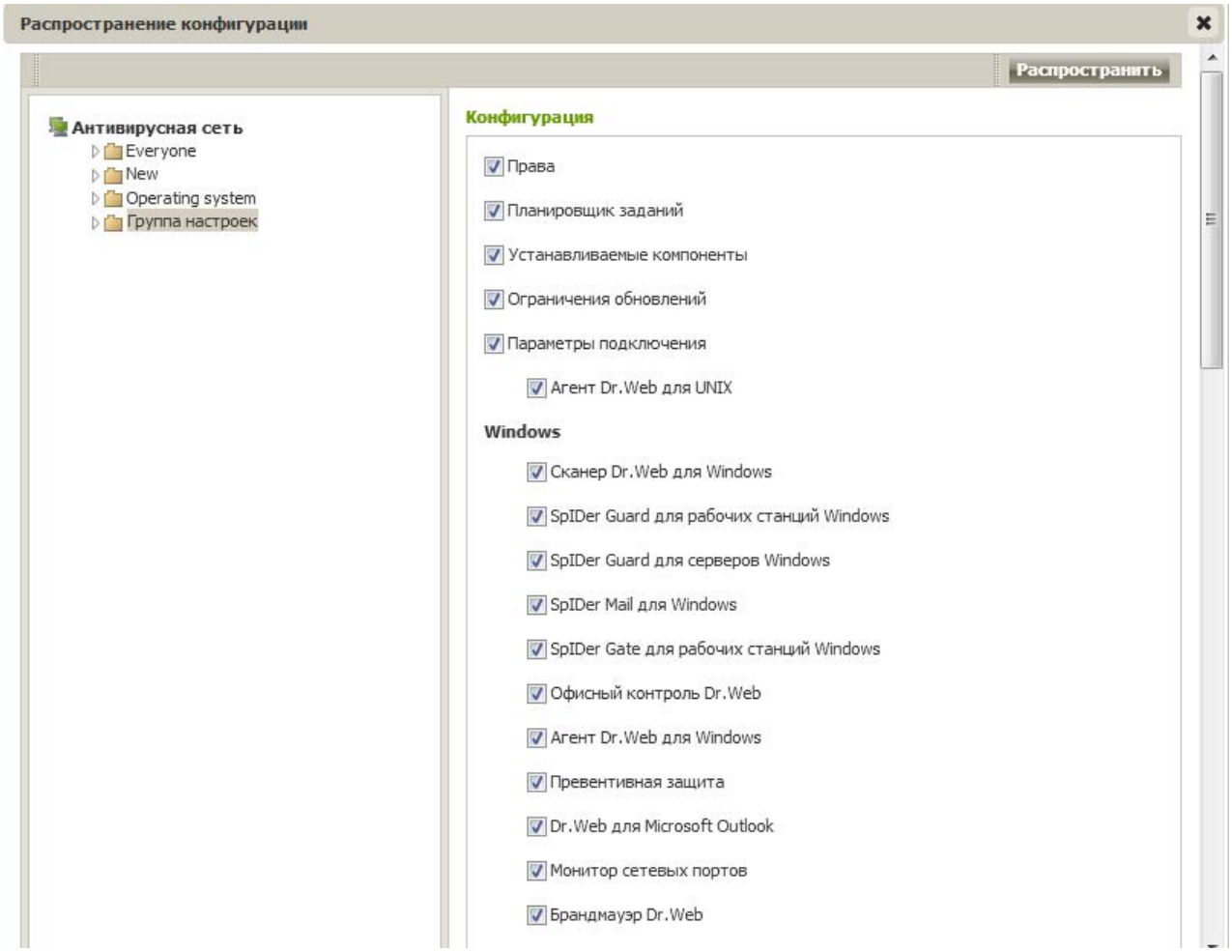
Администратор антивирусной сети имеет возможность экспорта, импорта и распространения конфигурации группы или рабочей станции на другие группы и станции антивирусной сети, что позволяет, в частности, быстро изменять политики, применяя их к определенным группам. Для экспорта конфигурации необходимо выбрать станцию или группу, нажать последовательно кнопки  и  , выбрать сохраняемую информацию и нажать кнопку **Экспорт**.

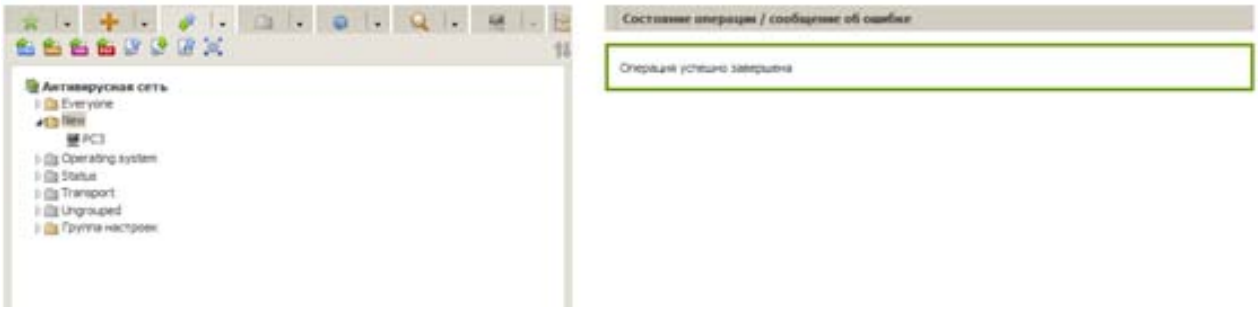


Для импорта необходимой конфигурации выбрать станцию или группу, нажать последовательно кнопки  и  , выбрать файл конфигурации и импортируемую информацию, нажать кнопку **Импорт**.



Для распространения информации на иные группы необходимо выбрать станцию или группу, нажать последовательно кнопки  и  , выбрать распространяемую информацию и указать группу, на которую будет распространена информация, и нажать **Распространить**.





Администратор сети также имеет возможность экспорта и импорта настроек отдельных антивирусных компонентов станции из Центра управления в XML-файл.

7.5.11. Управление группами. Назначение администраторов групп

Управление административными учетными записями осуществляется в меню **Администраторы**, доступном в разделе **Администрирование** главного меню.

Раздел **Администраторы** доступен всем администраторам, но полное иерархическое дерево администраторов доступно только администраторам из группы **Administrators**, для которых установлено право **Просмотр свойств и конфигурации групп администраторов**. Для остальных администраторов в иерархическом дереве будет отображаться только собственная группа и ее подгруппы с входящими в них учетными записями.

Иерархический список администраторов отображает древовидную структуру административных групп и учетных записей администраторов. Узлами данной структуры являются административные группы и входящие в них администраторы. Каждый администратор входит только в одну группу. Уровень вложенности групп не ограничен.

После установки антивирусного сервера автоматически создаются две предустановленные группы: **Administrators** (изначально в группу входит только администратор **admin** с полным набором прав, автоматически создаваемый при установке антивирусного сервера) и **Newbies** — в эту группу автоматически перемещаются администраторы с внешним типом авторизации через LDAP, Active Directory и RADIUS, а изначально она пуста. Администраторам из группы **Newbies** по умолчанию назначаются права только на чтение.

Администраторы с полными правами имеют полный доступ к управлению **Сервером Dr.Web** и антивирусной сетью в целом. Они могут просматривать и редактировать конфигурацию антивирусной сети, а также создавать новые административные учетные записи. Администратор с такими правами также имеет полные права на управление антивирусным ПО на рабочих станциях. При этом они имеют возможность ограничить, вплоть до полного запрета, вмешательство пользователей рабочих станций в управление антивирусным ПО (см. п. 7.5.11.4. Установка или ограничение прав пользователей).

Система административных прав включает следующие возможности управления правами:

- **Назначение прав**

Назначение прав осуществляется при создании администратора или административной группы. Права наследуются от родительской группы, в которую администратор или административная группа помещаются при создании. При создании возможность изменения прав не предоставляется.

- **Наследование прав**

По умолчанию права администраторов и административных групп наследуются от родительской группы, но наследование может быть отключено.

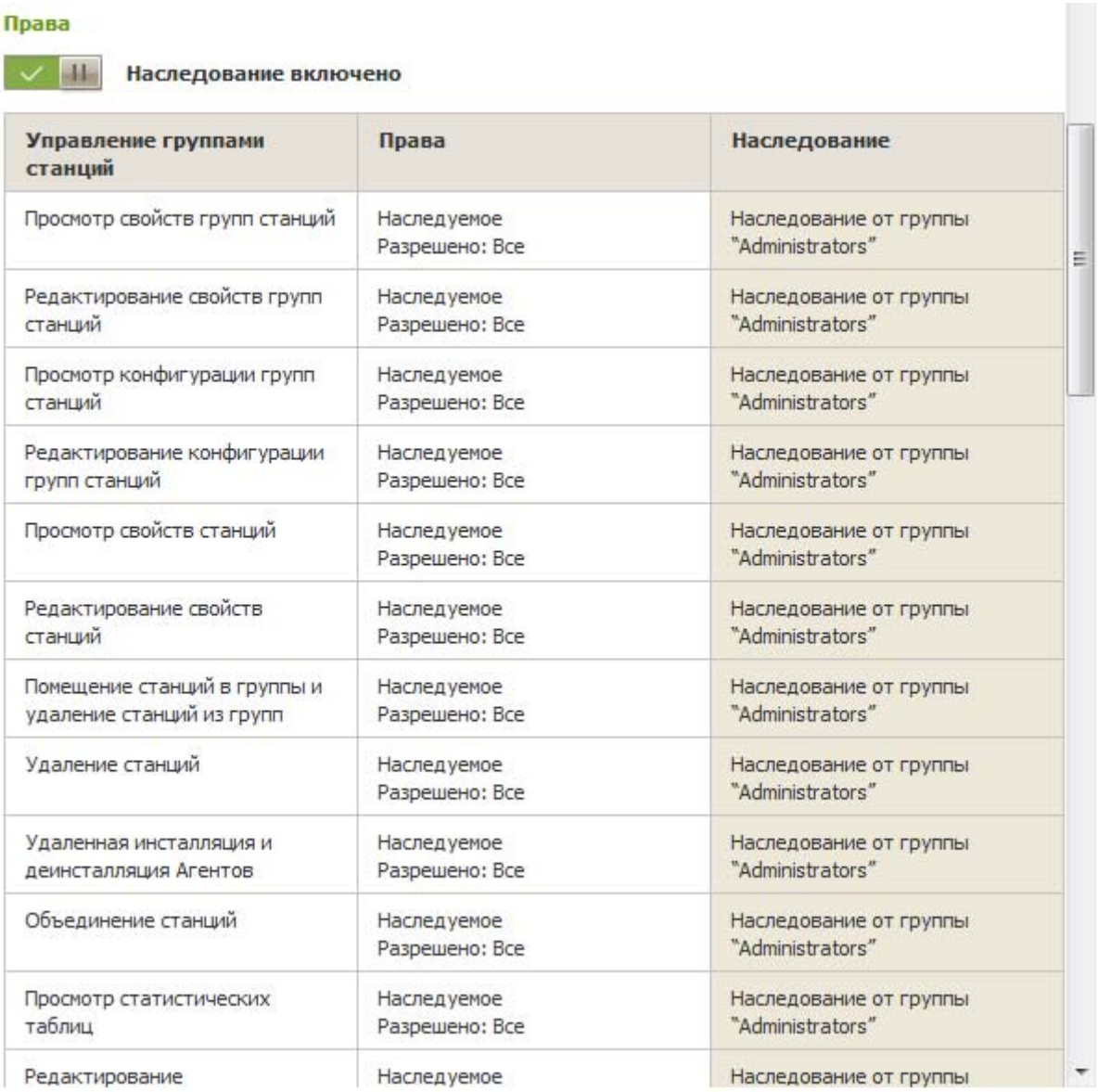
▫Если наследование отключено, администратор использует независимый набор персональных прав, который задается непосредственно для его учетной записи. Права родительской группы при этом не учитываются.

▫При наследовании прав администратора или группы осуществляется не переназначение правами родительской группы, а перерасчет назначенного права исходя из всех прав родительских групп вверх по иерархическому дереву. Таблица для расчета результирующего права объекта в зависимости от назначенных прав и прав родительской групп приведена в п. Объединение прав.

- **Редактирование прав**

При создании администраторов и административных групп возможность редактирования прав не предоставляется. Редактирование прав доступно только для уже созданных объектов и осуществляется в разделе настроек учетной записи или группы. При редактировании собственных настроек допускается только понижение прав. Редактирование прав предустановленного администратора **admin** и предустановленных групп **Administrators** и **Newbies** не предоставляется.

Процедура редактирования прав приведена в разделе Редактирование прав.



При наличии распределенной сети или большого количества групп с различными правами, для каждой из групп может быть назначен отдельный администратор. Администраторы групп имеют доступ ко всем системным группам и к тем пользовательским группам, управление которыми для них разрешено (включая вложенные). Для такого администратора в иерархическом дереве будут отображаться только те группы, к которым он имеет доступ.

Администраторы групп могут обладать как полными правами для редактирования доступных им групп, так и правами «только для чтения».

Администраторы групп не могут просматривать список имеющихся административных учетных записей. Администратор группы может подключиться к Серверу только при помощи Центра управления.

Администратору антивирусной сети для текущего управления антивирусной сетью не требуются администраторские полномочия на компьютерах, включенных в эту антивирусную сеть. Однако удаленная установка и удаление ПО Агента возможны только в локальной сети и требует полномочий администратора в этой сети, а отладка Сервера Dr.Web — полного доступа к каталогу его установки.

Рекомендуется назначать администратором антивирусной сети надежного, квалифицированного работника, имеющего опыт администрирования локальной сети и

компетентного в вопросах антивирусной защиты. Такой сотрудник должен иметь полный доступ к каталогам установки **Сервера Dr.Web**. В зависимости от политики безопасности и кадровой ситуации в организации, администратор антивирусной сети должен иметь полномочия администратора локальной сети либо работать в тесном контакте с таким лицом.

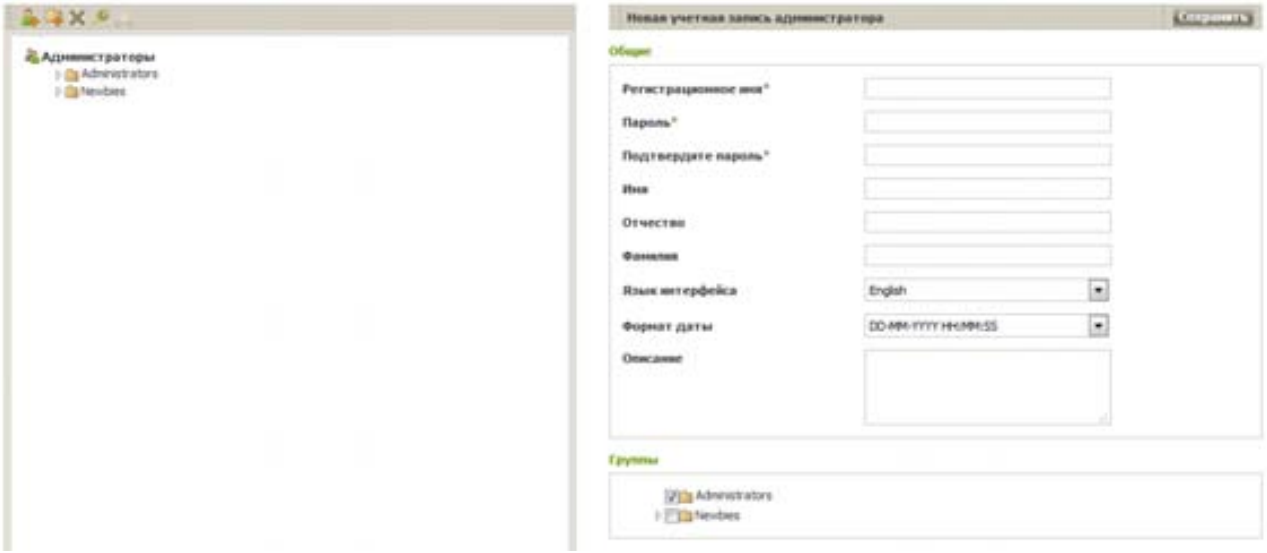
Dr.Web ESS позволяет любому администратору с полными правами редактировать настройки (в том числе имя и п ароль администратора), создавать новые и удалять имеющиеся учетные записи.

По умолчанию, если не было задано другое, Сервер устанавливается с учетной записью администратора с полными правами (с именем **admin** и паролем, который указывается при установке). В случае если установка производилась с параметрами по умолчанию, желательно при первом же входе администратора на Сервер изменить пароль. Также рекомендуется отредактировать описание учетной записи.

Для того чтобы добавить нового администратора, необходимо в разделе **Администрирование → Конфигурация → Администраторы** нажать на кнопку (Создать учетную запись).

Для администраторов групп панель настроек учетной записи открывается сразу при нажатии на пункт **Администраторы**.

В открывшейся слева панели необходимо указать данные администратора.



В поле **Регистрационное имя** задайте регистрационное имя администратора, которое будет использоваться для доступа к Центру управления. Разрешается использовать строчные буквы (a — z), заглавные буквы (A — Z), цифры (0–9), символы «_» и «.».

В списке **Тип авторизации** выберите один из вариантов: **Внутренняя** (авторизация такого администратора в Центре управления осуществляется на основе учетных данных в БД **Dr.Web Server**) или **Внешняя** (авторизация такого администратора в Центре управления осуществляется через внешние системы LDAP, Active Directory или RADIUS).

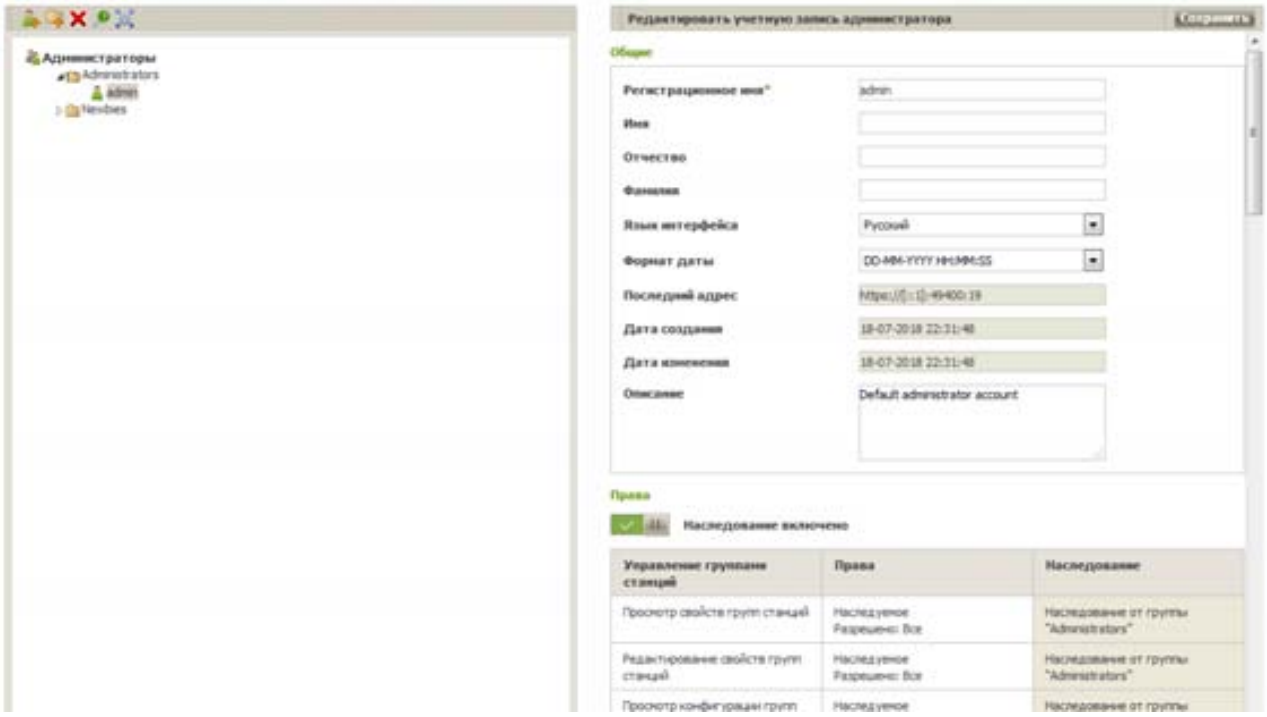
Внимание! Если соответствующие протоколы доступа не заданы для Сервера (в том числе при первичной установке Сервера, пункт **Тип авторизации** будет отсутствовать).

В полях **Пароль** и **Еще раз пароль** задайте пароль для доступа к **Серверу**. После чего при необходимости заполните рабочий информацию: Ф . И. О. сотрудника, язык интерфейса Центра управления для данного администратора, формат даты и уточняющее описание.

В подразделе **Группы** задается родительская административная группа. Напротив группы, для которой будет назначен создаваемый администратор, установлен флажок. По умолчанию создаваемые администраторы размещаются в родительской группе текущего администратора. Чтобы изменить назначенную группу, установите флажок напротив нужной группы. Каждый администратор может входить только в одну группу.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

После заполнения формы нажмите **Сохранить**.



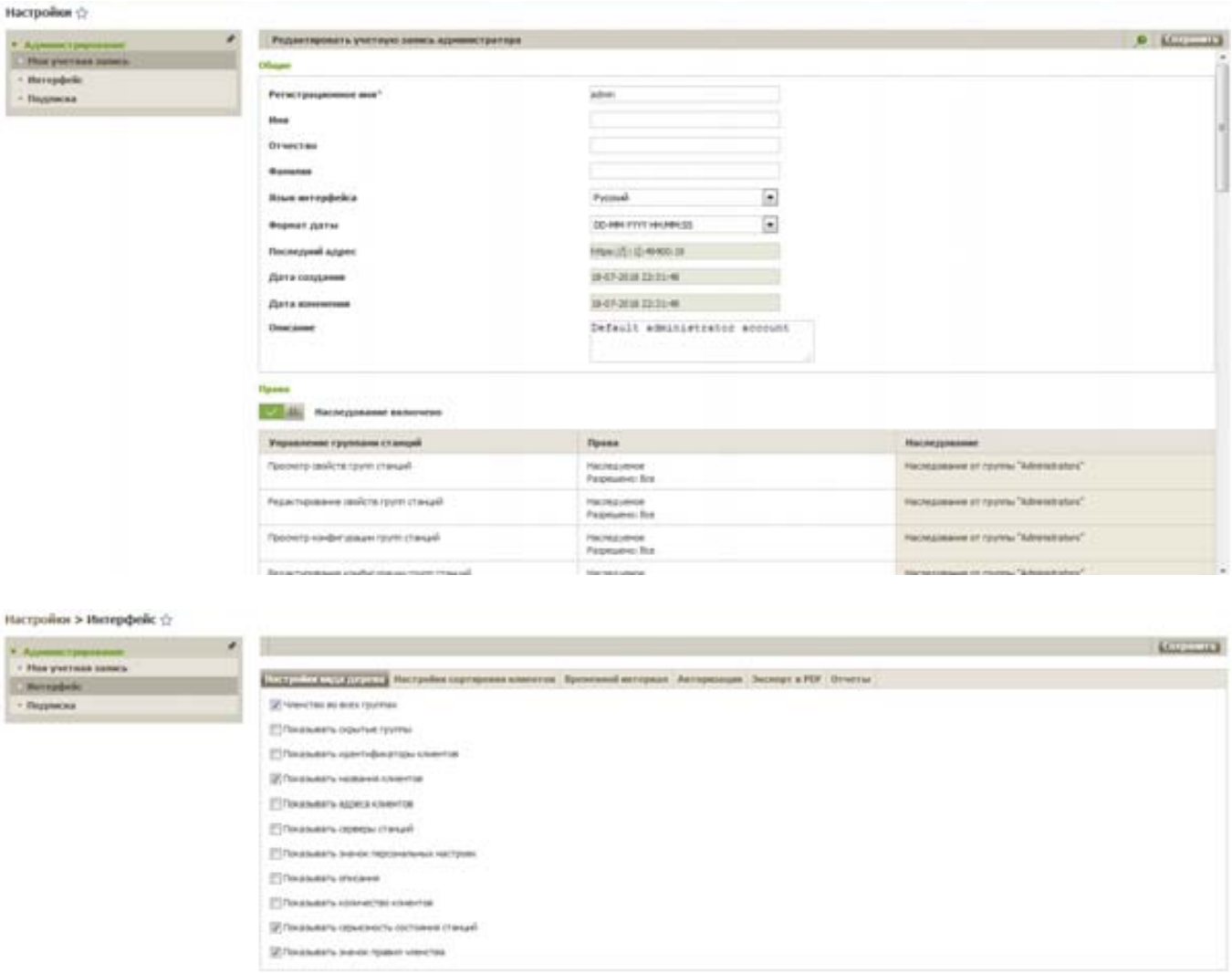
Следующие параметры доступны только для чтения:

- Даты создания учетной записи и последнего изменения ее параметров.
- Последний адрес — отображает сетевой адрес последнего подключения под данной учетной записью.

Для того чтобы удалить учетную запись, выберите ее в списке, после чего на панели инструментов нажмите значок **Удалить выбранные объекты**.

Для изменения пароля для доступа к учетной записи нажмите на значок **Новый пароль**.

Дополнительные настройки могут быть также заданы в меню **Настройки** соответствующей учетной записи.



7.5.11.1. Аутентификация администраторов

Подключение администраторов через внешние системы авторизации будет невозможно, если на **Сервере** уже существует администратор с таким же регистрационным именем.

Аутентификация администратора для подключения к Серверу Dr.Web возможна следующими способами:

- С хранением данных об администраторах в БД Сервера.
- С помощью настроек LDAP/AD, позволяющих подключение к серверам LDAP и Active Directory.
- С использованием RADIUS-протокола.
- С использованием PAM (только под ОС семейства UNIX).

При обновлении Сервера с предыдущей версии также могут быть доступны следующие типы аутентификации (если они были включены в предыдущей версии):

После отключения данных типов аутентификации их разделы будут исключены из настроек Центра управления.

При первичной установке Сервера данные разделы не предоставляются.

- С помощью Active Directory (в версиях Сервера для ОС Windows).
- С использованием LDAP-протокола.

Методы аутентификации используются последовательно согласно следующим принципам:

Первой всегда осуществляется попытка аутентификации администратора из БД Сервера.

Порядок использования методов аутентификации через внешние системы зависит от порядка их следования в настройках, задаваемых в Центре управления.

Методы аутентификации через внешние системы по умолчанию отключены.

7.5.11.1.1. Изменение порядка аутентификации администраторов

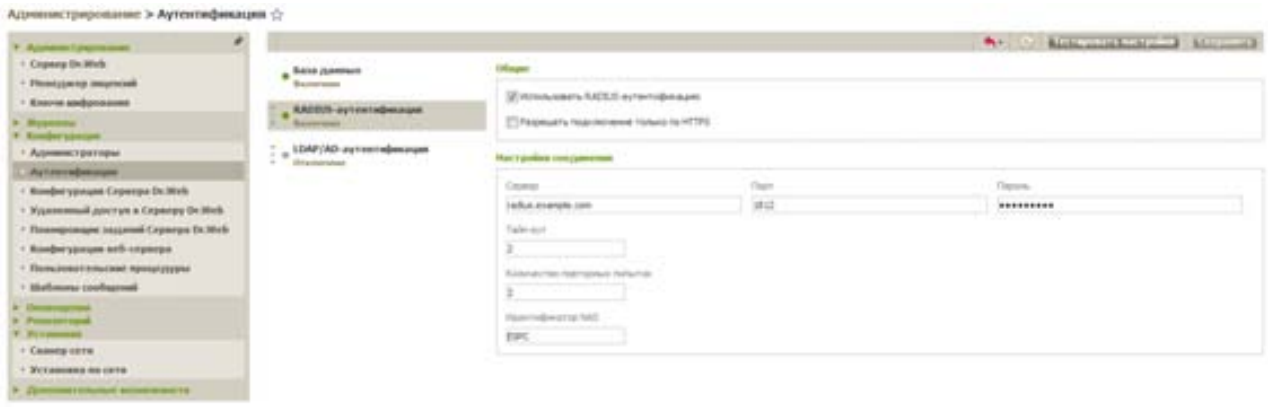
Для управления списком администраторов, данные о которых сохранены в БД антивирусного сервера, выберите **Администрирование → Конфигурация → Администраторы**. Откроется список всех зарегистрированных на Сервере администраторов. Подробная информация о порядке управления правами администраторов описана в разделе «Управление учетными записями администраторов и административными группами» документа Руководство администратора.

Внимание! В настройках Сервера методы аутентификации отдельно через LDAP и Active Directory присутствуют только при обновлении Сервера с предыдущих версий, при чистой установке сервера доступна единая LDAP/AD-аутентификация.

Методы идентификации RADIUS и LDAP/AD можно поменять местами, но первой всегда осуществляется попытка аутентификации администратора из БД. Для изменения порядка использования авторизации сделайте следующее.

Внимание! При аутентификации администраторов из Active Directory в **Центре управления** настраивается только разрешение использования данного метода аутентификации. Редактирование свойств администраторов Active Directory осуществляется вручную на сервере Active Directory.

1. В управляющем меню **Администрирование** выберите раздел **Авторизация**.



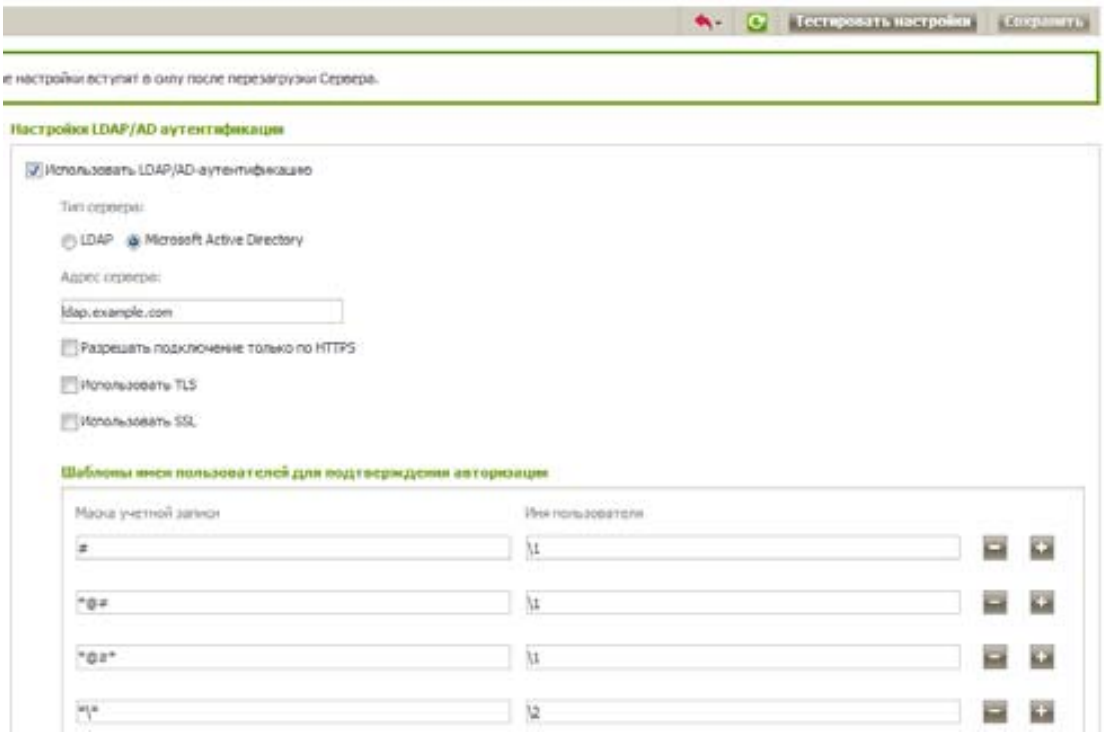
2. В открывшемся окне представлен список типов авторизации в том порядке, в котором они используются. Для изменения порядка следования перетащите (drag-and-drop) методы авторизации в списке и разместите их в таком порядке, в каком необходимо проводить авторизацию, или воспользуйтесь стрелками слева от них.
3. Для применения внесенных изменений перезапустите антивирусный сервер.

Нажмите и подтвердите выбор.

Для включения аутентификации с использованием Active Directory (параметр доступен только при обновлении с более ранних версий Сервера, при чистой установке параметр на доступен):

1. В меню **Администрирование** выберите раздел **Авторизация**.
2. В открывшемся окне зайдите в раздел **Microsoft Active Directory** и установите флажок **Использовать авторизацию Microsoft Active Directory**.

Проверить правильность настроек авторизации можно, нажав на кнопку **Тестировать настройки**. Функция доступна для тестирования настроек авторизации внешних администраторов Active Directory, LDAP, LADP/AD и RADIUS.



3. Нажмите **Сохранить**.
4. Для применения внесенных изменений перезапустите Сервер.

7.5.11.1.2. Редактирование свойств администраторов Active Directory

При аутентификации администраторов из Active Directory в Центре управления настраивается только разрешение использования данного метода аутентификации.

Редактирование свойств администраторов Active Directory осуществляется вручную на сервере Active Directory.

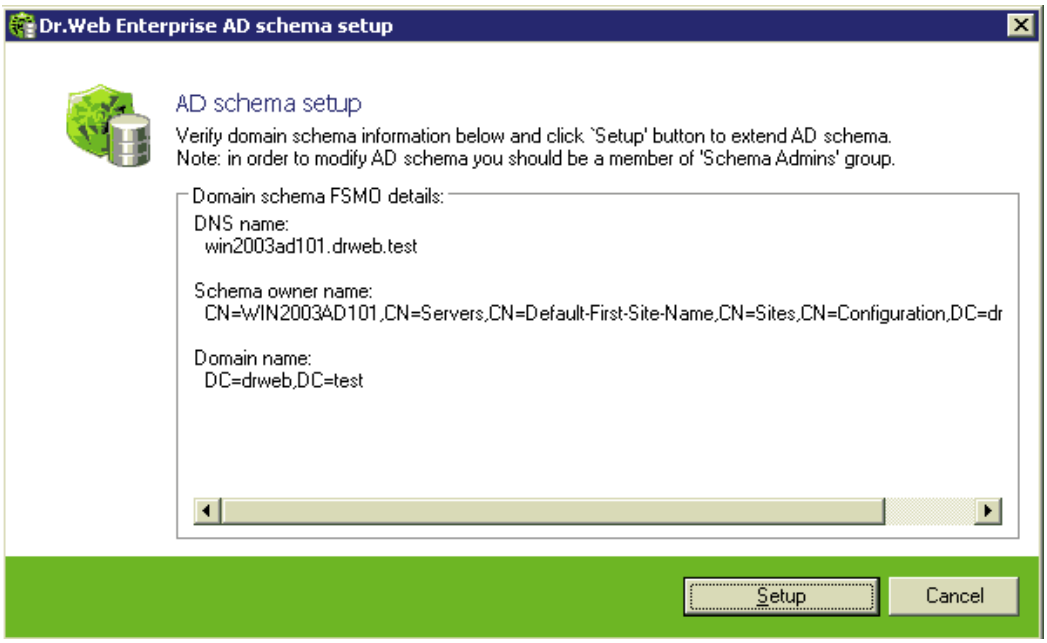
Внимание! Все операции необходимо выполнять на ПК, где присутствует оснастка для администрирования Active Directory.

Для получения возможности редактирования параметров администраторов Active Directory необходимо выполнить следующие операции.

1. Для модификации схемы Active Directory запустите утилиту *drweb-11.00.0-<сборка>-esuite-modify-ad-schema-<версия_ОС>.exe,* которую необходимо скачать с сайта «Доктор Веб» с помощью Мастера скачиваний по лицензионному ключу. Утилита создает новый класс объектов DrWebEnterpriseUser для Active Directory и описывает новые атрибуты для данного класса. Модификация схемы Active Directory может занять некоторое время.

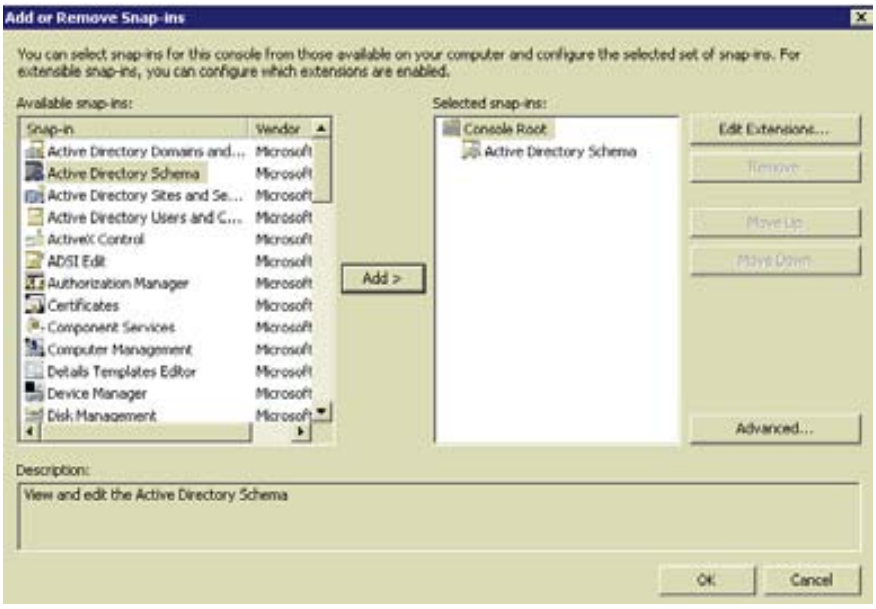
Примечание. Если ранее была произведена модификация схемы Active Directory с использованием данной утилиты от Сервера версии 6, нет необходимости повторно выполнять модификацию с использованием утилиты от версии Сервера 11.0.

В зависимости от конфигурации вашего домена для синхронизации и применения модифицированной схемы может потребоваться до 5 минут и более.

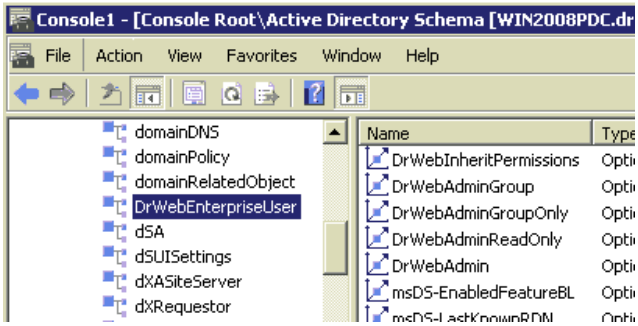


2. Для регистрации оснастки Active Directory Schema (Схема Active Directory) выполните с административными полномочиями команду *regsvr32 schmmgmt.dll*, после чего выполните команду *mmc* (вызов Консоли управления Windows) и добавьте оснастку Active Directory Schema.
3. Используя добавленную оснастку Active Directory Schema, добавьте к классу User и (если необходимо) к классу Group вспомогательный класс DrWebEnterpriseUser.

   Для этого запустите оснастку, выполнив команду mmc, откройте меню File и выполните команду Add/Remove Snap-in…. В левом списке доступных выберите **Active Directory Schema**, нажмите кнопку **Add** и затем **OK**.

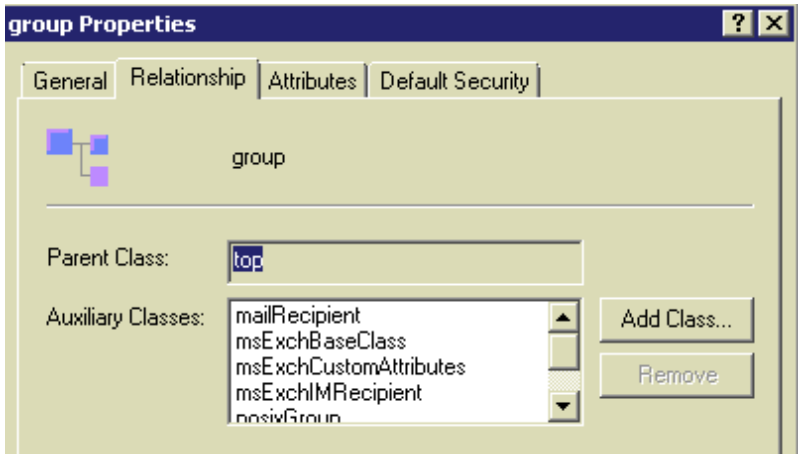


Проверьте в списке доступных классов DrWebEnterpriseUser.



Если применение модифицированной схемы еще не завершилось, класс DrWebEnterpriseUser может быть не найден. В таком случае подождите некоторое время и повторите попытку.

Выберите последовательно классы **User** и **Group** и откройте их свойства. На закладке **Relationship** нажмите **AddClass** и выберите **DrWebEnterpriseUser**.



4. С административными полномочиями запустите файл *drweb-11.00.0-<сборка>-esuite-aduac-<версия_ОС>.msi* и дождитесь окончания установки.

Графический интерфейс для редактирования атрибутов доступен на панели управления Active Directory **Users and Computers → Users** в окне редактирования свойств выбранного пользователя **Administrator Properties →** на вкладке **Dr.Web Authentication**.

Для редактирования доступны следующие параметры (значение каждого атрибута может быть **yes**, **no** или **not set**):

- **User is administrator** — указывает на то, что пользователь является полноправным администратором.
- **Inherit permissions from groups** — параметр, разрешающий наследование значений для остальных параметров из групп пользователя. Если какой-либо параметр (или несколько параметров) принимают значение **not set** и для **Inherit permissions from groups** указано значение **yes**, то значения незаданных параметров наследуются от групп, в которые входит данный пользователь.

Алгоритмы принципа работы и разбора атрибутов при авторизации приведены в Приложении С1.

7.5.11.2. Настройки группы. Использование групп для настройки рабочих станций

Сразу после установки все группы и рабочие станции имеют единые настройки, заданные по умолчанию (эти настройки наследуются от группы Everyone). В дальнейшем вы можете установить разные настройки для разных ОС, изменив настройки соответствующих групп. Вы также можете изменять настройки новых (созданных вами) групп.

Чтобы задать настройки группы (настройки по умолчанию рабочих станций группы):

1. Выберите группу в каталоге сети.
2. Выберите нужную настройку в управляющем меню Центра управления и отредактируйте ее.

Настройки группы включают конфигурацию антивирусных средств, родительской группы (для вложенных групп), расписание и настройку прав пользователей. Настройка прав аналогична настройке прав отдельных рабочих станций, описанной в п. 7.5.11.4. Установка или ограничение прав пользователей.

Настройки Агента входят в конфигурацию группы и, следовательно, могут быть заданы через механизм групп.

Администратор может задавать в параметрах группы состав компонентов антивирусного пакета. Данные настройки будут наследоваться всеми станциями, для которых группа является первичной. Для всех создаваемых станций будет производиться установка только тех антивирусных компонентов, которые указаны в настройке первичной группы.

Как для отдельной группы, так и для нескольких выбранных групп вы можете запускать, просматривать и прекращать задания на сканирование, просматривать статистику (в том числе по угрозам, запуску/завершению, ошибкам сканирования и установки) и суммарную статистику для всех рабочих станций группы или нескольких групп.

При просмотре или редактировании элементов конфигурации рабочей станции, унаследованных от первичной группы, в соответствующих окнах отображается информация о том, что данная настройка унаследована от первичной группы станции.

Если вы измените конфигурацию рабочей станции, то станция получит персональную настройку и указанная надпись исчезнет. Вы можете восстановить конфигурацию, унаследованную от первичной группы; для этого выберите нужную станцию в древе групп и станций и нажмите кнопку **Удалить персональные настройки** на панели инструментов Центра управления.

7.5.11.3. Наследование элементов конфигурации рабочей станции. Первичные группы

При создании новой рабочей станции элементы ее конфигурации заимствуются от одной из групп, в которую она входит. Такая группа называется первичной. При изменениях в настройках первичной группы они автоматически наследуются входящими в нее станциями, за исключением случаев, когда станции были заданы персональные настройки. При создании станции вы можете указать, какая из групп будет считаться первичной, по умолчанию это Everyone.

Если первичная группа не Everyone и у указанной первичной группы нет персональных настроек, также наследуются настройки группы Everyone.

Возможно создание вложенных групп, в которых, если для станции не заданы персональные настройки, наследование элементов конфигурации осуществляется в соответствии со структурой вложенных групп. Поиск осуществляется вверх по иерархическому древу, начиная с первичной группы станции, ее родительской группы и далее до корневого элемента древа. Если при этом не были обнаружены персональные настройки, то наследуются элементы конфигурации группы Everyone.

Например, структура иерархического списка представляет собой следующее дерево:

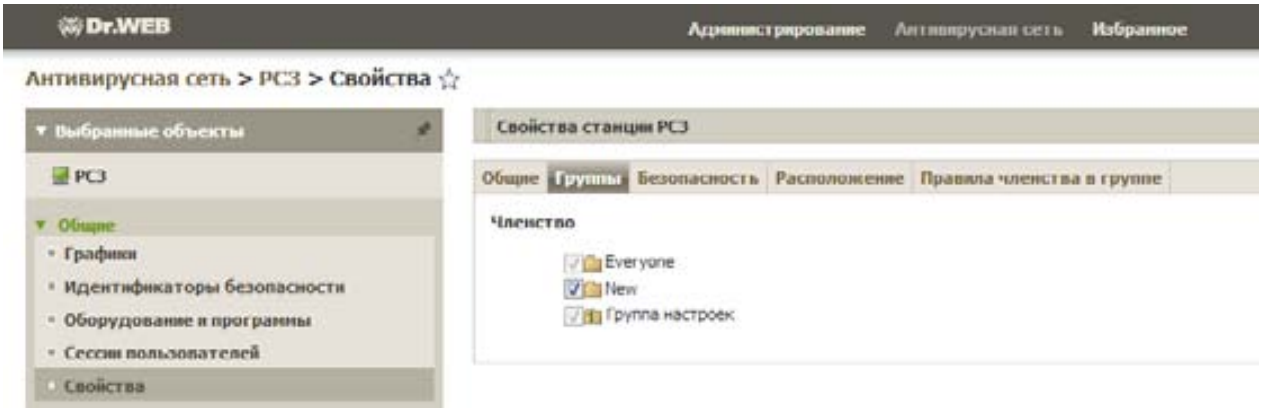
Группа Group4 является первичной для станции Station1. При этом при наследовании настроек станцией Station1 будет осуществляться поиск настроек в следующем порядке: Station1 → Group4 → Group3 → Group2 → Group1 → Everyone.

Задание первичной группы

Существует несколько способов задания первичной группы для рабочей станции и группы рабочих станций.

Чтобы установить первичную группу для рабочей станции:

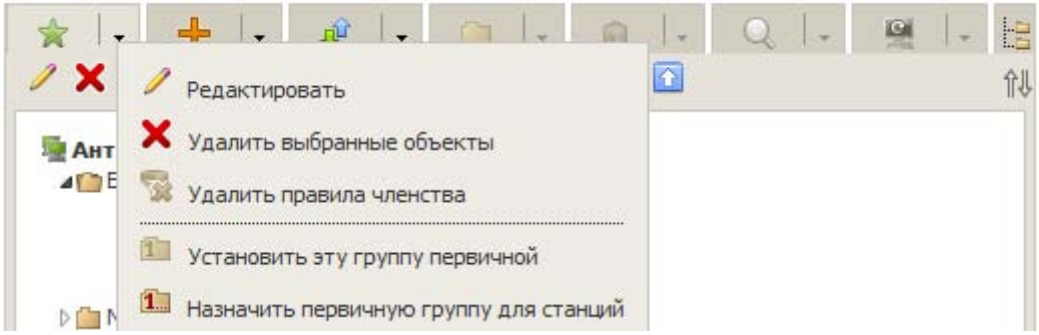
1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции. В открывшемся управляющем меню (панель слева) выберите пункт **Общие → Свойства → Группы**.



2. Для назначения первичной группы для станции, щелкните по имени группы, на ее значке появится цифра «1», это будет означать, что данная группа назначена первичной для станции.
3. Нажмите **Сохранить**.

Чтобы установить первичную группу для нескольких рабочих станций:

1. Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название нужных станций (можно также выбирать группы — при этом действие будет распространено на все входящие в них станции), для выбора нескольких станций и групп можно воспользоваться выделением мышью при нажатых клавишах CTRL или SHIFT.
2. На панели инструментов нажмите **Общие → Назначить первичную группу для станций**. Откроется окно со списком групп, которые могут быть назначены первичными для этих станций.



3. Для указания первичной группы нажмите на название группы.

Вы можете сделать группу первичной для всех входящих в нее рабочих станций. Для этого выберите нужную группу в каталоге, после чего на панели инструментов Центра управления нажмите **Общие → Установить эту группу первичной**.

По умолчанию структура сети представлена таким образом, чтобы продемонстрировать вхождения станций во все группы, членом которых она является. Если вы хотите отображать в каталоге сети членство станций только в первичных группах, на панели инструментов Центра управления в пункте **Настройки вида дерева** снимите флажок **Членство во всех группах**.

7.5.11.4. Установка или ограничение прав пользователей

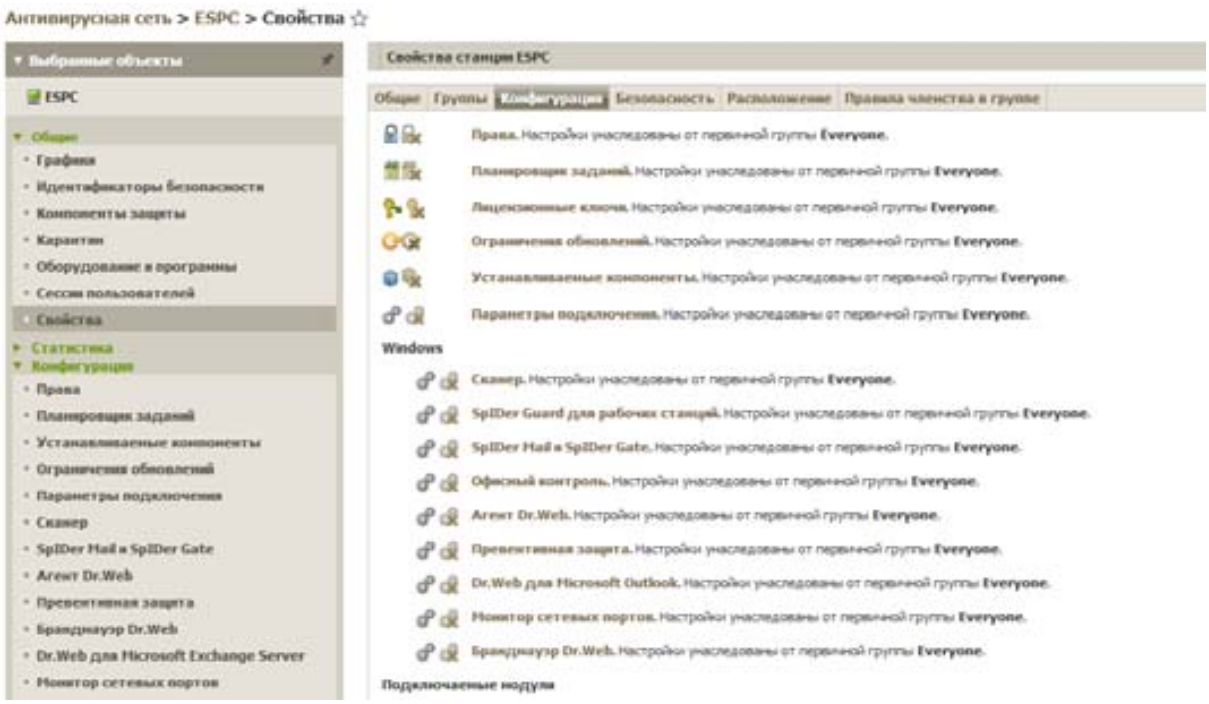
Внимание! Для того чтобы пользователь Сервера Dr.Web имел возможность изменить настройки Агента на станции или в группе, он должен быть администратором данной группы с правами на запись.

Для облегчения управления групповыми политиками на Сервере Dr.Web присутствует возможность управлять пользовательскими правами на запуск, конфигурирование и остановку различных компонентов антивируса.

Рабочие станции наследуют права от первичной группы, однако вы можете не только изменить настройки прав группы в целом, но и рабочей станции в частности.

Для того чтобы настроить права пользователей рабочей станции, выделите ее в дереве станций и нажмите кнопку (**Редактировать**). В левом меню выберите **Свойства**, чтобы получить доступ к группам настроек: **Общие**, **Группы**, **Конфигурация**, **Безопасность**, **Расположение**, **Правила членства в группе**. Их содержание и настройка описаны ниже.

Для сохранения изменений необходимо нажать кнопку **Сохранить**.



В разделе **Общие** приведены следующие поля, доступные только для чтения:

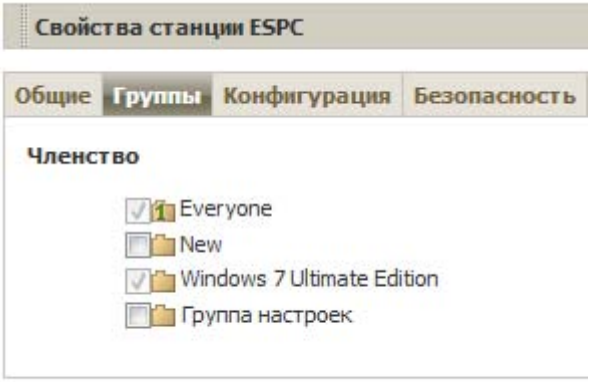
- **Идентификатор** — уникальный идентификатор станции.
- **Название** — название станции.

Также вы можете задать значения следующих полей:

- В поле **Пароль** — пароль для авторизации станции на Сервере (необходимо повторить тот же пароль в поле **Еще раз пароль**). При смене пароля, для возможности подключения Агента, аналогичную процедуру необходимо произвести в настройках соединения Агента на станции.
- В поле **Описание** — добавить дополнительную информацию.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.

В разделе **Группы** настраивается список групп, в которые входит данная рабочая станция. В списке **Членство** перечислены все группы, в которые входит рабочая станция и в которые ее можно включить.



Для управления членством рабочей станции необходимо:

1. Для добавления станции в пользовательскую группу установите флажок напротив этой группы в списке **Членство**.

2. Для удаления рабочей станции из пользовательской группы снимите флажок напротив этой группы в списке **Членство**.

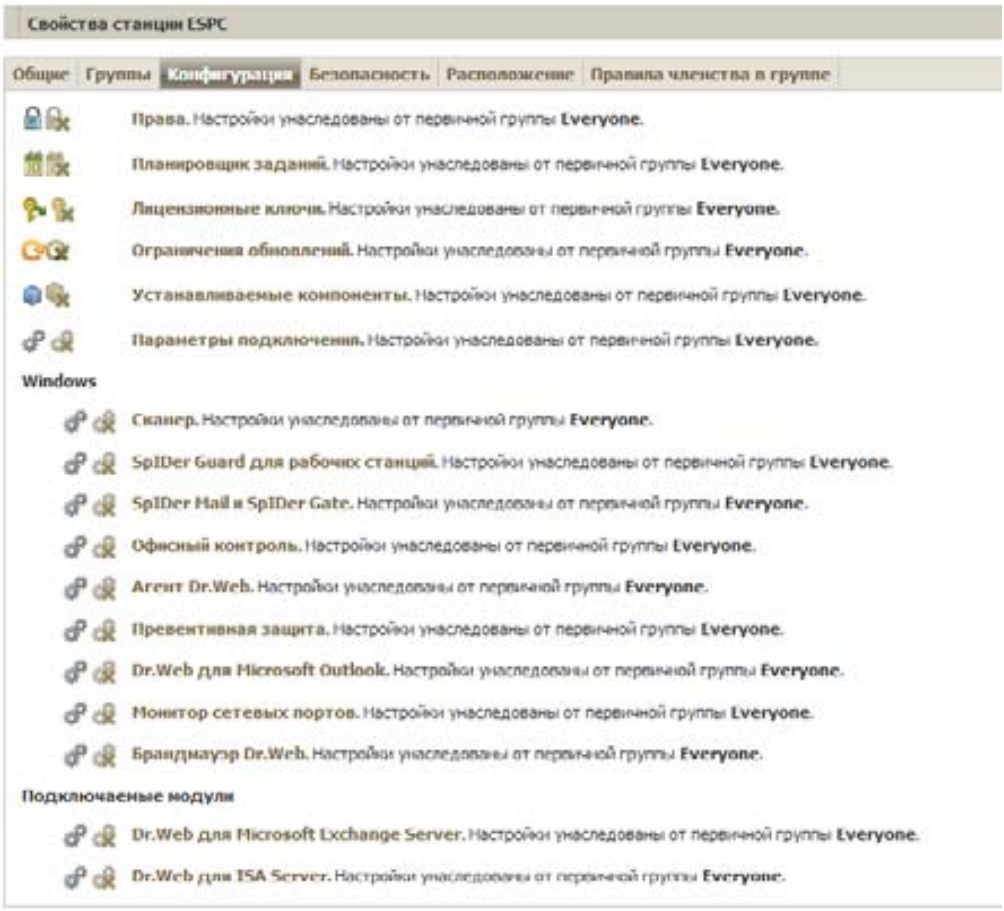
Примечание. Удаление станций из предустановленных групп невозможно.

3. При необходимости назначить другую первичную группу нажмите на значок нужной группы в списке **Членство**. При этом на значке группы появится **1**.

В разделе **Конфигурация** вы можете изменить конфигурацию станций, которая включает:

Значок	Настройки	Раздел с описанием
	Права пользователей станции	Права пользователей станции
	Централизованное расписание запуска заданий на рабочей станции	Расписание заданий рабочей станции
	Лицензионные ключи для станции	Лицензионные ключи
	Ограничения при распространении обновлении антивирусного ПО	Ограничение обновлений рабочих станций
	Список устанавливаемых компонентов	Устанавливаемые компоненты антивирусного пакета
	Настройки компонентов антивирусного пакета для данной станции	Настройка антивирусных компонентов

При изменении настроек SpIDer Gate и/или Офисного контроля необходимо учитывать, что настройки данных компонентов взаимосвязаны, поэтому, если были удалены персональные настройки одного из них при помощи кнопки **Удалить персональные настройки**, то также будут удалены настройки второго компонента (устанавливается наследование настроек от родительской группы).



Здесь же находятся настройки всех компонентов антивирусного пакета на станции, включая Агент Dr.Web и подключаемые модули антивируса. Для изменения настроек нажмите на кнопку напротив соответствующего компонента.

Для каждого параметра из перечисленных выше доступна кнопка удаления персональных настроек. Она расположена справа от соответствующей кнопки настройки конфигурации. При удалении персональной конфигурации рабочей станции вновь будет установлена конфигурация, унаследованная от первичной группы.

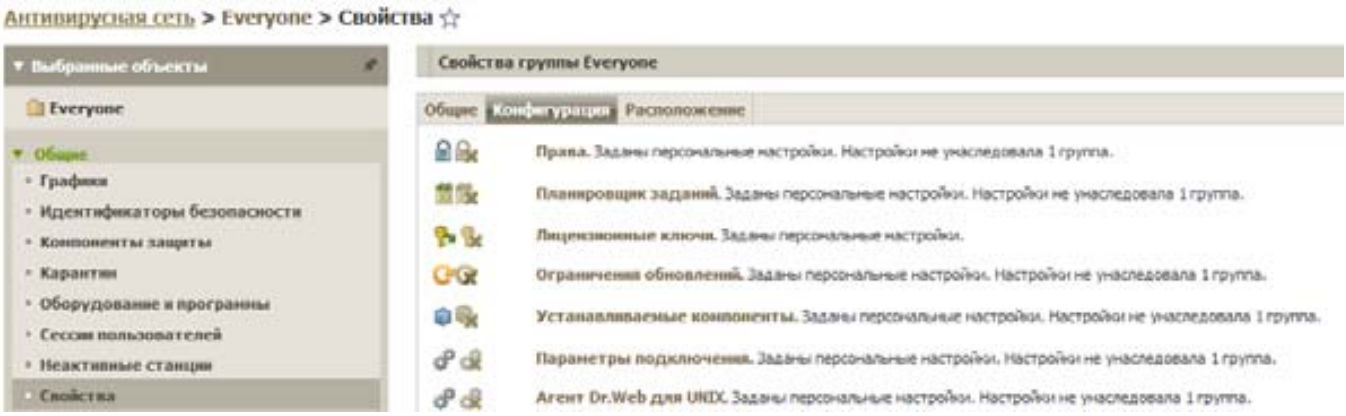
Состав параметров компонентов и рекомендации по их настройке содержатся в Руководстве пользователя Dr.Web для Windows.

Также определить состав компонентов защиты и права по управлению их настройками можно, используя пункт меню в пункте меню **Конфигурация → Права**.

В появившемся окне системный администратор может задать, какие действия над компонентами антивируса будут разрешены или запрещены для данной группы.

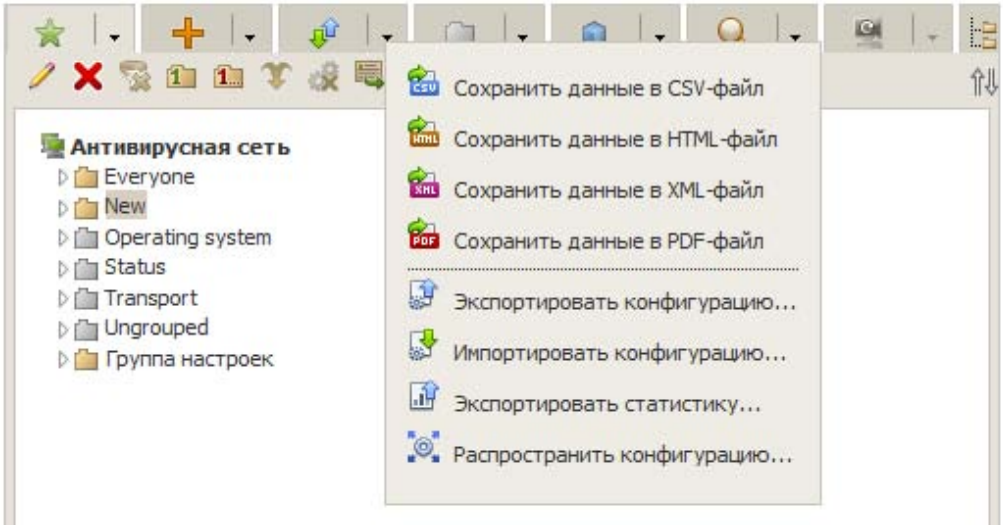
При отключении какого-либо из пунктов, отвечающих за изменение настроек Агента, будет использоваться значение, которое было задано для данной настройки в последний раз перед отключением.

Для того чтобы отказаться от данной конфигурации прав и вернуться к конфигурации по умолчанию, унаследованной от предустановленных групп, нажмите в разделе **Общие → Свойства → Конфигурация** на кнопку **Удалить эти настройки**.



Для того чтобы принять сделанные изменения прав, нажмите на кнопку **Сохранить**.

Задав свойства для одной группы или станции, вы можете импортировать их в файл или распространить на другой объект. Для этого выберите исходный объект в дереве раздела Антивирусная сеть и укажите необходимое действие в меню **Экспортировать данные** ( ).



Чтобы экспортировать настройки в файл, выберите в списке нужный формат, например CSV.

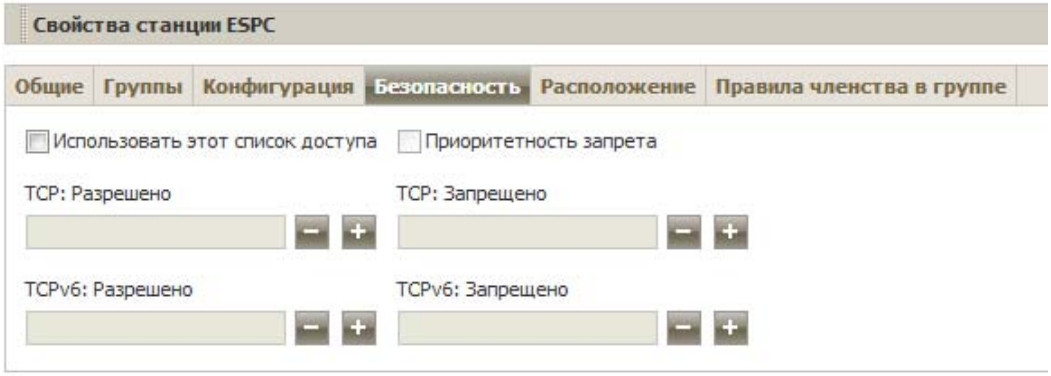
Управление настройками через Центр управления имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса:

- чтобы изменить значения параметров, принимающих значения **Да** или **Нет**, щелкните по соответствующему значению; поля ввода и выпадающие списки имеют стандартный интерфейс;
- для управления отдельными параметрами используйте кнопки, расположенные справа от соответствующих настроек:
  - восстановить значение, которое параметр имел до редактирования,
  - установить для параметра значение по умолчанию;
- для управления совокупностью параметров используйте наборы кнопок вида 

на панели инструментов (правая верхняя часть большинства окон настроек, например **Параметры подключения**, компоненты антивируса и т. д.):
  - распространить данные настройки на другие объекты (группу или несколько групп и рабочих станций,
  - восстановить значения, которые все параметры имели до редактирования,
  - установить для всех параметров значения по умолчанию,
  - экспортировать параметры в файл с указанием формата,
  - импортировать параметры из файла указанного формата,

- для Центра управления — удалить заданную конфигурацию для данной рабочей станции (при этом вновь будет установлена унаследованная от групп конфигурация, см. п. 7.5.4. Настройки группы. Использование групп для настройки рабочих станций. Настройки полномочий пользователей).
- Сохранить — сохраняет все внесенные изменения.

В разделе **Безопасность** задаются ограничения на сетевые адреса, с которых разрешен доступ к данной станции.



Чтобы разрешить все соединения, снимите флажок **Использовать этот список доступа** для настройки списка разрешенных и запрещенных адресов, укажите адреса ниже и установите данный флажок.

Для того чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.

Для того чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.

Для добавления адреса в список:

1. Введите сетевой адрес в соответствующее поле и нажмите на кнопку **Сохранить**.
2. Для добавления нового поля адреса нажмите на кнопку соответствующего раздела. Для удаления поля — на кнопку .

Сетевой адрес задается в виде: <IP-адрес>/[<префикс>].

Пример использования префикса:

> Префикс 24 обозначает сети с маской 255.255.255.0 — содержит 254 адреса, адреса хостов в этих сетях вида: 195.136.12.*
>
> Префикс 8 обозначает сети с маской 255.0.0.0 — содержит до 16387064 адресов (256*256*256), адреса хостов в этих сетях вида: 125.*.*.*

Вы можете удалять адреса из списка и редактировать внесенные в список адреса.

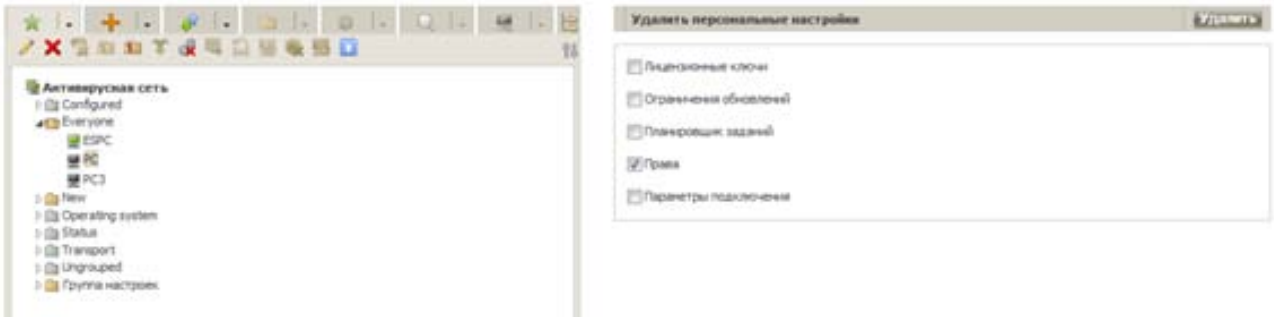
Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от установки флажка **Приоритетность запрета**: при его включении адреса, не внесенные ни в один из списков (или внесенные в оба), запрещаются. В противном случае такие адреса разрешаются.

В разделе **Расположение** задаются параметры географического местоположения станции.

Можно создавать различные группы пользователей по признаку, какие права и настройки для них оптимальны. Задание основных параметров работы станций через группы позволит вам сэкономить усилия по редактированию настроек каждой отдельной станции.

Чтобы удалить персональные настройки станции:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке выберите станцию и нажмите на панели инструментов ★**Общие → Удалить персональные настройки**. Откроется список настроек станции, персональные будут отмечены флажками.



2. Снимите флажки с настроек, которые необходимо удалить и нажмите **Удалить**. Настройки станции, унаследованные от первичной группы по этим параметрам, будут восстановлены.

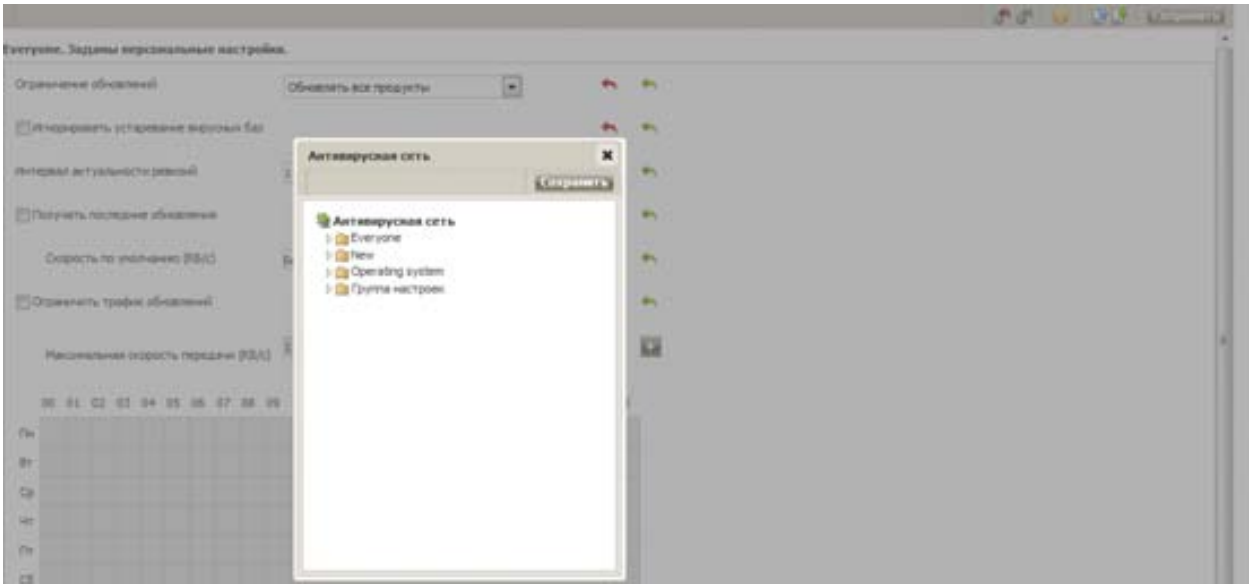
При редактировании конфигурации рабочей станции для компонентов SpIDer Guard для Windows, а также Сканер для Windows ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows версий: Server 2003/2008, 2000, Vista, 7. Статья, содержащая необходимую информацию, находится по адресу http://support.microsoft.com/kb/822158/ru. Материал, изложенный в статье, поможет оптимизировать производительность системы при работе с антивирусом.

Если на момент редактирования настроек рабочей станции она не подключена к Серверу, то настройки будут приняты, как только Агент восстановит связь с Сервером.

7.5.11.5. Распространение настроек, в том числе на станции, которые недоступны в момент настройки.

Настройки конфигурации антивирусных средств, расписаний и прав пользователей группы или рабочей станции могут быть скопированы (распространены) на группу или несколько групп и рабочих станций. Это можно сделать для всех наборов параметров, находящихся в меню **Конфигурация** группы или рабочей станции.

Для этого в соответствующем окне нажмите на кнопку **Распространить эти настройки на другой объект** (ее вид будет меняться в зависимости от того, какие настройки вы хотите распространить, общим будет наличие зеленой стрелки, например: ). Откроется окно каталога сети, в котором нужно выбрать группы и станции, на которые необходимо распространить настройки.



Для принятия произведенных изменений нажмите кнопку **Сохранить**.

7.5.11.6. Изменение отображения скрытых групп

По умолчанию в Центре управления выключено отображение групп, не содержащих в данный момент станций, что неудобно для первичной настройки. Для включения отображения таких групп перейдите в раздел **Настройки → Интерфейс** и установите флажок **Показывать скрытые группы**, после чего нажмите кнопку **Сохранить**.

7.6. Управление параметрами защиты рабочих станций и серверов Windows

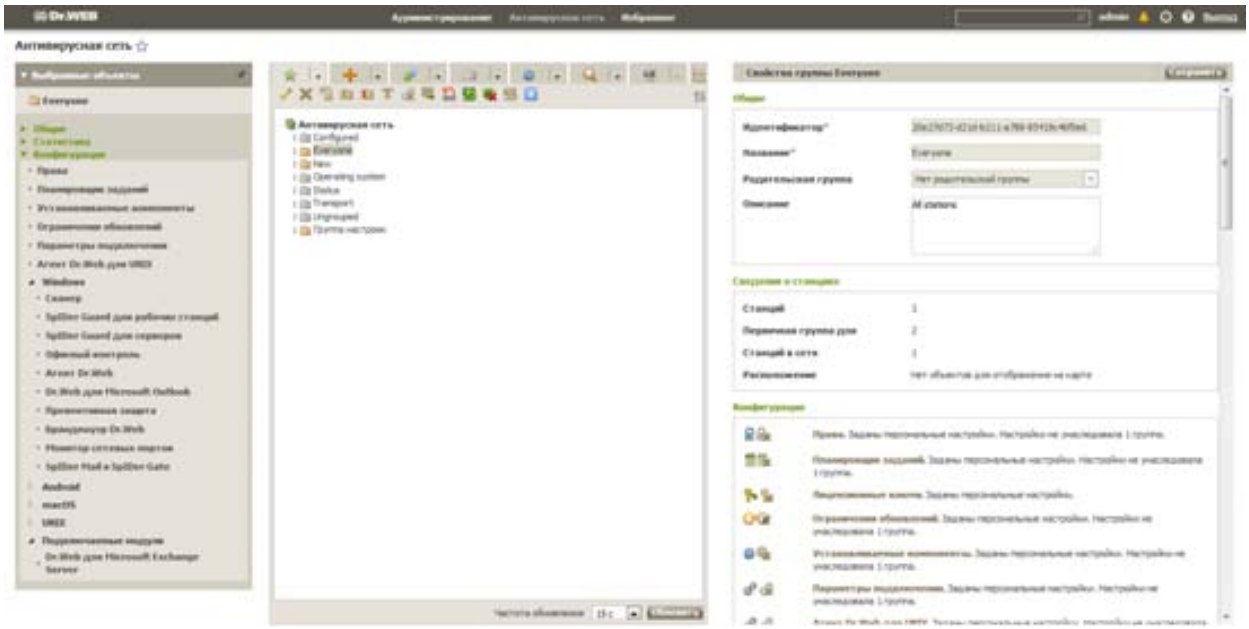
Антивирусная сеть, работающая под управлением **Dr.Web ESS**, позволяет централизованно:

- настраивать конфигурационные параметры антивирусных средств,
- настраивать расписание запуска заданий на сканирование,
- запускать отдельные задания на рабочих станциях, независимо от настроек расписания,
- запускать процесс обновления антивирусного ПО на рабочих станциях, в том числе после ошибки обновления со сбросом состояния ошибки.

При этом администратор антивирусной сети может сохранить за пользователем рабочей станции права на самостоятельную настройку конфигурации и запуск заданий, запретить эти действия или в значительной мере их ограничить.

Изменения в конфигурацию рабочей станции можно вносить даже тогда, когда она временно недоступна для Сервера. Эти изменения будут приняты рабочей станцией, как только ее связь с Сервером восстановится.

Для управления защитой рабочих станций необходимо переключиться в меню **Антивирусная сеть**. Центральная часть открывшегося окна содержит список доступных для управления групп. Раскрыть группу и просмотреть список входящих в нее станций вы можете, кликнув по имени группы.

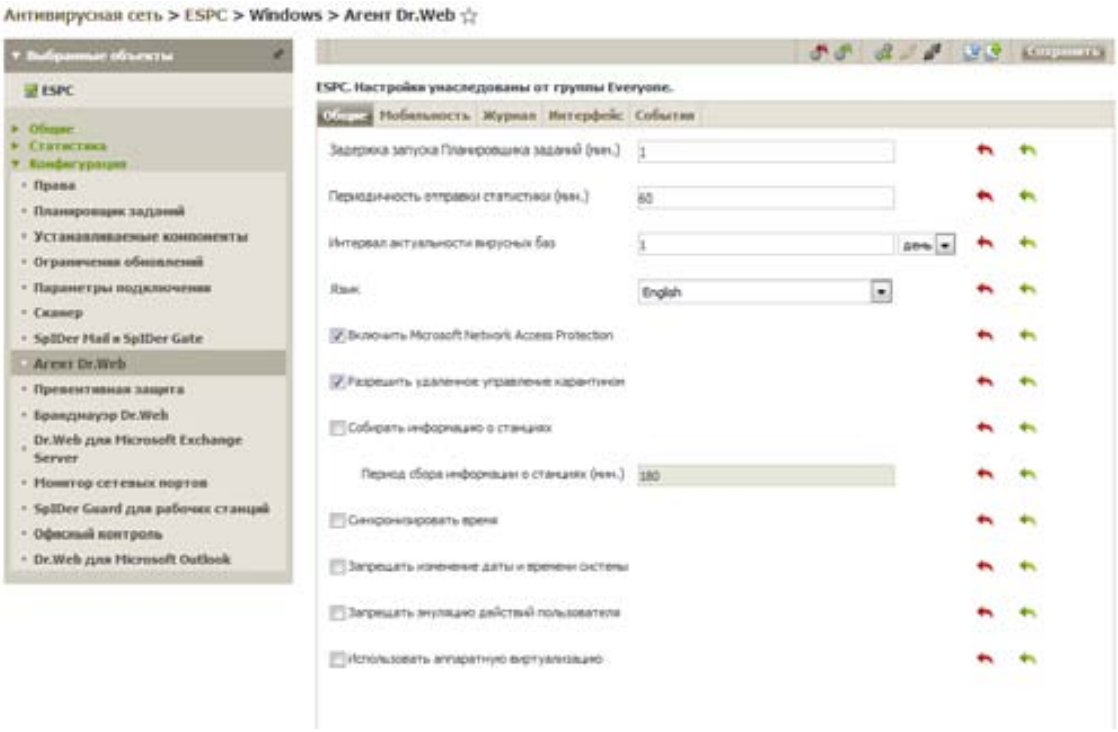


7.6.1. Настройка параметров защиты рабочих станций и серверов Windows

Администратор может определять настройки как для групп в целом, так и по отношению к отдельным станциям в группах.

Чтобы просмотреть или изменить настройки Агента Dr.Web на рабочей станции под управлением ОС Windows:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления и в открывшемся окне в иерархическом списке нажмите на название станции или группы.
2. В открывшемся управляющем меню (панель слева) выберите пункт Агент **Dr.Web** в группе **Windows** — откроется окно настроек Агента.



Чтобы принять сделанные изменения, нажмите на кнопку **Сохранить**.

Внимание! Внесение изменений в настройки, не согласованное с настройками Сервера (в частности, изменение режима шифрования и сжатия, а также ключа шифрования), приведет к утрате связи между Агентом и Сервером.

На вкладке **Общие** вы можете настроить следующие параметры Агента:

- В поле **Задержка запуска Планировщика заданий (мин.)** задайте величину тайм-аута между запуском ОС и началом выполнения стартового задания на сканирование, если оно задано в расписании заданий Агента. По умолчанию указана задержка в 1 минуту. При указании значения 0 задание на сканирование будет запущено без задержки, т. е. сразу после загрузки ОС.
- В поле **Периодичность отправки статистики (мин.)** задайте значение временного интервала в минутах для отправки Агентом на Сервер всей статистической информации, собранной на станции компонентами SpIDer Guard, SpIDer Mail и SpIDer Gate. Задайте значение 0, чтобы отключить отправку статистики.
- В поле **Интервал актуальности вирусных баз** задайте значение временного интервала, в течение которого вирусные базы, установленные на станциях, будут считаться актуальными. Начало интервала — момент создания вирусных баз. В данный период уведомления о том, что вирусные базы устарели, не показываются.
- В выпадающем списке **Язык** задается язык интерфейса Агента и компонентов Антивируса Dr.Web на рабочей станции или на группе рабочих станций.
- Включите опцию **Включить Microsoft Network Access Protection**, чтобы включить мониторинг состояния станции с использованием технологии Microsoft® Network Access Protection. При этом активируется Агент работоспособности системы (System Health Agent — SHA), который автоматически устанавливается вместе с ПО Агента Dr.Web на рабочую станцию.
- Включите опцию **Разрешить удаленное управление карантином**, чтобы разрешить удаленное управление карантином на рабочих станциях с Сервера.

Пункт **Разрешить удаленное управление карантином** доступен, если в разделе **Администрирование → Конфигурация Сервера Dr.Web →** вкладка **Статистика** включена опция **Состояние карантина**.

- Включите опцию **Собирать информацию о станциях**, чтобы разрешить собирать информацию о программно-аппаратном обеспечении станций. При включенной опции выберите в выпадающем списке **Период сбора информации о станциях (мин.)** периодичность в минутах отправки Агентами на Сервер актуальной информации о программно-аппаратном обеспечении на станции.
- Включите опцию **Синхронизировать время** для включения синхронизации системного времени на ПК с установленным Агентом и времени на ПК, на котором установлен Сервер Dr.Web.
- Включите опцию **Запрещать изменение даты и времени системы**, чтобы запретить ручное и автоматическое изменение системных даты и времени, а также часового пояса, за исключением синхронизации времени с Сервером Dr.Web (включается при помощи опции **Синхронизировать время**).
- Включите опцию **Запрещать эмуляцию действий пользователя**, чтобы запретить любые изменения в работе Dr.Web, кроме вносимых пользователем вручную. Данная опция позволяет предотвратить любые изменения в работе программы Dr.Web, производимые автоматизированно. В том числе будет запрещено исполнение скриптов, эмулирующих работу пользователя с программой Dr.Web и запущенных самим пользователем.
- Включите опцию **Использовать аппаратную виртуализацию**, чтобы использовать больше возможностей компьютера для обнаружения и лечения угроз, а также для усиления самозащиты Dr.Web. Для включения этой опции потребуется перезагрузка станции.

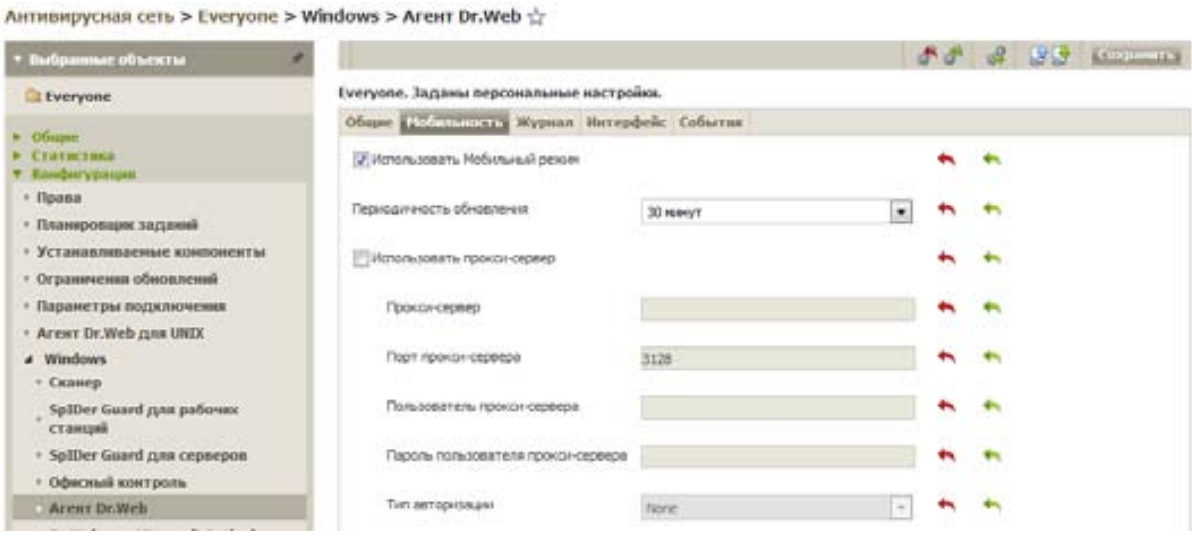
Аппаратная виртуализация работает только в том случае, если аппаратные особенности станции и операционная система поддерживают аппаратную виртуализацию.

Включение этой опции может вызвать конфликт совместимости со сторонним программным обеспечением.

При возникновении проблем отключите эту опцию.

Для 32-разрядных операционных систем аппаратная виртуализация не поддерживается.

На вкладке **Мобильность** вы можете настроить параметры работы Агента в Мобильном режиме:



Включение флажка **Использовать Мобильный режим** активирует на Агенте использование Мобильного режима, в котором Агент работает автономно от Сервера, получая обновления напрямую с ВСО.

В поле **Периодичность обновления** укажите временной промежуток между обновлениями антивирусного ПО на станции с серверов ВСО.

При выборе варианта **Вручную** автоматические обновления будут отключены. В этом случае для получения последних вирусных баз пользователь должен самостоятельно запустить обновление в настройках Агента на станции.

•Включите опцию **Использовать прокси-сервер** для использования HTTP прокси-сервера при получении обновлений из сети Интернет. При этом станут активными поля настроек используемого прокси-сервера.

Обновление мобильных Агентов Dr.Web

Если компьютер пользователя долгое время не будет иметь связи с Сервером Dr.Web, для своевременного получения обновлений с серверов ВСО Dr.Web рекомендуется установить мобильный режим работы Агента Dr.Web на станции.

В мобильном режиме Агент пытается подключиться к Серверу, делает три попытки и, если не удалось, выполняет HTTP-обновление. Попытки найти Сервер идут непрерывно с интервалом около минуты.

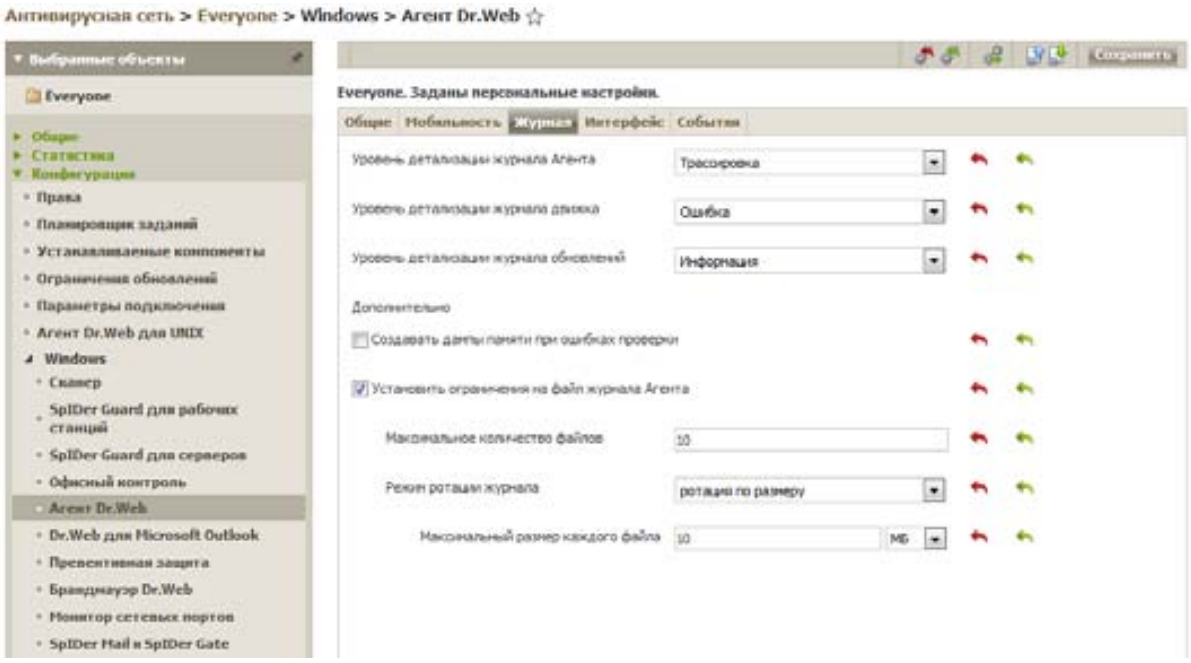
Включение мобильного режима в настройках Агента будет доступно при условии, что использование мобильного режима разрешено в Центре управления в разделе **Антивирусная сеть → Права → Windows → Общие → Запуск в мобильном режиме**.

Во время функционирования Агента в мобильном режиме связь Агента с Сервером Dr.Web прерывается. Все изменения, которые задаются на Сервере для такой станции, вступят в силу, как только мобильный режим работы Агента будет выключен и связь Агента с Сервером возобновится.

В мобильном режиме производится обновление только вирусных баз.

Описание настроек Мобильного режима на стороне Агента приведено в Руководстве пользователя Агент Dr.Web для Windows.

На вкладке **Журнал** вы можете настроить параметры ведения журнала Агента и некоторых компонентов Антивируса Dr.Web:



- Уровень детализации журнала Агента определяет уровень подробности ведения журналов по работе Агента (файлы dwservice.log и es-service.log).
- Уровень детализации журнала движка определяет уровень подробности ведения журнала по работе поискового движка (записывается в системный журнал событий).
- Уровень детализации журнала обновлений определяет уровень подробности ведения журнала по работе модуля обновлений Dr.Web (файл dwupdater.log).

- Включите опцию **Создавать дампы памяти при ошибках проверки**, чтобы создавать дампы памяти в случаях возникновения ошибок при сканировании. Рекомендуется включать данную настройку для анализа ошибок в работе Dr.Web.
- Включите опцию **Установить ограничения на файл журнала Агента**, чтобы ограничить количество файлов журнала, размер каждого файла или длительность их записи.

    - Максимальное количество файлов — максимальное количество файлов журнала (включая текущий и архивные), которые будут храниться.
    - Режим ротации журнала — режим ротации работы журнала. Выберите одно из представленных значений:

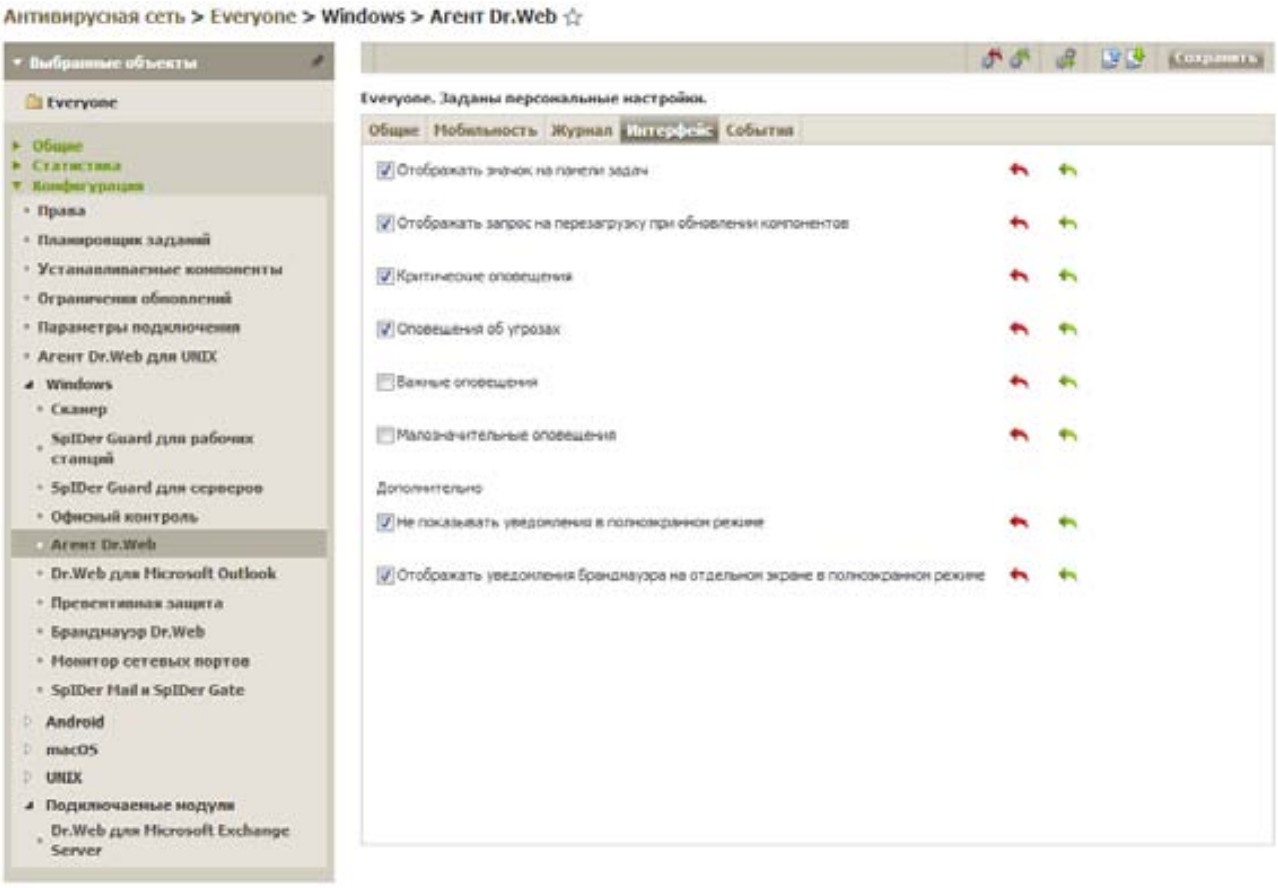
        - ротация по размеру определяет ограничение на размер каждого из файлов журнала.

Максимальный размер каждого файла — максимально допустимый размер каждого файла журнала. Когда текущий файл достигает заданного размера, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.

        - ротация по времени определяет длительность записи каждого из файлов журнала.

Максимальное время записи файла — максимальная длительность для записи каждого файла журнала. Когда время записи файла достигает заданной длительности, он списывается в архив с соответствующим изменением имени и создается новый файл журнала.

На вкладке **Интерфейс** вы можете настроить параметры интерфейса Агента Dr.Web:



- Включите опцию **Отображать значок на панели задач**, чтобы выводить значок Агента на панели задач. Если значок отключен, пользователь не сможет просматривать и изменять настройки Агента и антивирусного пакета.
- Включите опцию **Отображать запрос на перезагрузку при обновлении компонентов**, чтобы выводить запрос на перезагрузку станции, если были получены обновления антивирусных компонентов, для применения которых требуется перезагрузка. Если опция отключена, оповещение на станции не выводится, автоматическая перезагрузка не осуществляется. В статистике станции, получаемой Центром управления, будет сообщено о необходимости перезагрузки станции. Информация о состоянии, требующем перезагрузку, отображается в таблице **Состояния**. При необходимости администратор может перезагрузить станцию из Центра управления.

Опция **Отображать запрос на перезагрузку при обновлении компонентов** не влияет на отображение запросов о перезагрузке, требуемых для завершения лечения обнаруженных угроз или изменения состояния аппаратной виртуализации. Данные запросы будут отображаться всегда.

Чтобы отметить типы сообщений о событиях, которые будет получать пользователь, включите соответствующие опции:

- **Критические оповещения** — получать только критические оповещения о следующих событиях:
    - обнаружены соединения, ожидающие ответа Брандмауэра;
    - имя пользователя (идентификатор) станции и пароль уже используются для подключения к Серверу.

Сообщение выводится только в том случае, если пользователь имеет права администратора.

- **Оповещения об угрозах** — получать только оповещения об угрозах. К данному типу оповещений относятся сообщения об обнаружении угроз безопасности одним из компонентов антивирусного ПО.
- **Важные оповещения** — получать только важные оповещения о следующих событиях:

    - истекает время работы за компьютером;
    - доступ к устройству заблокирован;
    - доступ к защищаемому объекту заблокирован Превентивной защитой;
    - заблокирована попытка изменения системных даты и времени;
    - вирусные базы устарели (при работе в Мобильном режиме).

- **Малозначительные оповещения** — получать только малозначительные оповещения о следующих событиях:

    - успешное обновление;
    - ошибка обновления;
    - истекает время работы в Интернет;
    - URL заблокирован модулем Офисный контроль;
    - URL заблокирован SpIDer Gate;
    - доступ к защищаемому объекту заблокирован модулем Офисный контроль;
    - процесс сканирования станции запущен администратором из Центра управления;
    - процесс сканирования станции запущен согласно централизованному расписанию;
    - сканирование станции завершено.

Если вы хотите, чтобы пользователь получал все группы сообщений, включите все четыре опции. В противном случае будут выводиться только сообщения указанных групп.

Оповещения о некоторых событиях не входят в перечисленные группы и всегда показываются пользователю:

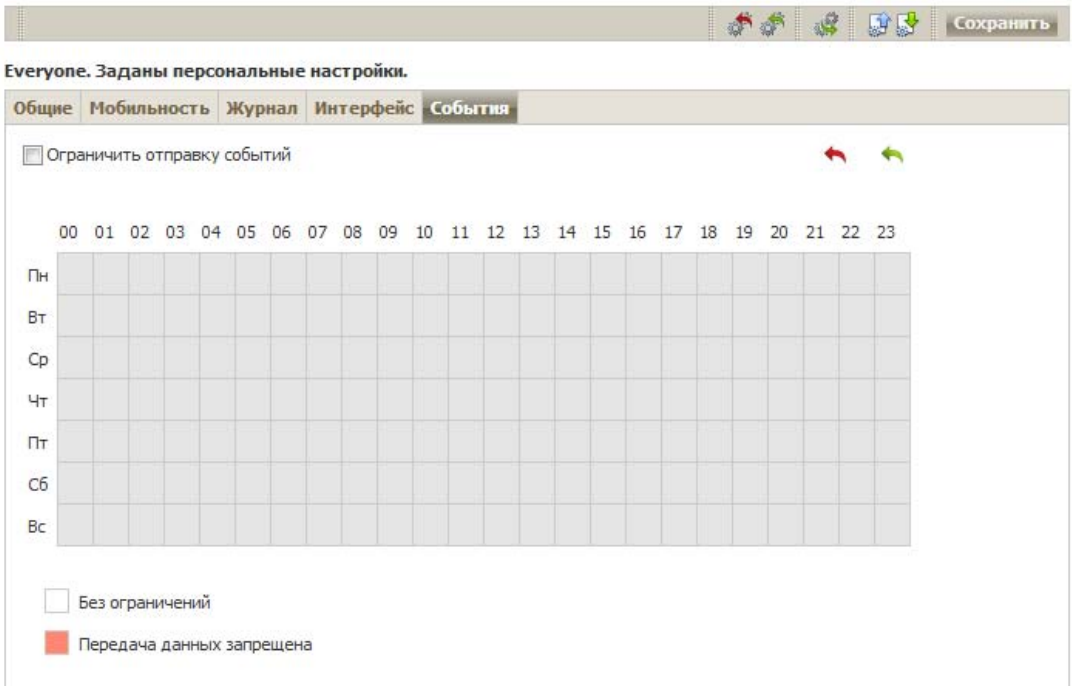
- установка приоритетных обновлений, для которых требуется перезагрузка;
- перезагрузка для завершения обезвреживания угроз;
- перезагрузка для включения/отключения гипервизора;
- запрос на разрешение процессу модификации объекта;
- сообщение, отправленное администратором из Центра управления;
- USB-устройство (клавиатура) подключено/заблокировано в рамках защиты от BadUSB-уязвимости.

В подразделе **Дополнительно** задаются следующие настройки:

- Включите опцию **Не показывать уведомления в полноэкранном режиме**, чтобы отключить всплывающие уведомления, если какая-либо программа запущена в полноэкранном режиме.
- Включите опцию **Отображать уведомления Брандмауэра на отдельном экране в полноэкранном режиме**, чтобы уведомления от Брандмауэра Dr.Web отображались на отдельном рабочем столе, т. е. поверх запущенного полноэкранного приложения. Рекомендуется включить данную настройку во избежание блокировки сетевых подключений, используемых приложением, запущенным в полноэкранном режиме, без возможности их разрешения в момент поступления требования от Брандмауэра Dr.Web.

Настройка сообщений от Агент Dr.Web Сервер производится в разделе **События**. По умолчанию Агент передает сообщения о следующих событиях:

- запуске и останове программы;
- обнаружении вирусов;
- выполнении заданий Планировщиком;
- блокировке устройств.



Сообщения передаются на сервер в момент наступления события. В случае если передача данных запрещена, сообщения накапливаются в базе данных. Сообщения будут отправлены на сервер, когда отправка событий будет разрешена.

Чтобы изменить режим отправки событий, включите опцию **Ограничить отправку событий**. По умолчанию передача данных запрещена.

В таблице временных промежутков задается режим ограничения отправки событий в цветовой градации, приведенной под таблицей:

- белый цвет — Без ограничений;
- красный цвет — Передача данных запрещена: полная блокировка отправки событий.

При этом ограничение задается отдельно на каждые 30 минут каждого дня недели.

Для изменения режима ограничений доступа нажмите на соответствующий блок таблицы. Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей. Также поддерживается выбор нескольких временных блоков по принципу drag-and-drop.

Параметры **Превентивной защиты** задаются в разделе **Конфигурация → Windows → Превентивная защита**. С ее помощью вы можете настроить реакцию Dr.Web на действия сторонних приложений, которые могут привести к заражению рабочей станции, также вы можете выбрать уровень защиты от эксплойтов.

При этом вы можете задать отдельный режим защиты для конкретных приложений и общий режим, настройки которого будут применяться ко всем остальным процессам.

Блокировка WSL

Включите опцию **Блокировать WSL**, чтобы блокировать Windows Subsystem for Linux на станциях с установленным Агентом Dr.Web.

Примечание. Настройка доступна только для операционной системы Windows 10.

Защита от эксплойтов

В разделе **Защита от эксплойтов** вы можете настроить режим блокировки вредоносных объектов, которые используют уязвимости в популярных приложениях. В соответствующем выпадающем списке выберите подходящий уровень защиты от эксплойтов.

Уровень защиты	Описание
Блокировать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически заблокирована.
Интерактивный режим	При попытке вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы, Dr.Web выведет соответствующее сообщение. Ознакомьтесь с информацией и выберите нужное действие.
Разрешать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически разрешена.

Уровень блокировки подозрительных действий

В разделе **Уровень блокировки подозрительных действий** вы можете задать общий режим защиты, настройки которого будут применяться ко всем процессам, если для них не задан персональный режим в разделе ниже. Также вы можете защитить данные пользователей от нежелательных изменений.

Выберите один из уровней защиты, обеспечиваемой антивирусом:

- **Параноидальный** — максимальный уровень защиты при необходимости полного контроля за доступом к критическим объектам ОС Windows.

Примечание. В данном режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

- **Средний** — уровень защиты при повышенной опасности заражения. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.
- **Оптимальный** — уровень защиты, запрещающий автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему.
- **Пользовательский** — уровень защиты, определяемый пользователем (администратором Сервера) на основе настроек, заданных в таблице ниже.

Для задания пользовательских настроек уровня превентивной защиты включите в таблице данного раздела опции в одно из следующих положений:

- **Разрешать** — всегда разрешать действия с данным объектом или со стороны данного объекта.
- **Спрашивать** — выводить диалоговое окно для задания необходимого действия самим пользователем для конкретного объекта.
- **Запрещать** — всегда запрещать действия с данным объектом или со стороны данного объекта.

При изменении настроек в таблице, если был задан один из предустановленных уровней в поле **Уровень блокировки подозрительных действий**, он автоматически изменяется на **Пользовательский**.

Вы можете создать несколько независимых пользовательских профилей.

Чтобы добавить новый пользовательский профиль, нажмите кнопку  . В открывшемся окне задайте название для нового профиля и нажмите **Сохранить**.

Чтобы удалить созданный вами пользовательский профиль, выберите его из списка **Уровень блокировки подозрительных действий** и нажмите кнопку  . Возможность удалять предустановленные профили не предоставляется.

Настройки Превентивной защиты позволяют контролировать следующие объекты:

- Целостность запущенных приложений — отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера. Не

отслеживается поведение тех процессов, которые добавлены в исключения компонента SpIDer Guard.

- Целостность файлов пользователей — отслеживать процессы, которые модифицируют пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера. Не отслеживается поведение тех процессов, которые добавлены в исключения компонента SpIDer Guard. Для того чтобы защитить данные пользователей от несанкционированных изменений, рекомендуется настроить создание защищаемых копий важных файлов.
- HOSTS файл — данный файл используется операционной системой для упрощения доступа к сети Интернет. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
- Низкоуровневый доступ к диску — запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
- Загрузка драйверов — запрещать приложениям загрузку новых или неизвестные драйверов.

Остальные настройки отвечают за критические области ОС Windows и позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей).

Защищаемые ветки реестра

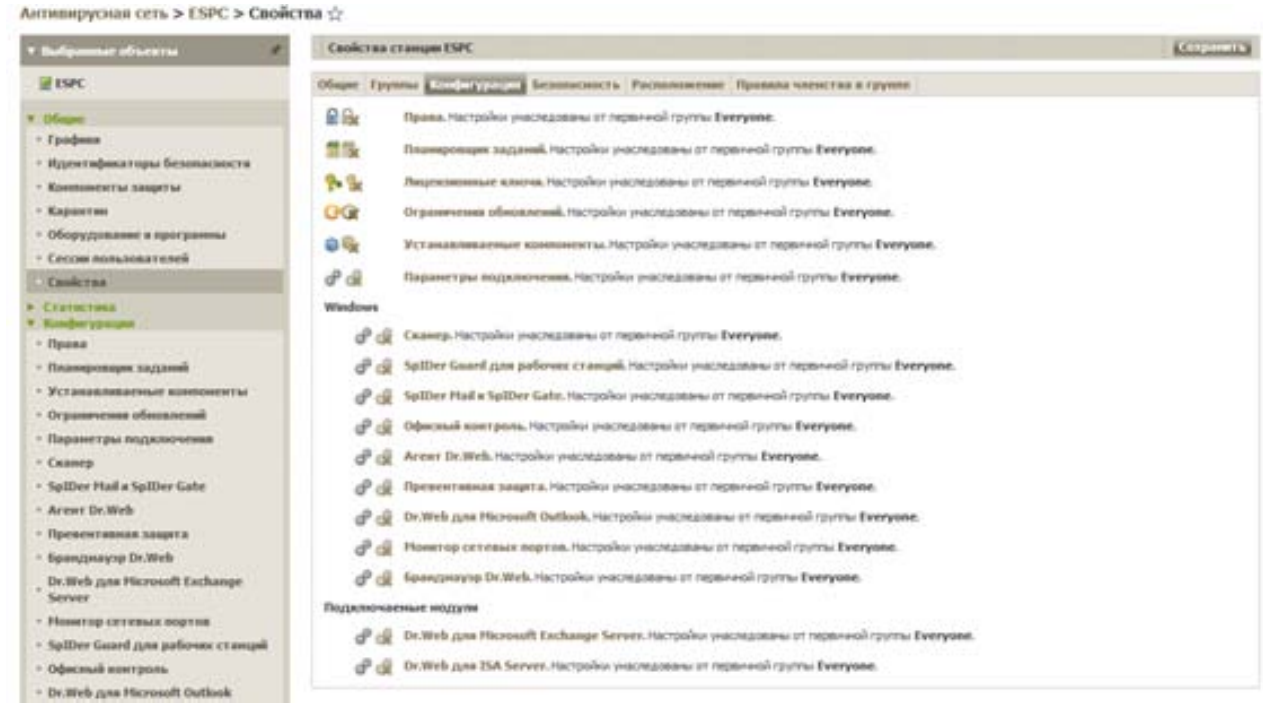
Настройка	Ветка реестра
Image File Execution Options	Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
User Drivers	Software\Microsoft\Windows NT\CurrentVersion\Drivers32 Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Параметры оболочки Winlogon	Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Нотификаторы Winlogon	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Автозапуск оболочки Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib
Ассоциации исполняемых файлов	Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи)
Политики ограничения запуска программ (SRP)	Software\Policies\Microsoft\Windows\Safer
Плагины Internet Explorer (BHO)	Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Автозапуск программ	Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\RunOnce Software\Microsoft\Windows\CurrentVersion\RunOnceEx Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup

Настройка	Ветка реестра
	Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup Software\Microsoft\Windows\CurrentVersion\RunServices Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
Автозапуск политик	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Конфигурация безопасного режима	SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Параметры Session Manager	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
Системные службы	System\CurrentControlXXX\Services

Если при установке важных обновлений от Microsoft или при установке и работе программ (в том числе программ дефрагментации) возникают проблемы, отключите соответствующие опции в этой группе настроек.

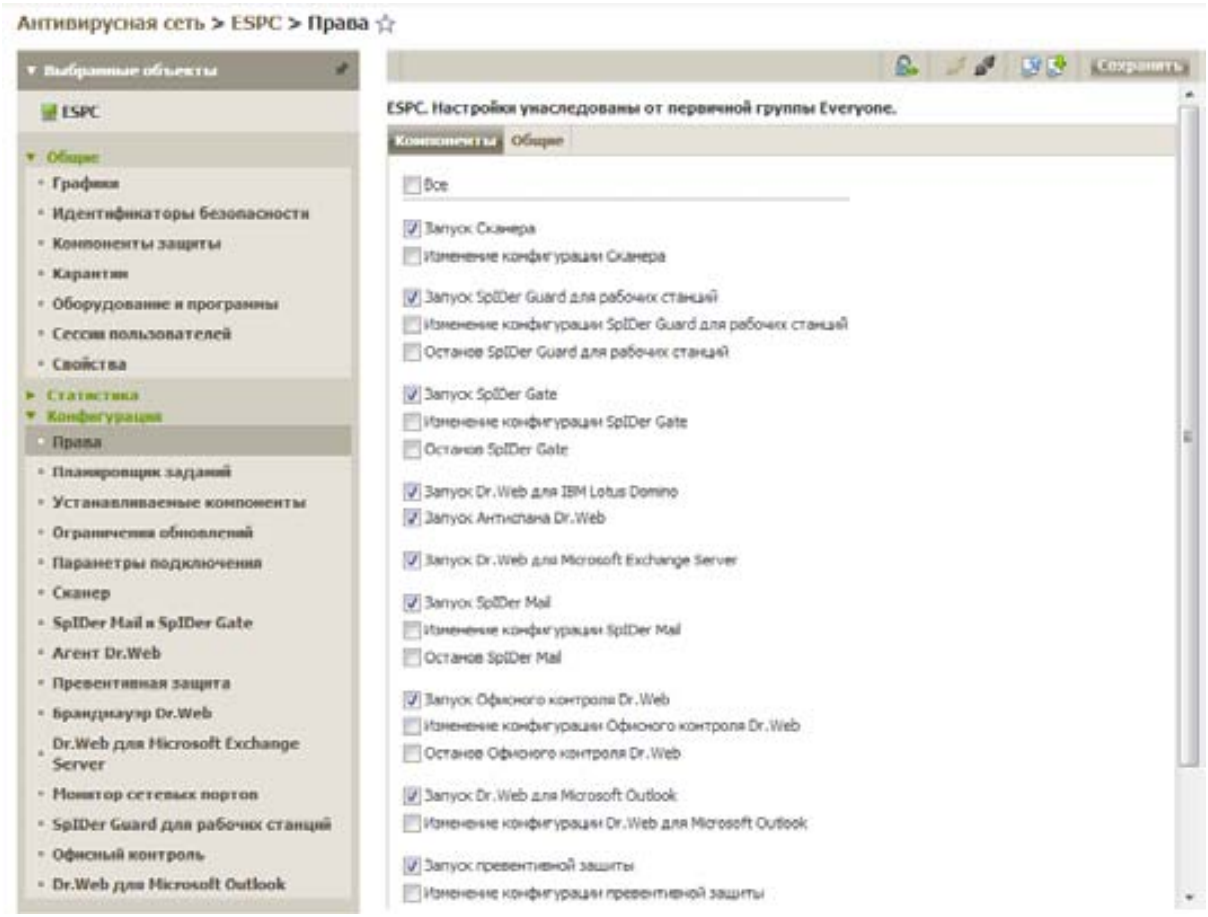
Параметры антивирусной защиты для отдельных станций и групп можно указать, выбрав соответствующую группу или станцию в разделе **Антивирусная сеть**.

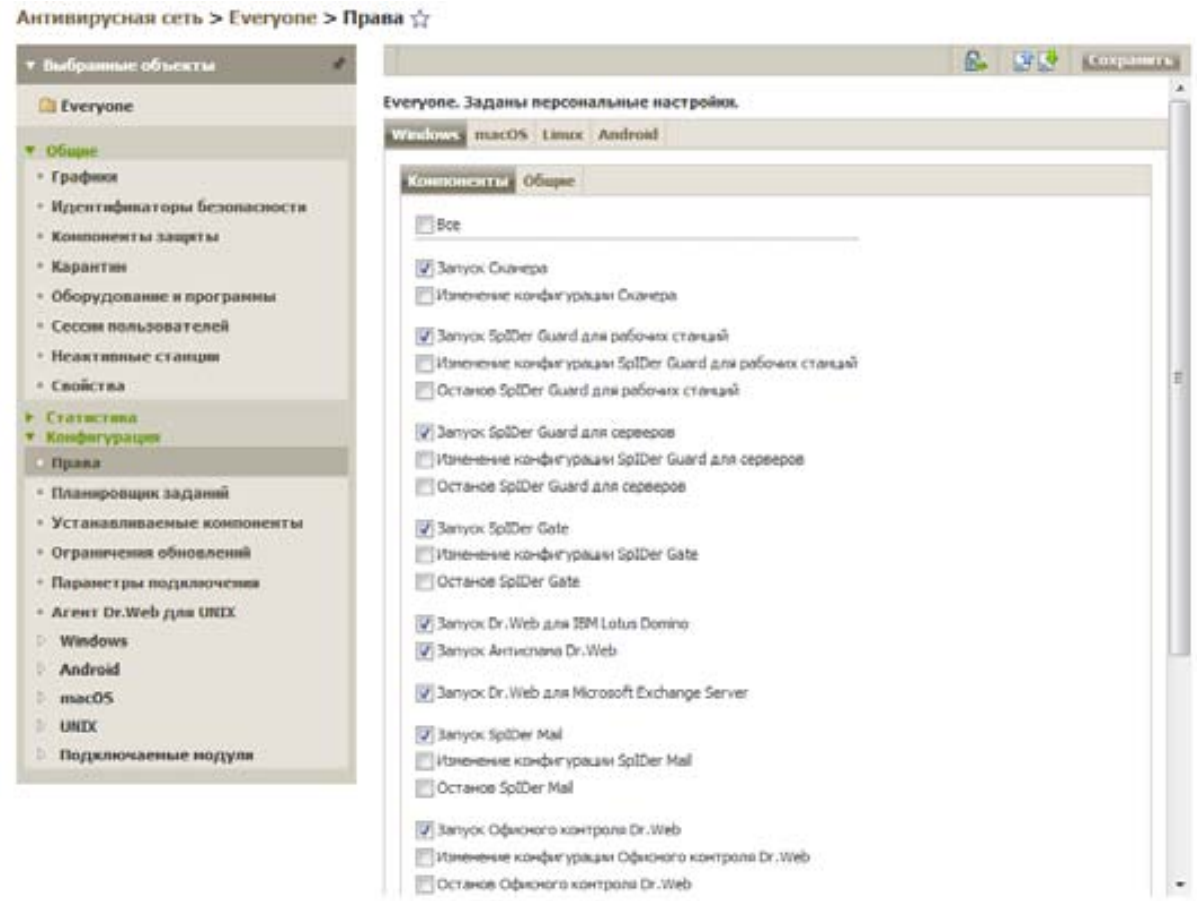
После выбора пользователя администратор может узнать текущие параметры, связанные с пользователем, выбрав пункт **Свойства** в группе **Общие**.



Выбрав вкладку **Конфигурация → Права → Компоненты,** администратор может задать индивидуальные параметры прав, которыми располагают пользователи или группы, для настройки защитных компонентов, что позволяет формировать необходимые настройки в зависимости от структуры организации и функций сотрудников. В частности, на этой закладке определяется использование мобильного режима, состав запускаемых компонентов и права на изменение настроек этих компонентов самими пользователями.

Внимание! Параметры защиты, задаваемые через параметры групп, различаются для сервисов защиты рабочих станций под различными ОС, каждой из которых соответствует своя вкладка с параметрами: Windows, macOS, Linux, Android.



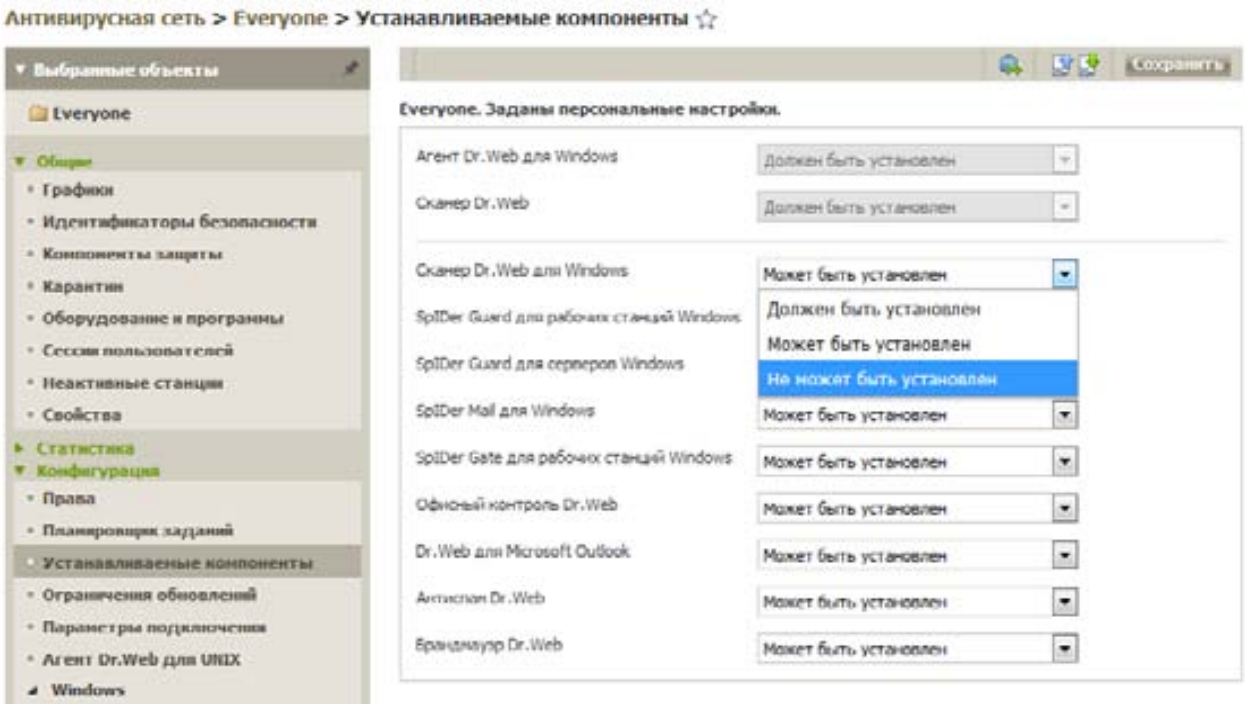


Администратор может просмотреть и определить список устанавливаемых на станциях компонентов, используя пункт **Устанавливаемые компоненты** той же группы.

Внимание! Настроить состав установленных компонентов можно только для Агентов на ОС Windows, для остальных ОС конфигурация компонентов определяется при установке Агента и не может быть изменена через Центр управления.

Для каждого компонента антивируса может быть выбрано одно из условий установки:

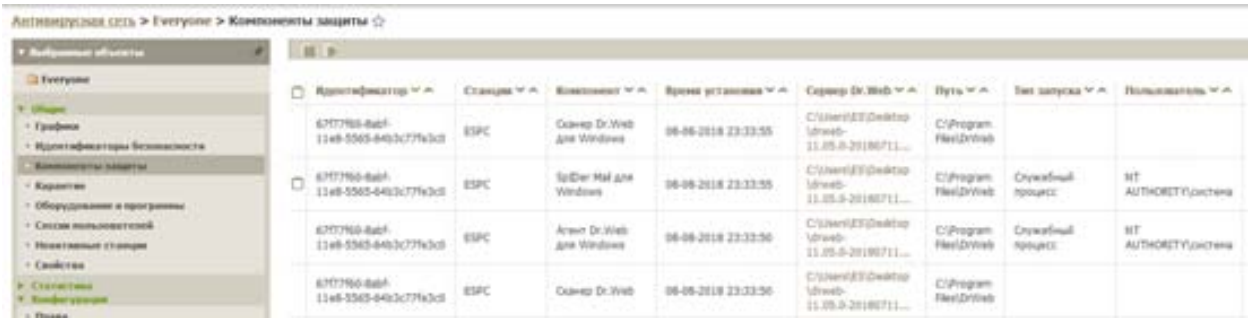
- **Должен быть установлен** — задает обязательное наличие компонента на станции. При создании новой станции компонент входит в состав устанавливаемого антивирусного пакета в обязательном порядке. При задании значения **должен** в настройках уже существующей станции компонент будет добавлен в состав имеющегося антивирусного пакета;
- **Может быть установлен** — определяет возможность установки антивирусного компонента; решение об установке принимает пользователь;
- **Не может быть установлен** — запрещает наличие компонента на станции. При создании новой станции компонент не входит в состав устанавливаемого антивирусного пакета. При задании значения **не может** в настройках уже существующей станции компонент будет удален из состава антивирусного пакета.



Нажмите кнопку **Сохранить** для сохранения настроек и соответствующего изменения состава антивирусного пакета на станции.

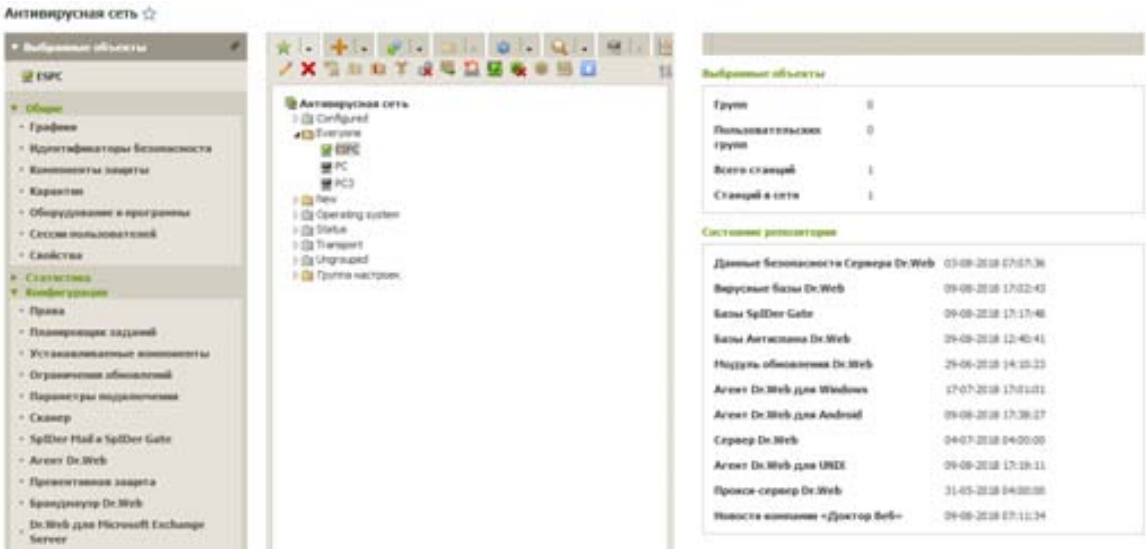
Сразу после сохранения этих изменений состав компонентов на всех станциях группы (или конкретной станции, для которой проводились настройки) будет приведен в соответствие с этим списком.

В разделе **Компоненты защиты** отображается список всех компонентов, которые установлены у пользователя рабочей станции или на нескольких станциях (для группы).



Чтобы узнать, какие вирусные базы установлены на рабочей станции:

1) В меню **Антивирусная сеть** щелкнуть по имени станции.

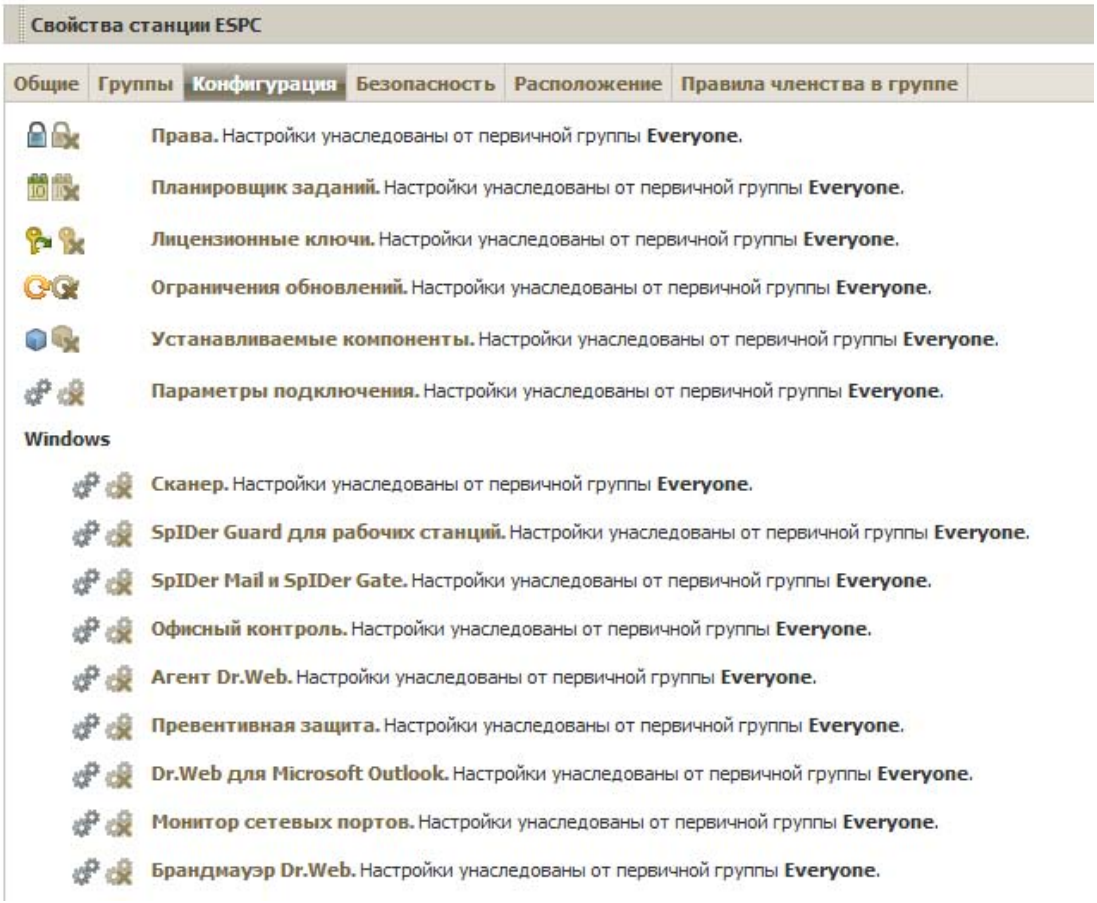


2) Выбрав пункт **Статистика → Вирусные базы**, в меню справа можно просмотреть информацию об установленных вирусных базах: названия файлов, содержащих конкретную вирусную базу; их версии; количество записей; даты создания.

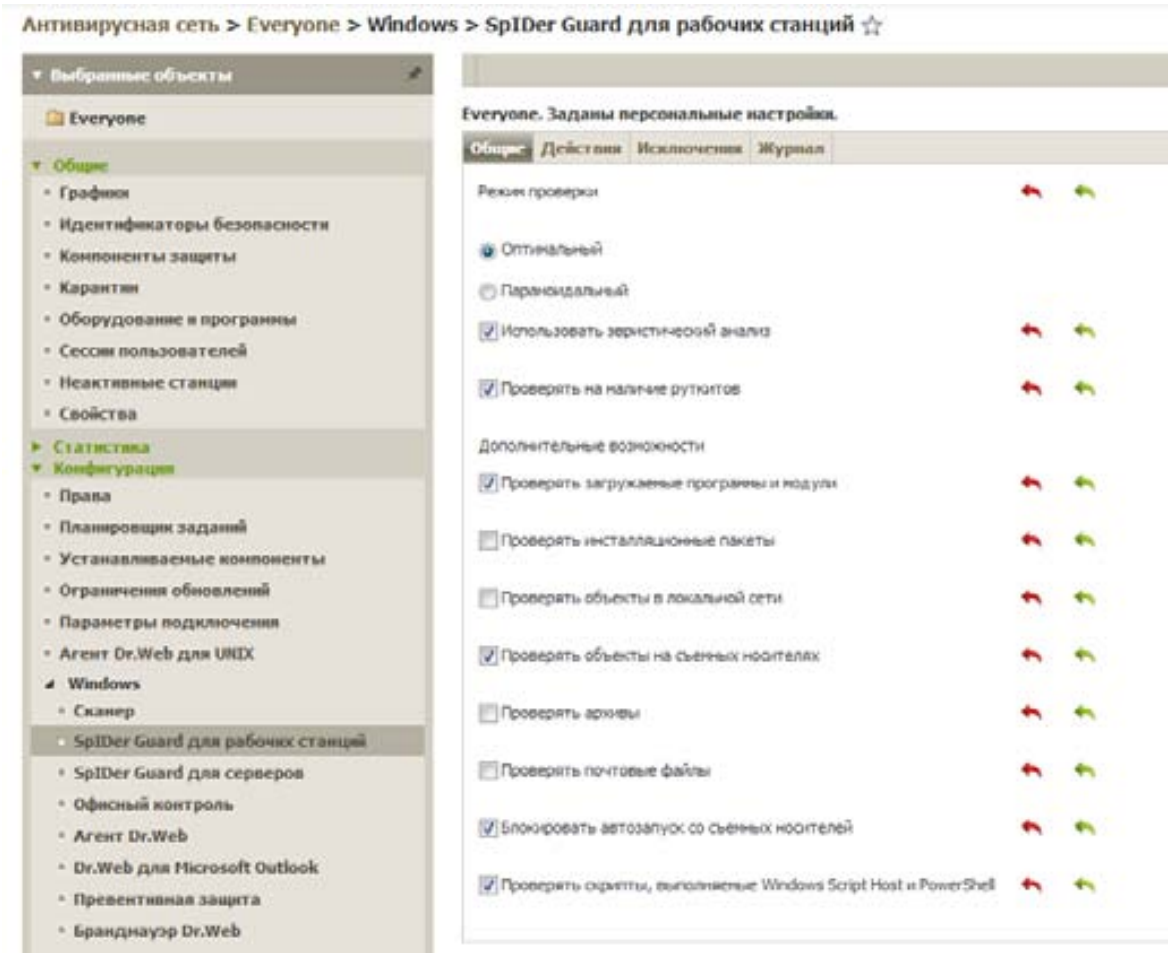
Если отображение пункта **Вирусные базы** отключено, для его включения выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**. На вкладке **Статистика** установите флажки **Состояние вирусных баз** и **Состояние станции**, после чего перезагрузите Сервер.

7.6.2. Настройка параметров защиты рабочих станций и серверов Windows. Выбор параметров защиты от вирусов и спама. Настройка параметров проверки. Выбор состава проверяемых объектов, типа применяемых к ним действий, в том числе применяемых к неизлечимым объектам и зараженным архивам

Настроить параметры защиты рабочих станций и серверов, а также групп станций можно, выделив соответствующий объект в дереве антивирусной сети и выбрав соответствующий пункт в группе настроек **Свойства → Конфигурация**.

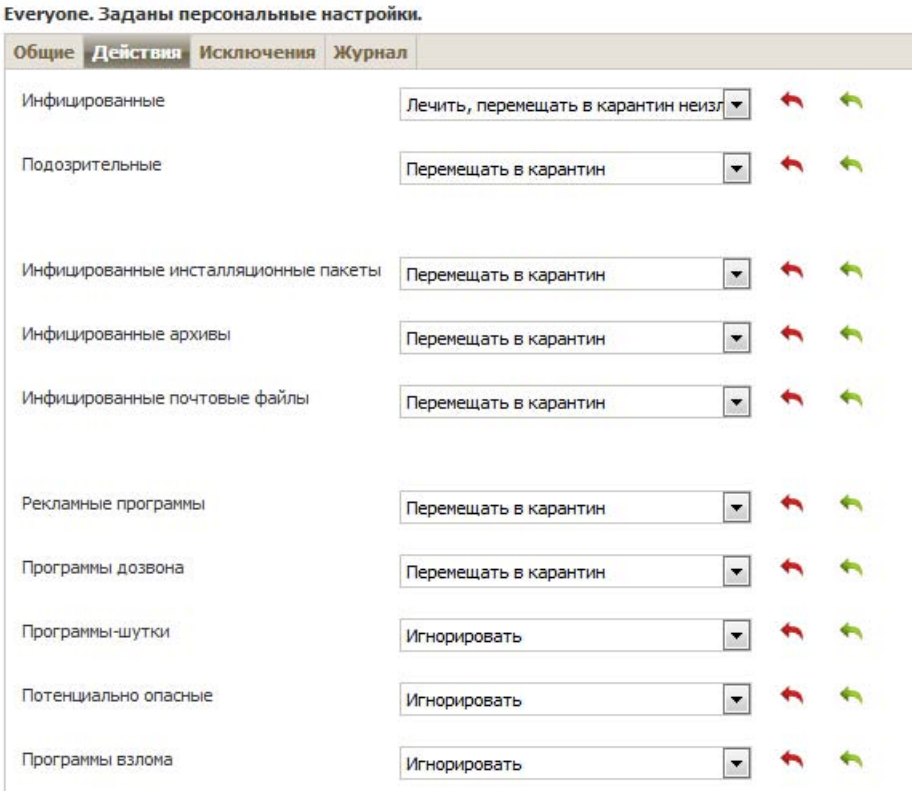


Так, для компонента **SpIDer Guard** администратор может задать параметры проверки отдельных типов файлов.

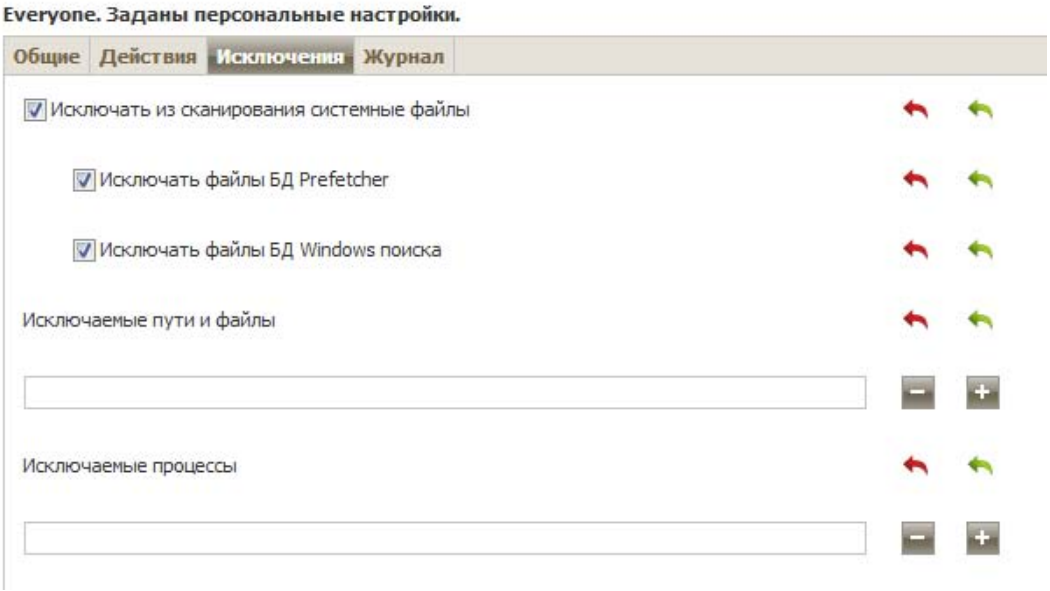


Использование значков  справа от параметров позволяет вернуть редактируемые значения либо в начальное на момент редактирования значение, либо в значение по умолчанию.

Действия программы для различных типов вредоносных объектов:



Исключаемые из проверки пути и маски файлов (что может быть полезно для ускорения проверки, но снижает общий уровень защиты):



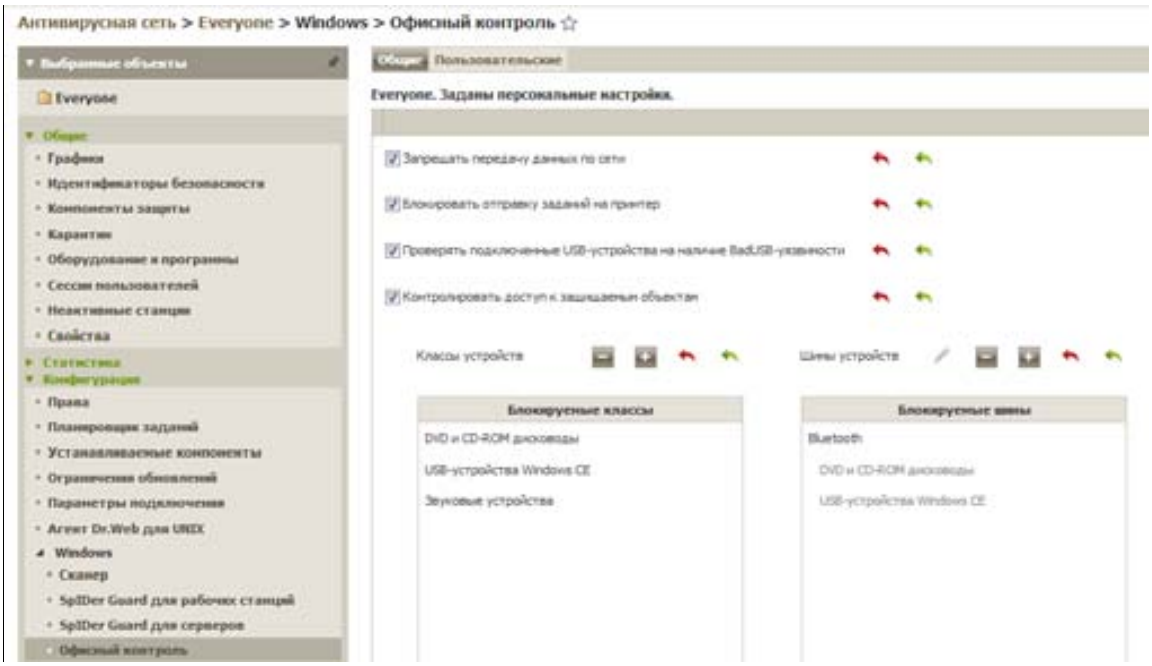
В том случае, если администратор меняет настройки для конкретной станции или группы, к ее названию в меню настроек добавляется примечание **Заданы персональные настройки**, в

противном случае — **Настройки унаследованы от первичной группы <название группы>**.

Все настройки работы компонентов антивирусной защиты станций и серверов в Dr.Web Enterprise Security Suite соответствуют настройкам этих же компонентов в продукте Антивирус Dr.Web для Windows или Dr.Web Security Space, в зависимости от приобретенной лицензии.

7.6.3. Ограничение доступа пользователей станции к сетевым ресурсам и оборудованию локального компьютера

Используя возможности Центра управления, администратор может настроить права доступа пользователя удаленного ПК к сетевым ресурсам, принтерам и оборудованию рабочей станции, что позволяет снизить риски распространения вирусов. Для открытия окна редактирования настроек выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы и затем пункт **Конфигурация → Windows → Офисный контроль** и настройте нужные типы защиты — например, отметив **Контролировать доступ к защищаемым объектам**, вручную добавив шины и классы устройств, доступ к которым необходимо заблокировать. Эти параметры задаются для рабочей станции или группы в целом и находятся на вкладке **Общие**.



На вкладке **Общие** вы можете настроить доступ к ресурсам локальной файловой системы и ограничить их использование:

- Включите опцию **Запрещать передачу данных по сети**, чтобы блокировать передачу данных по локальным сетям и сети Интернет. Обратите внимание, что при этом станции не смогут подключаться к Серверу Dr.Web.
- Включите опцию **Блокировать отправку заданий на принтер**, чтобы запретить передачу на принтер задания на печать.
- Включите опцию **Запрещать доступ к данным на съемных носителях**, чтобы блокировать доступ к USB флеш-накопителям, дискетам, CD/DVD приводам, ZIP-дискам и т. п.

- Включите опцию **Проверять подключенные USB-устройства на наличие BadUSB-уязвимости**, чтобы проверять, действительно ли подключаемое USB-устройство является клавиатурой.
- Включите опцию **Контролировать доступ к защищаемым объектам**, чтобы получить возможность редактировать список блокируемых классов и шин устройств.

Формирование списка заблокированных устройств

- Чтобы настроить список заблокированных классов устройств:

1. В разделе **Классы устройств** нажмите  , чтобы добавить устройство в список блокируемых классов.
2. В открывшемся окне выберите те классы устройств, доступ к которым должен быть заблокирован. Для этого установите опцию **Запрещать** напротив соответствующего класса в приведенном списке.
3. Нажмите **Сохранить**.
4. Чтобы удалить устройство из списка, выберите его в списке и нажмите  .
5. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

- Чтобы настроить список заблокированных шин устройств:

1. В разделе **Шины устройств** нажмите  , чтобы добавить устройство в список блокируемых шин.
2. В открывшемся окне выберите из выпадающего списка те шины устройств, доступ к которым должен быть заблокирован. Затем выберите классы, которые будут заблокированы этой шине. Чтобы заблокировать шину целиком, выберите все классы.
3. Нажмите **Сохранить**.
4. Чтобы удалить устройство из списка, выберите его в списке и нажмите  .
5. Чтобы отредактировать список классов, заблокированных на данной шине, выберите ее в списке блокируемых шин и нажмите  .
6. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

Обратите внимание: при включении следующих опций станции не смогут подключиться к Серверу Dr.Web:

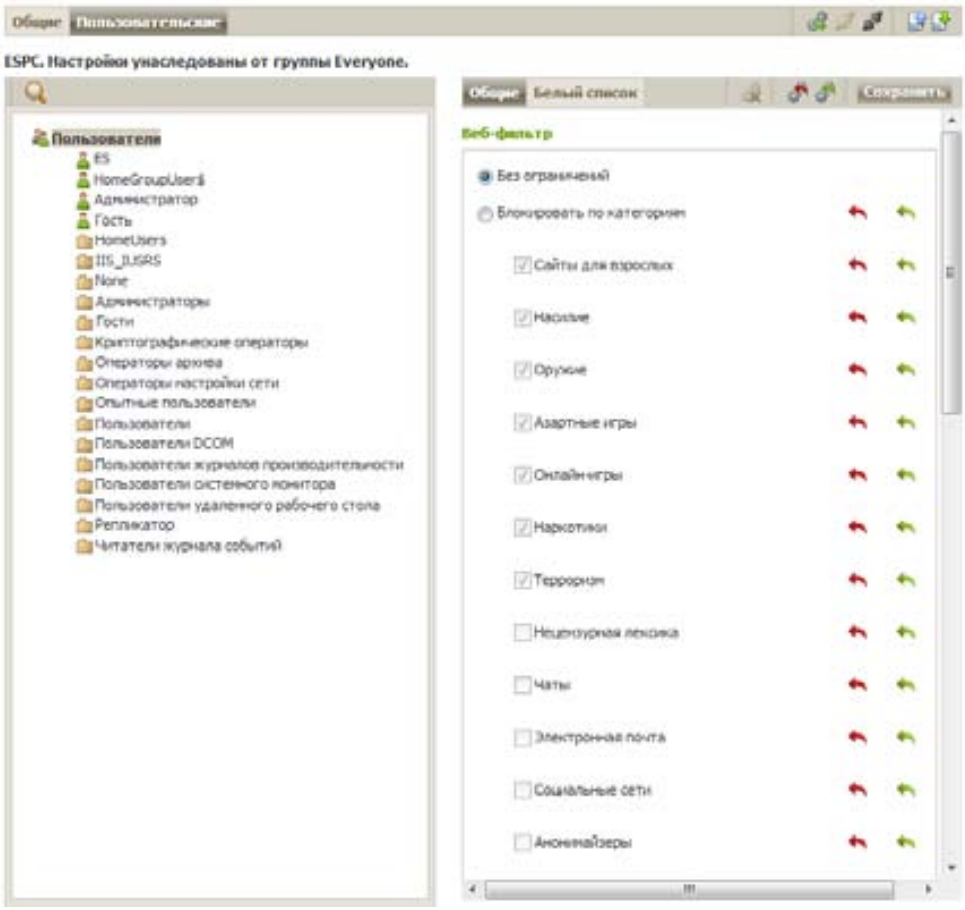
- **Запрещать передачу данных по сети**.
- **Контролировать доступ к следующим объектам → Классы устройств → Сетевые адаптеры**.

Данные опции запрещают всё сетевое взаимодействие для станции. При этом любое удаленное изменение настроек через Центр управления также невозможно.

По окончании настройки нажмите на кнопку **Сохранить**. Настройки вступят в силу после подтверждения новой конфигурации станции.

7.6.4. Настройка доступа пользователей к локальным папкам, Интернету и ограничения времени работы

Ограничение доступа к ресурсам сети Интернет позволит не только уменьшить риск заражения компьютеров, но и во многих случаях поднять производительность труда сотрудников, снизить время простоя и отвлечения от работы. Для настройки параметров доступа необходимо выбрать пункт **Антивирусная сеть → Конфигурация → Windows → Офисный контроль** и перейти на вкладку **Пользовательские**.



Параметры офисного контроля распространяются одновременно на всех пользователей компьютера, на котором установлен Dr.Web для ОС Windows. По умолчанию для всех учетных записей разрешен неограниченный доступ к ресурсам сети Интернет и к локальным ресурсам, ограничения по времени отсутствуют.

Структура пользователей станции

- Структура пользователей станции отображается в виде дерева, состоящего из групп пользователей и самих пользователей. По умолчанию заданы группы **Администраторы**, **Гости** и **Пользователи**.
- Все существующие группы пользователей становятся доступны после подключения станции к Серверу.
- Если в вашей локальной сети развернута служба Active Directory, вы можете добавить отдельных ее пользователей. Для этого нажмите  и в открывшемся разделе **Поиск пользователей на LDAP-сервере** задайте параметры поиска. Выбранные пользователи появятся в группе **Active Directory**.

Типы пользовательских настроек

- *Общие* — настройки корневой группы **Пользователи**, которые используются по умолчанию.

- *Наследуемые* — настройки, которые наследуются от корневой группы **Пользователи** в случае, если настройки для групп пользователей и отдельных пользователей не заданы. При этом раздел пользовательских настроек пуст.
- *Персональные* — настройки групп пользователей и отдельных пользователей, которые не наследуются от корневой группы.

a) Чтобы задать персональные настройки, выберите соответствующую группу пользователей или пользователя в подразделах дерева и нажмите **Задать настройки**. Скопируются настройки из корневой группы, которые можно по желанию изменять.

b) Если пользовательские настройки заданы, их можно удалить. Для этого выберите соответствующую группу пользователей или пользователя и нажмите  . При этом будут использоваться настройки корневой группы.

Веб-фильтр

- Выберите режим **Без ограничений**, чтобы доступ к веб-сайтам не контролировался. Этот режим установлен по умолчанию.
- Выберите режим **Блокировать по категориям**, чтобы самостоятельно указать категории тех ресурсов, доступ к которым будет запрещаться или разрешаться вне зависимости от других ограничений.
- Выберите режим **Блокировать все, кроме сайтов из белого списка**, чтобы запретить доступ ко всем веб-ресурсам, кроме указанных в белом списке.

В любом из режимов, кроме режима **Без ограничений**, вы можете активировать опцию **Включить безопасный поиск**, которая влияет на выдачу результатов поисковых систем. Эта функция позволяет исключить нежелательные ресурсы из результатов поиска.

Белый и черный списки сайтов

Вы можете задать списки сайтов, доступ к которым разрешается или блокируется вне зависимости от остальных настроек. По умолчанию списки пусты. При необходимости вы можете добавить адреса веб-сайтов в белый или черный список.

Формирование списка доменных адресов

1. Введите доменное имя или часть доменного имени веб-сайта в поле **Белый список** или **Черный список**, в зависимости от того, хотите ли вы разрешить или запретить доступ к нему соответственно.

a) Чтобы добавить в список определенный сайт, введите его полный адрес (например, www.example.com). Доступ ко всем ресурсам, расположенным на этом сайте, будет определяться данной записью.

b) Чтобы настроить доступ к веб-сайтам с похожими именами, введите в поле общую часть их доменных имен. Пример: если вы введете текст example, то доступ к example.com,example.test.com, test.com/example, test.example222.ru и другим похожим сайтам будет определяться данной записью.

c) Чтобы настроить доступ к сайтам на определенном домене, укажите имя домена с символом «.». В таком случае доступ ко всем ресурсам, находящимся на этом домене, будет определяться данной записью. Если при указании домена используется символ «/», то та часть подстроки, что стоит слева от символа «/», будет считаться доменным именем, а части справа от символа — частью адреса сайтов на данном домене, доступ к

которым настраивается. Пример: если вы введете текст example.com/test, то будут обрабатываться такие адреса какexample.com/test11, template.example.com/test22 и т. п.

Введенная строка при добавлении в список может быть преобразована к универсальному виду.

2. Чтобы добавить еще один объект в список, нажмите  .

3. Чтобы удалить адрес из списка, нажмите  напротив элемента списка, соответствующего этому адресу.

4. При необходимости повторите шаги 1 и 2 для добавления других ресурсов.

Для зашифрованного трафика (HTTPS-сайты) белый и черный списки могут содержать только доменные адреса (например, https://example.com).

Доступ к отдельным страницам домена можно настроить только для незашифрованного трафика (HTTP-сайты) (например, http://example.com/test).

Каталоги и файлы

Включите опцию **Защищать каталоги и файлы**, чтобы заблокировать доступ ко всем объектам, указанным в списке ниже.

Для формирования списка защищаемых объектов:

1. Чтобы добавить необходимый объект, задайте путь к нему в соответствующем поле.

2. Выберите режим ограничения:

a) **Только чтение** — добавленный объект будет доступен пользователю только для чтения.

b) **Заблокировано** — полностью заблокировать доступ к заданному объекту.

3. В каждом поле задается только один объект. Чтобы добавить еще один объект в список, нажмите  .

4. Чтобы удалить объект из списка, нажмите  напротив элемента списка, соответствующего этому объекту.

5. Чтобы снять все ограничения сразу для всех объектов списка, отключите опцию **Защищать каталоги и файлы**.

Ограничение времени

Вы можете задать промежутки времени, в течение которых пользователю будет запрещен доступ к сети Интернет или полностью заблокирован доступ к компьютеру. По умолчанию пользователям разрешено работать за компьютером и в сети Интернет неограниченное время.

Чтобы установить режим ограничения времени для конкретного профиля:

1. Нажмите  , чтобы добавить профиль в список.

2. В окне **Новый профиль** укажите имя для нового профиля.

3. Нажмите **Сохранить**.

4. Чтобы удалить профиль из списка, выберите его в списке и нажмите  .

5. При необходимости повторите шаги 1 и 2 для добавления других профилей.

В таблице временных промежутков задается режим ограничения доступа в цветовой градации, приведенной под таблицей:

- белый цвет — **Без ограничений**;
- синий цвет — **Блокировать доступ в Интернет**;
- красный цвет — **Запретить все**: полностью заблокировать пользователю доступ к компьютеру.

При этом ограничение задается отдельно на каждые 30 минут каждого дня недели.

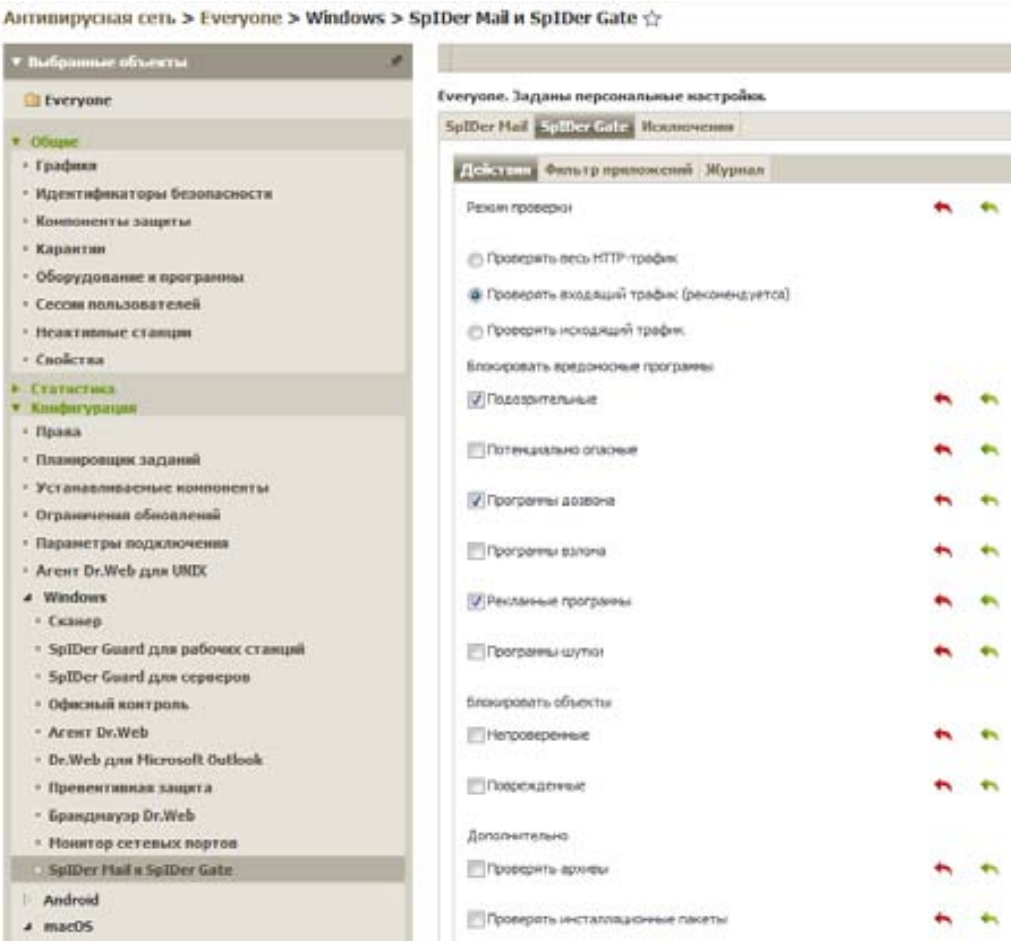
Для изменения режима ограничений доступа нажмите на соответствующий блок таблицы. Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей. Также поддерживается выбор нескольких временных блоков по принципу drag-and-drop.

По окончании настройки нажмите на кнопку **Сохранить**. Настройки вступят в силу после подтверждения новой конфигурации станции.

7.6.5. Настройка проверки HTTP-трафика. Выбор приложений для проверки / исключения из проверки их трафика, выбор контролируемых портов

Используя возможности компонента Dr.Web **SpIDer Gate**, администратор может гибко управлять защитой HTTP-трафика, настраивая уровень контроля и блокировки различного типа программ, определяя проверяемые порты и приложения, а также действия при обнаружении вредоносных объектов.

Основный параметры SpIDer Gate для станции или группы настраиваются на вкладке **Антивирусная сеть → Конфигурация → Windows → SpIDer Mail и SpIDer Gate → SpIDer Gate → Действия.**



На вкладке **Действия** задайте основные настройки проверки станций компонентом SpIDer Gate.

- **Режим проверки**. Выберите необходимый режим проверки трафика. По умолчанию выбрана опция **Проверять входящий трафик**.
- **Блокировать вредоносные программы**. Эта группа настроек позволяет вам выбрать вредоносные программы, которые подлежат блокировке. По умолчанию SpIDer Gate блокирует подозрительные и рекламные программы, а также программы дозвона.
- **Блокировать объекты**. SpIDer Gate может блокировать непроверенные или поврежденные объекты. По умолчанию эти опции выключены.
- **Дополнительно**. Эта группа настроек позволяет включить проверку архивов и инсталляционных пакетов. По умолчанию опция проверки архивов и инсталляционных пакетов отключена.
- **Приоритет сканирования**. Эта настройка позволяет вам регулировать ра спределение ресурсов в зависимости от приоритетности проверки трафика. При меньшем приоритете проверки скорость работы с сетью Интернет уменьшается, поскольку веб-антивирусу SpIDer Gate приходится дольше ждать загрузки данных и проверять больший объем информации. При увеличении приоритета проверка производится чаще, что позволяет сторожу отдавать данные быстрее, тем самым повышая скорость работы с сетью. Однако при более частых проверках повышается нагрузка на процессор.
- **Параметры блокировки**. В этой группе вы можете установить автоматическую блокировку доступа к URL, добавленных по обращению правообладателя, а также к нерекомендуемым сайтам, известным как неблагонадежные. Доступ к сайтам из белого списка будет разрешен, несмотря на установленные ограничения.

SpIDer Gate по умолчанию блокирует доступ к веб-сайтам, известным как источники вирусов или вредоносных программ других типов. При этом учитывается список приложений, исключаемых из проверки.

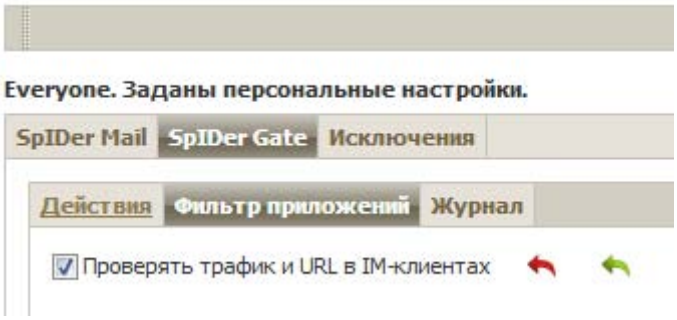
- **Белый список**. Задайте список сайтов, доступ к которым будет разрешаться вне зависимости от остальных настроек.

1. Укажите в соответствующем поле сайт, который вы хотите добавить в белый список.

2. В каждом поле задается только один сайт. Чтобы добавить еще один сайт в список, нажмите кнопку  .

3. Чтобы удалить сайт из белого списка, нажмите кнопку  напротив элемента списка, соответствующего этому сайту.

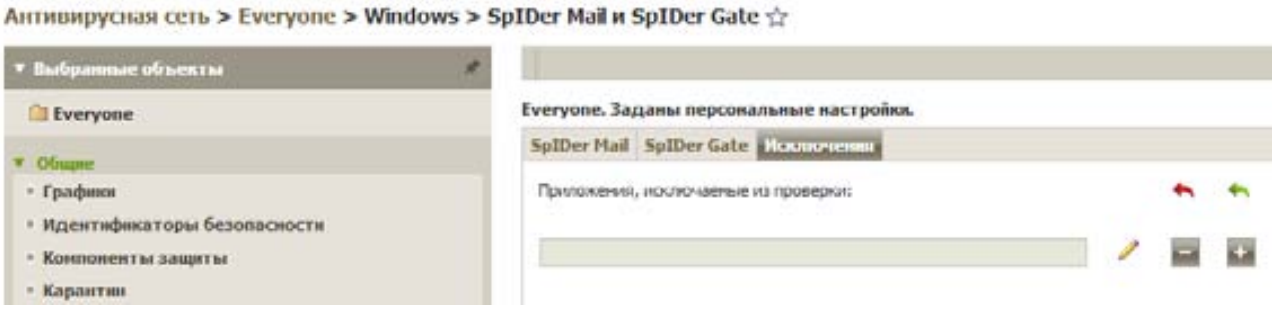
На вкладке **Фильтр приложений** можно включить параметр **Проверять трафик и URL в IM-клиентах**, чтобы проводилась проверка ссылок и данных, передаваемых клиентами систем обмена мгновенными сообщениями (Mail@RU Агент, ICQ и клиентов, работающих по протоколу Jabber). Проверяется только входящий трафик. По умолчанию опция включена.



На вкладке **Приложения, исключаемые из проверки** вы можете задать список программ и процессов, которые исключаются из проверки SpIDer Gate.

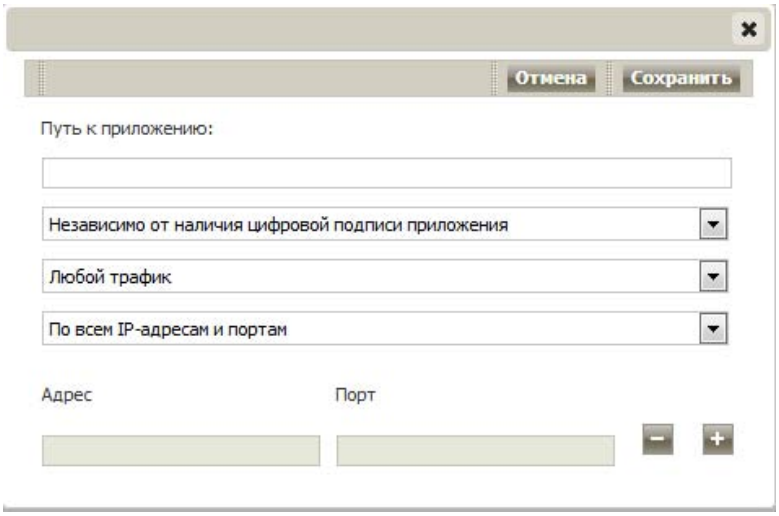
По умолчанию список пуст.

Внимание! Приложения, вносимые в данный список, будут исключены для проверки компонентами SpIDer Gate и SpIDer Mail одновременно.



Формирование списка исключений:

1. Нажмите  , чтобы добавить приложение в список.
2. В поле **Путь к приложению** задайте путь к исполняемому файлу приложения.
3. Укажите дополнительные настройки.



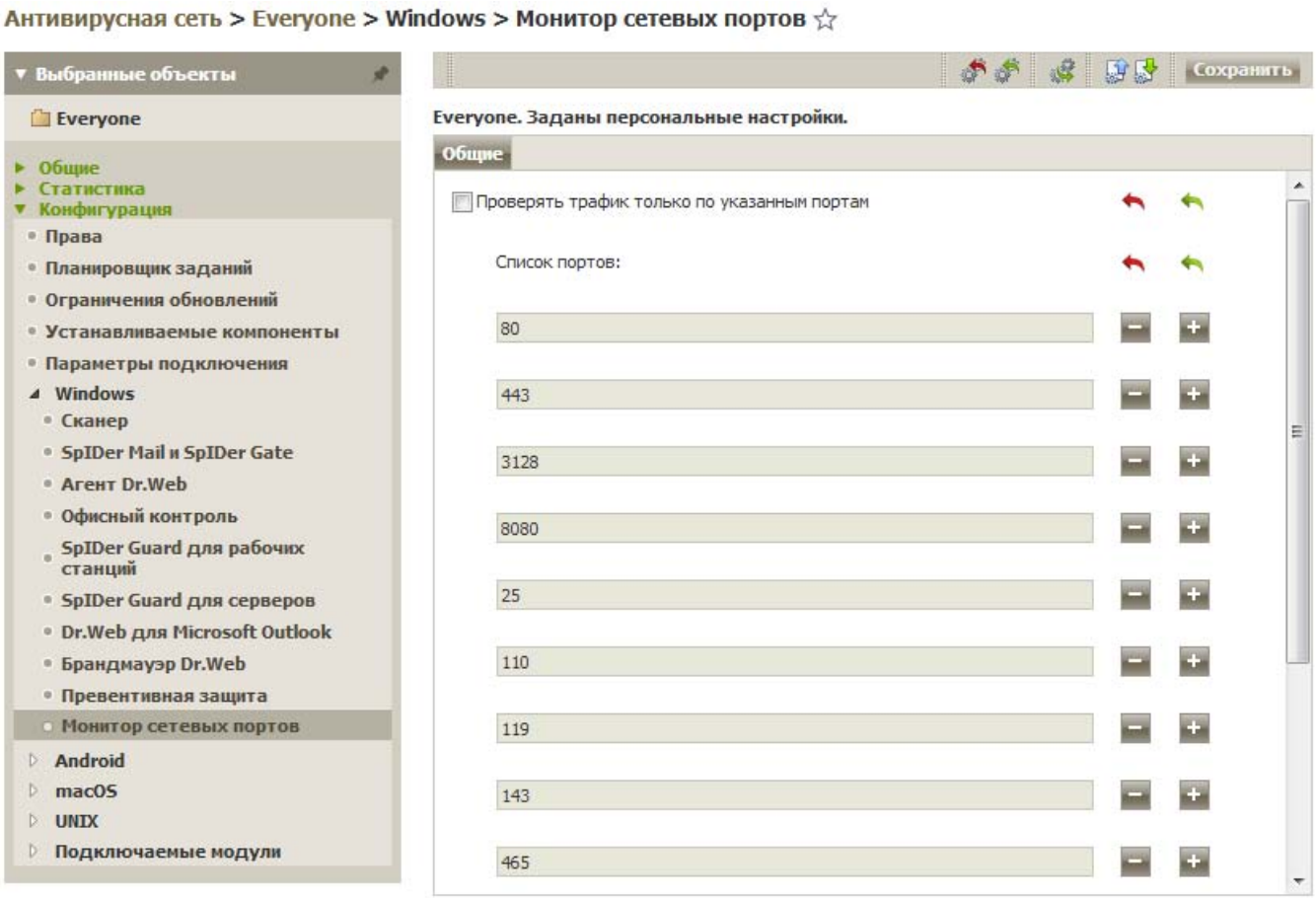
Настройка	Описание
Независимо от наличия цифровой подписи приложения	Выберите эту настройку, если приложение должно быть наличия у него действительной цифровой подписи.
При наличии действительной цифровой подписи приложения	Выберите эту настройку, если приложение должно быть действительной цифровой подписи приложения. В про компонентами SpIDer Mail и SpIDer Gate.
Любой трафик	Выберите эту настройку, чтобы исключить из проверки и приложения.
Зашифрованный трафик	Выберите эту настройку, чтобы исключить из проверки тол
По всем IP-адресам и портам	Выберите эту настройку, чтобы исключить из проверки порты.
По указанным IP-адресам и портам	Выберите эту настройку, чтобы указать IP-адреса или пор них трафика. Трафик, переданный с остальных IP-адресов другими настройками).
Задание адресов и портов	Для тонкой настройки исключений используйте следующие •чтобы исключить из проверки определенный домен п site.com:80; •для исключения из проверки трафика по нестандартному *:1111; •для исключения из проверки трафика от домена по любому

4. Нажмите **Сохранить**.

5. Чтобы удалить приложение из списка исключений, нажмите  напротив элемента списка, соответствующего этому приложению.

6. Чтобы отредактировать параметры исключения приложения из проверки, выберите приложение в списке и нажмите  .

Настроить проверку можно также непосредственно через компонент **Монитор сетевых портов.**



Монитор сетевых портов проверяет порты, используемые транспортными протоколами TCP. Перехваченное соединение анализируется, и по содержанию трафика определяется тип протокола. В зависимости от типа протокола используются необходимые настройки. Почтовые протоколы проверяются в соответствии с настройками SpIDer Mail, а остальные — в соответствии с настройками SpIDer Gate и Офисного контроля.

- SpIDer Mail перехватывает обращения любых почтовых клиентов компьютера к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP (под IMAP4 имеется в виду IMAPv4rev1), обнаруживает и обезвреживает почтовые вирусы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер.
- SpIDer Gate проверяет входящий HTTP-трафик и блокирует передачу объектов, содержащих вредоносные программы (при настройках по умолчанию). Через протокол HTTP работают веб-обозреватели (браузеры), менеджеры загрузки и многие другие приложения, обменивающиеся данными с веб-серверами, то есть работающие с сетью Интернет.
- Офисный контроль осуществляет ограничение доступа пользователей к сайтам в соответствии с настройками Веб-фильта, белого и черного списков сайтов.

По умолчанию **Монитор сетевых портов** проверяет входящий и исходящий трафик по всем портам. Включите опцию **Проверять трафик только по указанным портам**, чтобы компонент проверял трафик только по портам, указанным в Списке портов.

По умолчанию в Списке портов указаны номера портов, которые используются почтовыми и HTTP протоколами.

- Чтобы добавить новый порт в список, нажмите  .

•Чтобы удалить порт, нажмите кнопку напротив элемента списка, соответствующего этому порту.

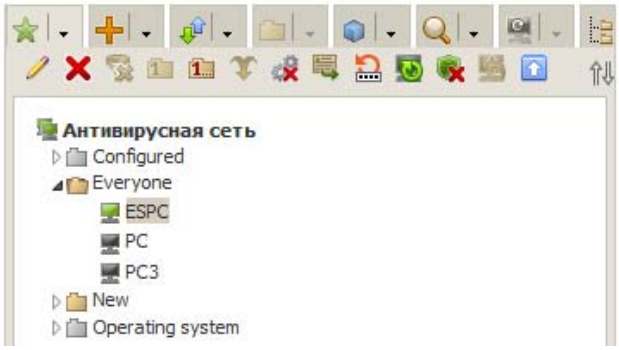
При обновлениях антивирусного ПО Dr.Web вместе с вирусными базами производится автоматическая загрузка обновленных списков адресов веб-сайтов по всем тематическим категориям.

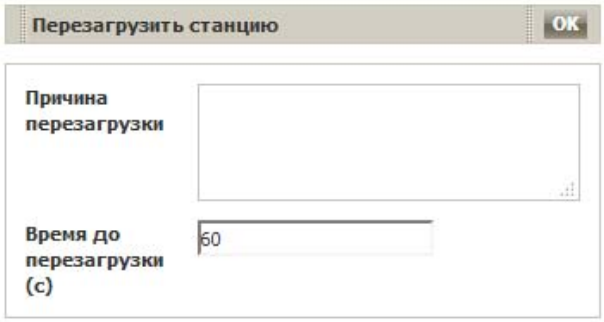
Сообщить о ложном срабатывании или пропуске вредных ссылок в модуле **Офисного контроля** можно на странице http://support.drweb.com/new/urlfilter.

По окончании настройки нажмите на кнопку **Сохранить**.

7.6.6. Перезагрузка рабочей станции через Центр управления

Администратор антивирусной сети имеет возможность принудительно перезагрузить станцию защищаемой сети — в том числе в случае необходимости экстренной установки обновлений. Для того чтобы перезагрузить станцию, необходимо выбрать станцию или группу, нажать значок , указать причину перезагрузки, задержку по времени и нажать **ОК**.

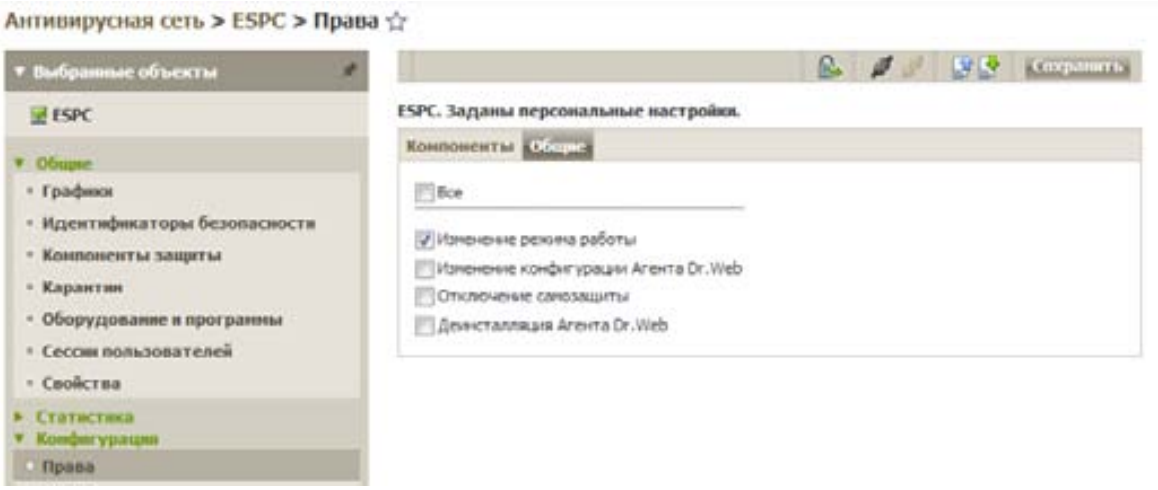




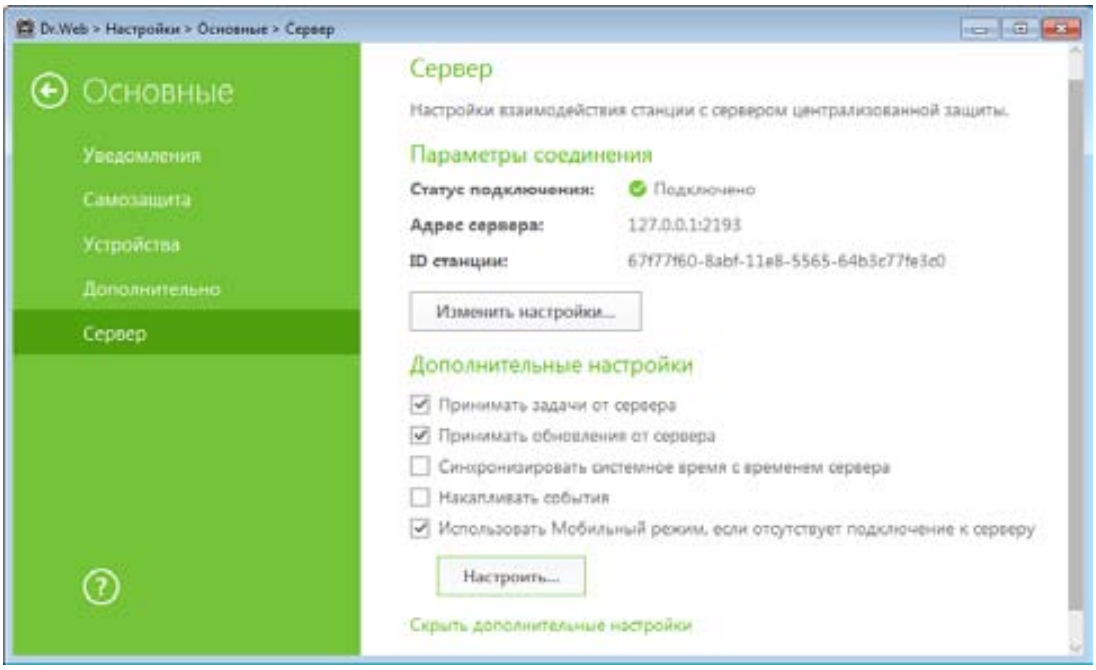
7.6.7. Настройки для мобильных пользователей

Наличие мобильного (автономного от Сервера) режима работы Агента позволяет обеспечить антивирусную защиту станции даже в том случае, если ее соединение с Сервером Dr.Web затруднено или невозможно по каким-то причинам. Например, это актуально для защиты ноутбуков сотрудников, которые по долгу службы часто бывают в командировках. Для таких пользователей администратор может как определять режим подключения Агента Dr.Web к Серверу Dr.Web, так и включать специальный мобильный режим работы с возможностью прямого подключения к серверам обновления ВСО.

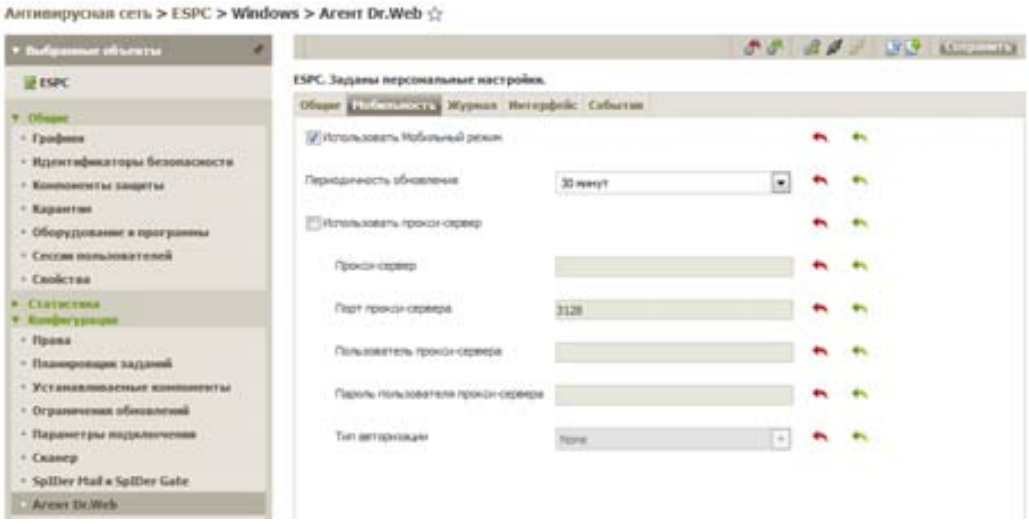
Для включения возможности включения мобильного режима работы на станции, необходимо выбрать ее в Центре управления, затем в разделе **Конфигурация → Права → Общие** отметить флажком пункт **Изменение режима работы**.



После этого на стороне пользователя рабочей станции в окне настроек Агента (**Настройки → Основные → Сервер → Дополнительные настройки)** отметьте флажком пункт **Использовать Мобильный режим, если отсутствует подключение к серверу**. После этого при отсутствии связи с Сервером Dr.Web антивирус будет автоматически получать обновления напрямую с серверов ВСО Dr.Web.



Для настройки параметров подключения к Интернету для конкретной станции или группы необходимо выбрать пункт **Конфигурация → Агент Dr.Web**, перейти на вкладку **Мобильность** и настроить режим подключения к Интернету.

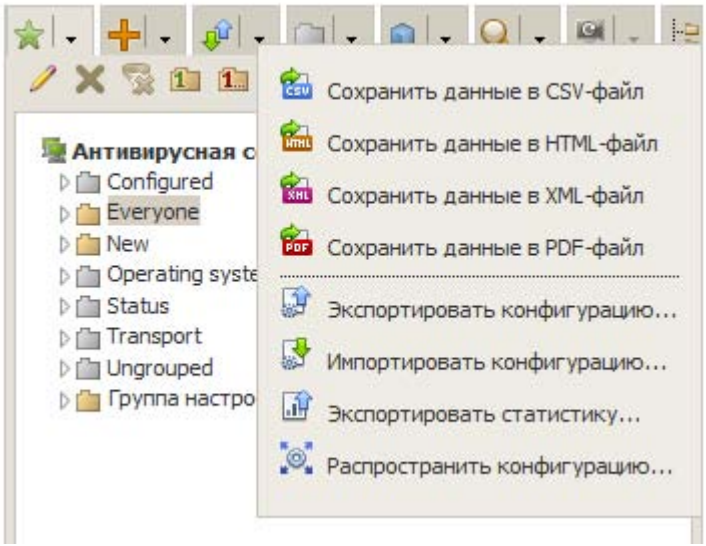


На вкладке **Мобильность** задаются параметры Мобильного режима **Агента**:

- В поле **Периодичность обновления** укажите временной промежуток между обновлениями антивирусного ПО.
- Флажок **Использовать прокси-сервер** указывает на необходимость использовать указанный HTTP прокси-сервер при получении обновлений из сети Интернет.

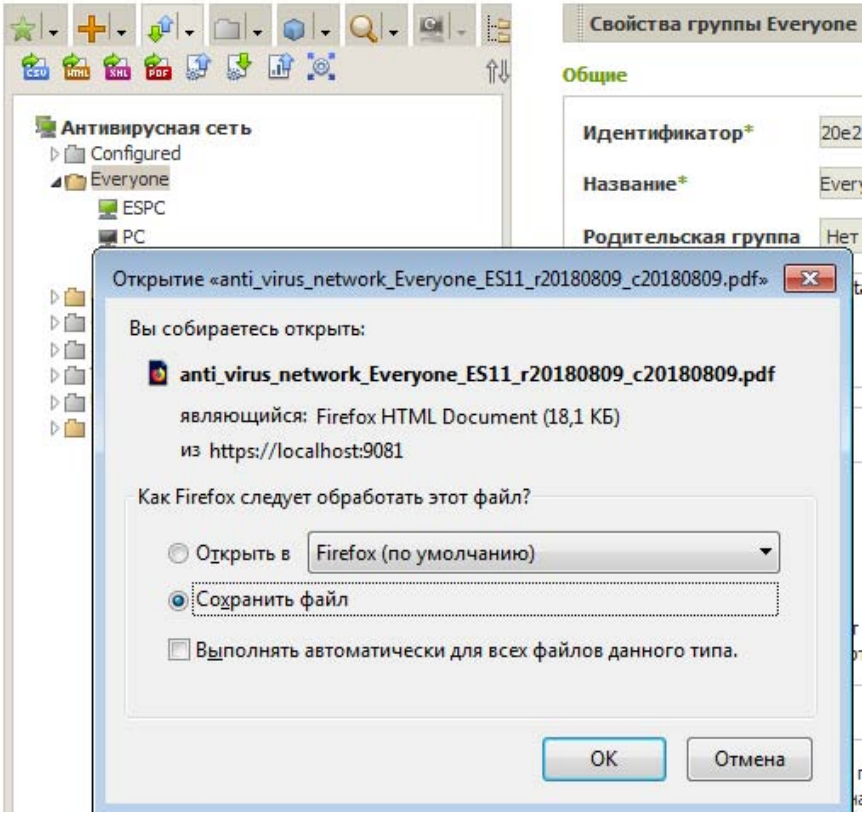
7.6.8. Экспорт и импорт данных о станциях антивирусной сети

В случае необходимости администратор может сохранить конфигурации любых компонентов антивирусной сети в отдельный файл, переключившись в режим показа дерева антивирусной сети и выбрав значок  .

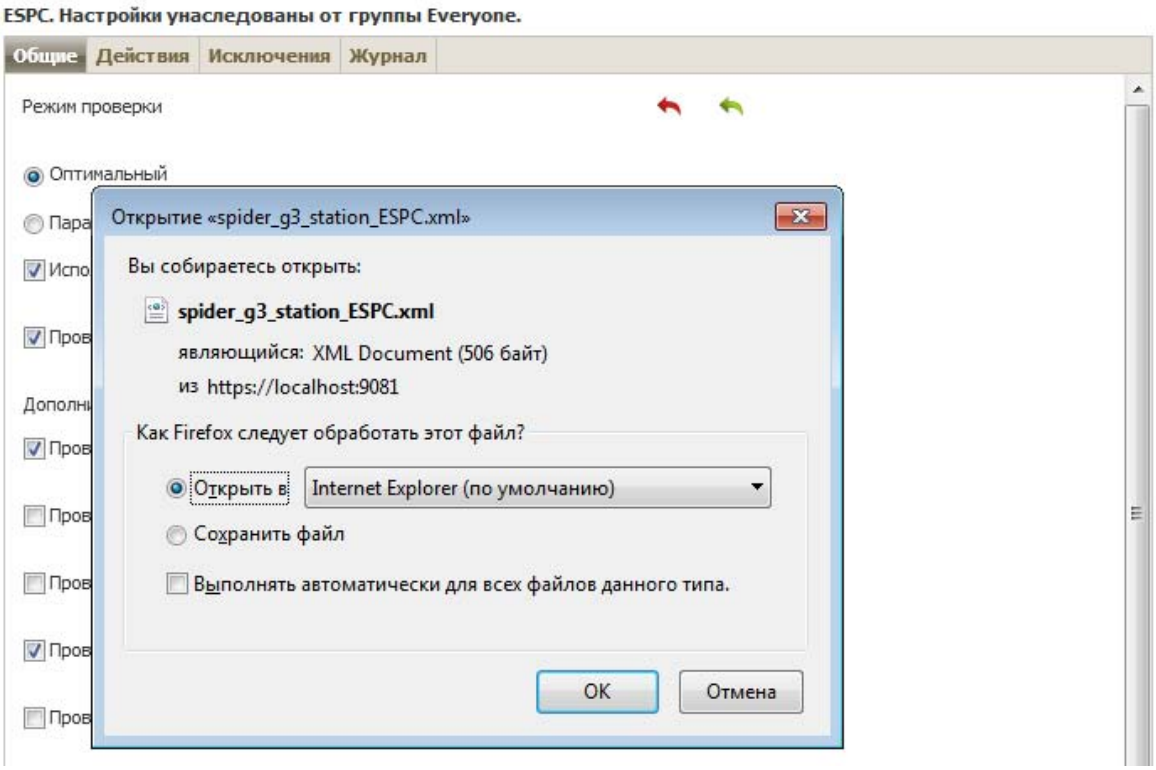


Экспорт возможен в форматы XML, PDF, HTML и CSV.

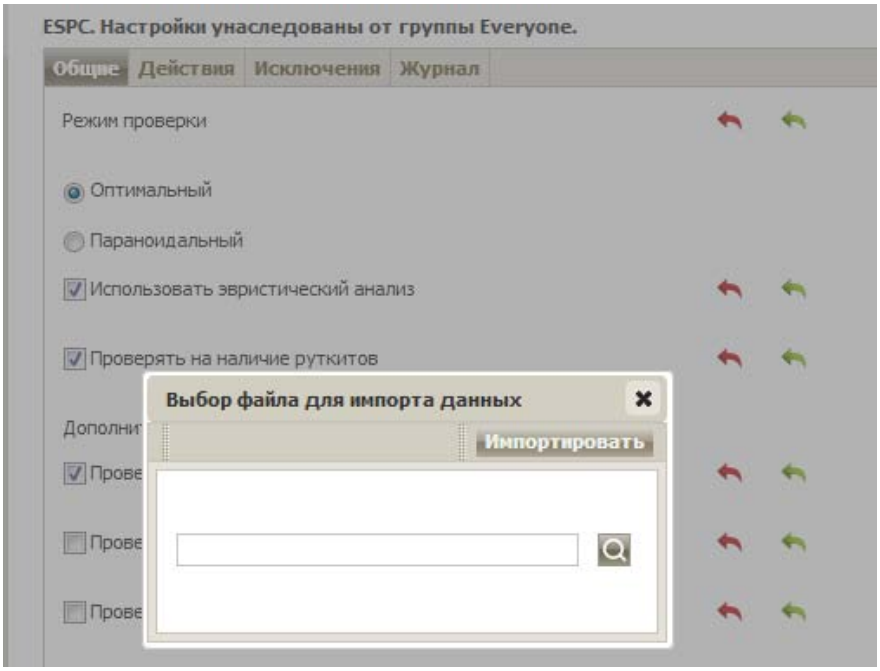
Подробно возможности экспорта, импорта и распространения конфигураций станций и групп описаны в разделе **Экспорт, импорт и распространение конфигураций**.



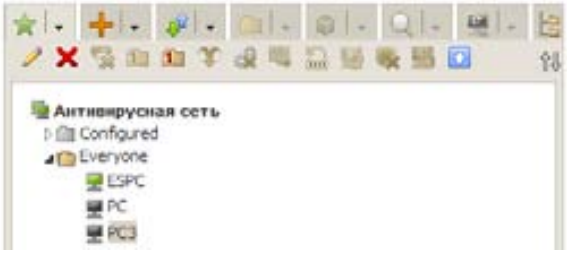
Администратор сети также имеет возможность экспорта и импорта настроек отдельных антивирусных компонентов станции из Центра управления в XML-файл. Для этого необходимо выбрать станцию или группу, затем интересующий компонент антивирусной защиты в группе **Конфигурация** меню **Антивирусная сеть** и на панели инструментов нажать кнопку  .

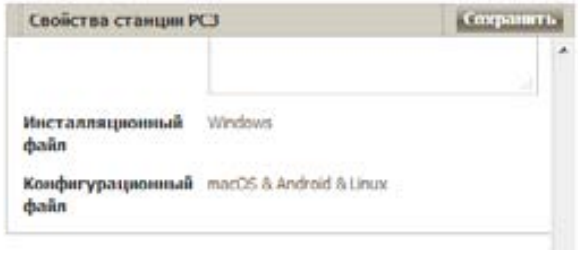


Сохраненные параметры администратор может в дальнейшем распространить по иным серверам антивирусной сети, импортировав их аналогичным образом.



Для выгрузки конфигурационного файла с настройками подключения Агентов Dr.Web под ОС Android, macOS и семейства UNIX, необходимо выбрать станцию или группу и нажать на ссылку **Конфигурационный файл** на панели справа.



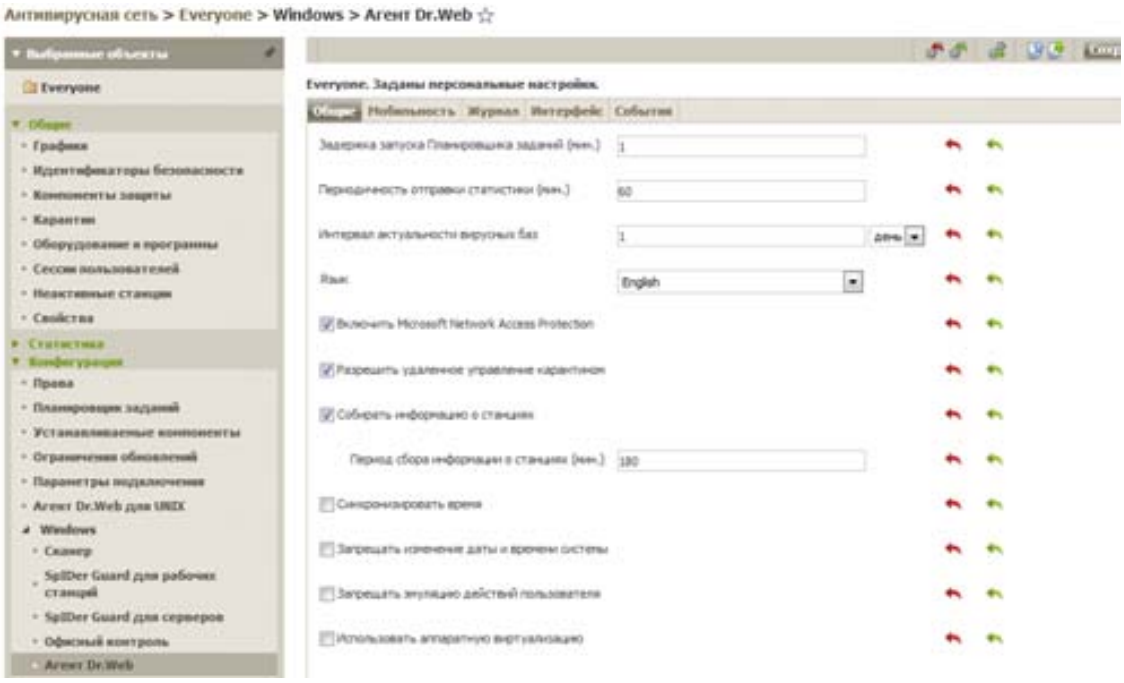


7.7. Контроль состояния антивирусной сети

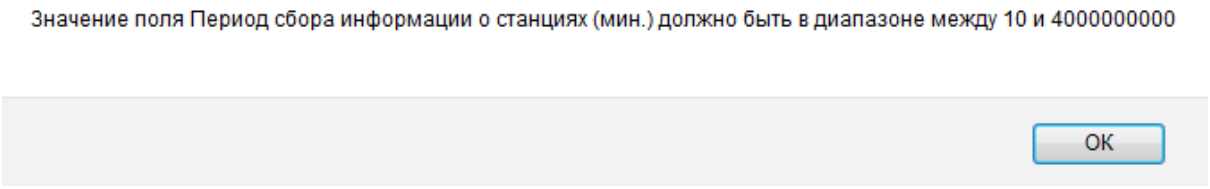
7.7.1. Просмотр и сравнение состава аппаратно-программного обеспечения на станциях антивирусной сети

Администратор антивирусной сети имеет возможность просмотра и сравнения состава аппаратно-программного обеспечения на станциях антивирусной сети.

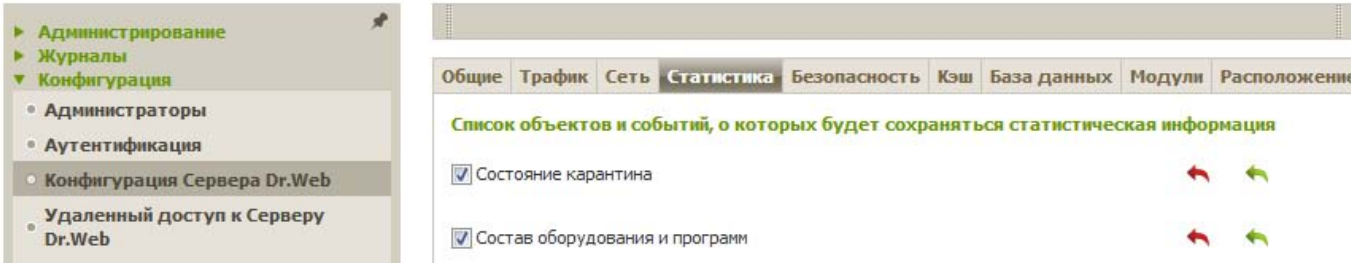
По умолчанию (в целях экономии трафика) возможность получения информации об аппаратном и программном обеспечении отключена. Для включения данной функции выберите интересующие станции или группы, для ОС Windows выберите в группе **Конфигурация → Windows → Агент Dr.Web** и на вкладке **Общие** установите флажок **Собирать информацию о станциях**. Задайте в соответствующем поле **Период сбора информации о станциях (мин.)** периодичность отправки **Агентами** на **Сервер** актуальной информации о программно-аппаратном обеспечении.



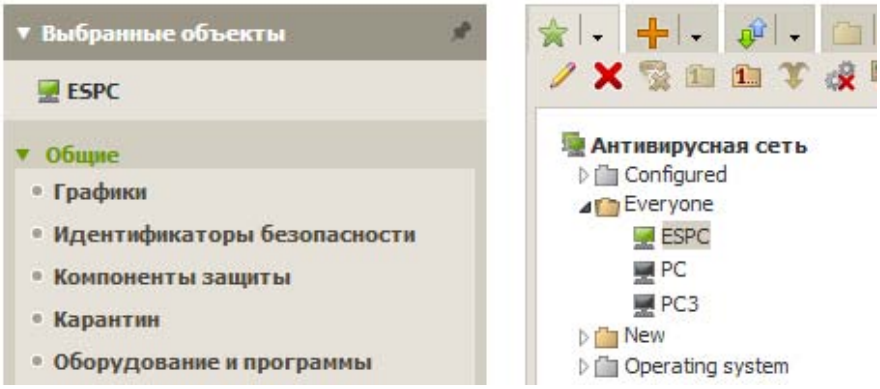
При этом если флажок выставлялся для группы, необходимо убедиться, что у станции, по которой просматривается статистика, флажок унаследован — у модуля агента не заданы персональные настройки.



В разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** на вкладке **Статистика** указывается, какая статистическая информация должна записываться в журнал протокола и заноситься в базу данных антивирусного сервера. Для регистрации и добавления в БД соответствующего типа информации установите флажок **Состав оборудования и программ**, что обеспечит мониторинг состава аппаратно-программного обеспечения станций и запись информации в базу данных.

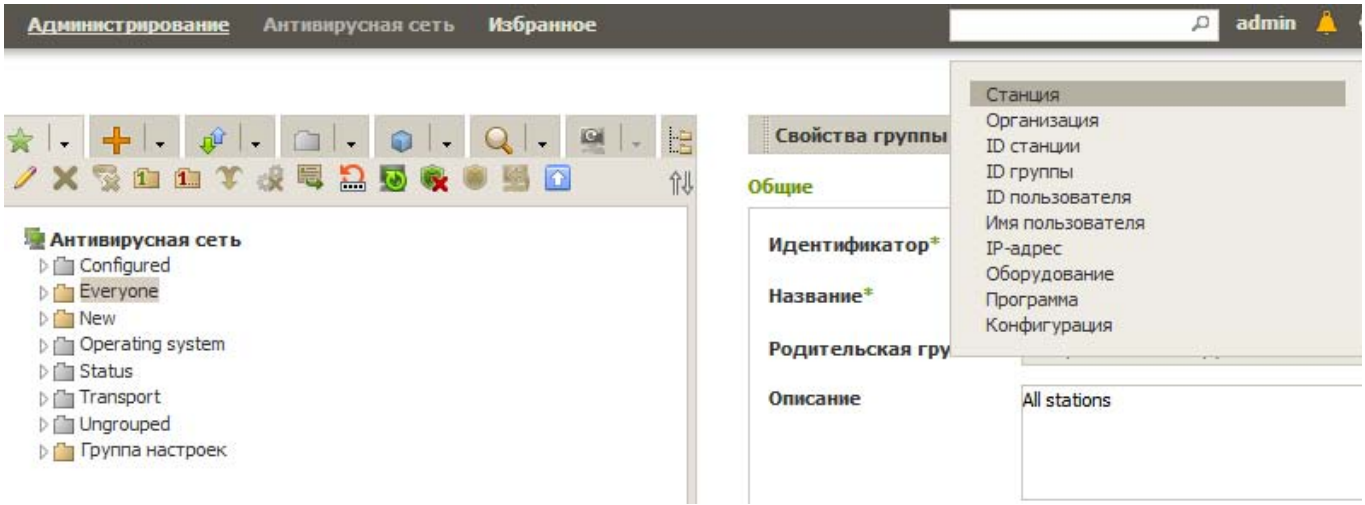


При выборе станции в антивирусной сети в меню **Общие** становится доступным пункт **Оборудование и программы**.



Администратор антивирусной сети имеет возможность поиска станций в сети по критериям имеющегося программного или аппаратного обеспечения. Для этого после выбора группы необходимо нажать на поле поиска и в выпадающем меню выбрав один из двух пунктов:

- **Оборудование** — для поиска станций по названию аппаратного обеспечения, установленного на станции,
- **Программа** — для поиска станций по названию программного обеспечения, установленного на станции.

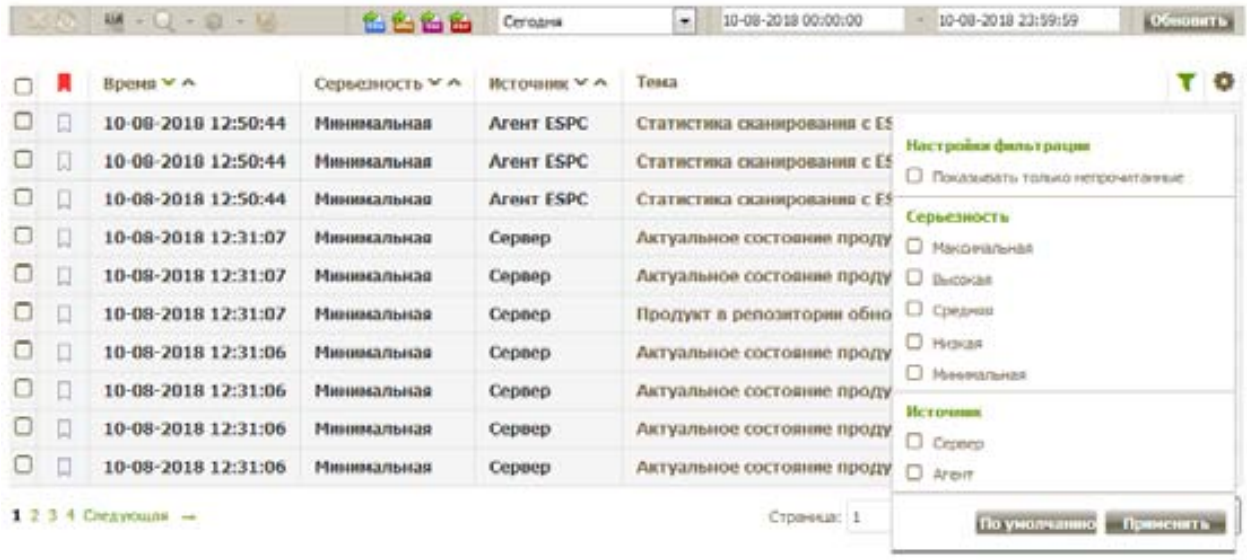


7.7.2. Контроль состояния защиты сети

Контролировать состояние антивирусной сети, построенной на базе Dr.Web Enterprise Security Suite, можно с помощью таблицы состояния станций, доступной в меню **Антивирусная сеть**, а также с помощью отчетов и оповещений, формируемых антивирусным сервером.

Таблицу **Состояние**, которая показывает состояние станций, можно посмотреть, выделив в дереве групп и станций группу станций или конкретную станцию, состояние которой необходимо отобразить, и выбрать в меню слева **Статистика → Состояние**.

В таблице **Состояние** с помощью фильтра ( ) можно выбирать уровень минимальной серьезности отображаемых проблем. Так, если выбрать уровень **Минимальная**, то будут отображены все сообщения о проблемах — как с очень высокой серьезностью, так и с очень низкой (информативной). Наоборот, если выбрать уровень сообщений **Максимальная**, то будут выведены только сообщения с очень высоким уровнем серьезности (критичные).



Также можно выбрать типы источников, информация от которых будет отображаться, с помощью группы настроек **Источник**. В качестве источников могут выступать антивирусные агенты и антивирусные серверы. Также может выводиться информация по станциям, которые в данный момент не подключены к антивирусному серверу, или по станциям, с которых к настоящему моменту был удален антивирусный агент.

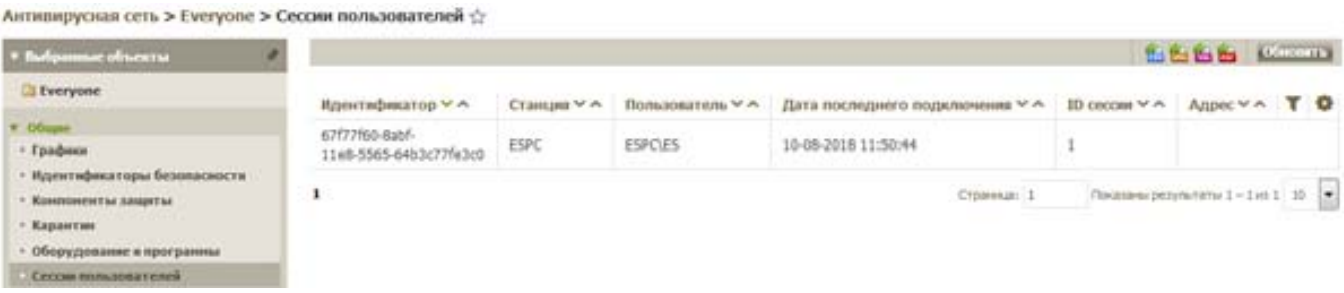
7.7.3. Просмотр списка неактивных станций антивирусной сети

Для поиска неактивных станций выберите группу антивирусной сети и далее п ункт **Неактивные станции** меню **Общие**.

7.7.4. Просмотр сессий пользователей антивирусной сети

Для включения функции сбора информации о сессиях пользователей антивирусной сети (статистической информации, которая записывается в журнал протокола и заносится в базу данных антивирусного сервера) в разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**, на вкладке **Статистика** установите флажок **Сессии пользователей станции**. После этого начнется мониторинг сессий пользователей рабочих станций и запись в базу данных регистрационных имен пользователей, вошедших в систему на компьютере с установленным **Агентом**.

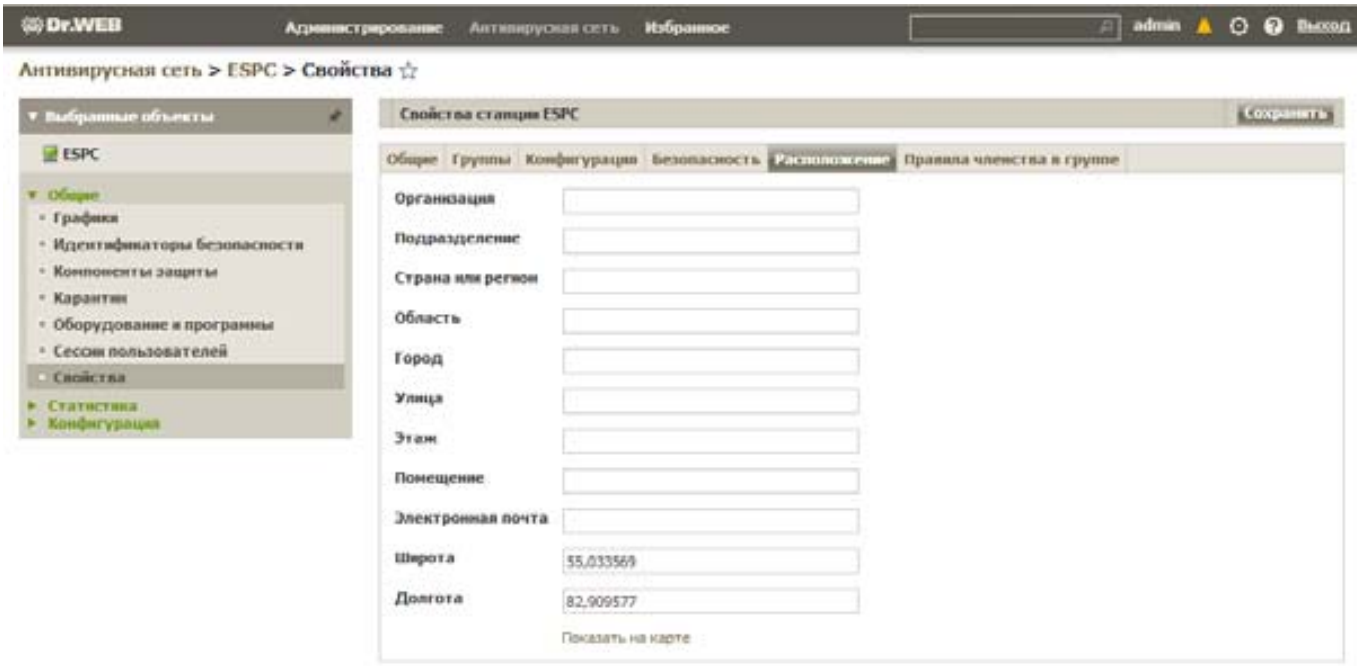
Для просмотра сессий пользователей на станциях выберите станцию или группу и далее пункт **Сессии пользователей** меню **Общие**.



7.7.5. Указание места расположения станций сети

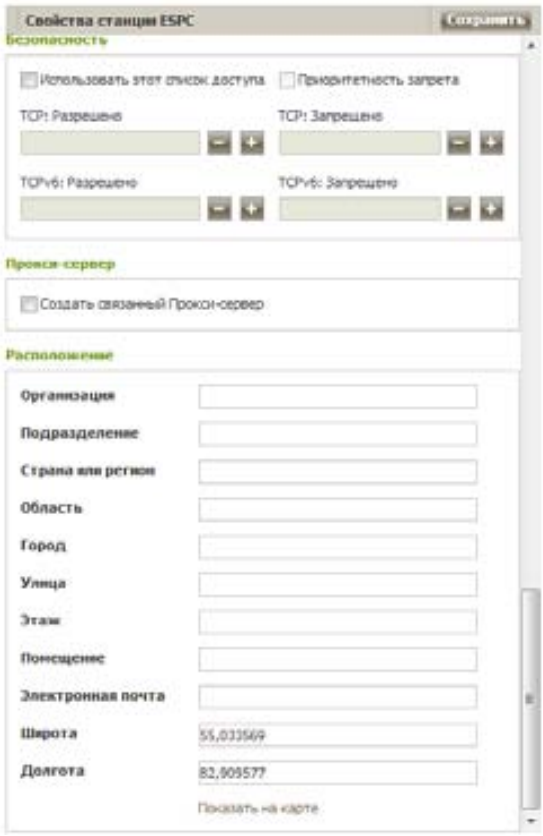
В разделе **Расположение** свойств станции вы можете задать дополнительную информацию о физическом расположении станции.

1. Задайте в полях **Широта** и **Долгота** географические координаты станции в формате десятичных градусов (Decimal Degrees), например: 55,033569.
2. Нажмите кнопку **Сохранить** для сохранения введенных данных.



3. На вкладке **Расположение** отобразится превью карты OpenStreetMaps с меткой, соответствующей заданным координатам.

   В случае если загрузка превью невозможна, отображается текст **Показать на карте**.



Также на данной вкладке вы можете просмотреть расположение станции на географической карте — для просмотра полноразмерной карты нажмите на превью или на текст **Показать на карте**.

7.8. Отчеты

Dr.Web Enterprise Server ведет несколько журналов событий, происходящих в антивирусной сети. Среди них **Журнал аудита** и **Протокол выполнения заданий**.

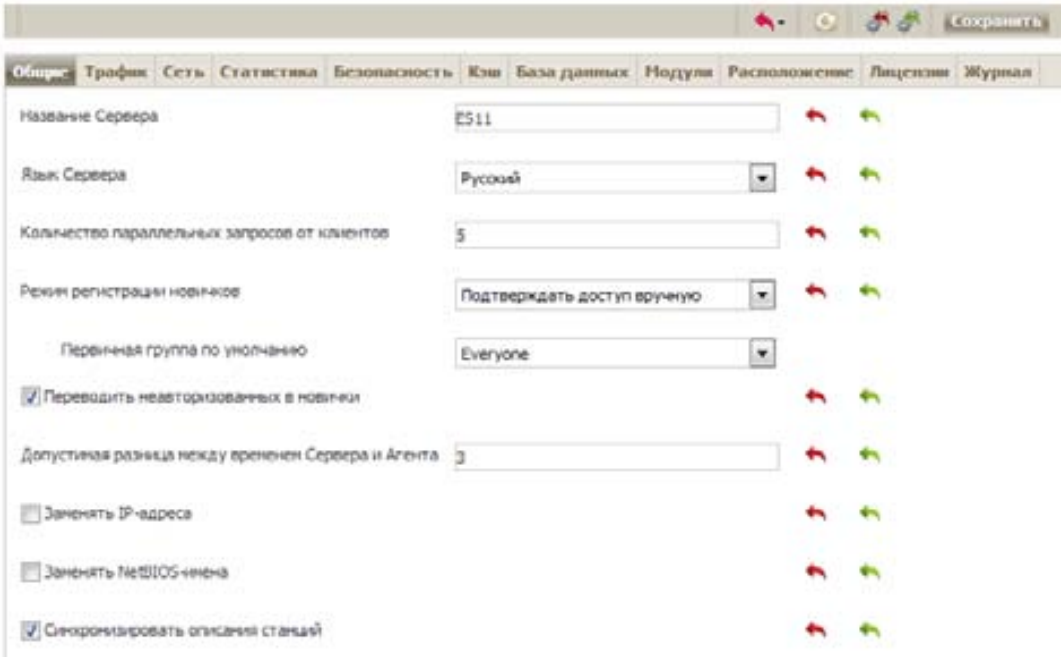
Настройка параметров аудита производится на странице **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web на вкладке Безопасность.** Управление журналом аудита сервера осуществляется при помощи соответствующих флажков:

- **Аудит операций** включает ведение журнала аудита операций администратора с Центром управления, а также запись журнала в БД.

- **Аудит внутренних операций сервера** включает ведение журнала аудита внутренних операций Сервера и запись журнала в БД.
- **Аудит операций Web API** включает ведение журнала аудита операций через XML API и запись журнала в БД.

Также на формат журнала влияет установка некоторых флажков на вкладке **Общие**:

- **Заменять IP-адреса** предписывает программе заносить в файл протокола не IP-адреса рабочих станций, а их доменные имена.
- **Заменять NetBios-имена** предписывает отображать в каталоге антивирусной сети Центра управления не наименования рабочих станций, а их доменные имена (при невозможности определения доменных имен отображаются IP-адреса).



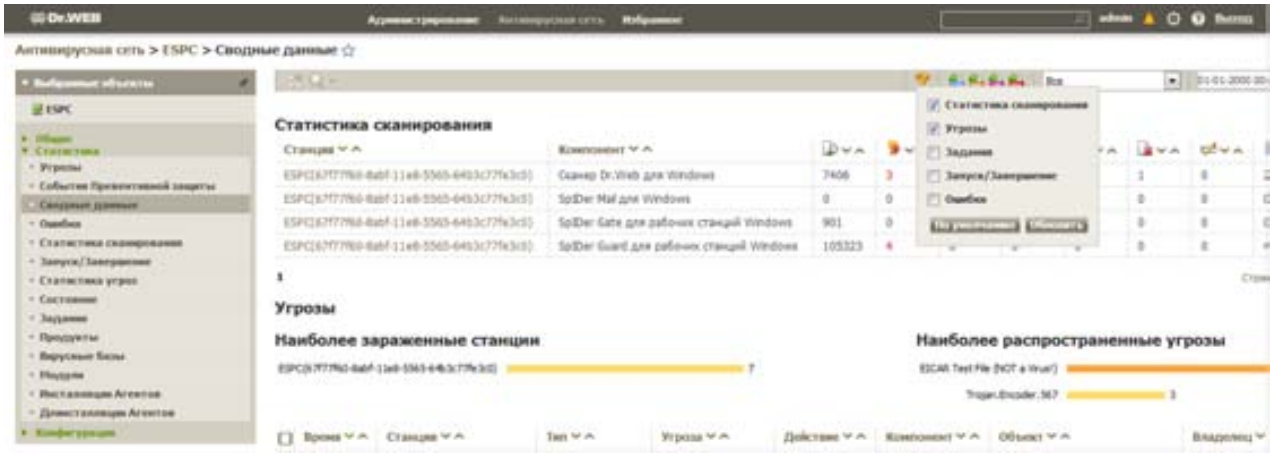
Внимание!

- Параметры **Заменять IP-адреса** и **Заменять NetBios-имена** по умолчанию отключены. При неправильной настройке службы DNS их включение может значительно замедлить работу Сервера. При включении любого из этих режимов рекомендуется разрешить кэширование имен на DNS-сервере.
- Если флажок **Заменять NetBios-имена** установлен и в антивирусной сети используется Прокси-сервер, то для всех станций, подключенных к Серверу через Прокси-сервер, в Центре управления в качестве названий станций будет отображаться название компьютера, на котором установлен Прокси-сервер.
- **Синхронизировать описания станций** — предписывает синхронизацию описания компьютера пользователя с описанием станции в Центре управления. Если описание

станции в Центре управления отсутствует, то в данное поле будет записано описание компьютера на стороне пользователя. Если описания различаются, то данные в Центре управления будут заменены на пользовательские.

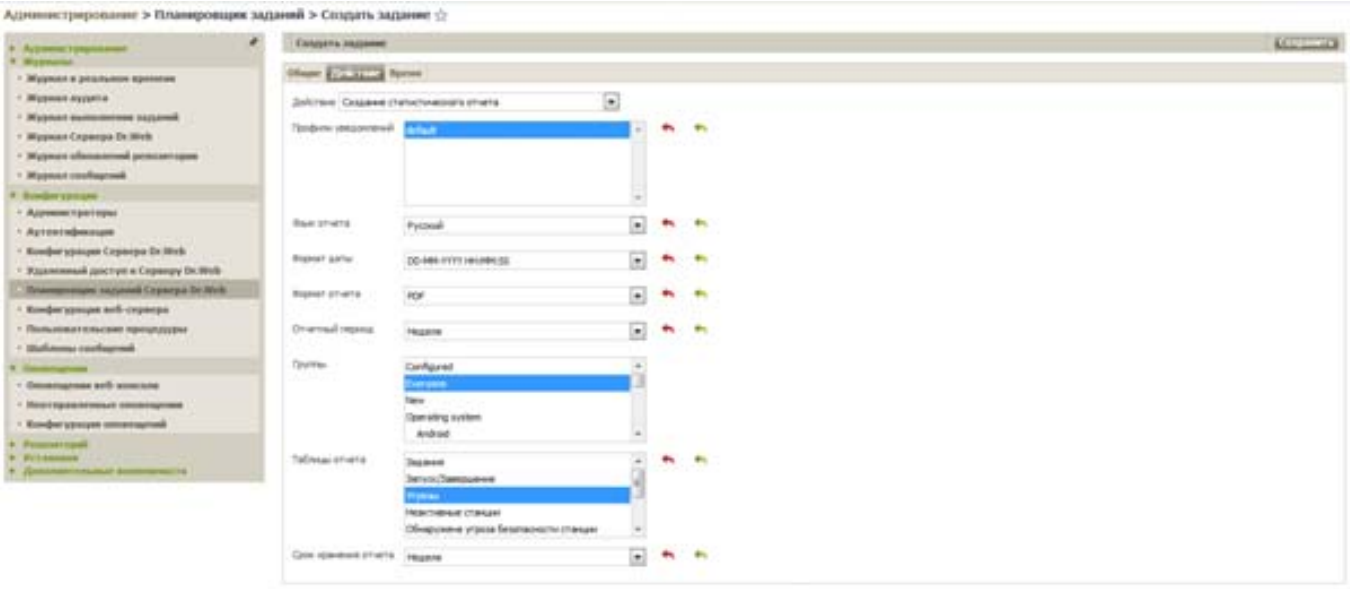
Для просмотра отчетов:

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите **Статистика → Сводные данные**.
2. Откроется окно, содержащее табличные данные отчета. Для того чтобы включить в отчет определенные статистические данные, нажмите на кнопку  на панели инструментов и выберите требуемые типы в выпадающем списке: **Статистика**, **Инфекции**, **Задания**, **Запуск/завершение**, **Ошибки**. Статистика, включаемая в данные разделы отчета, соответствует статистике, содержащейся в соответствующих пунктах раздела **Статистика**. Для просмотра отчета с выбранными таблицами нажмите на кнопку **Обновить**.



3. Для выбора отчетных данных за предопределенный период укажите диапазон из выпадающего списка на панели задач: отчет за определенный день или месяц. Либо вы можете выбрать произвольный диапазон дат, для этого введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для просмотра данных нажмите на кнопку **Обновить**.
4. При необходимости сохранить отчет для распечатки или дальнейшей обработки нажмите на кнопку, вы можете сделать это, экспортировав его в один из форматов: CSV, HTML, XML и PDF с помощью соответствующих кнопок на панели инструментов:  .

Если статистические отчеты необходимо формировать регулярно, этот процесс можно автоматизировать с помощью расписания заданий Сервера Dr.Web. Для этого в меню **Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web** на вкладке **Действие** в выпадающем списке **Действие** выберите пункт **Создание статистического отчета** и, настроив его параметры, нажмите **Сохранить**.



7.8.1. Аудит действий администраторов

Журнал аудита содержит информацию о действиях, осуществляемых при помощи управляющих подсистем Dr.Web Enterprise Security Suite, в том числе администраторами антивирусной сети. Таким образом, есть возможность в случае необходимости проверить все действия администраторов антивирусной сети. Журнал можно отобразить в Центре управления, перейдя в раздел **Администрирование → Журналы → Журнал аудита**. Диапазон дат можно задать, используя значки календаря слева от дат, расположенных непосредственно над журналом.

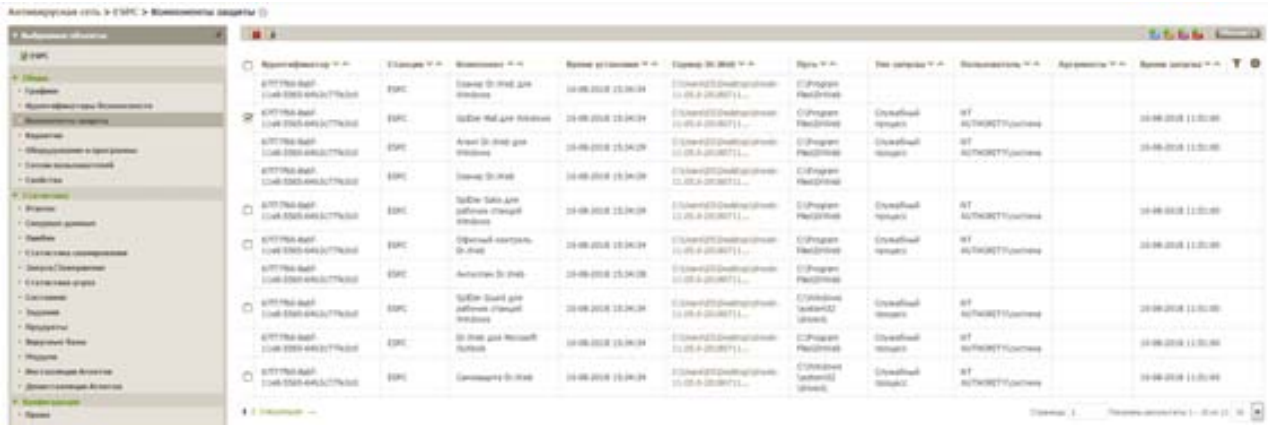
7.8.2. Анализ выполнения запланированных заданий

Журнал выполнения заданий содержит отчет об успешности или неуспешности выполнения заданий, запланированных к выполнению антивирусным сервером. Для его просмотра, выберите р аздел **Администрирование → Журналы → Журнал выполнения заданий**. Диапазон дат можно задать, используя значки календаря слева от дат, расположенных непосредственно над журналом.

Аналогичным образом можно просматривать и остальные журналы: **Сервера Dr.Web** (содержит набор логов Сервера), **Обновления репозитория, Сообщений** и **В реальном времени**.

7.8.3. Контроль запущенных процессов

Администратор может контролировать все запущенные процессы с помощью меню **Антивирусная сеть → Общие → Компоненты защиты** для выбранной группы или рабочей станции. В таблице приведена информация по установленным компонентам и их статус.

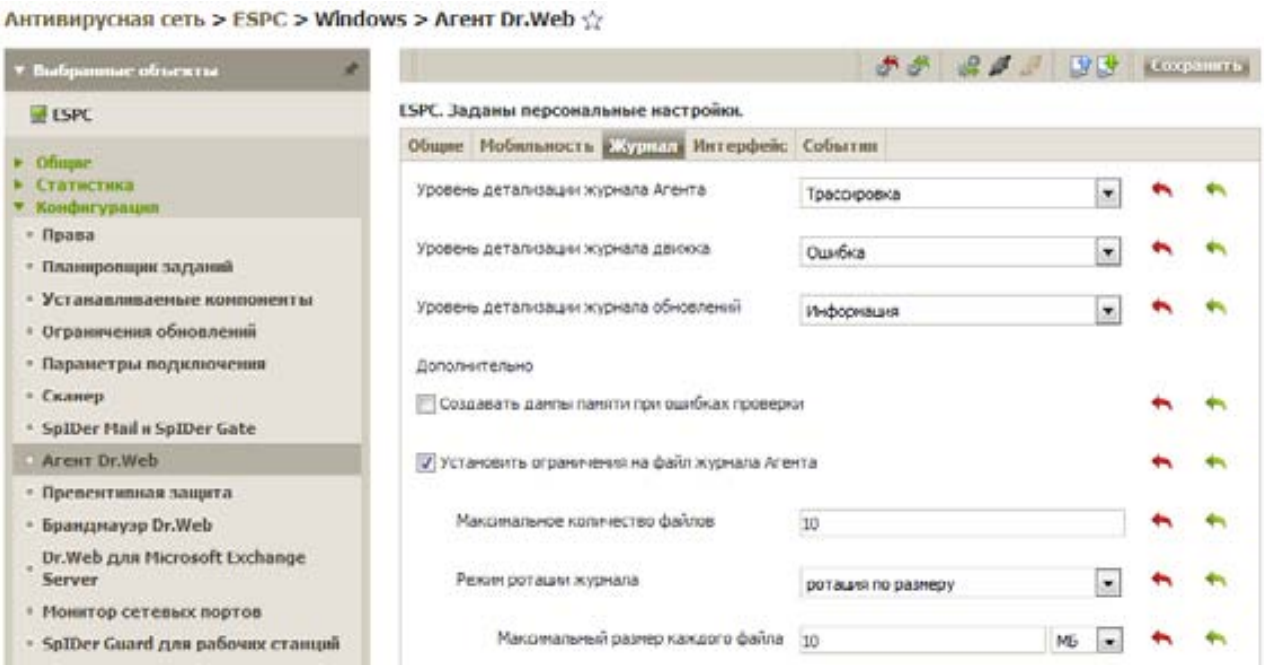


В списке отображаются в том числе и процессы, запущенные пользователем.

В случае необходимости администратор может прервать выполнение любого из них или вновь запустить, используя кнопки  и  соответственно.

7.8.4. Создание отчетов по компонентам

В случае необходимости администратор может автоматизировать создание отчетов, указывая при этом интересующую его степень подробности отчета. Для этого необходимо выбрать интересующую станцию или группу и задать параметры отчета на вкладке **Журнал** меню **Антивирусная сеть → Конфигурация → Агент Dr.Web**.

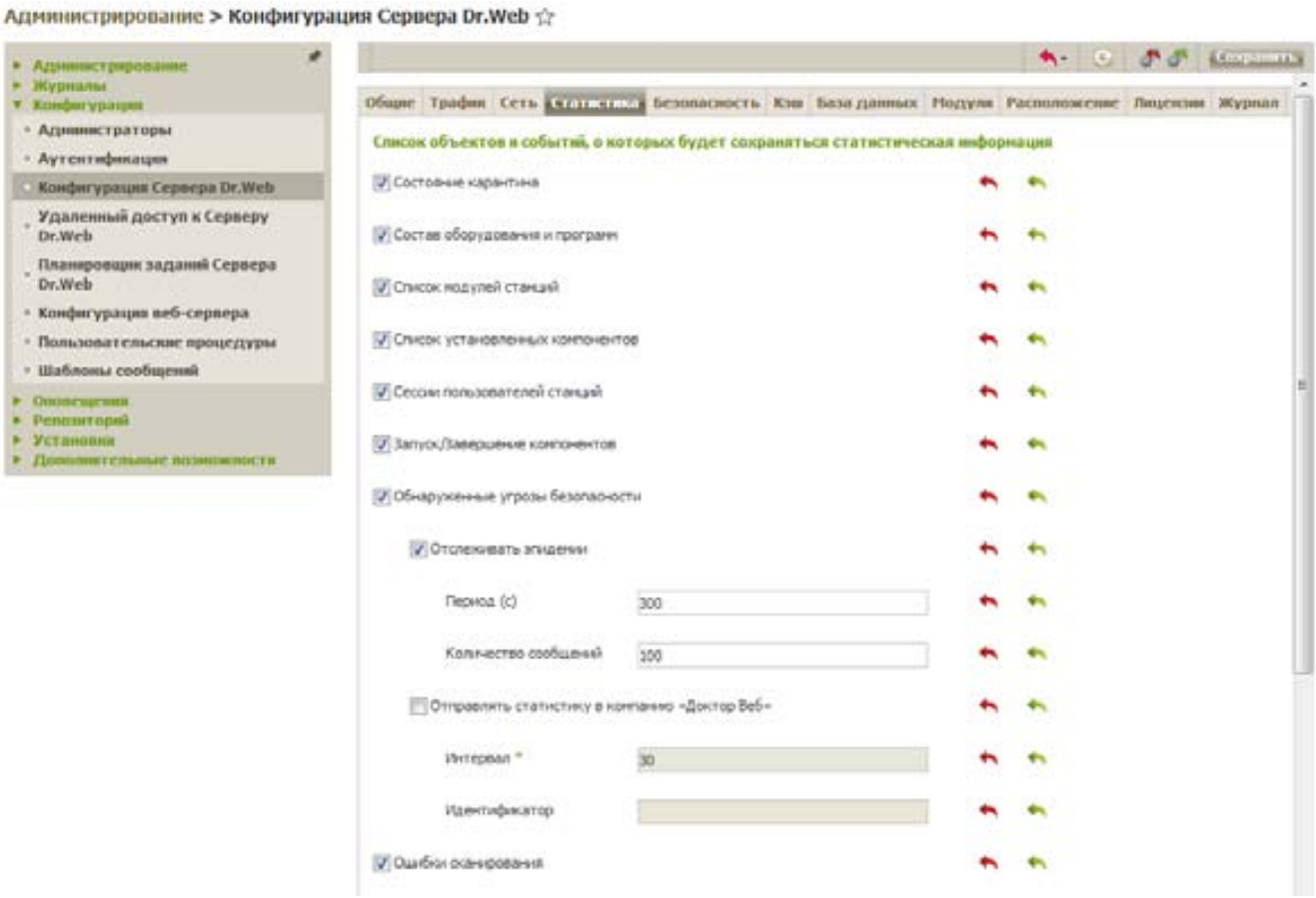


7.9. Сбор статистики. Формирование графиков активности вирусов, статистики по найденным типам вредоносных объектов, произведенным над ними действиям

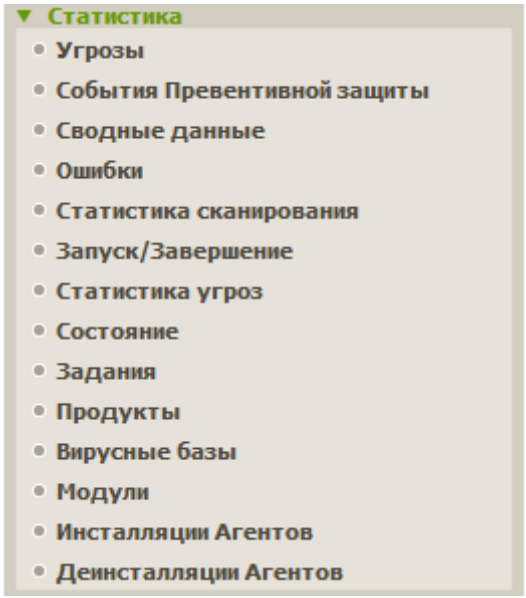
Используя возможности Центра управления, администратор может формировать отчеты о состоянии антивирусной защиты, в том числе о количестве обнаруженных вредоносных объектов, произведенных над ними действий.

Вы можете просматривать результаты работы компонентов рабочей станции — обновлений ПО, антивирусных сканирований и антивирусного мониторинга. Для этого служат статистические таблицы и графики.

Настройка видов собираемой статистики производится на вкладке **Статистика** раздела **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**.



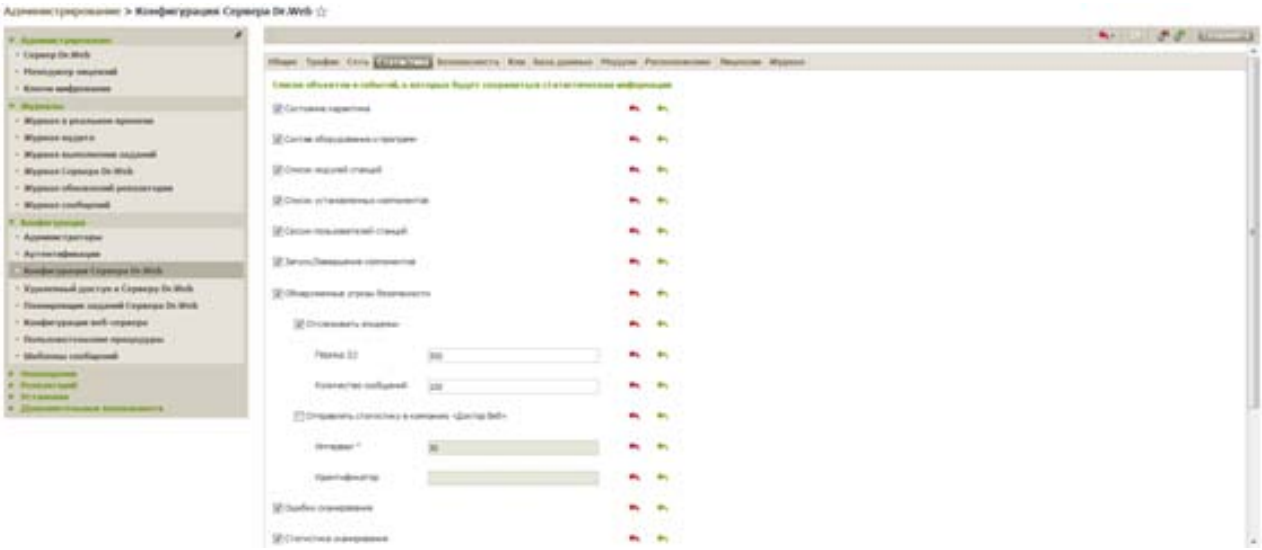
Для просмотра статистики выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы и в открывшемся управляющем меню (панель слева) выберите нужный пункт из группы **Статистика**:



- Сводные данные — для просмотра и сохранения отчетов, содержащих все сводные статистические данные или выборочные сводки по заданным типам таблиц. Не отображается в меню, если скрыты все остальные пункты меню в разделе **Статистика**.

- **Угрозы** — для просмотра информации об обнаруженных угрозах безопасности защищаемых станций: перечень зараженных объектов, расположение по станциям, названия угроз, действия антивируса и т. п.
- **События Превентивной защиты —** для просмотра информации о проблемах безопасности, обнаруженных компонентом **Превентивная защита**.
- **Ошибки** — для просмотра списка ошибок сканирования на выбранной рабочей станции за определенный период.
- **Статистика сканирования** — для получения статистики о работе антивирусных средств на станции.
- **Запуск/завершение** — для просмотра списка компонентов, запускавшихся на рабочей станции.
- **Статистика угроз** — для просмотра сведений об обнаружении угроз безопасности защищаемых станций, сгруппированных по типам угроз и по количеству угроз на станциях.
- **Состояние** — для просмотра сведений о необычном состоянии рабочих станций, возможно требующем вмешательства.
- **Задания** — для просмотра списка заданий, назначенных для рабочей станции в заданный период.
- **Продукты** — для просмотра информации об установленных продуктах на выбранных станциях. Под продуктами в данном случае понимаются продукты репозитория Сервера.
- **Вирусные базы** — для просмотра информации об установленных вирусных базах: название файла, содержащего конкретную вирусную базу; версия вирусной базы; количество записей в вирусной базе; дата создания вирусной базы. Пункт доступен только при выборе единичных станций.
- **Модули** — для просмотра подробной информации обо всех модулях антивируса Dr.Web: описание модуля: его функциональное название; файл, определяющий отдельный модуль продукта; полная версия модуля и т. д. Пункт доступен только при выборе станций.
- **Инсталляции Агентов** — для просмотра списка установок Агента на рабочую станцию или группу рабочих станций.
- **Деинсталляции Агентов** — для просмотра списка рабочих станций, с которых было удалено антивирусное ПО Dr.Web.

Для отображения скрытых пунктов раздела **Статистика** выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Сервера Dr.Web**. На вкладке **Статистика** установите соответствующие флажки (см. ниже), после чего нажмите кнопку **Сохранить** и перезагрузите Сервер.



Окна просмотра результатов работы различных компонентов и итоговой статистики рабочей станции имеют одинаковый интерфейс, и действия по детализации информации, предоставляемой ими, аналогичны.

Рассмотрим примеры использования меню **Статистика** Центра управления. Окна просмотра результатов работы различных компонентов и итоговой статистики рабочей станции имеют одинаковый интерфейс, и действия по детализации информации, предоставляемой ими, аналогичны.

Для получения статистики о работе антивирусных средств на станции:

1. Выберите в списке нужную станцию или группу. При необходимости просмотра статистики по нескольким станциям или группам возможен одновременный выбор нужных станций и групп с помощью клавиш SHIFT или CTRL.
2. Для того чтобы получить суммарную статистику без разбиения на сеансы, нажмите на пункт **Статистика сканирования** в разделе **Статистика**.
3. Откроется окно статистики. По умолчанию отображается статистика за последние сутки.
4. Для просмотра статистики за требуемый период выберите на панели инструментов интервал дат, в котором должны находиться отображаемые данные. Для выбора даты нажмите на значок календаря рядом с полем даты. Для того чтобы загрузить данные, нажмите на кнопку **Обновить**. В окно будут загружены таблицы со статистическими данными.
5. В разделе **Статистика сканирования** приведены суммарные данные:

   - при выборе станций — по выбранным станциям;
   - при выборе групп — по выбранным группам (при выборе нескольких групп будут показаны только группы, содержащие станции);
   - при выборе станций и групп одновременно — отдельно по всем станциям, в том числе входящим в выбранные не пустые группы.

6. Для того чтобы посмотреть подробную статистику работы конкретных антивирусных средств, нажмите на название станции в таблице. Если были выбраны группы, нажмите на название группы в таблице общей статистики, после чего — на название станции в показанной таблице. Откроется окно (или раздел текущего окна), содержащее таблицу с подробными статистическими данными.

7. Из таблицы со статистикой работы антивирусных средств станции или группы можно открыть окно настройки конкретного антивирусного компонента. Для этого нажмите на соответствующее название компонента в статистической таблице.
8. Чтобы произвести сортировку данных столбца таблицы, нажмите на соответствующую стрелку (сортировка по убыванию или по возрастанию) в заголовке соответствующего столбца.
9. При необходимости сохранить полученную таблицу статистики для распечатки или дальнейшей обработки, можно экспортировать ее в нужный формат, нажав на одну из соответствующих кнопок  .

Чтобы просмотреть сведения о необычном и (возможно) требующем вмешательства состоянии рабочих станций за определенный период:

1. Выберите в управляющем меню в разделе **Статистика** пункт **Состояние**.

   Если пункт **Состояние** не отображается в управляющем меню, то выберите пункт **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**. На вкладке **Статистика** установите флажок **Состояние станции**, после чего перезагрузите Сервер.

2. Сведения о состоянии станций отображаются в окне автоматически в соответствии с параметрами, указанными на панели инструментов.
3. Для того чтобы ограничить список сообщений о состоянии только сообщениями определенной серьезности, выберите уровень серьезности в выпадающем списке **Серьезность** на панели инструментов. По умолчанию выбран уровень **Минимальная**, что соответствует отображению максимально полного списка событий, поскольку в него включаются события, имеющие любую серьезность.
4. Действия по детализации и форматированию информации данной таблицы аналогичны описанным выше для таблицы статистики.

Для того чтобы просмотреть статистику по вирусным событиям в форме диаграмм:

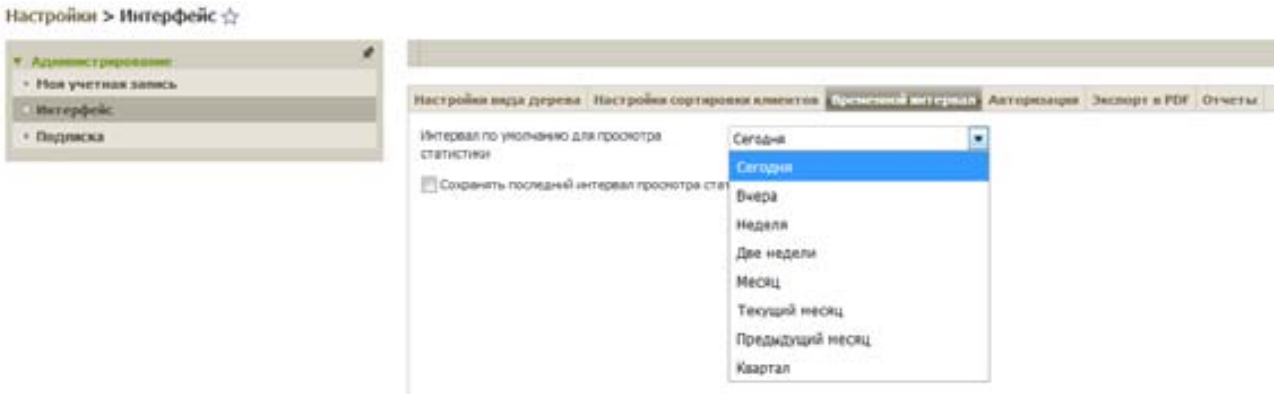
1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите в разделе **Общие** пункт **Графики**.

2. Откроется окно, содержащее графические данные. В зависимости от того, какой объект выбран в иерархическом списке (группа или станция), будут отображаться различные наборы графиков.

- **Вирусная активность** — на графике отображается общее количество вредоносных объектов, найденных в пределах каждого временного промежутка для всех выбранных станций и групп. График отображается, если задан временной период, превышающий одни сутки.
- **Наиболее распространенные угрозы** — приводится список из десяти угроз, встречающихся в наибольшем количестве файлов. На графике отображаются численные данные по объектам, соответствующим конкретной угрозе.
- **Классы угроз** — приводится список угроз в соответствии с классификацией вредоносных объектов. На круговой диаграмме отображается процентное соотношение между всеми обнаруженными угрозами.
- **Наиболее зараженные станции** — приводится список станций, на которых были обнаружены угрозы безопасности. На графике отображается общее количество угроз для каждой станции.
- **Произведенные действия** — приводится список действий, произведенных над обнаруженными вредоносными объектами. На круговой диаграмме отображается процентное соотношение между всеми произведенными действиями.

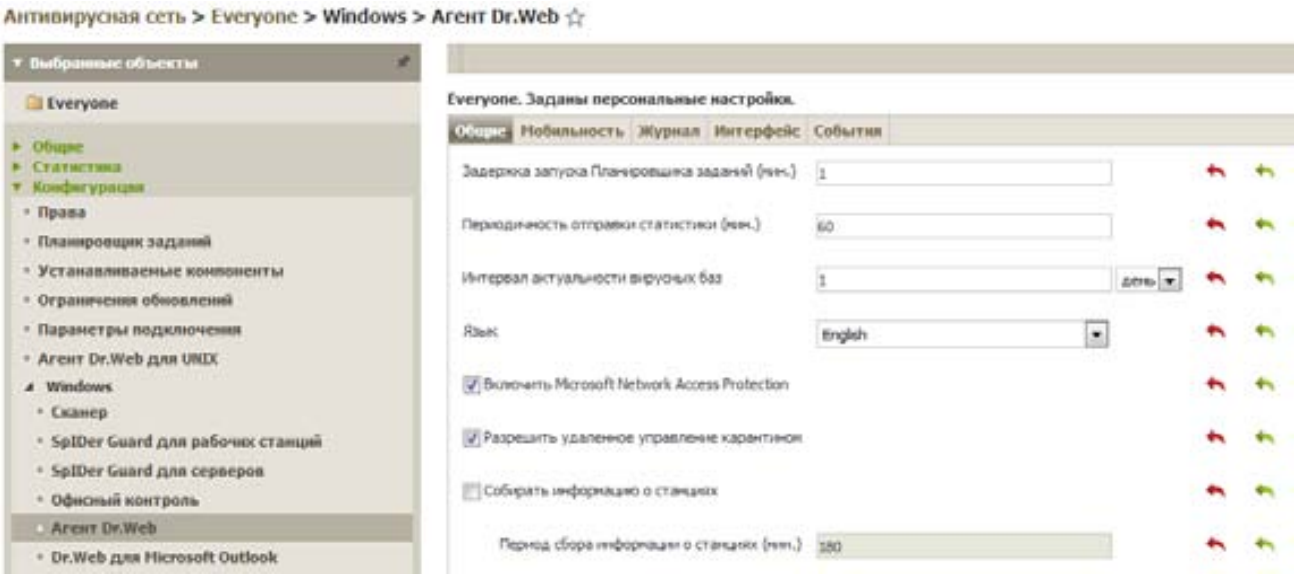
3. Для просмотра графических данных за предопределенный период выберите диапазон из выпадающего списка на панели задач: отчет за определенный день или месяц. Либо вы можете выбрать произвольный диапазон дат, для этого введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для просмотра данных нажмите на кнопку **Обновить**.
4. Чтобы исключить какой-либо пункт из отображения на графике (кроме графика **Вирусная активность**), нажмите на название этого пункта в легенде под графиком.

Администратор может задать временно интервал для вывода статистики, а также сохранить интервал, который был выбран последним при просмотре статистики. Для этого необходимо выбрать в разделе **Настройки → Администрирование → Интерфейс** вкладку **Временной интервал** и в списке **Интервал по умолчанию для просмотра статистики** задать нужное значение, а при помощи флажка **Сохранять последний интервал просмотра статистики** всегда сохранять тот интервал, который был выбран последним при просмотре статистики. Для сохранения изменений нажмите **Сохранить**.



7.10. Управление серверным карантином

Для того чтобы администратор сети мог удаленно управлять карантином, выберите пункт **Антивирусная сеть** главного меню Центра управления и в открывшемся окне в иерархическом списке нажмите на название станции или группы. Далее в открывшейся панели слева выберите пункт **Конфигурация → Windows → Агент Dr.Web** и на вкладке **Общие** установите флажок **Разрешить удаленное управление карантином**.



Внимание! Для управления **Карантином** с сервера необходимо, чтобы станции с установленным модулем Карантина работали под ОС, на которые возможна установка SpIDer Guard G3: Windows 2000 с SP4 и Update Rollup1, Windows 2003 с SP1 и выше, Windows Vista и выше.

Для управления содержимым серверного карантина необходимо выбрать в меню **Антивирусная сеть** интересующую станцию или группу и затем пункт **Общие → Карантин**.

Если была выбрана одна станция, то будет отображена таблица с объектами, находящимися в карантине данной станции; если было выбрано несколько станций, группа или несколько групп, то будет отображен набор таблиц, содержащих объекты карантина каждой станции в отдельности.

Если необходимо найти объекты, попавшие в карантин в определенный момент времени, то этот период можно указать, используя поля ввода 

. После выбора интересующего периода необходимо нажать **Обновить**.

В базу **Карантина** может быть перемещен любой зараженный или подозрительный объект. Файлы в **Карантин** могут быть добавлены одним из антивирусных компонентов, например **Сканером**, или вручную пользователем через менеджер **Карантина**.

При попадании в **Карантин** файлы автоматически сканируются повторно. При этом уточняется статус заражения — наличие угрозы, ее название и тип (поскольку при ручном добавлении в **Карантин** информация о статусе заражения файлов недоступна).

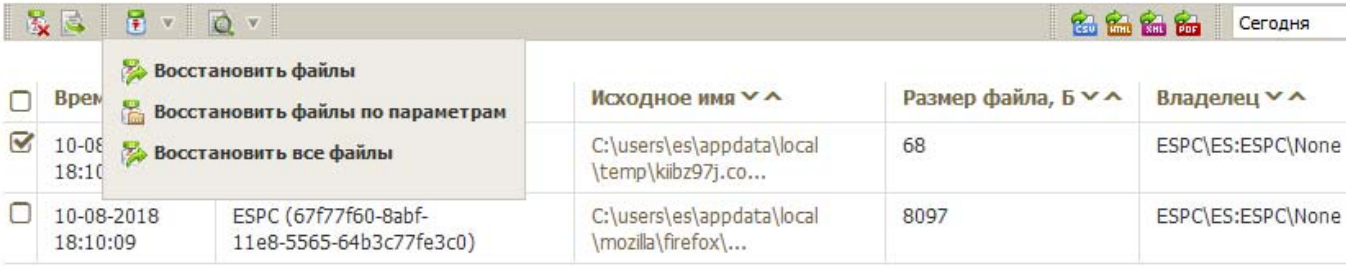
Пользователь может сам повторно сканировать файлы, находящиеся в **Карантине**, через **Центр управления** или через менеджер **Карантина** на станции.

Для каждого объекта, перемещенного в Карантин, фиксируется следующая информация:

- дата и время перемещения в Карантин;
- станция, на которой был обнаружен файл;
- исходное имя зараженного файла и его размер;
- владелец файла;
- компонент, переместивший файл;
- информация о заражении.

Для восстановления файлов необходимо, предварительно выбрав станцию в разделе **Антивирусная сеть** и перейдя в раздел **Карантин**, выбрать интересующий файл или группу файлов, а затем выбрать значок и в выпадающем меню указать один из вариантов:

- восстановить первоначальное местоположение файла на компьютере (восстановить файл в папку, в которой он находился до перемещения);
- переместить файл в указанную папку.



Для удаления выбранных файлов из карантина необходимо выбрать значок .

Для сканирования выбранных файлов — .

Для отправки выбранных файлов с рабочей станции на сервер для дополнительного анализа необходимо использовать кнопку (**Экспорт**).

Также возможно экспортировать данные о состоянии **Карантина** в файл в формате: CSV, HTML, XML, PDF.

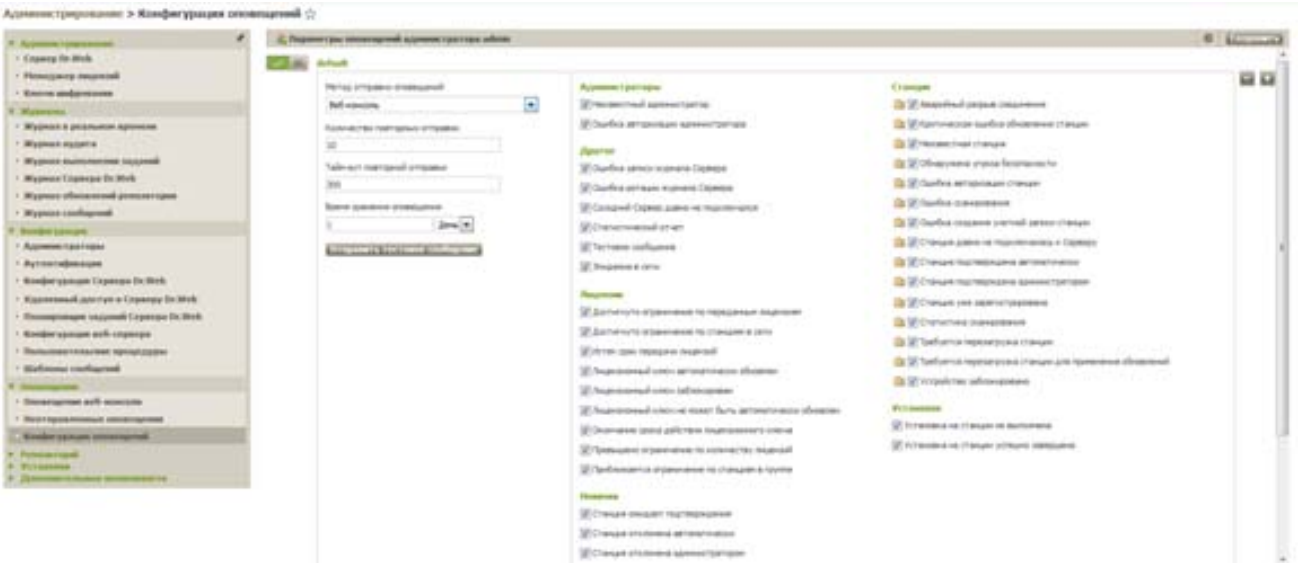
7.10.1. Доступ к журналам работы антивирусного сервера

Для экспорта архивированных файлов журнала антивирусного сервера из Центра управления выберите пункт **Администрирование → Журналы → Журнал Сервера Dr.Web**, в открывшемся окне отметьте интересующие журналы и нажмите **Экспортировать выбранные файлы журнала** ().

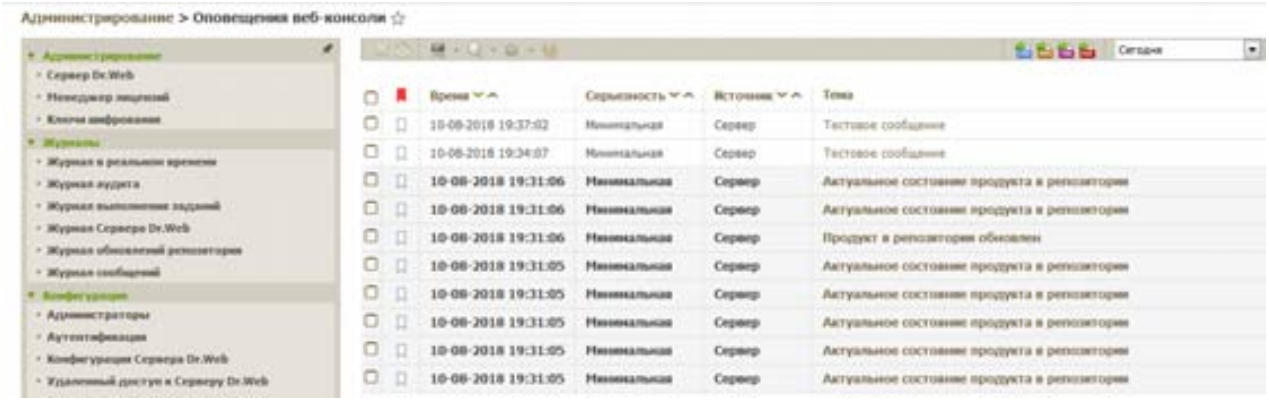
7.11. Оповещения

Сервер Dr.Web может автоматически сообщать о проблемах, обнаруженных в процессе функционировании антивирусной сети, с помощью почтовых сообщений. Кроме того, администратор может вручную рассылать уведомления пользователям. Использование оповещений дает возможность уведомлять пользователей о наступлении тех или иных событий, рассылать им инструкции и предупреждения.

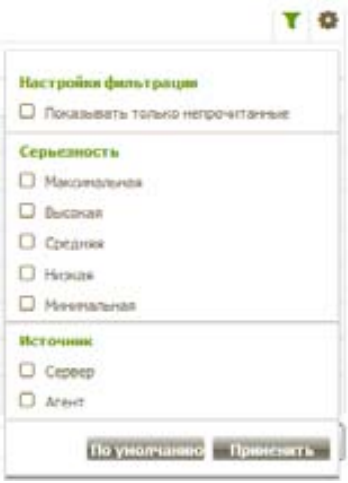
Рассылка оповещений для администраторов настраивается в разделе **Администрирование → Оповещения → Конфигурация оповещений**. Здесь указываются метод доставки оповещений, а также события, оповещения о которых необходимо доставлять администратору.



Например, если оповещения доставляются посредством веб-консоли, то они отображаются в разделе **События** () главного меню.

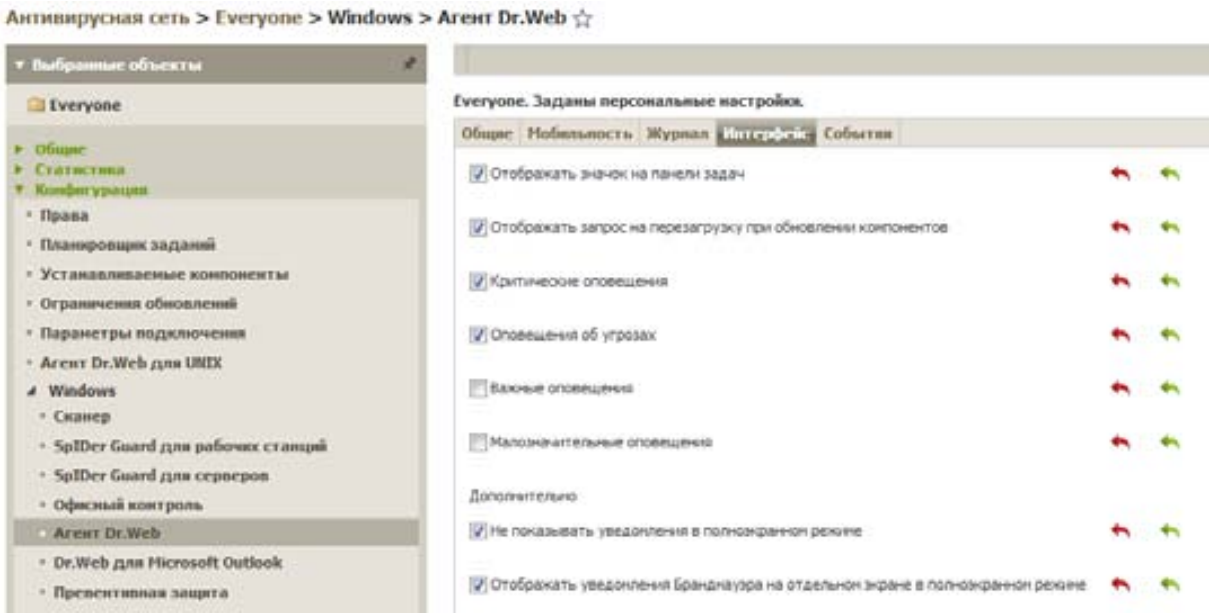


При необходимости с помощью фильтра можно настроить получение только оповещений, имеющих определенную степень серьезности:



7.11.1. Настройка предопределенных правил оповещений. Выбор способа реакции на инциденты

Для централизованной настройки оповещений о событиях, происходящих на компьютере клиента (обновлениях, ошибках, найденных вирусах и т. д.), администратор антивирусной сети должен выбрать группу (например, **Everyone**, если необходимо осуществить настройку для всех агентов) и в панели слева выбрать пункт **Конфигурация → Windows → Агент Dr.Web**, перейти на вкладку **Интерфейс** и отметить те сообщения, которые будут показываться пользователю. Р екомендуется, чтобы Агент выводил пользователю как минимум **Критические оповещения** и **Оповещениях об угрозах**.

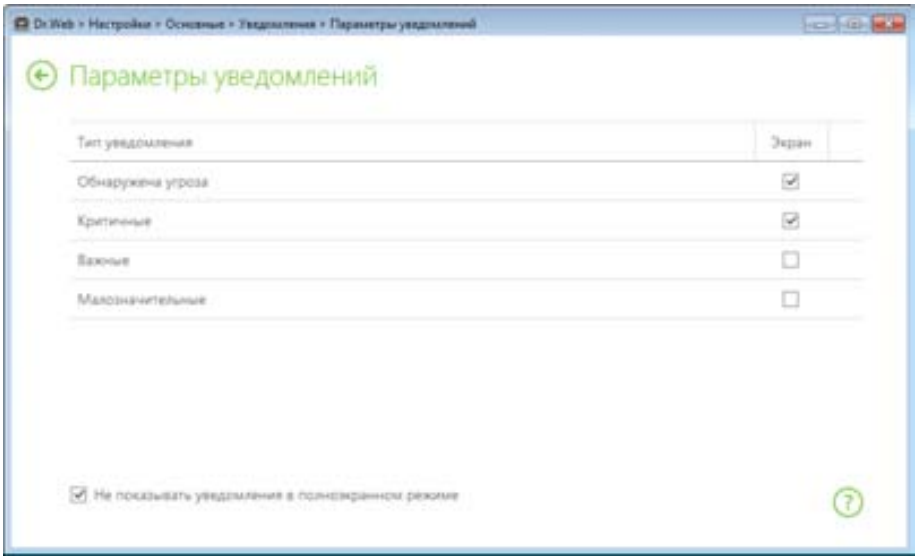


Если вы хотите, чтобы пользователь получал все группы сообщений, установите все четыре флажка. В противном случае будут выводиться только сообщения указанных групп.

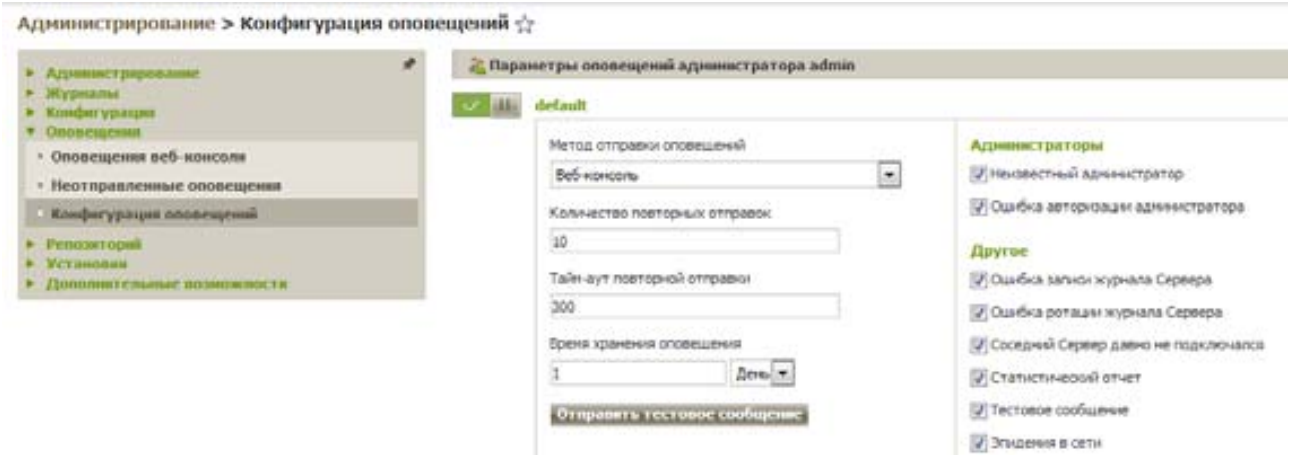
Тип уведомления	Описание
Обнаружена угроза	Установите флажки внутри этой группы, чтобы получать уведомления об угрозах, обнаруженных SpIDer Guard и SpIDer Gate. Снимите флажки, чтобы не получать подобных уведомлений. По умолчанию уведомления включены.
Критичные уведомления	Установите флажки внутри этой группы, чтобы получать критичные уведомления о следующих событиях: •обнаружены соединения, ожидающие ответа Брандмауэра; •ваши имя пользователя и пароль уже используются для подключения к серверу централизованной защиты. Снимите флажки, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.
Важные уведомления	Установите флажки внутри этой группы, чтобы получать важные

Тип уведомления	Описание
	уведомления о следующих событиях: •истекает время работы за компьютером; •заблокировано устройство; •заблокирована попытка изменения системных даты и времени; •попытка доступа к защищаемому объекту заблокирована Превентивной защитой; •вирусные базы устарели (при работе в Мобильном режиме). Снимите флажки, чтобы не получать перечисленные уведомления. По умолчанию уведомления включены.
Малозначительные уведомления	Установите флажки внутри этой группы, чтобы получать малозначительные уведомления о следующих событиях: •успешное обновление; •ошибка обновления; •истекает время работы в Интернет; •URL был заблокирован модулем Офисный контроль; •URL был заблокирован SpIDer Gate; •попытка доступа к защищаемому объекту заблокирована модулем Офисный контроль; •администратором антивирусной сети запущен процесс проверки вашего компьютера; •процесс проверки вашего компьютера запущен по расписанию; •проверка вашего компьютера завершена. Снимите флажки, чтобы не получать перечисленные уведомления. По умолчанию уведомления выключены.

В дальнейшем пользователь сможет самостоятельно включить/отключить те или иные оповещения на своем компьютере, щелкнув правой кнопкой мыши на значке Агента в трее и выбрав пункт **Настройки → Основные → Параметры уведомлений**.

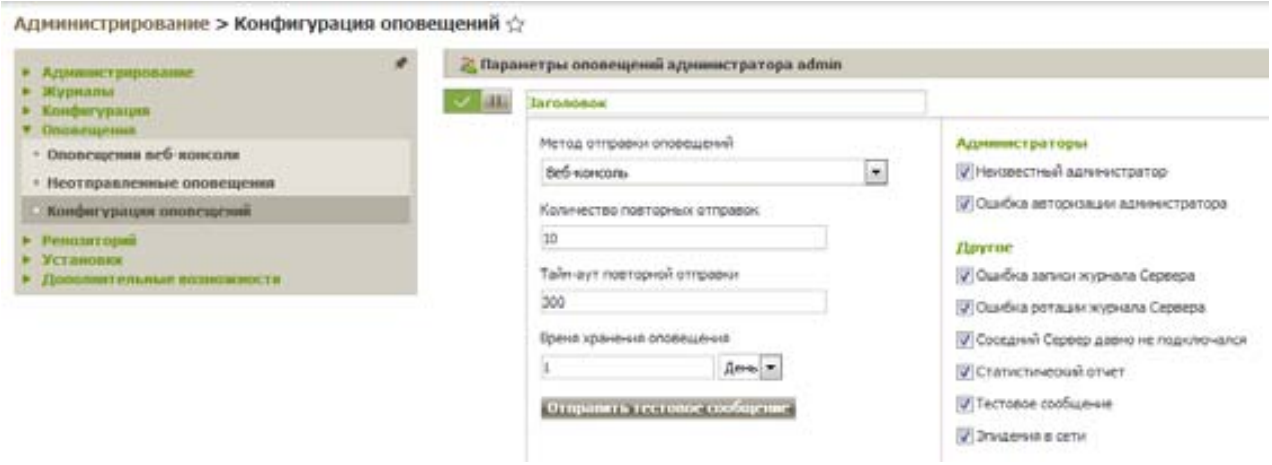


Для того чтобы настроить автоматические оповещения, необходимо в Центре управления выбрать **Администрирование → Оповещения → Конфигурация оповещений**.



При первоначальной настройке существует только список оповещений по умолчанию (default) с базовыми настройками. Вы можете внести изменения в него или создать новый набор правил для уведомлений. Для этого необходимо сделать следующее:

1. Нажмите **Добавить уведомление (** **)**. Вновь созданный список изначально полностью дублирует набор уведомлений **dafault**. При необходимости наборы уведомлений можно добавлять и удалять, используя, соответственно, кнопки .



2. Чтобы включить отправку оповещений, установите переключатель слева от заголовка блока оповещения в соответствующее положение:
3.  — отправка оповещений для данного блока включена.
4.  — оповещения данного блока отправляться не будут.
5. Настройка различных блоков оповещений, как и текстов их шаблонов, осуществляется независимо.
   a. В поле **Заголовок** задайте название добавленного блока оповещений. Это название будет использоваться, например, при настройке задания **Создание статистического отчета** в расписании Сервера. В дальнейшем для редактирования заголовка нажмите на него левой кнопкой мыши и введите необходимое название. Если имеется более одного блока оповещений, при нажатии на текст заголовка будет предложен выпадающий список с заголовками существующих блоков оповещений.
   b. Выберите необходимый тип отправки оповещения в выпадающем списке **Метод отправки оповещений**:

      - **Агент Dr.Web** — отправлять оповещения через протокол **Агента**.

        Для оповещений через протокол Агента задайте следующие параметры:

        - Количество повторных отправок — количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию — 10.
        - Тайм-аут повторной отправки — период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
        - Станция — идентификатор станции, на которую будут отправляться оповещения.
        - Редактировать — нажав эту кнопку, вы сможете выбрать одну или несколько станций (при выборе группы в рассылку добавятся все входящие в нее станции), куда будут рассылаться оповещения.
        - Время хранения оповещения — время, в течение которого требуется хранить оповещение, начиная с момента его получения. По умолчанию один день. По истечении указанно срока оповещение помечается как устаревшее и удаляется согласно заданию **Очистка устаревших сообщений** в настройках расписания антивирусного сервера.
        - Отправить тестовое сообщение — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.
      - **Email** — отправлять оповещения по электронной почте.

Для оповещений по электронной почте задайте следующие параметры:

- Редактировать общие заголовки — позволяет настроить служебную информацию в заголовках отправляемых сообщений, которая поможет администратору получить больше информации. Подробнее о шаблонах системы оповещения изложено в Приложении к Руководству администратора.

- Количество повторных отправок — количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию — 10.
- Тайм-аут повторной отправки — период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- E-mail адреса получателей — адреса электронной почты получателей сообщения. В каждое поле вводится только один адрес электронной почты получателя. Для добавления еще одного поля получателя нажмите кнопку . Для удаления поля нажмите кнопку .
- Параметры отправки электронной почты:

Параметры отправки электронной почты настраиваются в меню **Администрирование**, в разделе **Конфигурация Сервера Dr.Web**, на вкладке **Сеть**, на внутренней вкладке **Электронная почта**.

- **Электронная почта отправителя** — адрес ящика электронной почты, от имени которого будут отправляться электронные письма.
- **Адрес сервера** — адрес SMTP-сервера, который будет использоваться для отправки электронной почты.
- **Порт** — порт для подключения к SMTP-серверу. По умолчанию порт 465 при открытии отдельного защищенного TLS-соединения или порт 25 в противном случае.
- **Пользователь**, **Пароль** — при необходимости задайте имя пользователя и пароль пользователя SMTP-сервера, если SMTP-сервер требует авторизации.
- **Тайм-аут соединения с SMTP-сервером** — тайм-аут в секундах для установления соединения с SMTP-сервером. Значение — целое положительное число большее или равное 1.
- Установите флажок **Использовать STARTTLS** для шифрованного обмена данными. При этом переключение на защищенное соединение осуществляется через команду STARTTLS. По умолчанию для соединения предусматривается использование 25 порта.
- Установите флажок **Использовать CRAM-MD5 аутентификацию** для использования *CRAM-MD5* аутентификации на почтовом сервере.
- Установите флажок **Использовать DIGEST-MD5 аутентификацию** для использования *DIGEST-MD5* аутентификации на почтовом сервере.
- Установите флажок **Использовать LOGIN аутентификацию** для использования *LOGIN* аутентификации на почтовом сервере.

- Установите флажок **Использовать AUTH-NTLM аутентификацию** для использования *AUTH-NTLM* аутентификации на почтовом сервере.
- Установите флажок **Использовать обычную аутентификацию** для использования *plain text* аутентификации на почтовом сервере.
- Установите флажок **Использовать TLS** для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование 465 порта.
- Установите флажок **Проверять правильность сертификата Сервера** чтобы проверять правильность TLS-сертификата почтового сервера. В поле **Сертификат Сервера** укажите путь к корневому TLS-сертификату Сервера Dr.Web.
- Установите флажок **Отладочный режим** для получения детального журнала SMTP-сессии.
- В поле **Электронная почта получателей** можете задать адреса ящиков электронной почты, чтобы проверить отправку электронной почты. Нажмите кнопку **Отправить тестовое сообщение**, чтобы отправить тестовое письмо аналогичное оповещению Сервера) по электронной почте в соответствии с заданными настройками в данном разделе.

- Отправить тестовое сообщение — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.
- **Push** — отправлять push-оповещения на **Мобильный центр управления Dr.Web**. Пункт будет доступен в выпадающем списке **Метод отправки оповещений** только после подключения **Мобильного центра управления Dr.Web** к данному Серверу **Dr.Web**.
- **SNMP** — отправлять оповещения через SNMP-протокол.

Для оповещений через SNMP-протокол задайте следующие параметры:

- **Количество повторных отправок** — количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию — 10.
- **Тайм-аут повторной отправки** — период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Получатель** — сущность, принимающая SNMP-запрос. Например, IP-адрес или DNS-имя компьютера. В каждое поле вводится только один получатель. Для добавления еще одного поля получателя нажмите кнопку . Для удаления поля нажмите кнопку .
- **Отправитель** — сущность, отправляющая SNMP-запрос. По умолчанию “localhost” для ОС Windows и “” для ОС семейства UNIX.
- **Общность** — SNMP-общность или контекст. По умолчанию public.
- **Отправить тестовое сообщение** — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.
- **Веб-консоль** — отправлять оповещения в Веб-консоль.
- **Количество повторных отправок** — количество повторных попыток, предпринимаемых при неудачной отправке оповещения. По умолчанию — 10.
- **Тайм-аут повторной о тправки** — период в секундах, по истечении которого осуществляется повторная попытка отправки оповещения. По умолчанию 300 секунд.
- **Время хранения оповещения** — время, в течение которого требуется хранить оповещение, начиная с момента его получения. По умолчанию один день. По истечении указанно срока оповещение помечается как устаревшее и удаляется согласно заданию **Очистка устаревших сообщений** в настройках расписания антивирусного

сервера. Для оповещений, полученных данным методом отправки, вы можете задать неограниченный срок хранения в разделе **Оповещения** Центра управления.

- **Отправить тестовое сообщение** — отправить тестовое оповещение в соответствии с заданными настройками системы оповещений. Текст тестового оповещения задается в шаблонах оповещений.

c. Для отправки оповещений предоставляется предустановленный набор стандартных оповещений Сервера. Чтобы настроить конкретные оповещения, необходимо:

d. В списке оповещений установите флажки напротив тех оповещений, которые будут отправляться в соответствии с методом отправки текущего блока оповещений.

e. Для изменения настроек оповещений нажмите ⚙ слева от оповещения. Откроется шаблон оповещения.

При необходимости отредактируйте текст отправляемого сообщения. В тексте оповещения можете использовать переменные шаблона (в фигурных скобках). Для добавления переменных предоставляются выпадающие списки в заголовке сообщения. При подготовке сообщения система оповещения заменяет переменные шаблона на конкретный текст, зависящий от ее текущих настроек.

Для метода отправки **SNMP** тексты шаблонов оповещений задаются на стороне клиента SNMP.

После окончания редактирования нажмите кнопку **Сохранить**, чтобы применить все внесенные изменения.

В правой части окна установите флажки для тех событий, сообщения о которых будут отсылаться.

Чтобы ознакомиться со статистикой работы Dr.Web Сервера:

1. Выберите пункт **Администрирование → Дополнительные возможности → Статистика Сервера Dr.Web** меню Центра управления.

3. В открывшемся окне представлены следующие разделы статистических данных:

- Активность клиентов — данные по количеству обслуживаемых клиентов, подключенных к данному Серверу: Агентов Dr.Web, соседних Серверов Dr.Web и инсталляторов Агентов Dr.Web.
- Сетевой трафик — параметры входящего и исходящего сетевого трафика при обмене данными с Сервером.
- Использование системных ресурсов — параметры использования системных ресурсов компьютера, на котором установлен Сервер.
- Microsoft NAP — параметры работы Dr.Web NAP Validator.
- Использование базы данных — параметры обращения к базе данных Сервера.
- Использование файлового кэша — параметры обращения к файловому кэшу компьютера, на котором установлен Сервер.
- Использование DNS кэша — параметры обращения к кэшу, хранящему за просы к DNS-серверам, на компьютере, на котором установлен Сервер.
- Оповещения — параметры работы подсистемы оповещений администратора.
- Репозиторий — параметры обмена данными репозитория Сервера с серверами ВСО.
- Веб-статистика — параметры использования сети.
- Статистика веб-сервера — параметры обращения к Веб-серверу.
- Кластер — параметры обращений по протоколу межсерверной синхронизации при использовании кластера Серверов в многосерверной конфигурации сети.

Передача групповых обновлений — данные по объемам передачи групповых обновлений.

4. Чтобы посмотреть статистические данные конкретного раздела, нажмите на название нужного раздела.

5. В открывшемся списке приведены параметры раздела с динамическими счетчиками значений.

6. Одновременно при раскрытии статистического раздела включается графическое представление изменений для каждого из параметров. При этом:

- Чтобы отключить графическое представление, нажмите на название нужного раздела. При отключении графического представления числовое значение параметров продолжит динамически обновляться.
- Чтобы повторно включить графическое представление данных, повторно нажмите на название нужного раздела.
- Названия разделов и их параметров, для которых включено графическое отображение, выделяются полужирным шрифтом.

7. Для изменения частоты обновления параметров воспользуйтесь следующими инструментами на панели управления:

- В выпадающем списке **Частота обновления** выберите требуемый период обновления данных. При изменении значения выпадающего списка, автоматически применяется временной период обновления числовых и графических данных.
- Нажмите кнопку **Обновить**, чтобы единожды обновить все значения статистических данных одновременно.

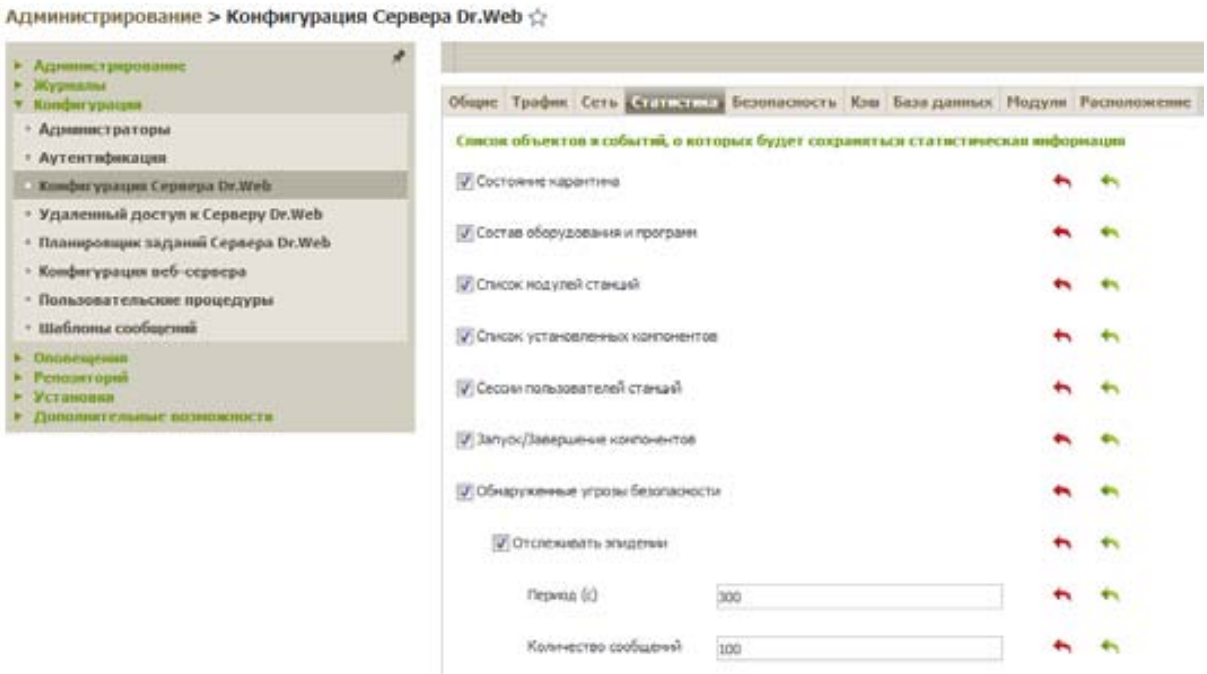
8. При наведении указателя мыши на графические данные выводится числовое значение выбранной точки в виде:

- Abs — абсолютное значение параметра.
- Delta — прирост значения параметра относительно его предыдущего значения согласно частоте обновления данных.

9. Чтобы скрыть параметры раздела, нажмите на стрелку слева от названия этого раздела. При скрытии параметров раздела графическое представление статистики очищается и при повторном открытии параметров отрисовка начинается заново.

7.11.2. Контроль за возникновением эпидемий

Для получения уведомлений о возникновении эпидемий (превышения порога количества обнаруженных угроз) выберите пункт **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** и перейдите на вкладку **Статистика**.



Установите флажок **Отслеживать эпидемии**, чтобы включить режим оповещения администратора о случаях вирусных эпидемий. Если флажок снят, оповещения о вирусных заражениях будут осуществляться в обычном режиме, В противном случае вы также можете задать следующие параметры отслеживания вирусных эпидемий:

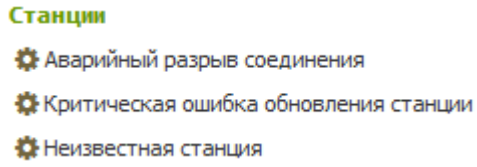
- **Период (сек.) —** промежуток времени в секундах, за который должно прийти заданное количество сообщений о заражениях, чтобы Сервер Dr.Web отправил администратору единое уведомление об эпидемии на все случаи заражения.
- **Количество сообщений —** количество сообщений о заражениях, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправил администратору единое уведомление об эпидемии на все случаи заражения.

7.11.3. Редактирование шаблонов предопределенных оповещений

Текст оповещения определяется заданным для него шаблоном. Шаблоны хранятся в подкаталоге var/templates каталога установки Сервера. Вы можете настроить текст оповещения, отсылаемого при наступлении определенного события, отредактировав соответствующий шаблон.

При подготовке текста оповещения происходит автоматическая замена переменных в шаблоне (фразы в фигурных скобках) на конкретный текст, зависящий от текущих настроек.

Для редактирования шаблонов оповещений перейдите в раздел **Администрирование → Оповещения → Конфигурация оповещений**, в блоках уведомлений найдите интересующее уведомление и нажмите кнопку слева от него. Откроется шаблон оповещения.



При необходимости его можно отредактировать, изменив текст и добавив переменные с помощью выпадающих списков в заголовке окна.

Для сохранения измененного шаблона нажмите на кнопку **Сохранить**.

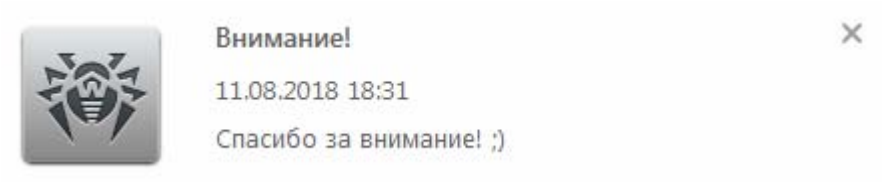
Внимание! В том случае, если вы используете для редактирования шаблонов внешний редактор, сохраняйте файлы шаблонов в кодировке UTF-8. Крайне не рекомендуется использовать Блокнот и другие редакторы, вставляющие в текст маркер порядка байтов (BOM) для определения кодировки UTF-8, UTF-16 или UTF-32.

7.11.4. Отправка мгновенных сообщений пользователю

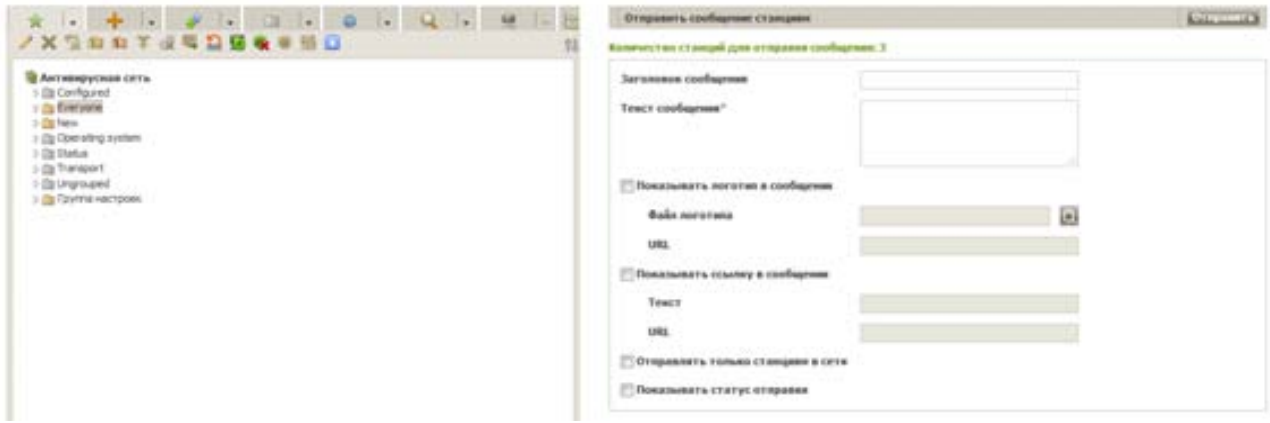
В случае необходимости администратор может отправить пользователям одной или нескольких рабочих станций мгновенные сообщения произвольного содержания, которое сразу после отправки отобразится на экране пользователей в виде всплывающего окна. Такое сообщение может содержать:

- любую текстовую информацию;
- ссылки на интернет-ресурсы;
- графическое изображение, например логотип вашей компании;

В заголовке окна сообщения также указываются дата и время его получения.



Для отправки уведомления необходимо выбрать пользователя или группу и нажать на кнопку .



В открывшемся окне заполните следующие поля.

- **Текст сообщения** — обязательное поле. Содержит непосредственно само сообщение.
- **Показывать логотип в сообщении** — установите данный флажок, если хотите, чтобы в заголовке окна сообщения отобразился графический объект. Для загрузки файла логотипа с локального ресурса необходимо нажать на кнопку **Обзор** справа от поля **Файл логотипа** и выбрать необходимый объект в открывшемся браузере по файловой системе. Если флажок не установлен, то к сообщению будет автоматически прикреплен логотип антивируса Dr.Web.

Также вы можете задать заголовок сообщения в поле **Заголовок сообщения**. Данный текст будет отображен в заголовке окна сообщения (справа от логотипа). Если поле не заполнено, то заголовком автоматически станет текст «Новое сообщение».

В поле **URL** можно указать ссылку на веб-страницу, которая будет открываться при нажатии на логотип и заголовок окна.

Установите флажок **Показывать ссылку в сообщении**, если хотите, чтобы сообщение пользователю содержало гиперссылки на ресурсы в сети. Для добавления ссылки необходимо:

1. В поле **URL** ввести ссылку на интернет-ресурс.
2. В поле **Текст** указать название ссылки — текст, который будет отображаться на месте ссылки в сообщении.
3. В поле **Текст** сообщения указать тег {link} везде, где необходимо добавить ссылку. В результирующем сообщении на его месте будет вставлена ссылка с указанными параметрами. Количество тегов {link} в тексте неограниченно, но все они будут содержать одинаковые параметры (из полей **URL** и **Текст** соответственно).

Например:

Для отправки сообщения, приведенного выше, были заданы следующие параметры ссылки:

Текст сообщения:

> Уважаемый пользователь!
>
> Вам был установлен компонент Dr.Web Firewall, выполняющий функции межсетевого экрана.
>
> Подробную информацию о функционале данного компонента можно получить {link}.
>
> С уважением,
>
> администрация.

URL: https://www.drweb.ru

Текст: здесь

По умолчанию уведомление о доставке выключено, включить его можно, выбрав пункт **Показывать статус доставки**.

Файл с графическим изображением (логотипом), включаемый в сообщение, должен удовлетворять следующим условиям.

1. Графический формат файла: BMP, JPG, PNG, GIF, SVG.

2. Размер файла логотипа не должен превышать 512 КБ.

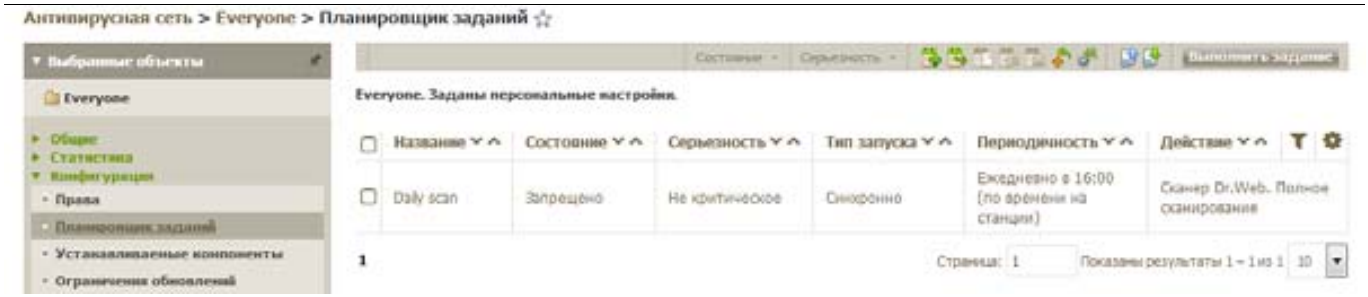
3. Габаритные размеры изображения — 72 × 72 пикселя. Изображения другого размера будут масштабироваться при отправке до размера по умолчанию.

4. Глубина цвета (bit depth) — любая (8–24 бит).

Перед отправкой пользовательского сообщения (особенно многоадресного) рекомендуется предварительно отправить его на любой компьютер с установленным Агентом, чтобы проверить корректность результата.

7.12. Расписание

Важной функцией системы управления является возможность настройки заданий. Так, например, для каждого пользователя администратор может добавлять и отменять задания для выбранной станции или группы, используя страницу **Антивирусная сеть → Конфигурация → Планировщик заданий.**

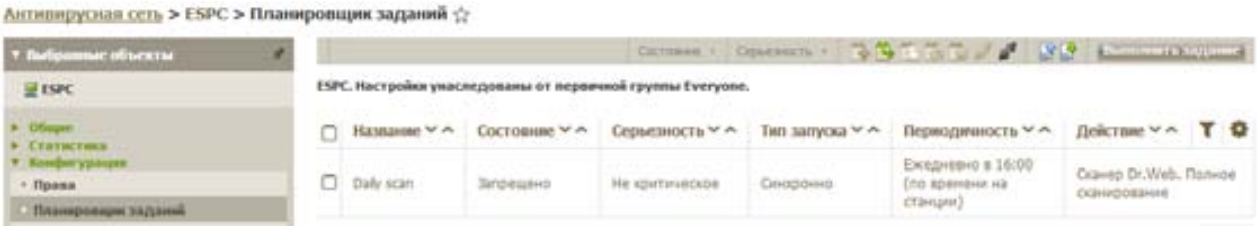


Централизованное расписание, задаваемое администратором антивирусной сети и подчиняющееся всем правилам наследования конфигураций, — это список действий, выполняемых автоматически в заданное время на станциях. Основное применение расписаний — осуществлять сканирование станций на вирусы в наиболее удобное для пользователей время без необходимости ручного запуска Сканера. Кроме этого, **Агент** позволяет выполнять некоторые другие типы действий, описанные ниже.

7.12.1. Настройка централизованного расписания группы станций

Все подключенные к антивирусному серверу защищаемые станции являются членами группы **Everyone**, поэтому настройки (в том числе и расписание) этой группы будут автоматически наследоваться всеми подключаемыми станциями. Все доступные для редактирования группы отображаются в главном окне Центра управления. Однако администратор может задать отдельные настройки расписания для каждой группы или станции. Для настройки расписания необходимо выбрать группу или станцию в иерархическом дереве **Антивирусная сеть** Центра управления и в меню, расположенном слева, выбрать пункт **Конфигурация → Планировщик заданий**. Настройка расписания станций, входящих в другие группы, а также расписание отдельных станций производится аналогично.

По умолчанию для станций под управлением ОС Windows и ОС Windows Mobile расписание содержит одно задание — Daily scan — ежедневное сканирование станции, которое изначально запрещено.



В этом разделе можно отредактировать существующие задания и добавить новые по аналогии с подобными операциями для расписания Сервера Dr.Web. Вы можете запретить выполнение задания, если оно временно стало неактуальным, или разрешить выполнение ранее запрещенного задания, если в нем вновь возникла необходимость.

Если в результате редактирования будет создано пустое (не содержащее заданий) расписание, Центр управления предложит вам либо использовать наследуемое от групп расписание, либо использовать пустое расписание. Пустое расписание необходимо задать в том случае, если вы хотите отказаться от расписания, наследуемого от групп.

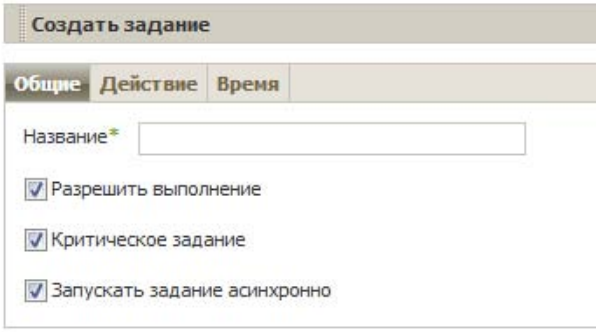
Для добавления задания в расписание нажмите **Создать задание** (). Поля, отмеченные знаком *, должны быть заполнены обязательно.

На вкладке **Общие** задайте следующие параметры:

- В поле **Название** — наименование задания, под которым оно будет отображаться в расписании.
- Чтобы активировать выполнение задания, установите флажок **Разрешить выполнение**. Если он не установлен, задание будет присутствовать в списке, но не будет исполняться.

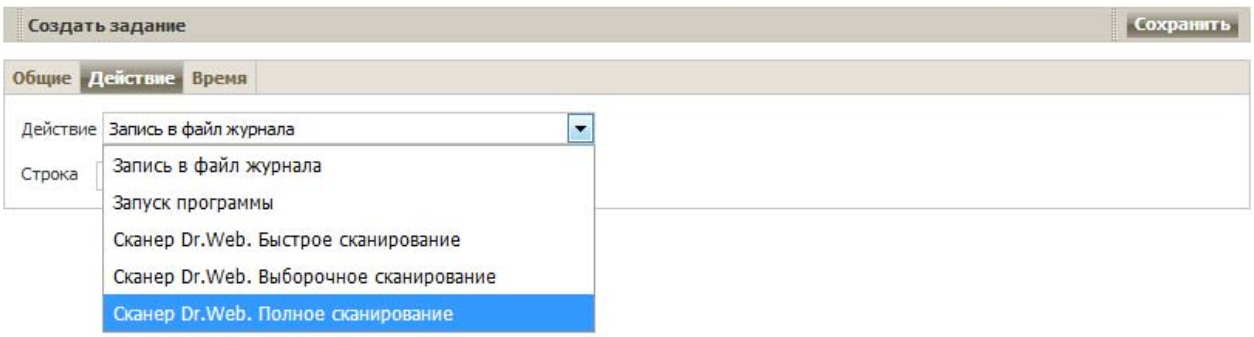
  При включении параметра **Критическое задание** оно будет выполнено при следующем запуске **Агента**, если в текущей сессии выполнение данного задания по какой-либо причине будет пропущено (например, **Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Агента** оно выполняется один раз. Аналогичное действие осуществляется из главного окна расписания при помощи элемента панели инструментов **Важность**.

- Если флажок **Запускать задание асинхронно** снят, задание будет помещено в общую очередь заданий Планировщика, выполняемых последовательно. Установите флажок, чтобы выполнять данное задание параллельно вне очереди.



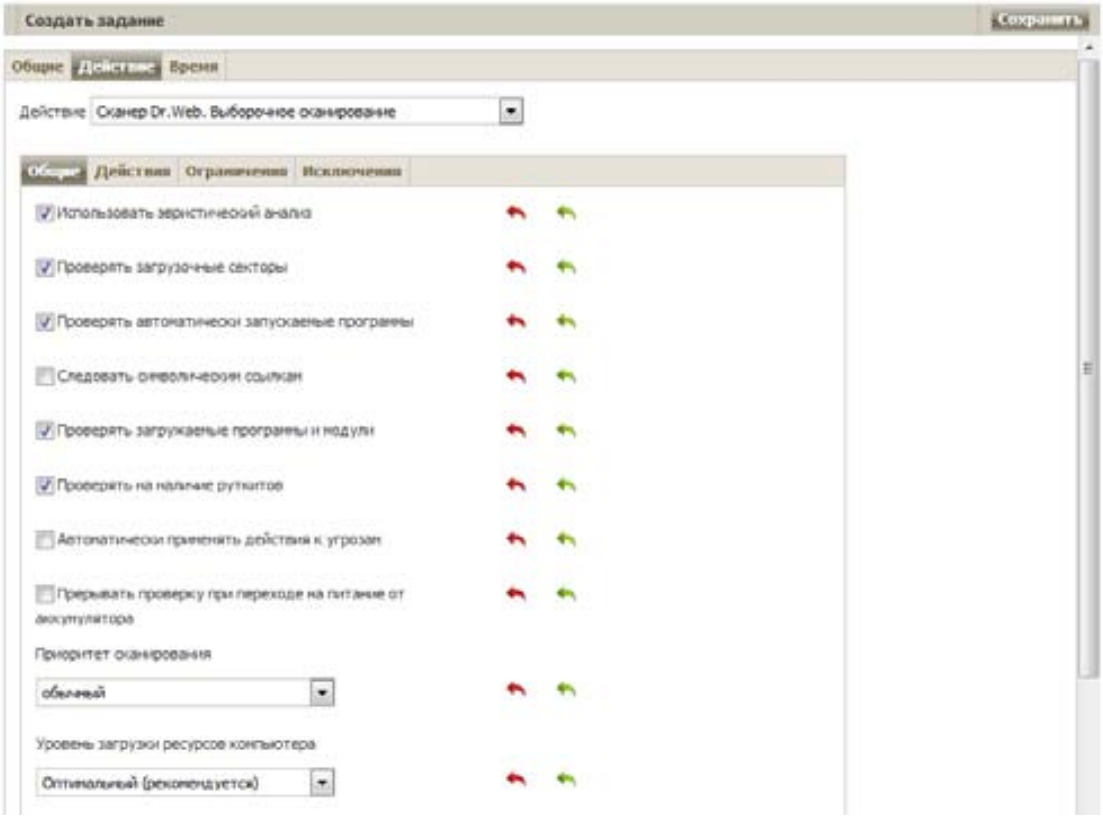
Внимание! Если должны выполняться несколько заданий на сканирование, то будет выполнено только одно из них — то, которое стоит в очереди первым. Например, если разрешено выполнение задания **Daily scan** и в результате было отложено критическое задание на сканирование при помощи **Сканера**, то будет выполняться **Daily scan**, а отложенное критическое сканирование не будет выполнено.

На вкладке **Действие** нажмите на кнопку слева от меню **Действие** и выберите из выпадающего списка тип задания. После сделанного выбора нижняя часть окна будет различной в зависимости от выбранного типа задания.

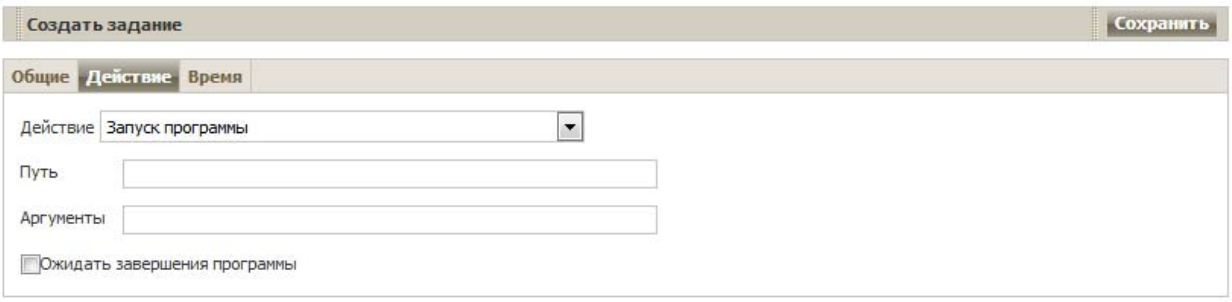


Возможны пять видов действий, исполняемых по расписанию:

- **Dr.Web Сканер. Б ыстрое, полное или выборочное сканирование —** проверка рабочих станций Сканером.



- **Запуск программы** — выполнение произвольного приложения на стороне рабочей станции. Задайте следующие параметры:



• В поле **Путь —** полный путь к исполняемому файлу программы, которую необходимо запускать.
• В поле **Аргументы —** параметры командной строки для запускаемой программы.
• Установите флажок **Ожидать завершения программы** для ожидания завершения программы, запущенной данным заданием. При этом Агент протоколирует запуск программы, код возврата и время завершения программы. Если флажок **Ожидать завершения программы** снят, задание считается завершенным сразу после запуска программы, и Агент протоколирует только запуск программы.

На вкладке **Время**:

- В выпадающем списке **Периодичность** выберите режим запуска задания и настройте время в соответствии с выбранной периодичностью:

Режим запуска	Параметры и описание
Стартовое	Задание будет запускаться при старте работы Агента. Запускается без дополнительных параметров.
Через N минут после исходного задания	Необходимо выбрать в выпадающем списке **Исходное задание** то задание, относительно которого устанавливается время выполнения текущего задания. В поле **Минута** задайте или выберите из предлагаемого списка количество минут, которое должно пройти после выполнения исходного задания, чтобы началось выполнение редактируемого задания.
Ежедневно	Необходимо ввести час и минуту — задание будет запускаться ежедневно в указанное время.
Ежемесячно	Необходимо выбрать число (день месяца), ввести час и минуту — задание будет запускаться в заданный день месяца в указанное время.
Еженедельно	Необходимо выбрать день недели, ввести час и минуту — задание будет запускаться в заданный день недели в указанное время.
Ежечасно	Необходимо ввести число от 0 до 59, задающее минуту каждого часа, в которую будет запускаться задание.
Каждые N минут	Необходимо ввести значение **N** для задания временного интервала выполнения задания. При **N** равном 60 или больше задание будет запускаться каждые **N** минут. При **N** меньше 60 задание будет запускаться в каждую минуту часа, кратную **N**.

- Установите флажок **Запретить после первого выполнения** для однократного выполнения задания в соответствии с указанным временем. Если флажок снят, задание будет выполняться многократно с указанной периодичностью. Чтобы повторить выполнение однократного задания, которое уже было выполнено, воспользуйтесь кнопкой **Запланировать повторно** на панели инструментов раздела расписания.
- Установите флажок **Запускать задание по UTC**, чтобы запускать задание относительного всемирного времени (часовой пояс UTC+0). Если флажок снят, задание будет запущено по локальному времени на станции.

Чтобы отредактировать имеющееся задание, выберите задание из списка, нажав на него левой кнопкой мыши. Дальнейшие действия аналогичны вводу нового задания, описанного выше.

По окончании ввода параметров задания нажмите на кнопку **Сохранить** для принятия изменений в параметрах задания, если вы редактировали уже существующее задание, или для создания задания с заданными параметрами, если вы выполняли процедуру создания нового задания.

Для управления уже существующими заданиями установите флажки напротив нужных заданий или в заголовке та блицы для выбора всех заданий в списке. При этом станут доступны элементы панели инструментов для управления выбранными заданиями.

Вы можете:

- **Разрешить выполнение** — Активировать выполнение выбранных заданий согласно заданному для них расписанию, если они были запрещены.
- **Запретить выполнение** — Запретить выполнение выбранных заданий. При этом задания будет присутствовать в списке, но не будет выполняться.
- **Сделать задание критическим или некритическим** — Осуществить внеочередной запуск задания при следующем запуске **Агента Dr.Web**, если выполнение данного задания было пропущено по расписанию, или выполнять только в указанное для него время. Аналогичное действие осуществляется из редактора задания на вкладке **Общие** при помощи флажка **Критическое задание**.
- Дублировать задания, выбранные в списке текущего расписания. При задании действия **Дублировать настройки** () создаются новые задания с настройками, аналогичными выбранным заданиям.
- **Запланировать повторное выполнение для однократных заданий** (): выполнить задание еще один раз в соответствии с заданными для него настройкам времени.

Чтобы удалить какое-либо задание:

1. Установите флажок напротив нужного задания.
2. Нажмите на кнопку  **Удалить выбранные задания**.

Если запланированная проверка проводится для станций, которые находятся в спящем режиме, то в расписании антивирусного сервера нужно настроить задание **Пробуждение станций**.

Станции, выводимые из спящего режима, задаются при помощи следующих параметров задания:

- **Будить все станции** — предписывает разбудить все станции, подключенные к данному **Серверу**.
- **Будить станции по заданным параметрам** — предписывает разбудить только станции, соответствующие указанным ниже параметрам:
  - **IP-адреса и MAC-адреса** — список IP/ MAC-адресов станций, которые необходимо разбудить. IP-адреса задаются в формате: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Также IP-адреса можно заменять DNS-именами компьютеров. Октеты

MAC-адреса разделяются знаком ':'. При задании списка адресов используйте запятую или переход на новую строку в качестве разделителя.

- **Группы —** с помощью кнопки Редактировать можно выбрать в иерархическом дереве (с помощью клавиш CTRL и SHIFT) станции или группы, станции которых необходимо разбудить.

Для выполнения данного задания на пробуждаемых станциях должны быть установлены сетевые карты с поддержкой опции Wake-on-LAN. Поддержку опции Wake-on-LAN вы можете проверить в документации к сетевой карте или в свойствах сетевой карты (**Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера → Свойства → Настроить → Дополнительно**, задать для свойства **Wake on Magic Packet** значение **Enabled**).

7.12.2. Запуск заданий независимо от текущих настроек расписания. Запуск и останов антивирусного сканера

На каждой станции вы можете запускать вручную задания на антивирусное сканирование с настройкой параметров сканирования. Пользователь рабочей станции может производить антивирусное сканирование станции самостоятельно, используя компонент **Сканер для Windows**. Значок для запуска этого компонента при установке антивирусного ПО размещается на рабочем столе. Запуск и успешная работа Сканера возможна даже при неработоспособности Агента, в том числе при загрузке ОС Windows в безопасном режиме.

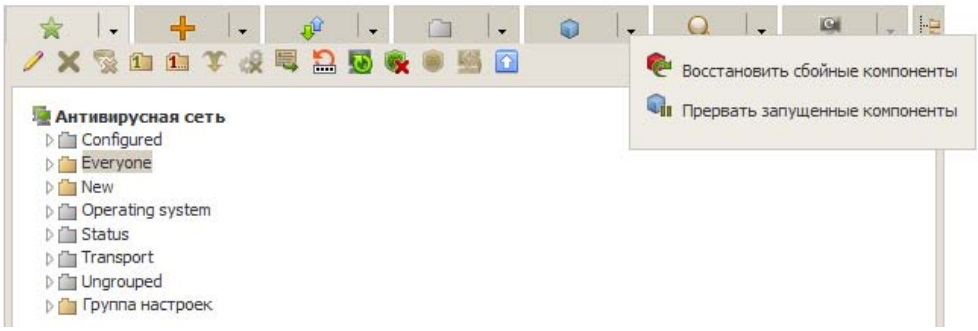
Вы можете просматривать список всех активных в настоящее время сканирований (как запущенных вручную вами или пользователем, так и по расписанию).

Для просмотра списка и завершения работы запущенных компонентов:

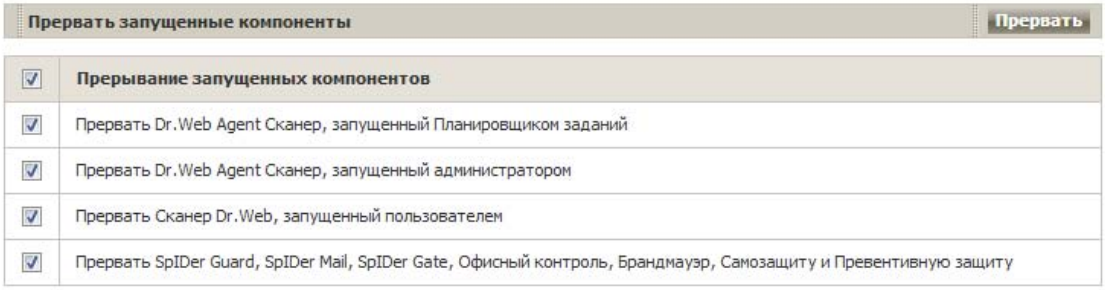
1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите пункт **Компоненты защиты**. Откроется список работающих компонентов.
2. При необходимости прервать работу какого-либо из компонентов антивируса установите флажок напротив этого компонента, после чего на панели инструментов нажмите на кнопку **(Прервать выбранные компоненты)**.

   Также для того, чтобы прервать все исполняемые компоненты определенного типа:

   1. Выберите пункт **Антивирусная с еть** главного меню Центра управления, в открывшемся окне в иерархическом списке выберите необходимую группу или отдельные антивирусные станции.
   2. На панели инструментов каталога антивирусной сети нажмите **Управление компонентами**. В выпадающем списке выберите пункт **Прервать запущенные компоненты**. Откроется окно настройки типа прерываемых компонентов.

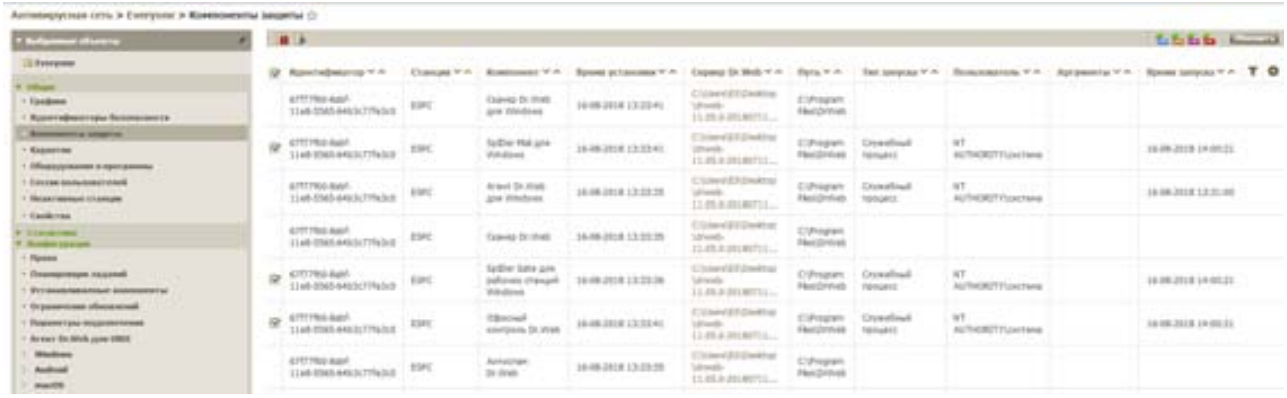


3. Установите флажки напротив названий тех типов компонентов, которые вы хотите немедленно прервать, либо напротив заголовка области **Прерывание запущенных компонентов** — для выбора всех процессов из списка.

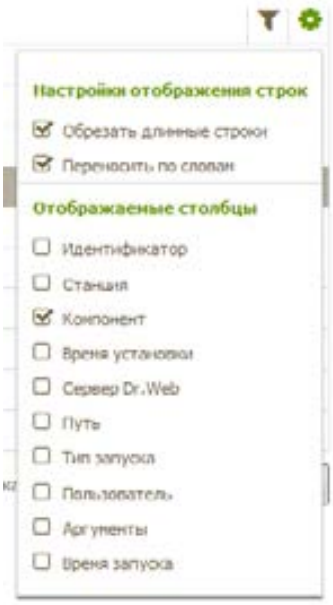


4. Нажмите на кнопку **Прервать**.

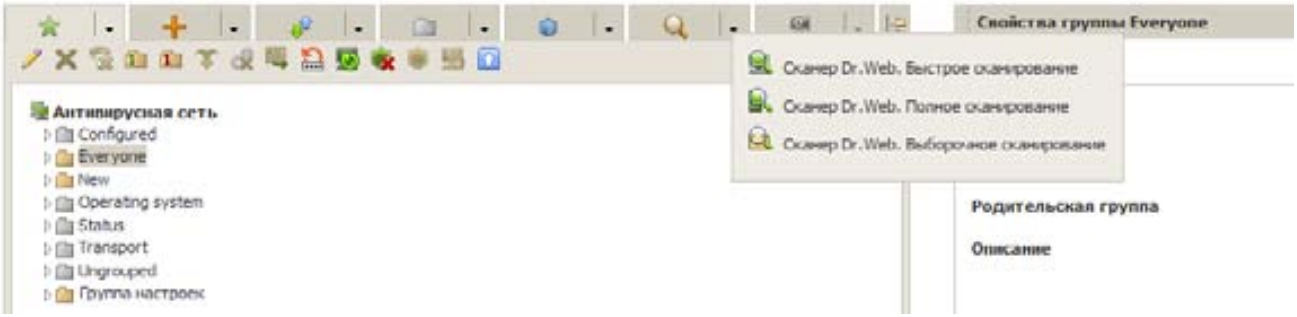
Внимание! Массово запустить компоненты антивируса заново можно только через меню **Компоненты защиты** для выбранных групп или станций. Отметьте флажками все необходимые компоненты (или поставьте флажок в заголовке первого столбца, чтобы запустить все компоненты на всех станциях) и нажмите  (**Запустить выбранные компоненты**).



Вы можете прервать компоненты на рабочей станции — запущенные вручную вами или пользователем, а также запущенные по расписанию. Вы также можете прервать сразу все исполняемые компоненты, удовлетворяющие определенному критерию, для чего используется кнопка настройки отображения строк. Это особенно удобно, если такую команду выдают сразу многим станциям ().



Для запуска антивирусной проверки в произвольный момент независимо от расписания необходимо в меню **Антивирусная сеть** выбрать необходимую группу или станцию и нажать на  (при выборе группы пункт **Сканировать** будет доступен только в том случае, если в группе есть хотя бы одна активная (online) станция). При этом, если будет нажат значок меню слева от лупы, то откроется меню, позволяющее выбрать тип сканера и параметры проверки, зависящие от выбранного типа сканера:



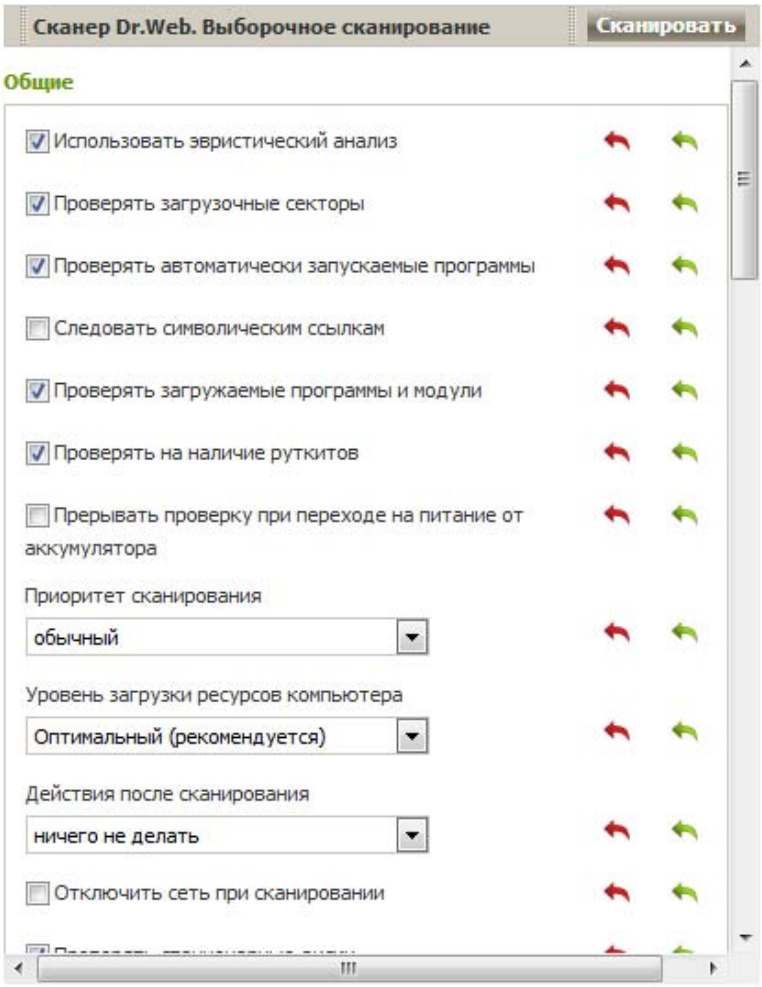
- **Сканер Dr.Web. Быстрое сканирование**. В данном режиме сканируются следующие объекты:
  - оперативная память,
  - загрузочные секторы всех дисков,
  - объекты автозапуска,
  - корневой каталог загрузочного диска,
  - корневой каталог диска установки ОС Windows,
  - системный каталог ОС Windows,
  - папка Мои документы,
  - временный каталог системы,
  - временный каталог пользователя.

При выборе данного пункта начнется проверка на вирусы с параметрами Сканера, заданными по умолчанию.

- **Сканер Dr.Web. Полное сканирование**. В данном режиме производится полное сканирование всех жестких дисков и сменных носителей (включая загрузочные

секторы). При выборе данного пункта начнется сканирование с параметрами Сканера, заданными по умолчанию.

- **Сканер Dr.Web. Выборочное сканирование**. Данный режим предоставляет возможность выбрать любые каталоги и файлы для последующего сканирования, а также настроить расширенные параметры проверки. При выборе данного пункта откроется окно настройки Сканера. Задайте параметры сканирования и состав проверяемых объектов файловой системы (эти действия подробно описываются ниже) и нажмите кнопку **Сканировать**.



В том случае, если существует подозрение на заражение станции, можно выбрать пункт **Отключить сеть при сканировании**.

Также возможен запуск сканирования любого типа по расписанию.

7.12.2.1. Пробуждение станций для проведения проверки

Если запланированная проверка проводится для станций, которые находятся в спящем режиме, то в расписании антивирусного сервера нужно настроить задание **Пробуждение станций**.

Станции, выводимые из спящего режима, задаются при помощи следующих параметров задания:

- **Будить все станции** — предписывает разбудить все станции, подключенные к данному **Серверу**.
- **Будить станции по заданным параметрам** — предписывает разбудить только станции, соответствующие указанным ниже параметрам:
  - **IP-адреса и MAC-адреса** — список IP/ MAC-адресов станций, которые необходимо разбудить. IP-адреса задаются в формате: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Также IP-адреса можно заменять DNS-именами компьютеров. Октеты MAC-адреса разделяются знаком ':'. При задании списка адресов используйте запятую или переход на новую строку в качестве разделителя.
- **Группы** — с помощью кнопки Редактировать можно выбрать в иерархическом дереве (с помощью клавиш CTRL и SHIFT) станции или группы, станции которых необходимо разбудить.

Для выполнения данного задания на пробуждаемых станциях должны быть установлены сетевые карты с поддержкой опции Wake-on-LAN. Поддержку опции Wake-on-LAN вы можете проверить в документации к сетевой карте или в свойствах сетевой карты (**Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера → Свойства → Настроить → Дополнительно**, задать для свойства **Wake on Magic Packet** значение **Enabled**).

На закладке **Время** нужно установить флажок **Запретить после первого выполнения**.

7.12.2.2. Настройка параметров сканирования для ОС Windows

Для просмотра и редактирования параметров **Сканера** доступны несколько вариантов.

1. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите пункт **Сканер**.

   В случае выбора группы Сканер доступен в группе **Windows**.

2. Выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы. На панели инструментов нажмите на пункт **Сканировать**. В открывшемся списке на панели инструментов выберите пункт **Сканер Dr.Web. Выборочное сканирование**. На панели справа откроется окно настроек **Сканера**. Данный список

параметров позволяет задать основные параметры для Сканера, входящие в группы настроек **Общие**, **Исключения Действия** и **Ограничения**.

Перед запуском процесса сканирования ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows версий: Server 2003/2008, 2000, Vista, 7. Статья, содержащая необходимую информацию, находится по адресу http://support.microsoft.com/kb/822158/ru. Материал, изложенный в статье, поможет оптимизировать производительность системы при работе с антивирусом.

Внимание! Наличие ***** после названия опции означает, что данная опция не поддерживается при проверке станций, работающих под ОС семейства UNIX и macOS.

Общие

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и macOS, заключены в квадратные скобки **[ ]**.

Настройки, которые не поддерживаются при проверке станций, работающих под ОС Android, заключены в круглые скобки **( )**.

В разделе **Общие** вы можете задать следующие настройки антивирусной проверки:

- Установите флажок **Использовать эвристический анализ**, чтобы Сканер осуществлял поиск неизвестных вирусов при помощи эвристического анализатора. В данном режиме возможны ложные срабатывания Сканера.
- Установите флажок **Проверять загрузочные секторы**, чтобы Сканер осуществлял проверку загрузочных секторов. Проверяются как загрузочные секторы ло гических дисков, так и главные загрузочные секторы физических дисков.
- Установите флажок **[Проверять автоматически запускаемые программы]**, чтобы проверять программы, автоматически запускаемые при старте операционной системы.
- Установите флажок **Следовать символическим ссылкам**, чтобы следовать символическим ссылкам при сканировании.
- Установите флажок **[(Проверять загружаемые программы и модули)]**, чтобы проверять процессы, запущенные в оперативной памяти.
- Установите флажок **[(Проверять на наличие руткитов)]**, чтобы включить сканирование на наличие вредоносных программ, скрывающих свое присутствие в системе.
- Установите флажок **[(Прерывать проверку при переходе на питание от аккумулятора)]**, чтобы прерывать антивирусную проверку при переходе компьютера пользователя на питание от аккумулятора.
- Выпадающий список **[(Приоритет сканирования)]** определяет приоритет процесса проверки относительно имеющихся вычислительных ресурсов операционной системы.
- Установите флажок **[(Уровень загрузки ресурсов компьютера)]**, чтобы ограничивать и спользование ресурсов компьютера при проверке, и выберите из выпадающего списка максимально допустимую загрузку ресурсов Сканером. При отсутствии других задач ресурсы компьютера будут использоваться максимально.

Опция **Уровень загрузки ресурсов компьютера** не оказывает влияния на фактическую величину загрузки ресурсов при запуске сканирования на однопроцессорной системе с одним ядром.

- Выпадающий список **(Действия после сканирования)** определяет автоматическое выполнение заданного действия сразу после окончания процесса проверки:
  - **ничего не делать** — после завершения проверки не предпринимать никаких действий с компьютером пользователя.
  - **[выключить станцию]** — после завершения проверки выключить компьютер пользователя. Перед выключением компьютера Сканер применит заданные действия к обнаруженным угрозам.
  - **[перезагрузить станцию]** — после завершения проверки перезагрузить компьютер пользователя. Перед перезагрузкой компьютера Сканер применит заданные действия к обнаруженным угрозам.
  - **[перевести станцию в ждущий режим]**.
  - **перевести станцию в спящий режим**.
- Установите флажок **[Отключить сеть при сканировании]**, чтобы отключить компьютер от локальной сети и Интернета на время сканирования.
- Установите флажок **Проверять стационарные диски** для проверки стационарных жестких дисков (винчестер и т. п.).
- Установите флажок **Проверять объекты на съемных носителях** для проверки всех сменных носителей информации, таких как накопители на магнитных дисках (дискеты), CD/DVD-диски, флеш-накопители и т. д.
- В поле **Пути, выбранные для сканирования** задайте список проверяемых путей (способ их задания описывается ниже).
  - Для того чтобы добавить новую строку в список, нажмите кнопку  и в открывшуюся строку введите требуемый путь.
  - Для того чтобы удалить элемент из списка, нажмите кнопку  напротив соответствующей строки.

При установке флажка **Пути, выбранные для сканирования** осуществляется антивирусная проверка только указанных путей. Если флажок снят, проводится проверка всех дисков.

В разделе **Исключения** задается список каталогов и файлов, исключаемых из антивирусной проверки.

Для редактирования списков исключаемых путей и файлов:

1. Введите путь к требуемому файлу или каталогу в строку **Исключаемые пути и файлы**.

2. Для того чтобы добавить новую строку в список, нажмите кнопку  и в открывшуюся строку введите требуемый путь.

3. Для того чтобы удалить элемент из списка, нажмите кнопку  напротив соответствующей строки.

Список исключаемых объектов может содержать элементы следующих видов:

1. Прямой путь в явном виде до исключаемого объекта. При этом:

- Символ \ или / — исключение из проверки всего диска, на котором находится каталог установки ОС Windows,
- Путь, заканчивающийся символом \ — данный каталог исключается из проверки,
- Путь, не заканчивающийся символом \ — любой подкаталог, путь к которому начинается на указанную строку, исключается из проверки.

Например: C:\Windows — не проверять файлы каталога C:\Windows и все его подкаталоги.

2. Маски объектов, исключаемых из проверки. Для задания масок допускается использование знаков ? и *.

Например: C:\Windows**.dll — не проверять все файлы с расширением dll, расположенные во всех подкаталогах каталога C:\Windows.

3. Регулярное выражение. Пути могут задаваться регулярными выражениями. Также любой файл, полное имя которого (с путем) соответствует регулярному выражению, исключается из проверки.

Примечание. Перед запуском процесса сканирования на вирусы ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows Server 2003. Статья, содержащая необходимую информацию, находится по адресу — http://support.microsoft.com/kb/822158/ru. Материал данной статьи призван помочь оптимизировать производительность системы.

Синтаксис регулярных выражений, и спользуемых для записи исключаемых путей, следующий:

qr{выражение}флаги

Наиболее часто в качества флага используется символ i, данный флаг означает "не принимать во внимание различие регистра букв".

Примеры записи исключаемых путей и файлов при помощи регулярных выражений

Регулярное выражение	**Значение**
qr{\\pagefile\.sys$}i	не проверять файлы подкачки ОС Windows NT
qr{\\notepad\.exe$}i	не проверять файлы notepad.exe
qr{^C:}i	не проверять вообще ничего на диске C
qr{^.:\\WINNT\\}i	не проверять ничего в каталогах WINNT на всех дисках
qr{(^C:)|(^.:\\WINNT\\)}i	объединение двух предыдущих случаев
qr{^C:\\dir1\\dir2\\file\.ext$}i	не проверять файл c:\dir1\dir2\file.ext
qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i	не проверять файл file.ext, если он в каталоге c:\dir1\dir2 и его подкаталогах
qr{^C:\\dir1\\dir2\\}i	не проверять каталог c:\dir1\dir2 и его подкаталоги
qr{dir\\[^\\]+}i	не проверять подкаталог dir, находящийся в любом каталоге, но проверять подкаталоги
qr{dir\\}i	не проверять подкаталог dir, находящийся в любом каталоге, и его подкаталоги

Использование регулярных выражений кратко описано в документе **Приложения**, в разделе Приложение J. Использование регулярных выражений в Dr.Web Enterprise Security Suite.

В подразделе **Проверять содержимое следующих файлов** вы можете отключить проверку составных объектов. Для этого снимите следующие флажки:

- Флажок **Архивы** предписывает Сканеру искать вирусы в файлах, упакованных в файловые архивы.
- Флажок **Почтовые файлы** предписывает проверять почтовые ящики.
- Флажок **Инсталляционные пакеты** предписывает Сканеру проверять пакеты для установки программ.

В разделе **Действия** задается реакция Сканера на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов.

Настройки, которые не поддерживаются при проверке станций, работающих под ОС семейства UNIX и macOS, заключены в квадратные скобки **[ ]**.

Dr.Web Agent Сканер автоматически применяет действия, заданные для обнаруженных вредоносных объектов.

Предусмотрены следующие действия над обнаруженными угрозами:

- **Лечить** — восстановить состояние инфицированного объекта до заражения. Если объект неизлечим или попытка лечения не была успешной, будет применено действие, заданное для неизлечимых объектов.

  Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров).
- **Удалять** — удалить зараженные объекты.
- **Перемещать в карантин** — переместить зараженные объекты в каталог Карантина на станции.
- **Сообщать** — отправить в Центр управления уведомление об обнаружении вируса (о настройке режима оповещений см. в п. Настройка оповещений).
- **Игнорировать** — пропустить объект без выполнения каких-либо действий, в том числе не присылать оповещения в статистике сканирования.

Действия Сканера над обнаруженными вредоносными объектами

Объект	**Действие**				
	Лечить	**Удалять**	**Перемещать в карантин**	**Сообщать**	**Игнорировать**
Инфицированные	+/*	+	+		
Подозрительные		+	+/*		+
Неизлечимые		+	+/*		
Инсталляционные пакеты		+	+/*		
Архивы		+	+/*		

Объект	Действие				
	Лечить	**Удалять**	**Перемещать в карантин**	**Сообщать**	**Игнорировать**
Почтовые файлы			+/*		+
Загрузочные секторы	+/*			+	
Рекламные программы		+	+/*		+
Программы дозвона		+	+/*		+
Программы-шутки		+	+/*		+
Потенциально опасные		+	+/*		+
Программы взлома		+	+/*		+

Для задания действий над обнаруженными угрозами служат следующие настройки:

- Выпадающий список **Инфицированные** задает реакцию Сканера на обнаружение файла, зараженного известным вирусом.
- Выпадающий список **Подозрительные** задает реакцию Сканера на обнаружение файла, предположительно зараженного вирусом (срабатывание эвристического анализатора).

При сканировании, включающем каталог установки ОС, рекомендуется выбрать для подозрительных файлов реакцию **Информировать**.

- Выпадающий список **Неизлечимые** задает реакцию Сканера на обнаружение файла, зараженного известным неизлечимым вирусом, а также когда предпринятая попытка излечения не принесла успеха.
- Выпадающий список **Инфицированные инсталляционные пакеты** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в составе пакетов для установки программ.
- Выпадающий список **Инфицированные архивы** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в составе файлового архива.
- Выпадающий список **Инфицированные почтовые файлы** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в формате электронной почты.

При обнаружении вирусов или подозрительного кода внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров) действия по отношению к угрозам внутри таких объектов выполняются над всем объектом, а не только н ад зараженной его частью. По умолчанию во всех этих случаях предусмотрено информирование.

- Выпадающий список **Инфицированные загрузочные секторы** задает реакцию Сканера на обнаружение вирусов или подозрительного кода в области загрузочных секторов.
- Следующие выпадающие списки задают реакцию Сканера на обнаружение соответствующего нежелательного ПО:
  - **Рекламные программы**;
  - **Программы дозвона**;
  - **Программы-шутки**;
  - **Потенциально опасные**;

- **Программы взлома**.

При задании действия **Игнорировать** не будет произведено никаких действий: в Центр управления не будет отправлено уведомление, как в случае включенной опции **Информировать** при обнаружении вируса.

Установите флажок **[Перезагружать компьютер автоматически]** для автоматической перезагрузки компьютера пользователя после окончания сканирования, если в процессе проверки были обнаружены инфицированные объекты, для завершения лечения которых требуется перезагрузка операционной системы. Если флажок снят, перезагрузка компьютера пользователя не будет осуществляться. В статистике сканирования станции, получаемой Центром управления, будет сообщено о необходимости перезагрузки станции для завершения лечения. Информация о состоянии, требующем перезагрузку, отображается в таблице Состояния. При необходимости администратор может перезагрузить станцию из Центра управления (см. раздел Антивирусная сеть).

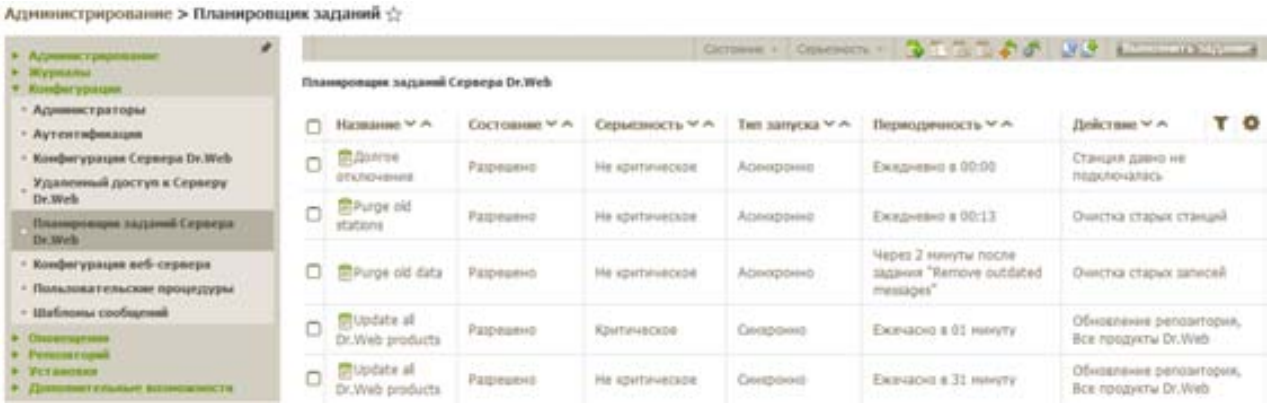
Установите флажок **Показывать ход проверки**, чтобы отображать в Центре управления индикатор и строку состояния процесса сканирования станции.

- В разделе **Ограничения** доступны следующие настройки:
  - **Максимальное время сканирования (мс)** — по истечении указанного в миллисекундах времени проверка объекта будет прекращена.
  - **Максимальный уровень вложенности в архив** — если уровень вложенности в архив превышает заданное ограничение, проверка будет производиться только до указанного уровня вложенности.
  - **Максимальный размер архива (КБ)*** — если размер архива превышает заданное в килобайтах ограничение, распаковка и проверка производиться не будет.
  - **Максимальный коэффициент сжатия архива** — если **Сканер** определяет, что коэффициент сжатия архива превышает заданное ограничение, распаковка и проверка производиться не будет.
  - **Максимальный размер распакованного объекта (КБ)*** — если **Сканер** определяет, что после распаковки размер файлов архива превышает заданное в килобайтах ограничение, распаковка и проверка производиться не будет.
  - **Порог проверки уровня сжатия (КБ)*** — минимальный размер файла в килобайтах, начиная с которого будет производиться проверка коэффициента сжатия.

Вы можете просматривать результаты работы компонентов рабочей станции — обновлений ПО, антивирусных сканирований и антивирусного мониторинга. Для этого служат статистические таблицы и графики.

7.12.3. Настройка расписания антивирусного сервера

Для выполнения настройки расписания антивирусного сервера необходимо выбрать раздел **Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web**. Будет отображен перечень текущих заданий ES-сервера.

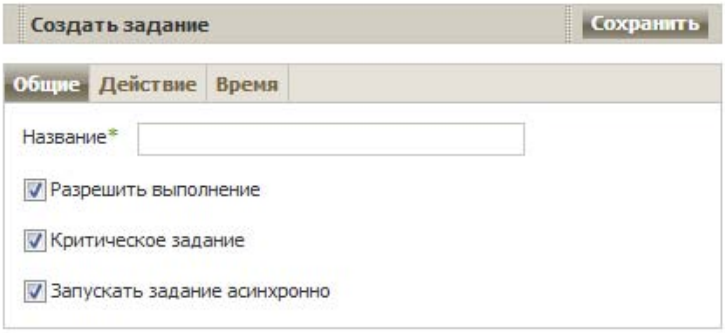


Для того чтобы удалить задание из списка, выделите его с помощью флажка, после чего нажмите на панели инструментов кнопку (**Удалить выбранные задания**).

Вы также можете запретить выполнение задания или разрешить выполнение ранее запрещенного задания.

Для того чтобы отредактировать параметры задания, нажмите на название соответствующего задания (оно выполнено в виде ссылки). При этом откроется **Редактор заданий**, описанный ниже. Укажите необходимые параметры и нажмите на кнопку **Сохранить**.

Для того чтобы добавить задание в список, нажмите на панели инструментов кнопку (**Создать задание**). Откроется соответствующее окно настроек (аналогично для создания и редактирования задания).

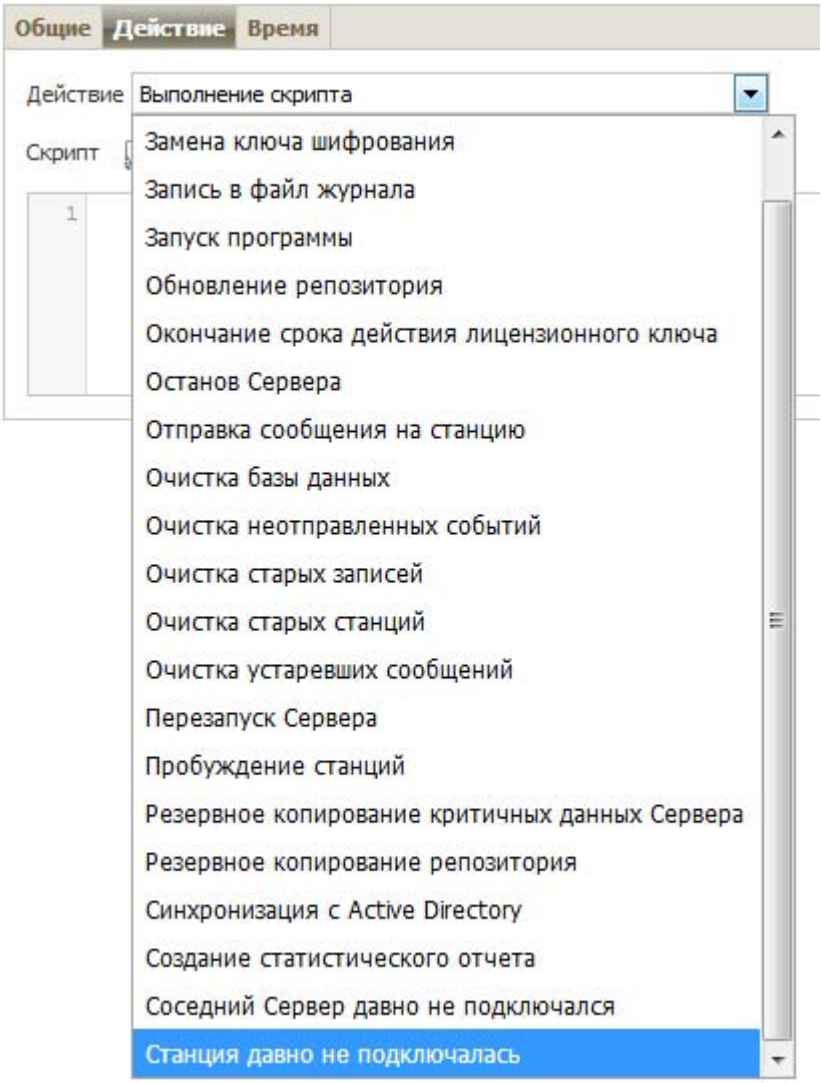


Для того чтобы отредактировать или задать параметры задания:

На вкладке **Общие**:

1. Введите в поле **Название** наименование задания, под которым оно будет отображаться в расписании.
2. С помощью флажка **Разрешить исполнение** определите, будет ли данное задание выполняться. Если флажок не установлен, задание будет присутствовать в списке, но не будет исполняться.
3. С помощью флажка **Критическое задание** определите, является ли данное задание критичным для выполнения. Установленный флажок дает указание выполнить задание при следующем запуске **Сервера Dr.Web**, если выполнение данного задания будет пропущено (**Сервер** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Сервера** оно выполняется один раз. Аналогичное действие осуществляется из главного окна расписания при помощи элемента панели инструментов **Серьезность**.

На вкладке **Действие** выберите в раскрывающемся списке **Действие** тип задания. При этом изменится вид нижней части окна, содержащей параметры данного типа задания. Введите эти параметры (ниже параметры типа задания рассмотрены отдельно).



На вкладке **Время** выберите периодичность и время запуска задания и настройте время в соответствии с выбранной периодичностью (это действие аналогично настройке времени в расписании рабочей станции).

Установите флажок **Запретить после первого выполнения** для однократного выполнения задания в соответствии с указанным временем. Если флажок снят, задание будет выполняться многократно с установленной периодичностью. Чтобы повторить выполнение однократного задания, которое уже было выполнено, воспользуйтесь кнопкой **Запланировать повторно** на панели инструментов раздела расписания.

Нажмите на кнопку **Сохранить**.

Типы заданий по действиям и их параметры:

Тип задания	**Параметры и описание**
Выполнение	Задание предназначено для выполнения lua-скрипта, приведенного в

Тип задания	Параметры и описание
скрипта	поле **Скрипт**. Одновременное выполнение задания типа **Выполнение скрипта** на нескольких Серверах, использующих одну БД, может приводить к ошибкам выполнения данного задания. При выполнении lua-скриптов администратор получает доступ ко всей файловой системе в пределах каталога Сервера и некоторым системным командам на компьютере с установленным Сервером. Чтобы запретить доступ к расписанию, отключите право **Редактирование расписания Сервера** для соответствующего администратора (см. п. Администраторы и административные группы).
Замена ключа шифрования	Задание предназначено для периодической замены следующих инструментов, обеспечивающих шифрование между компонентами: •закрытый ключ drwcsd.pri на Сервере, •открытый ключ drwcsd.pub на рабочих станциях, •сертификат drwcsd-certificate.pem на рабочих станциях. Поскольку некоторые рабочие станции могут оказаться выключены на момент замены, процедура делится на два этапа. Необходимо создать два задания для выполнения каждого из этих этапов, при этом второй этап рекомендуется выполнять спустя некоторое время после первого этапа, за которое станции наверняка подключатся к Серверу. При создании задания выберите соответствующий этап из выпадающего списка: •**Добавление нового ключа** — первый этап процедуры, на котором создается новая неактивная пара ключей шифрования и сертификат. Станции получают новый открытый ключ и сертификат, когда подключаются к Серверу. •**Удаление старого ключа и переход на новый ключ** — второй этап, на котором рабочие станции информируются о переходе на новые ключи шифрования и сертификат, после чего осуществляется замена действующих инструментов на новые: открытые ключи и сертификат на станциях и закрытый ключ на Сервере. Те станции, которые по каким-либо причинам не получили новые открытый ключ и сертификат, не смогут подключиться к Серверу. Для разрешения данной проблемы необходимо вручную подложить новый открытый ключ и сертификат на станции (с процедурой замены ключа на станции можно ознакомиться в документе **Приложения**, в разделе Подключение Агента Dr.Web к другому Серверу Dr.Web).
Запись в файл журнала	Задание предназначено для записи в файл отчета Сервера заданной строки. **Строка** — текст сообщения, записываемого в файл отчета.
Запуск	Задание предназначено для запуска произвольной программы.

Тип задания	Параметры и описание
программы	Программы, запущенные в рамках данного задания, выполняются в фоновом режиме. Необходимо задать следующие параметры: •В поле **Путь** — полное имя (с путем) исполняемого файла программы, которую предполагается запускать. •В поле **Аргументы** — параметры командной строки для запускаемой программы. •Установите флажок **Ожидать завершения программы** для ожидания завершения программы, запущенной данным заданием. При этом Сервер протоколирует запуск программы, код возврата и время завершения программы. Если флажок **Ожидать завершения программы** снят, задание считается завершенным сразу после запуска программы, и Сервер протоколирует только запуск программы.
Окончание срока действия лицензионного ключа	Задание предназначено для выдачи оповещения об окончании срока действия лицензии на продукт Dr.Web. Необходимо задать период до окончания срока действия лицензии, начиная с которого будет выдаваться напоминание.
Обновление репозитория	Задание предназначено для запуска обновления продуктов репозитория с ВСО. Необходимо задать следующие параметры: •В списке **Продукт** установите флажки напротив тех продуктов репозитория, которые будут обновляться согласно этому заданию. •Установите флажок **Обновлять лицензионные ключи**, чтобы активировать процедуру автоматического обновления лицензионных ключей при обновлении репозитория. Подробная информация приведена в разделе Автоматическое обновление лицензий.
Останов Сервера	Задание предназначено для завершения работы Сервера. Запускается без дополнительных параметров.
Отправка сообщения на станцию	Задание предназначено для отправки произвольного сообщения пользователям станции или группы станций. Настройки сообщения приведены в разделе Отправка сообщений станциям.
Очистка базы данных	Задание предназначено для сборки и удаления неиспользуемых записей в базе данных Сервера посредством выполнения команды vacuum. Запускается без дополнительных параметров.
Очистка неотправленных событий	Задание предназначено для удаления неотправленных событий из базы данных. Необходимо указать период хранения неотправленных событий, по истечении которого они будут удаляться. Здесь имеются в в иду события, передаваемые подчиненным Сервером главному Серверу. При неудачной передаче события оно

Тип задания	Параметры и описание
	заносится в список неотправленных. Подчиненный Сервер с заданной периодичностью осуществляет попытки передачи. При выполнении задания **Очистка неотправленных событий** осуществляется удаление всех событий, длительность хранения которых достигла и превысила заданный период.
Очистка старых записей	Задание предназначено для удаления устаревшей информации о станциях из базы данных. Необходимо указать количество дней, по истечении которых статистические данные о рабочих станциях (но не сами станции) признаются старыми и удаляются с Сервера. Период удаления статистических данных задается для каждого типа записей в отдельности.
Очистка старых станций	Задание предназначено для удаления устаревших станций из базы данных. Необходимо указать временной период (по умолчанию 90 дней), в течение которого не посещавшие Сервер станции признаются старыми и удаляются с Сервера.
Старые данные автоматически удаляются из базы данных с целью экономии дискового пространства. По умолчанию период для заданий **Очистка старых записей** и **Очистка старых станций** составляет 90 дней. Уменьшение этого параметра приводит к меньшей репрезентативности накопленной статистики о работе компонентов антивирусной сети. Увеличение параметра может серьезно увеличить потребность Сервера в ресурсах.	
Очистка устаревших сообщений	Задание предназначено для удаления из базы данных следующих сообщений: •агентские оповещения, •оповещения для веб-консоли, •отчеты, созданные по расписанию. При этом удаляются сообщения, помеченные как устаревшие, т. е. сообщения с истекшим сроком хранения, который вы можете настроить: •для оповещений: при создании оповещений для соответствующего способа отправки (см. п. Конфигурация оповещений). •для отчетов: в задании на создание отчетов. Задание запускается без дополнительных параметров.
Перезапуск Сервера	Задание предназначено для перезапуска Сервера. Запускается без дополнительных параметров.
Пробуждение станций	Задание предназначено для включения станций, например, перед запуском задания на сканирование. Включаемые станции задаются при помощи следующих параметров задания: •**Будить все станции** — предписывает включить все станции, подключенные к данному Серверу.

Тип задания	Параметры и описание
	•**Будить станции по заданным параметрам** — предписывает включить только станции, соответствующие указанным ниже параметрам: ▫**IP-адреса** — список IP-адресов станций, которые необходимо включить. Задается в формате: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. При задании списка адресов используйте запятую или переход на новую строку в качестве разделителя. Также IP-адреса можно заменять на DNS-имена компьютеров. ▫**MAC-адреса** — список MAC-адресов станций, которые необходимо включить. Октеты MAC-адреса разделяются знаком ':'. При задании списка адресов используйте запятую или переход на новую строку в качестве разделителя. ▫**Группы** — список групп, станции которых необходимо включить. Чтобы изменить список групп, нажмите кнопку **Редактировать** (или идентификаторы групп, если группы уже заданы) и выберите нужные группы в открывшемся окне. Для выбора нескольких групп используйте кнопки CTRL и SHIFT. Для выполнения данного задания на включаемых станциях должны быть установлены сетевые карты с поддержкой опции Wake-on-LAN. Поддержку опции Wake-on-LAN вы можете проверить в документации к сетевой карте или в свойствах сетевой карты (**Панель управления → Сеть и Интернет → Сетевые подключения → Настройка параметров подключения → Настроить → Дополнительно**).
Резервное копирование критичных данных сервера	Задание предназначено для создания резервной копии следующих критичных данных Сервера: •база данных, •лицензионный ключевой файл, •закрытый ключ шифрования. Необходимо задать следующие параметры: •**Путь** — путь к каталогу, в который будут сохранены данные (пустой путь означает каталог по умолчанию). •**Максимальное количество копий** — максимальное количество резервных копий (значение 0 означает отмену этого ограничения). Подробнее см. в документе **Приложения**, п. Приложение Н4.5. Каталог для резервного копирования должен быть пуст. В противном случае содержимое каталога будет удалено при выполнении резервного копирования.
Резервное копирование репозитория	Задание предназначено для периодического сохранения резервных копий репозитория. Необходимо задать следующие параметры: •**Путь** — полный путь до каталога, в котором будет сохраняться резервная копия. •**Максимальное количество копий** — максимальное количество

Тип задания	Параметры и описание
	резервных копий репозитория, сохраняемых заданием в указанном каталоге. При достижении максимального количества копий репозитория, для сохранения новой копии удаляется самая старая из имеющихся копий. •**Область репозитория** определяет, какой блок информации об антивирусном компоненте будет сохраняться: ▫**Весь репозиторий** — сохранять все ревизии из репозитория, для тех компонентов, которые выбраны в списке ниже. ▫**Только важные ревизии** — сохранять только ревизии, помеченные как важные, для тех компонентов, которые выбраны в списке ниже. ▫**Только конфигурационные файлы** — сохранять только конфигурационные файлы тех компонентов, которые выбраны в списке ниже. •Установите флажки напротив компонентов, выбранные области которых буду сохраняться. Каталог для резервного копирования должен быть пуст. В противном случае содержимое каталога будет удалено при выполнении резервного копирования.
Синхронизация с Active Directory	Задание предназначено для синхронизации структуры сети: контейнеры Active Directory, содержащие компьютеры, становятся группами антивирусной сети, в которые помещаются рабочие станции. Запускается без дополнительных параметров. По умолчанию данное задание отключено. Для активации выполнения задания установите опцию **Разрешить выполнение** в настройках задания или на панели инструментов как описано выше.
Соседний Сервер давно не подключался	Задание предназначено для выдачи оповещения о том, что соседние Серверы давно не подключались к данному Серверу. Настройка отображения оповещения осуществляется в разделе Конфигурация оповещений при помощи пункта **Соседний сервер давно не подключался**. В полях **Часов** и **Минут** задайте периоды времени, по истечении которых соседний Сервер будет считаться давно не подключавшимся.
Станция давно не подключалась	Задание предназначено для выдачи оповещения о том, что станции давно не подключались к данному Серверу. Настройка отображения оповещения осуществляется в разделе **Конфигурация оповещений** при помощи пункта **Станция давно не подключалась к серверу**. В поле **Дней** задайте период времени, по истечении которого станция будет считаться давно неподключавшейся.
Создание	Задание предназначено для создания отчета со статистическими

Тип задания	Параметры и описание
статистического отчета	данными по антивирусной сети. Для возможности создания отчета необходимо, чтобы было включено оповещение **Статистический отчет** (см. п. Конфигурация оповещений). Созданный отчет сохраняется на компьютере с установленным Сервером. Получение отчета зависит от типа оповещения: •Для метода отправки сообщения **Электронная почта**: на адрес почтового ящика, заданного в настройках оповещения, отправляется письмо со ссылкой на местоположение отчета и сам отчет во вложениях к письму. •Для всех остальных методов отправки: отп равляется соответствующее оповещение, которое содержит ссылку на местоположение отчета. Для создания задания в расписании необходимо задать следующие параметры: •**Профили уведомлений** — название группы оповещений с настройками, согласно которым будет создаваться отчет. Название заголовка задается при создании новой группы оповещений. •**Язык отчета** — язык, на котором будут представлены данные в отчете. •**Формат даты** — формат, в котором будет отображаться статистическая информация, содержащая даты. Доступны следующие форматы: ▫европейский: DD-MM-YYYY HH:MM:SS ▫американский: MM/DD/YYYY HH:MM:SS •**Формат отчета** — формат документа, в котором будет сохранен статистический отчет. •**Отчетный период** — период времени, статистические данные за который будут внесены в отчет. •**Группы** — список групп станций антивирусной сети, данные о которых будут занесены в отчет. Для выбора нескольких групп используйте кнопки CTRL или SHIFT. •**Таблицы отчета** — список статистических таблиц, данные из которых будут занесены в отчет. Для в ыбора нескольких таблиц используйте кнопки CTRL или SHIFT. •**Срок хранения отчета** — временной период хранения отчета на компьютере с установленным Сервером, начиная с момента создания отчета.

7.12.4. Автоматизация выполнения заданий

Для автоматизации выполнения определенных заданий **Сервера Dr.Web** возможно использование пользовательских процедур, реализованных в виде lua-скриптов. Скрипты должны располагаться в каталоге:

- для ОС Windows: var\extensions
- для ОС FreeBSD: /var/drwcs/extensions
- для ОС Linux: /var/opt/drwcs/extensions

каталога установки **Сервера Dr.Web**. Сразу после инсталляции **Сервера** в подкаталоге **disabled** данного каталога размещаются предустановленные процедуры, которые могут использоваться в процессе работы, но по умолчанию выключены.

Для того чтобы разрешить выполнение пользовательских скриптов расширения, необходимо:

- запустить **Сервер Dr.Web** с ключом -hooks;
- определить переменную DRWCS_HOOKS в файле /etc/init.d/drwcsd. Переменная DRWCS_HOOKS не имеет параметров.

Все скрипты по умолчанию отключены. Для включения скриптов необходимо в файле скрипта удалить начальный параметр disabled или весь комментарий полностью (оставить пустую строку). Включенные скрипты перемещаются в подкаталог **enabled** каталога **extensions**.

В том числе каталог extensions содержит следующие скрипты, часть из которых имеются только в виде шаблонов (отмечены знаком *):

- `*access_check.ds` — вызывается перед проверкой доступа согласно соответствующим ACL (Access Control List — списки контроля доступа);
- `*access_denied.ds` — вызывается при запрете доступа согласно настройкам ACL или результату выполнения процедуры ccess_check;
- `admin_logged.ds` — вызывается при успешной авторизации администратора на Сервере;
- `admin_noauth.ds` — вызывается при невозможности авторизации администратора на Сервере;
- `*agent_status.ds` — вызывается при сообщении **Агентом** его локальных политик;
- `*backup.ds` — вызывается при завершении резервного копирования файлов (backup), но перед удалением файлов предыдущего резервного копирования;
- `bad_connection.ds` — вызывается при невозможности установления соединения с клиентом;
- `connection_denied.ds` — вызывается при запрете нового соединения согласно ограничениям в лицензионном соглашении;
- `deinstallations.ds` — вызывается при деинсталляции Агента на подключенной к Серверу станции;
- `*database_load.ds` — вызывается после успешной загрузки БД Сервера;
- `*database_verifi.ds` — вызывается после успешной проверки БД Сервера;
- `*deinstallation.ds` — вызывается после завершения удаления **Агента**;
- `*device_blocked.ds` — вызывается, когда на станции блокируется какое-либо устройство;
- `*disconnected.ds` — вызывается после завершения соединения с клиентом;
- `*epidemic.ds` — вызывается при обнаружении Сервером возникновения эпидемии (превышении эпидемического порога заражений на станциях);
- `group_changed.ds` — вызывается при изменении настроек группы;
- `group_created.ds` — вызывается при создании новой группы;
- `group_deleted.ds` — вызывается при удалении группы;
- `*install.ds` — вызывается при получении события installation;
- `*installed_components.ds` — вызывается, когда Агент присылает уведомление об успешной установке компонентов антивируса;
- `*jobexecuted.ds` — вызывается при получении от **Агента** события job executed;
- `*key_renew_reminder.ds` — вызывается, когда срок действия ключа истекает или он был обновлен;

- *ldap_user_dn_translate.ds — вызывается модуль аутентификации LDAP преобразует имя пользователя в формат доменного имени;
- license_error.ds – вызывается в случае невозможности установления соединения с клиентом согласно ограничениям в лицензионном соглашении;
- *load_plugin.ds – вызывается при успешной загрузке модуля плагина;
- *load_protocol.ds – вызывается при успешной загрузке модуля протокола;
- *neighbor_connected.ds — вызывается при соединении с соседним **Сервером**;
- *neighbor_environment.ds — вызывается при изменении окружения соседнего **Сервера**;
- *neighbor_geolocation.ds — вызывается при получении данных расположения соседнего **Сервера**;
- *neighbor_install.ds — вызывается при выполнении инсталляции антивирусного ПО на станцию соседним **Сервером**;
- *neighbor_noauth.ds — вызывается при ошибке соединении с соседним **Сервером**;
- *neighbor_run_begin.ds — вызывается при получении с соседнего **Сервера** информации о запуске компонента;
- *neighbor_run_end.ds — вызывается при получении с соседнего **Сервера** информации об остановке компонента;
- *neighbor_scan_error.ds — вызывается при ошибке сканирования на станции, подключенной к соседнему **Серверу**;
- *neighbor_scan_statistics.ds — вызывается при получении статистики сканирования с соседнего **Сервера**;
- *neighbor_station_deleted.ds — вызывается при удалении станции на соседнем **Сервере**;
- *neighbor_station_status.ds — вызывается при получении статуса станций с соседнего **Сервера**;
- *neighbor_virus.ds — вызывается при обнаружении вредоносного ПО на станциях, подключенных к соседнему **Серверу**;
- newbie_accepted.ds — вызывается при предоставлении доступа новичку, успешной его авторизации и создании станции в базе данных;
- *newbie_came.ds — вызывается при подключении новичка;
- *newbie_registered.ds — вызывается при предоставлении доступа новичку, данных ко котором еще нет в БД;
- *pong.ds — вызывается при получении события PONG от **Агента**;
- *proxy_created.ds — вызывается при успешном создании прокси-сервера;
- *proxy_deleted.ds — вызывается при удалении прокси-сервера;
- *run_begin.ds — вызывается при успешном запуске подключенного к Серверу **Агента**;
- *run_end.ds — вызывается при остановке подключенного к Серверу **Агента**;
- scan_error.ds — вызывается при получении события scan error от **Агента**;
- *scan_statistics.ds — вызывается при получении статистики сканирования от подключенного к Серверу **Агента**;
- server_jobexecuted.ds – вызывается при выполнении Сервером полученной команды;
- *server_load.ds – вызывается при удачной загрузке в ОЗУ файлов Сервера (работа с Агентами невозможна до запуска Сервера);
- server_start.ds – вызывается при удачном запуске Сервера;
- server_terminate.ds – вызывается при остановке Сервера;
- *server_unload.ds – вызывается, если Сервер больше не выполняет часть своих функций по обслуживанию **Агентов**;

- *station_connected.ds – вызывается при удачном соединении Агента на станции с Сервером;
- *station_connecting.ds – вызывается при попытке станции установить соединении с Сервером;
- station_created.ds — вызывается при завершении создания станции;
- station_date.ds — вызывается при обнаружении некорректных времени/даты у станции;
- *station_geolocation.ds — вызывается при изменении местоположения станции;
- station_noauth.ds — вызывается при ошибке авторизации станции на Сервере;
- station_deleted.ds — вызывается при удалении станции;
- station_update_failed.ds – вызывается после получения сообщения от **Агента** об ошибке обновления станции;
- station_update_reboot.ds — вызывается после получения сообщения от **Агента** о необходимости перезагрузки станции после обновления;
- *unload_plugin.ds — вызывается при успешной выгрузке плагина на Сервере.
- *unload_protocol.ds — вызывается при успешной выгрузке протокола на Сервере;
- virus.ds — вызывается при получении события virus detected от **Агента** (обнаружение вируса);
- *virusbases.ds — вызывается при получении от Агента информации о вирусных базах.

7.12.4.1. Примеры пользовательских скриптов

В качестве примера рассмотрим скрипт **admin_noauth.ds.** Скрипт выполняется при попытке авторизации в сервере ES с неверными авторизационными данными (при условии, что разрешено исполнение пользовательских скриптов).

Скрипт вызывается с параметрами login, address, subsys, error.

Исходный код скрипта:

```
local args = ... -- args.login, args.address, args.subsys,
args.error

require('swatch/w7log')
require('swatch/syslog')

SwatchExportToW7Log:adminNoAuth(args)
SwatchExportToSysLog:adminNoAuth(args)
```

В первой строке определяется локальная переменная args и ей присваиваются переданные сервером скрипту параметры. Во второй и третьей строках подгружаются объекты из файлов w7log и syslog из директории swatch. В последних двух строках вызываются методы adminNoAuth классов SwatchExportToW7Log и SwatchExportToSysLog с параметром, определенным в первой строке args.

Содержимое скрипта w7log:

```
SwatchExportToW7Log = {

    _event = {
        what = { noun = '-', status = '-', verb = '-'},
        onwhat = { name = '-', path = '-', type = '-'},
```

```
        where = {name = dwcore.machine_name(), type = 'Dr.Web ES
Server'},
        who = { logonname = '-', realname = '-'},
        whereto = { name = '-', type = '-'},
        wherefrom = {name = '-', type = '-'},
        info = ''
    },
…
    adminNoAuth = function(self, args)
        if self:_isEnabled('adminNoAuth') then
            local event = self._event
            event.what = {
                noun = 'Administrator',
                status = 'Failure',
                verb = 'logon'
            }
            event.who.logonname = args.login
            self:_export('adminNoAuth', event)
        end
    end,
    ...
```

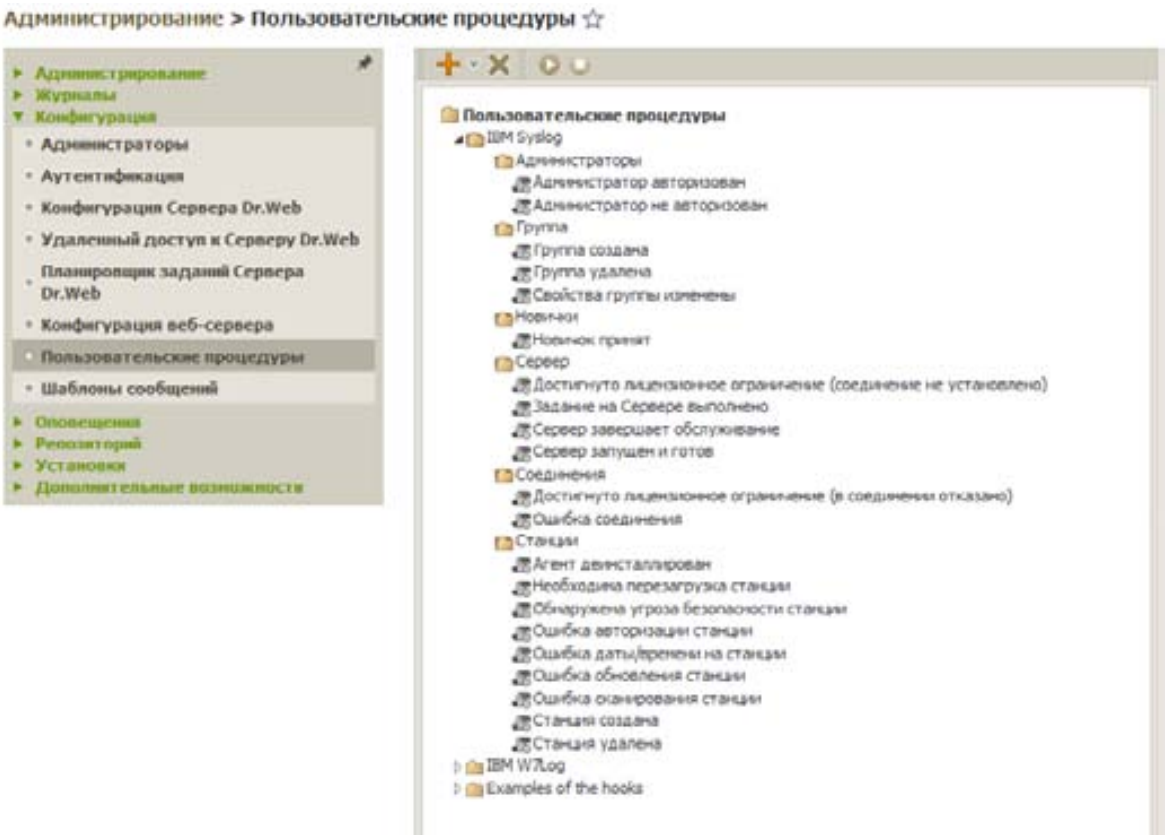
Содержимое скрипта syslog:

```
SwatchExportToSysLog = {

    _event = {
        host = server.my_uuid,
        prefix = '',
        message = ''
    },
…
    adminNoAuth = function(self, args)
        if self:_isEnabled('adminNoAuth') then
            local event = self._event
            event.prefix = 'Server'
       event.message = 'Authorization error for admin with
login \"'..args.login..'\"'
            self:_export('adminNoAuth', event, true)
        end
    end,
```

7.12.4.2. Выполнение пользовательских скриптов из Центра управления

Чтобы настроить выполнение пользовательских процедур, выберите пункт **Администрирование → Конфигурация → Пользовательские процедуры** управляющего меню.

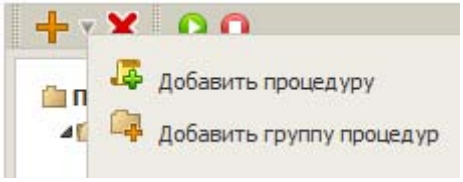


Иерархический список процедур отображает древовидную структуру, узлами которой являются группы процедур и входящие в них пользовательские процедуры.

Изначально в дереве процедур представлена предустановленная группа **Examples of the hooks**, которая содержит шаблоны всех доступных пользовательских процедур. На основе данных шаблонов вы можете создавать собственные пользовательские процедуры.

Для управления процедурами используются следующие элементы панели управления:

- Выпадающий список для добавления элемента дерева процедур:
  - **Добавить процедуру** — добавить пользовательскую процедуру на основе имеющегося шаблона.
  - **Добавить группу процедур** — создать новую пользовательскую группу для размещения в ней процедур.



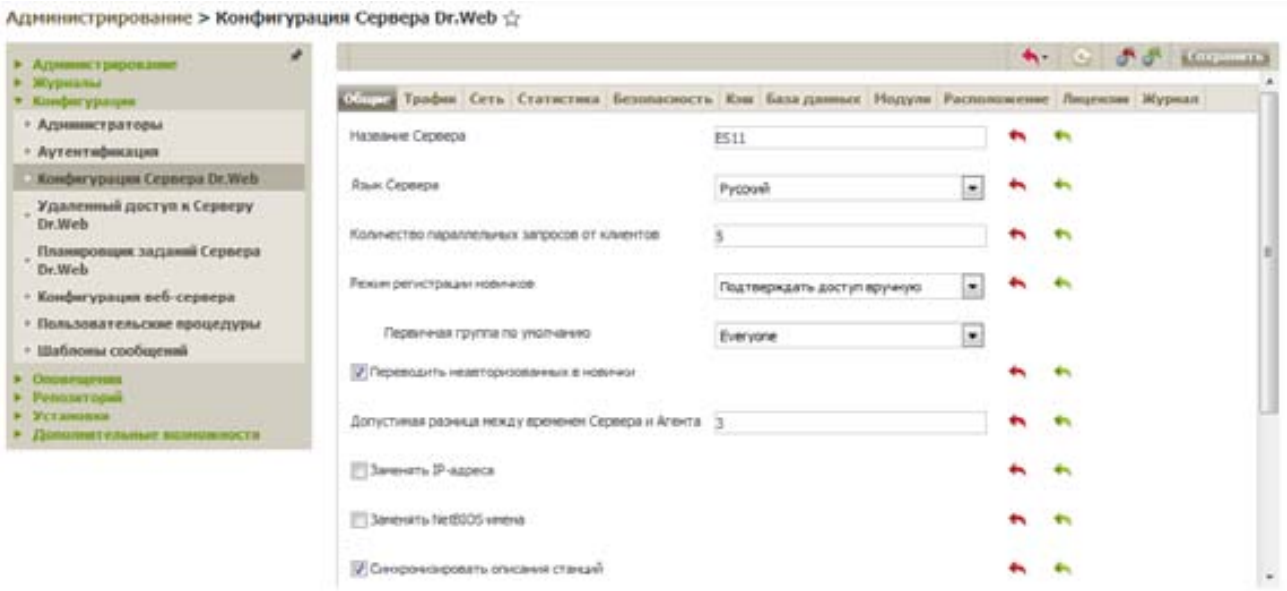
- **Удалить отмеченные объекты** — удалить пользовательскую процедуру или группу процедур, выбранную в дереве процедур.
- **Разрешить выполнение процедуры** — аналогичное действие производится из редактора процедур при помощи установки флажка **Разрешить выполнение процедуры**.
- **Запретить выполнение процедуры** — аналогичное действие производится из редактора процедур при помощи снятия флажка **Запретить выполнение процедуры**.

Отладка пользовательских скриптов как через меню **Пользовательские процедуры**, так и с помощью Lua-консоли.

8. Управление сервером Dr.Web Enterprise Security Suite

8.1. Настройка конфигурации Dr.Web Enterprise Server

Чтобы настроить конфигурационные параметры Сервера Dr.Web, выберите пункт **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**.



На панели инструментов доступны следующие кнопки управления настройками раздела:

- **Перезапустить Сервер Dr.Web** — перезапустить **Сервер** для принятия изменений, внесенных в данном разделе. Кнопка становится активной после внесения изменений в настройки раздела и нажатия кнопки **Сохранить**.
- **Восстановить конфигурацию из резервной копии** — выпадающий список, содержащий сохраненные копии настроек всего раздела, к которым можно вернуться после внесения изменений. Кнопка становится активной после внесения изменений в настройки раздела и нажатия кнопки **Сохранить**.

- **Установить все параметры в начальные значения** — восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).
- **Установить все параметры в значения по умолчанию** — установить для всех параметров данного раздела значения, заданные по умолчанию.

Чтобы принять изменения, внесенные в настройки раздела, нажмите кнопку **Сохранить**, после чего потребуется перезагрузка **Сервера**. Все доступные для заполнения поля, отмеченные знаком *, должны быть заполнены обязательно.

На вкладке **Общие** задаются следующие настройки работы Сервера:

- **Название Сервера** — имя данного Сервера. Если значение поля не задано, используется имя компьютера, на котором установлен Сервер Dr.Web.
- **Язык Сервера** — язык, который используется по умолчанию компонентами и системами Сервера Dr.Web, если не удалось получить настройки языка из базы данных Сервера. В частности, используется для Центра управления безопасностью Dr.Web и системы оповещений администратора, если база данных была повреждена, и получить настройки языка не представляется возможным.
- **Количество параллельных запросов от клиентов** — количество потоков для обработки данных, поступающих от клиентов: Агентов, инсталляторов Агентов, соседних Серверов. Данный параметр влияет на производительность Сервера. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой технической поддержки.

Начиная с версии 10 возможность редактирования параметра **Очередь авторизации** через Центр управления не предоставляется.

По умолчанию при установке нового Сервера данный параметр задается равным 50. При обновлении с предыдущей версии с сохранением файла конфигурации, значение очереди авторизации сохраняется из конфигурации предыдущей версии.

При необходимости изменения длины очереди авторизации отредактируйте значение следующего параметра в конфигурационном файле Сервера:

<!-- ***Maximun authorization queue length*** -->
<**maximum-authorization-queue** size='50'/>

- В выпадающем списке **Режим регистрации новичков** задается политика подключения новых рабочих станций (см. п. Политика подключения станций).
  - Выпадающий список **Первичная группа по умолчанию** определяет первичную группу, в которую будут помещены станции при автоматическом подтверждении доступа станций к Серверу.
- Установите флажок **Переводить неавторизованных в новички**, чтобы сбрасывать параметры получения доступа к Серверу у станций, не прошедших авторизацию. Данная опция может быть полезна при изменении настроек Сервера (таких, как открытый ключ шифрования) или при смене БД. В подобных случаях станции не смогут подключиться, и потребуется повторное получение новых параметров для доступа к Серверу.
- В поле **Допустимая разница между временем Сервера и Агента** задается допустимая разница между системным временем Dr.Web Сервера и Агентов Dr.Web в минутах. Если расхождение больше указанного значения, это будет отмечено в статусе станции на Сервере Dr.Web. По умолчанию допускается разница в 3 минуты. Значение 0 означает, что проверка не будет проводиться.

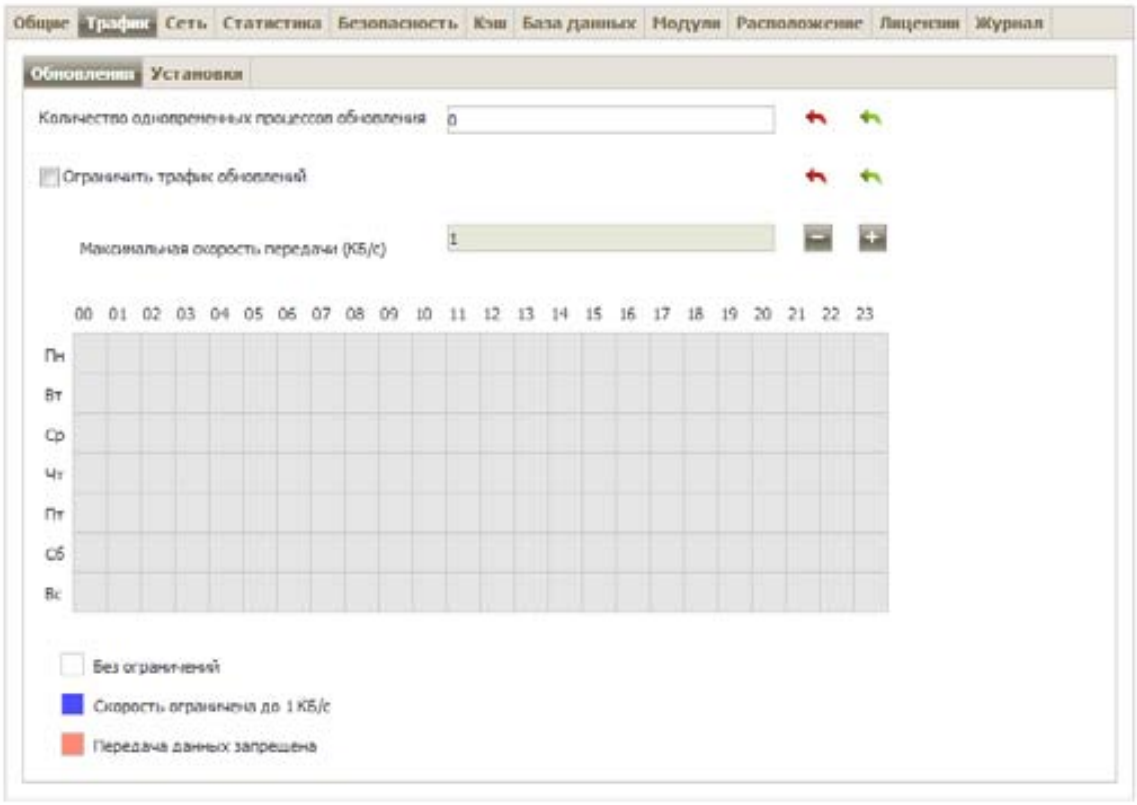
- Установите флажок **Заменять IP-адреса**, чтобы заменять IP-адреса DNS-именами компьютеров в файле журнала Сервера Dr.Web.
- Установите флажок **Заменять NetBIOS-имена**, чтобы отображать в каталоге антивирусной сети Центра управления не NetBIOS-имена рабочих станций, а их DNS-имена (при невозможности определения доменных имен отображаются IP-адреса).

Оба флажка **Заменять IP-адреса** и **Заменять NetBIOS-имена** по умолчанию сняты. При неправильной настройке службы DNS включение этих возможностей может значительно замедлить работу Сервера. При включении любого из этих режимов рекомендуется разрешить кэширование имен на DNS-сервере.

Если флажок **Заменять NetBIOS-имена** установлен и в антивирусной сети используется Прокси-сервер, то для всех станций, подключенных к Серверу через Прокси-сервер, в Центре управления в качестве названий станций будет отображаться название компьютера, на котором установлен Прокси-сервер.

- Установите флажок **Синхронизировать описания станций**, чтобы синхронизировать описание компьютера пользователя с описанием станции в Центре управления (поле Computer description на странице System properties). Если описание станции в Центре управления отсутствует, то в данное поле будет записано описание компьютера на стороне пользователя. Если описания различаются, то данные в Центре управления будут заменены на пользовательские.
- Установите флажок **Синхронизировать географическое положение**, чтобы активировать синхронизацию географического расположения станций между Серверами Dr.Web в многосерверной антивирусной сети. При установленном флажке вы также можете задать следующий параметр:
  - **Стартовая синхронизация** — количество станций без географических координат, информация о которых запрашивается при установлении соединения между Серверами Dr.Web.
- Установите флажок **Использовать политики**, чтобы разрешить использовать политики для настройки защищаемых станций (см. Политики).
  - **Количество версий политики** — максимальное количество версий, которые могут быть созданы для каждой политики.

На вкладке **Трафик** задаются параметры использования сетевого трафика для обновления компонентов антивируса и их установки:



На вкладке **Обновления** задаются ограничения на объем сетевого трафика при передаче обновлений между Сервером и Агентами.

Подробнее см. в п. Ограничение трафика обновлений.

Чтобы задать ограничения на трафик обновлений Агентов:

1. В поле **Количество одновременных процессов обновления** задается максимальное допустимое количество сессий раздачи обновлений, запущенных одновременно с данного Сервера. При достижении указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен. Установите значение **0**, чтобы снять ограничение на количество одновременных процессов.

2. Установите флажок **Ограничить трафик обновлений**, чтобы ограничить объем сетевого трафика при передаче обновлений между Сервером и Агентами.

Если флажок снят, обновления для Агентов передаются без ограничения полосы пропускания сетевого трафика.

3. Если флажок установлен, задайте в поле **Максимальная скорость передачи (КБ/с)** значение максимальной скорости передачи обновлений. При этом обновления будут передаваться в пределах заданной полосы пропускания совокупного сетевого трафика обновлений всех Агентов.

Допускается задание до пяти ограничений на скорость передачи обновлений. Для добавления еще одного поля ограничения скорости нажмите кнопку . Для удаления ограничения нажмите кнопку напротив ограничения, которое нужно удалить.

4. В таблице расписания задается режим ограничения обновлений отдельно на каждые 30 минут каждого дня недели.

Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков по принципу drag-and-drop.

Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей, начиная с варианта, при котором передача обновлений разрешена без ограничений трафика, до варианта, при котором передача обновлений запрещена.

5. После завершения редактирования нажмите кнопку **Сохранить** для принятия внесенных изменений.

На вкладке **Установки** задаются ограничения на объем сетевого трафика при передаче данных в процессе установки Агентов Dr.Web на станциях.

Подробнее см. в п. Ограничение трафика рабочих станций.

Чтобы задать ограничения на трафик при установке Агентов:

1. В поле **Количество одновременных процессов установки** задается максимальное допустимое количество сессий установки Агента, запущенных одновременно с данного Сервера. При достижении указанного ограничения запросы от Агентов размещаются в очереди ожидания. Размер очереди ожидания не ограничен. Установите значение **0**, чтобы снять ограничение на количество одновременных процессов.

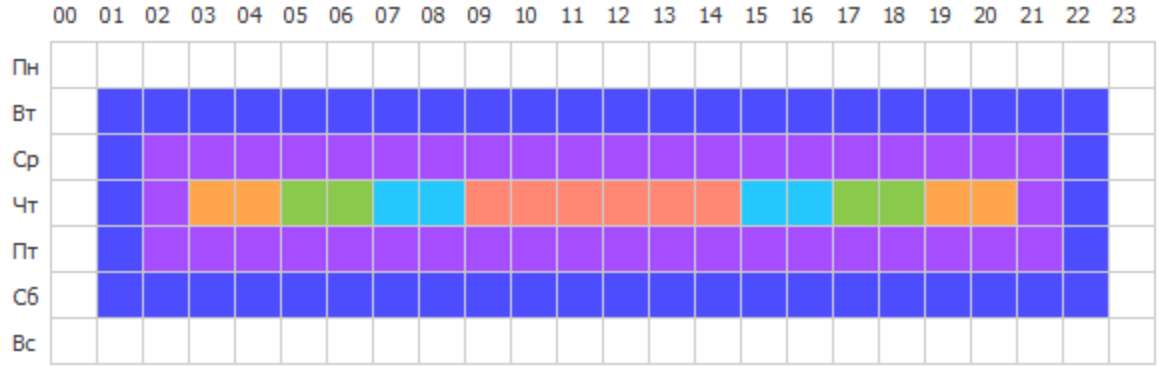
2. Установите флажок **Ограничить трафик при установке Агентов**, чтобы ограничить объем сетевого трафика при передаче данных с Сервера на станции в процессе установки Агентов Dr.Web.

Если флажок снят, передача данных при установке Агентов осуществляется без ограничения полосы пропускания сетевого трафика.

3. Если флажок установлен, задайте в поле **Максимальная скорость передачи (КБ/с)** значение максимальной скорости передачи данных. При этом данные для установки Агентов будут передаваться в пределах заданной полосы пропускания совокупного сетевого трафика всех Агентов.

Допускается задание до пяти ограничений на скорость передачи данных для установки Агентов. Для добавления еще одного поля ограничения скорости нажмите кнопку  . Для удаления ограничения нажмите кнопку  напротив ограничения, которое нужно удалить.

4. В таблице расписания задается р ежим ограничения на передачу данных отдельно на каждые 30 минут каждого дня недели.



Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков по принципу drag-and-drop.

Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей, начиная с варианта, при котором передача данных разрешена без ограничений трафика, до варианта, при котором передача данных запрещена.

5. После завершения редактирования нажмите кнопку **Сохранить** для принятия внесенных изменений.

В антивирусной сети Dr.Web Enterprise Security Suite существует возможность ограничить скорость передачи данных между Сервером и Агентами. Настройки делятся на ограничения передачи обновлений и ограничения при передаче данных при установках Агента.

Предоставляется возможность следующих вариантов ограничения трафика:

1. Ограничение общей скорости передачи данных всем станциям.

Настройка осуществляется в разделе конфигурации Сервера: пункт главного меню **Администрирование** → пункт управляющего меню **Конфигурация Сервера Dr.Web** → вкладка **Трафик** → внутренняя вкладка **Обновления** или **Установки** → параметр **Ограничить трафик обновлений** или **Ограничить трафик при установке Агентов** соответственно.

2. Персональное ограничение скорости передачи данных при обновлении конкретным станциям или группам станций.

Настройка осуществляется в разделе конфигурации станций: пункт главного меню **Антивирусная сеть** → выбрать станцию или группу в иерархическом списке сети → пункт управляющего меню **Ограничения обновлений** → параметр **Ограничить трафик обновлений**.

Ограничение трафика осуществляется по следующему принципу:

1. Если включено ограничение на общую скорость передачи данных в настройках Сервера, то суммарная скорость передачи данных от Сервера всем станциям не превысит указанного значения. При этом:

a) Вне зависимости от различий в пропускной способности каналов связи между Сервером и станциями, скорость передачи данных делится поровну между всеми станциями.

b) Если пропускная способность канала между Сервером и станцией меньше полученного среднего значения скорости для одной станции согласно пункту a), для такой станции устанавливается ограничение передачи данных равное максимальной ширине канала до этой станции. Оставшееся значение общего ограничения аналогично пункту a) делится поровну для остальных станций.

2. Если включено персональное ограничение на скорость передачи данных в настройках группы или конкретной станций, то скорость передачи данных на эти группы или станцию не превысит указанного значения. На все остальные станции ограничение не распространяется, и передача данных осуществляется с максимальной скоростью.

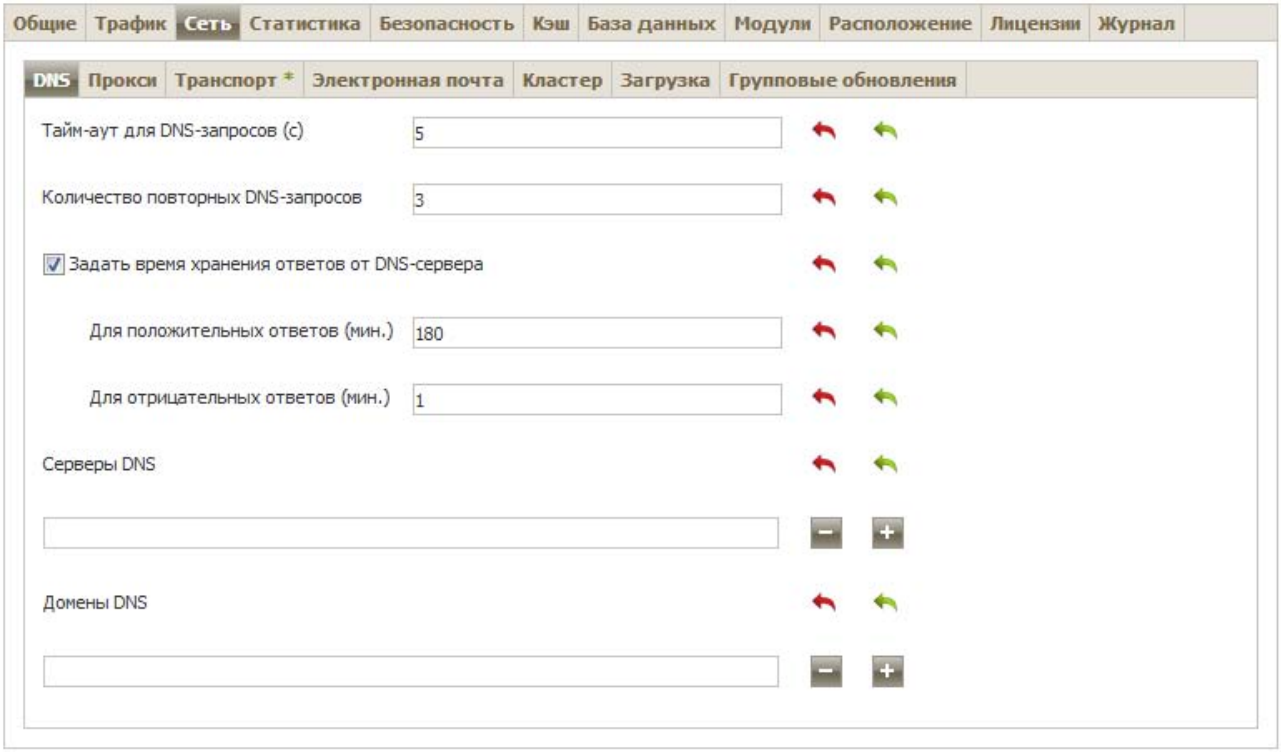
3. Если включено ограничение на общую скорость передачи данных в настройках Сервера и персональное ограничение на группу или станцию, то:

a) Скорость передачи данных на персонально ограниченные группы или станции не превысит значения, заданного в разделе настроек этих групп и станций.

b) Для передачи данных на остальные станции общее ограничение скорости передачи данных с учетом вычета ограничения станции из п. a) делится поровну.

c) Если пропускная способность канала между Сервером и станцией, не ограниченной индивидуально, меньше полученного среднего значения скорости для одной станции согласно пункту b), для такой станции устанавливается ограничение передачи данных, равное максимальной ширине канала до этой станции. Оставшееся значение общего ограничения аналогично пункту b) делится поровну для остальных станций, не ограниченных индивидуально.

На вкладке **Сеть** задаются параметры работы с сетью:

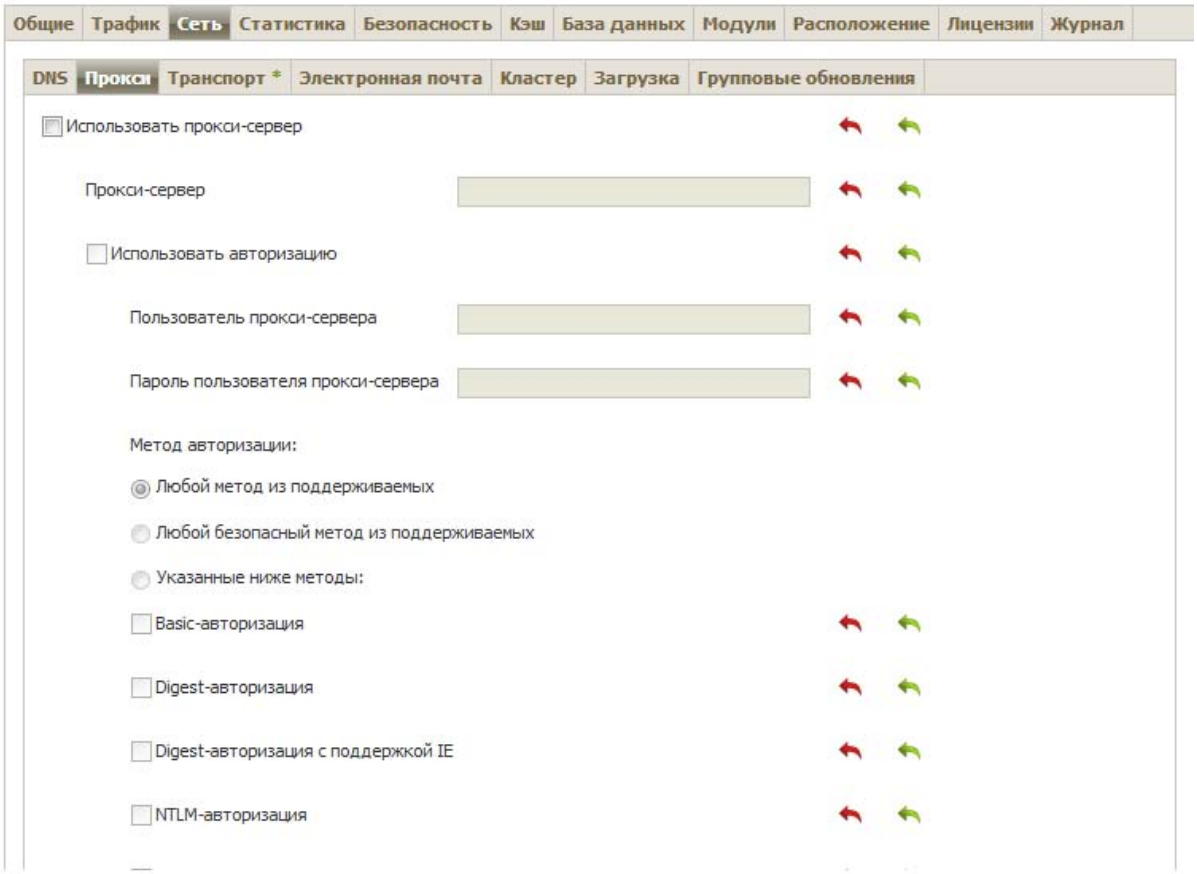


На вкладке **DNS** задаются параметры обращений к DNS-серверу:

- **Тайм-аут для DNS-запросов (с)** — тайм-аут в секундах для разрешения прямых/обратных DNS-запросов. Установите значение 0, чтобы не ограничивать время ожидания до окончания разрешения DNS-запроса.
- **Количество повторных DNS-запросов** — максимальное количество повторных DNS-запросов при неуспешном разрешении DNS-запроса.
- Установите флажок **Задать время хранения ответов от DNS-сервера**, чтобы задать время хранения в кэше ответов от DNS-сервера (TTL).
    - **Для положительных ответов (мин.)** — время хранения в кэше (TTL) положительных ответов от DNS-сервера в минутах.
    - **Для отрицательных ответов (мин.)** — время хранения в кэше (TTL) отрицательных ответов от DNS-сервера в минутах.

- **Серверы DNS** — список серверов DNS, заменяющий системный список по умолчанию.
- **Домены DNS** — список доменов DNS, заменяющий системный список по умолчанию.

На вкладке **Прокси** задаются параметры прокси-сервера.



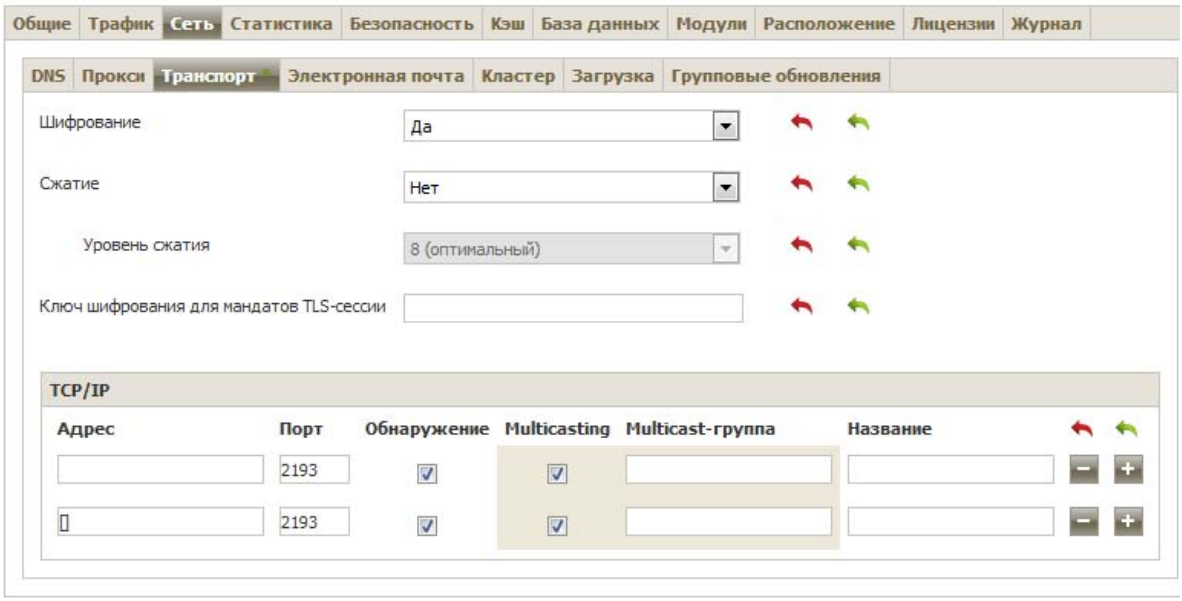
Установите флажок **Использовать прокси-сервер**, чтобы настроить соединения Сервера Dr.Web через прокси-сервер. При этом станут доступны следующие настройки:

- **Прокси-сервер** — IP-адрес или DNS-имя прокси-сервера. При необходимости в адресной строке допускается задание порта в формате <*адрес*>:<*порт*>. По умолчанию используется порт 3128.
- Чтобы использовать авторизацию для доступа к прокси-серверу согласно заданным методам, установите флажок **Использовать авторизацию** и задайте следующие параметры:
  - Заполните поля **Пользователь прокси-сервера** и **Пароль пользователя прокси-сервера**.
  - Выберите один из методов авторизации:

Опция	**Описание**
Любой метод из поддерживаемых	Использовать любой способ авторизации, поддерживаемый прокси-сервером. Если прокси-сервер поддерживает несколько методов авторизации, будет использоваться наиболее надежный.
Любой безопасный метод	Использовать любой безопасный способ авторизации,

Опция		Описание
из поддерживаемых		поддерживаемый прокси-сервером. В данном режиме метод авторизации Basic не используется. Если прокси-сервер поддерживает несколько методов авторизации, будет использоваться наиболее надежный.
Указанные ниже методы:	Basic-авторизация	Использовать Basic-авторизацию. Не рекомендуется использовать этот метод, поскольку передача учетных данных авторизации не шифруется.
	Digest-авторизация	Использовать Digest-авторизацию. Криптографический метод авторизации.
	NTLM-авторизация	Использовать NTLM-авторизацию. Криптографический метод авторизации. Для авторизации используется протокол NTLM компании Microsoft.
	GSS-Negotiate авторизация	Использовать GSS-Negotiate авторизацию. Криптографический метод авторизации.

На вкладке **Транспорт** настраиваются параметры транспортных протоколов, используемых Сервером для соединения с клиентами.



- В выпадающем списке **Шифрование** выбирается политика шифрования трафика, передаваемого по каналу связи между Сервером Dr.Web и подключаемыми к нему клиентами: Агентами, соседними Серверами, Сетевыми инсталляторами.

Подробнее об этих параметрах см. в п. Шифрование и сжатие трафика.

- В выпадающем списке **Сжатие** выбирается режим сжатия трафика, передаваемого по каналу связи между Сервером Dr.Web и подключаемыми к нему клиентами: Агентами, соседними Серверами, Сетевыми инсталляторами. Подробнее об этих параметрах см. в п. Шифрование и сжатие трафика.
  - При выборе значений **Да** и **Возможно** для сжатия трафика, станет доступен выпадающий список **Уровень сжатия**. В этом списке вы можете выбрать уровень сжатия данных от 1 до 9, где 1 — минимальный уровень, а 9 — максимальный уровень сжатия.

Более подробная информация приведена в разделе Шифрование и сжатие трафика.

- В поле **Ключ шифрования для мандатов TLS-сессии** задайте путь к файлу ключа шифрования для мандатов TLS-сессий. Используется для возобновления сеанса TLS на основе мандатов сессий (session tickets), которые шифруются с использованием заданного ключа.

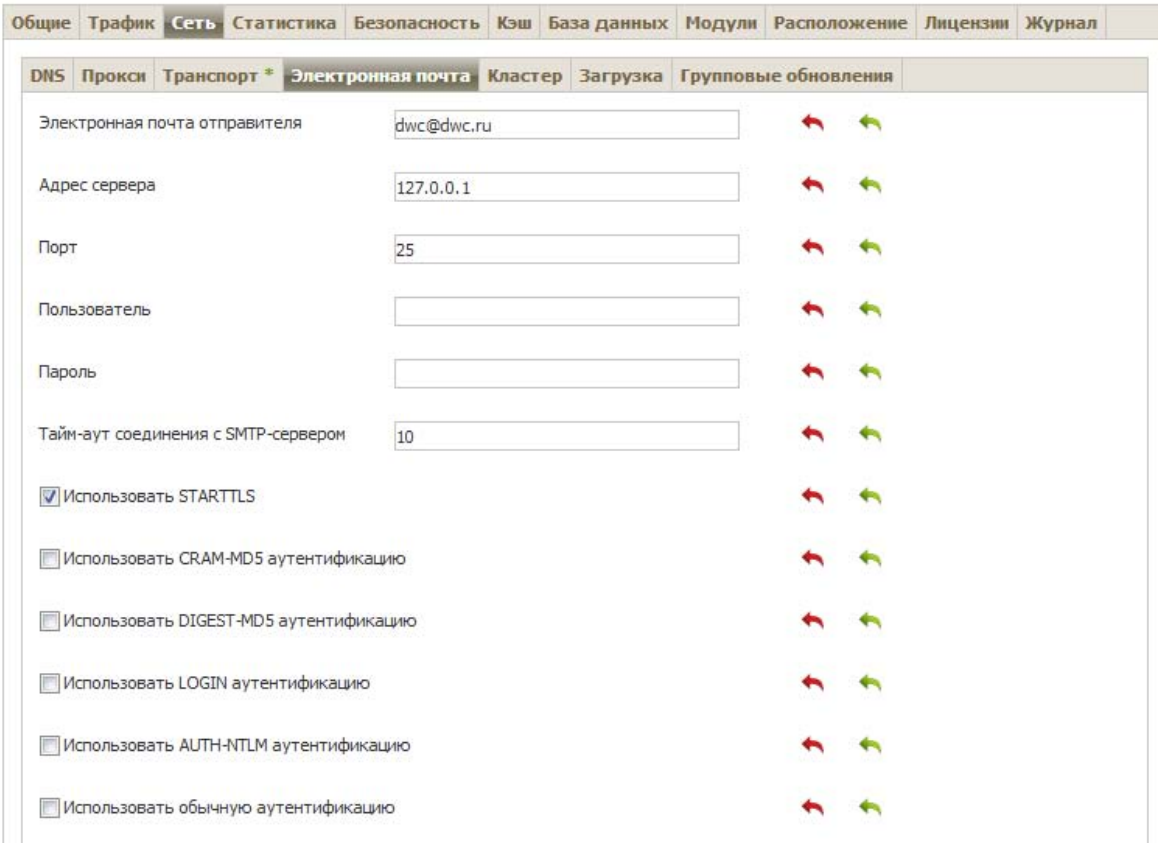
В подразделе **TCP/IP** настраиваются параметры соединений с Сервером по протоколам TCP/IP:

- **Адрес** и **Порт** — соответственно, IP-адрес и номер порта сетевого интерфейса, к которому привязывается данный транспортный протокол. Интерфейс с указанными настройками прослушивается Сервером для взаимодействия с Агентами, установленными на рабочих станциях.
- Установите флажок **Обнаружение**, чтобы включить службу обнаружения Сервера.
- Установите флажок **Multicasting**, чтобы использовать режим *Multicast over UDP* при обнаружении Сервера.
- **Multicast-группа** — IP-адрес multicast-группы, в которой зарегистрирован Сервер. Используется для взаимодействия с Агентами и Сетевыми инсталляторами при поиске активных Серверов Dr.Web сети. Если значение данного поля не задано, по умолчанию используется группа 231.0.0.1.
- **Название** — имя Сервера Dr.Web. Если оно не задано, используется имя, заданное на вкладке **Общие** (см. выше, в частности, если на указанной вкладке имя не задано, используется имя компьютера). Если для протокола задано иное имя, чем определенное на вкладке **Общие**, используется имя из описания протокола. Данное имя используется службой обнаружения для поиска Сервера Агентами и т. д.
- Только под ОС семейства UNIX: в поле **Путь** задается путь до сокета связи, например, с Агентом.

Более подробная информация приведена в разделе Настройка сетевых соединений.

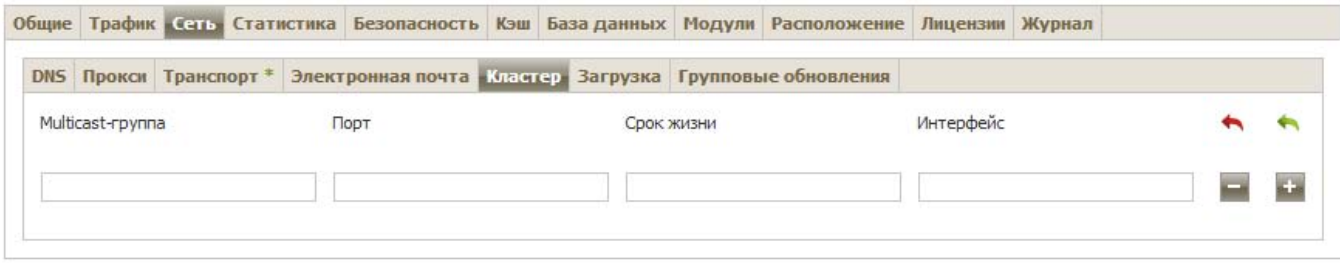
Данные параметры задаются в формате сетевого адреса, приведенного в документе **Приложения**, в разделе Приложение Е. Спецификация сетевого адреса.

На вкладке **Электронная почта** настраиваются параметры отправки электронной почты из Центра управления, например, в качестве оповещений администратора или при рассылке инсталляционных пакетов станций:



- **Электронная почта отправителя** — адрес ящика электронной почты, от имени которого будут отправляться электронные письма.
- **Адрес сервера** — адрес SMTP-сервера, который будет использоваться для отправки электронной почты.
- **Порт** — порт для подключения к SMTP-серверу. По умолчанию порт 465 при открытии отдельного защищенного TLS-соединения или порт 25 в противном случае.
- **Пользователь**, **Пароль** — при необходимости задайте имя пользователя и пароль пользователя SMTP-сервера, если SMTP-сервер требует авторизации.
- **Тайм-аут соединения с SMTP-сервером** — тайм-аут в секундах для установления соединения с SMTP-сервером. Значение — целое положительное число, большее или равное 1.
- Установите флажок **Использовать STARTTLS** для шифрованного обмена данными. При этом переключение на защищенное соединение осуществляется через команду STARTTLS. По умолчанию для соединения предусматривается использование 25-го порта.
- Установите флажок **Использовать CRAM-MD5 аутентификацию** для использования *CRAM-MD5* аутентификации на почтовом сервере.
- Установите флажок **Использовать DIGEST-MD5 аутентификацию** для использования *DIGEST-MD5* аутентификации на почтовом сервере.
- Установите флажок **Использовать LOGIN аутентификацию** для использования *LOGIN* аутентификации на почтовом сервере.
- Установите флажок **Использовать AUTH-NTLM аутентификацию** для использования *AUTH-NTLM* аутентификации на почтовом сервере.
- Установите флажок **Использовать обычную аутентификацию** для использования *plain text* аутентификации на почтовом сервере.
- Установите флажок **Использовать TLS** для шифрованного обмена данными. При этом будет открыто отдельное защищенное TLS-соединение. По умолчанию для соединения предусматривается использование 465-го порта.

- Установите флажок **Проверять правильность сертификата Сервера** чтобы проверять правильность TLS-сертификата почтового сервера. В поле **Сертификат Сервера** укажите путь к корневому TLS-сертификату Сервера Dr.Web.
- Установите флажок **Отладочный режим** для получения детального журнала SMTP-сессии.
- В поле **Электронная почта получателей** можете задать адреса ящиков электронной почты, чтобы проверить отправку электронной почты. Нажмите кнопку **Отправить тестовое сообщение**, чтобы отправить тестовое письмо (аналогичное оповещению Сервера) по электронной почте в соответствии с заданными настройками в данном разделе.
- На вкладке **Кластер** настраиваются параметры кластера Серверов Dr.Web для обмена информацией при многосерверной конфигурации антивирусной сети.

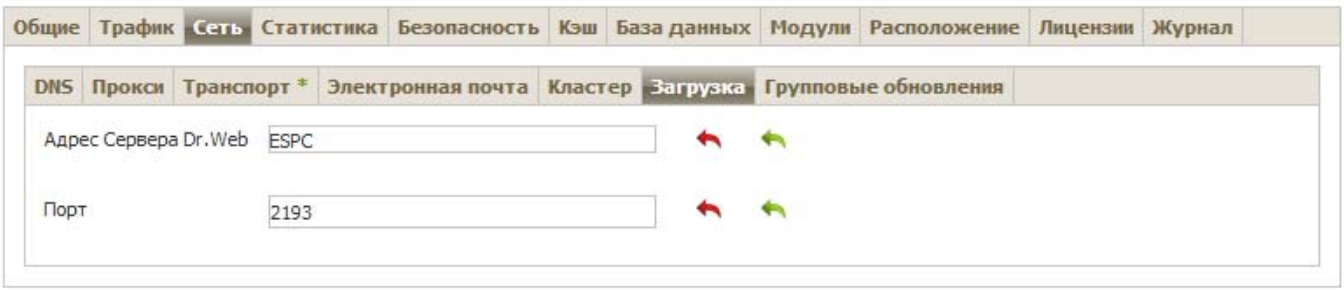


Для использования кластера задайте следующие параметры:

- **Multicast-группа** — IP-адрес multicast-группы, через которую Серверы будут осуществлять обмен информацией.
- **Порт** — номер порта сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу.
- **Срок жизни** — срок жизни датаграммы при передаче данных в кластере Серверов Dr.Web.
- **Интерфейс** — IP-адрес сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу.

Особенности создания кластера Серверов Dr.Web приведены в разделе Кластер Серверов Dr.Web.

На вкладке **Загрузка** настраиваются параметры Сервера, используемые при формировании файлов инсталляции Агента для станций антивирусной сети. В дальнейшем эти параметры используются при подключении инсталлятора Агента к Серверу:



- **Адрес Сервера Dr.Web** — IP-адрес или DNS-имя Сервера Dr.Web.

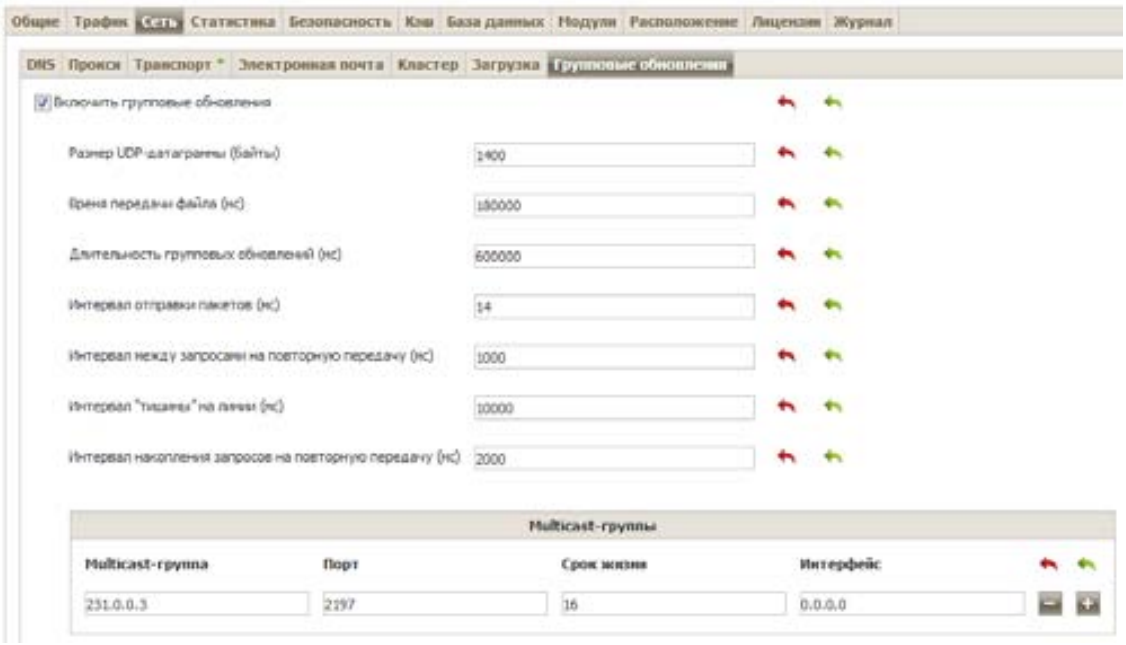
Если адрес Сервера не задан, то используется имя компьютера, возвращаемое операционной системой.

- **Порт** — номер порта, который будет использоваться при подключении инсталлятора Агента к Серверу.

Если номер порта не задан, то используется порт 2193 (настраивается в Центре управления в разделе **Администрирование → Конфигурация Сервера Dr.Web →** вкладка **Сеть →** вкладка **Транспорт**).

Настройки раздела **Загрузка** сохраняются в конфигурационном файле download.conf (см. документ **Приложения**, п. G3. Конфигурационный файл download.conf).

На вкладке **Групповые обновления** настраивается передача групповых обновлений на рабочие станции по multicast-протоколу.



Чтобы включить передачу обновлении на станции по multicast-протоколу, установите флажок **Включить групповые обновления**.

Основные принципы работы групповых обновлений:

1. Если групповые обновления включены, то для всех станций, подключенных к данному Серверу, обновление будет осуществляться в два этапа:

   a) Станции прослушивают заданные multicast-группы, в которые входит Сервер. При поступлении групповых обновлений станции скачивают их через *multicast over UDP*.

   b) После передачи групповых обновлений Сервер отправляет стандартное оповещение станциям о наличии обновлений. Все, что не удалось скачать через групповые обновления, станции докачивают как при стандартном обновлении по протоколу TCP.

2. Если групповые обновления отключены, обновление для всех станций осуществляется только штатным способом — по протоколу TCP.

Для настройки групповых обновлений используются следующие параметры:

- **Размер UDP-датаграммы (байты)** — размер в байтах UDP-датаграмм, используемых multicast-протоколом.

Допустимый диапазон 512–8192. Во избежание фрагментации рекомендуется задавать значение меньше MTU (Maximum Transmission Unit) используемой сети.

- **Время передачи файла (мс.)** — в течение заданного интервала осуществляется передача одного файла обновления, после чего Сервер начинает отправку следующего файла.

Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP.

- **Длительность групповых обновлений (мс.)** — длительность процесса обновления по multicast-протоколу.

Все файлы, которые не удалось передать на этапе обновления по multicast-протоколу, будут передаваться в процессе стандартного обновления по протоколу TCP.

- **Интервал отправки пакетов (мс.)** — интервал отправки пакетов в multicast-группу.

Малое значение интервала может привести к значительным потерям при передаче пакетов и перегрузить сеть. Не рекомендуется изменять этот параметр.

- **Интервал между запросами на повторную передачу (мс.)** — с данным интервалом Агенты отправляют запросы на повторную передачу потерянных пакетов.

Сервер Dr.Web накапливает эти запросы, после чего пересылает потерянные блоки.

- **Интервал «тишины» на линии (мс.)** — в случае завершения передачи файла до истечения отведенного времени, если в течение заданного интервала «тишины» от Агентов не поступило запросов на повторную передачу потерянных пакетов, Сервер Dr.Web считает, что все Агенты успешно получили файлы обновления, и начинает отправку следующего файла.
- **Интервал накопления запросов на повторную передачу (мс.)** — в течение указанного интервала Сервер накапливает запросы от Агентов на повторную передачу потерянных пакетов.

Агенты перезапрашивают потерянные пакеты. Сервер накапливает эти запросы в течение указанного времени, после чего пересылает потерянные блоки.

Чтобы задать список multicast-групп, через которые будет доступно групповое обновление, настройте следующие параметры в подразделе **Multicast-группы**:

- **Multicast-группа** — IP-адрес multicast-группы, через которую станции будут получать групповые обновления.
- **Порт** — номер порта сетевого интерфейса Сервера Dr.Web, к которому привязывается транспортный multicast-протокол для передачи обновлений.

Для групповых обновлений необходимо задавать любой свободный порт — в частности, отличный от порта, который назначен в настройках для работы транспортного протокола самого Сервера.

- **Срок жизни** — срок жизни датаграммы при передаче данных в процессе групповых обновлений.
- **Интерфейс** — IP-адрес сетевого интерфейса Сервера Dr.Web, к которому привязывается транспортный multicast-протокол для передачи обновлений.

В каждой строке задаются настройки одной multicast-группы. Для добавления еще одной multicast-группы нажмите  .

При задании нескольких multicast-групп обратите внимание на следующие особенности:

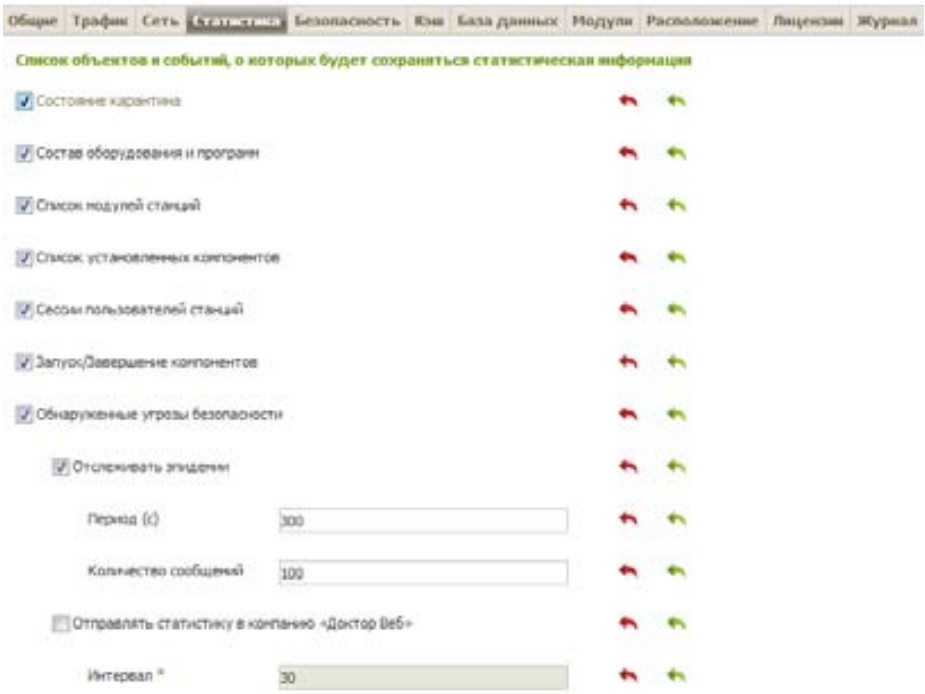
- Для разных Серверов Dr.Web, которые будут рассылать групповые обновления, должны задаваться различные multicast-группы.
- Для разных Серверов Dr.Web, которые будут рассылать групповые обновления, необходимо задавать различные параметры **Интерфейс** и **Порт**.
- При использовании нескольких multicast-групп наборы станций, входящие в данные группы, не должны пересекаться. Таким образом, каждая станция антивирусной сети может входить только в одну multicast-группу.

В разделе **Список контроля доступа** задаются ограничения на сетевые адреса станций, которые будут получать групповые обновления:

- Станции, которым разрешено получать групповые обновления, будут прослушивать заданные multicast-группы и получать обновления по стандартной схеме (см. процедура 1).
- Станции, которым запрещено получать групповые обновления, не прослушивают заданные multicast-группы на наличие обновлений, а скачивают все обновления по TCP (см. процедура 2).

Настройка списков осуществляется аналогично настройке списков раздела Безопасность.

На вкладке **Статистика** задается статистическая информация, которая записывается в журнал протокола и заносится в базу данных Сервера.



Для регистрации и добавления в БД информации соответствующего типа установите следующие флажки:

- **Состояние карантина** — разрешает мониторинг состояния Карантина на станциях и запись информации в базу данных.
- **Состав оборудования и программ** — разрешает мониторинг состава аппаратно-программного обеспечения станций и запись информации в базу данных.
- **Список модулей станций** — разрешает мониторинг списка модулей Антивируса, установленных на станциях, и запись информации в базу данных.
- **Список установленных компонентов** — разрешает мониторинг списка установленных компонентов Антивируса (Сканер, мониторы и т. п.), установленных на рабочей станции, и запись информации в базу данных.
- **Сессии пользователей станций** — разрешает мониторинг сессий пользователей рабочих станций и запись в базу данных регистрационных имен пользователей, вошедших в систему на компьютере с установленным Агентом.
- **Запуск/завершение компонентов** — разрешает мониторинг информации о запуске и завершении работы компонентов Антивируса (Сканер, мониторы и т. п.) на рабочих станциях и запись информации в базу данных.
- **Обнаруженные угрозы безопасности** — разрешает мониторинг обнаружения угроз безопасности рабочих станций и запись информации в базу данных.

Если флажок **Обнаруженные угрозы безопасности** установлен, вы также можете настроить дополнительные параметры статистики по угрозам.

  - Установите флажок **Отслеживать эпидемии**, чтобы включить режим оповещения администратора о случаях вирусных эпидемий. Если флажок снят, оповещения о вирусных заражениях будут осуществляться в обычном режиме. При установленном флажке вы также можете задать следующие параметры отслеживания вирусных эпидемий:
  - **Период (с)** — промежуток времени в секундах, за который должно прийти заданное количество сообщений о заражениях, чтобы Сервер Dr.Web отправлял администратору единое уведомление об эпидемии на все случаи заражения.
  - **Количество сообщений** — количество сообщений о заражениях, которые должны прийти за заданный промежуток времени, чтобы Сервер Dr.Web отправлял администратору единое уведомление об эпидемии на все случаи заражения.
  - Для активации отправки статистики по обнаруженным угрозам безопасности станций в компанию «Доктор Веб» установите флажок **Отправлять статистику в компанию «Доктор Веб»**. Станут доступны следующие поля:
- **Интервал** — интервал отправки статистики в минутах;
- **Идентификатор** — MD5-ключ (находится в конфигурационном файле Сервера).
- **Ошибки сканирования** — разрешает мониторинг обнаружения ошибок при сканировании на рабочих станциях и запись информации в базу данных.
- **Статистика сканирования** — разрешает мониторинг результатов сканирования на рабочих станциях и запись информации в базу данных.
- **Инсталляции Агентов** — разрешает мониторинг информации об инсталляциях Агентов на рабочих станциях и запись ее в базу данных.
- **Журнал выполнения заданий на станциях** — разрешает мониторинг результатов выполнения задания на станциях и запись их в базу данных.
- **Состояние станций** — разрешает мониторинг изменений состояния станций и запись информации в базу данных.

    - **Состояние вирусных баз** — разрешает мониторинг состояния (состава, изменения) вирусных баз на станции и запись информации в базу данных. Флажок доступен, только если установлен флажок **Состояние станций**.
- **Данные о местоположении** — разрешает получать информацию о местоположении станций и записывать информацию в базу данных.

Обязательным полем является только **Интервал** отправки статистики.

Для просмотра статистической информации:

1. Выберите пункт главного меню **Антивирусная сеть**.

2. В иерархическом списке выберите станцию или группу.

3. Откройте соответствующий раздел управляющего меню (см. таблицу ниже).

Подробное описание статистических данных приведено в разделе Просмотр статистики по рабочей станции.

В таблице ниже приведено соответствие флажков из раздела **Статистика** в настройках Сервера и пунктов управляющего меню на странице **Антивирусная сеть**.

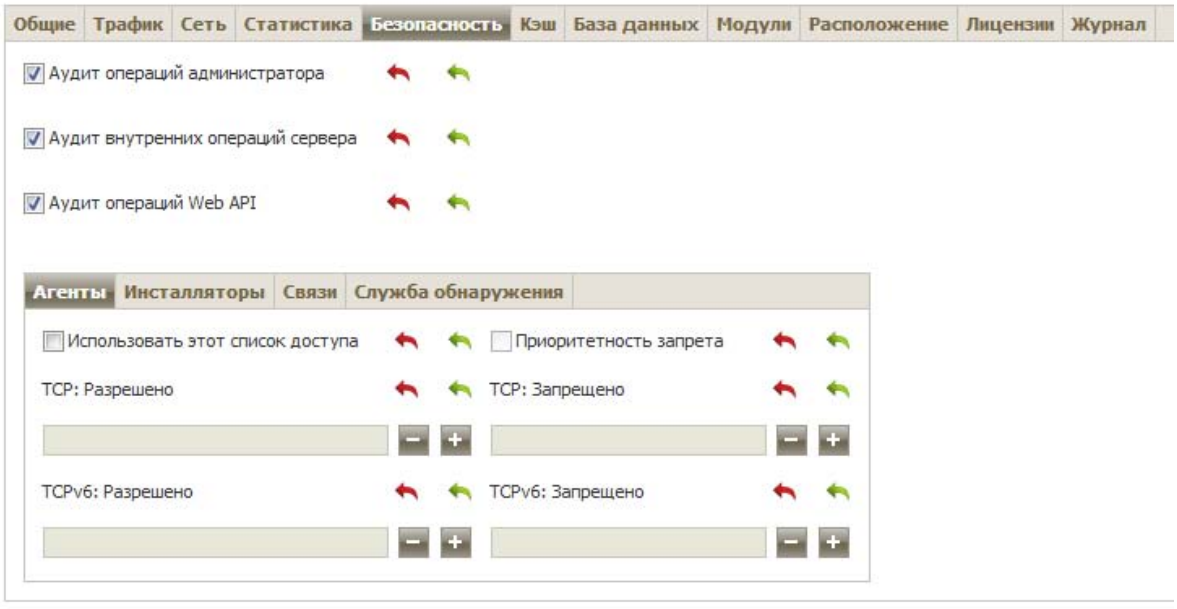
При снятии флажков на вкладке **Статистика**, соответствующие им пункты будут скрыты из управляющего меню.

Соответствие настроек Сервера и пунктов управляющего меню

Настройки Сервера	**Пункты меню**
Состояние карантина	Общие → Карантин Конфигурация → Windows → Агент Dr.Web → флажок Разрешить удаленное управление карантином
Состав оборудования и программ	Общие → Оборудование и программы Общие → Сравнение оборудования и программ
Список модулей станции	Статистика → Модули
Список установленных компонентов	Общие → Установленные компоненты
Сессии пользователей станции	Общие → Сессии пользователей
Запуск/Завершение компонентов	Статистика → Запуск/завершение
Обнаруженные угрозы безопасности	Статистика → Угрозы Статистика → Статистика угроз

Настройки Сервера	**Пункты меню**
Ошибки сканирования	Статистика → Ошибки
Статистика сканирования	Статистика → Статистика сканирования Таблицы → Суммарная статистика
Инсталляции Агентов	Статистика → Инсталляции Агентов
Журнал выполнения заданий на станции	Статистика → Задания Статистика → Вирусные базы
Состояние станций	Статистика → Состояние Статистика → Вирусные базы
Состояние вирусных баз	Статистика → Вирусные базы

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых Агенты, сетевые инсталляторы и другие (соседние) Серверы Dr.Web смогут получать доступ к данному Серверу.



Управление журналом аудита Сервера осуществляется при помощи следующих флажков:

- **Аудит операций а дминистратора** разрешает ведение журнала аудита операций администратора с Центром управления, а также запись журнала в БД.
- **Аудит внутренних операций сервера** разрешает ведение журнала аудита внутренних операций Сервера Dr.Web и запись журнала в БД.

- **Аудит операций Web API** разрешает ведение журнала аудита операций через XML API и запись журнала в БД.

Журнал аудита можно посмотреть, выбрав в главном меню **Администрирование** пункт **Журнал аудита**.

На вкладке **Безопасность** размещаются дополнительные вкладки, на которых настраиваются ограничения для соответствующих типов соединений:

- **Агенты** — список ограничений на IP-адреса, с которых Агенты Dr.Web могут подключаться к данному Серверу.
- **Инсталляторы** — список ограничений на IP-адреса, с которых инсталляторы Агентов Dr.Web могут подключаться к данному Серверу.
- **Соседи** — список ограничений на IP-адреса, с которых соседние Серверы Dr.Web могут подключаться к данному Серверу.
- **Служба обнаружения** — список ограничений на IP-адреса, с которых принимаются широковещательные запросы службой обнаружения Сервера.

Чтобы настроить ограничения доступа (задаются отдельно для Агентов, Инсталляции, Соседних Серверов или Службы обнаружения):

1. Установите флажок **Использовать этот список доступа**, чтобы задать списки разрешенных или запрещенных адресов. Если флажок снят, все соединения будут разрешены.

2. Чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.

3. Чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.

4. Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флажок **Приоритетность запрета**. Если флажок установлен, список **Запрещено** имеет более высокий приоритет, чем список **Разрешено**. Адреса, не включенные ни в один из списков или включенные в оба, запрещаются. Разрешаются только адреса, которые включены в список **Разрешено** и не включены в список **Запрещено**.

Чтобы отредактировать список адресов:

1. Введите сетевой адрес в соответствующее поле в виде: <*IP-адрес*>/[<*префикс сети*>].

2. Для добавления нового поля адреса нажмите кнопку  соответствующего раздела.

3. Для удаления поля нажмите кнопку  напротив удаляемого адреса.

4. Для применения настроек нажмите кнопку **Сохранить**.

Списки для ввода адресов TCPv6 будут отображены, только если на компьютере установлен интерфейс IPv6.

Пример использования префикса:

1. Префикс 24 обозначает сети с маской: 255.255.255.0

Содержит 254 адреса.

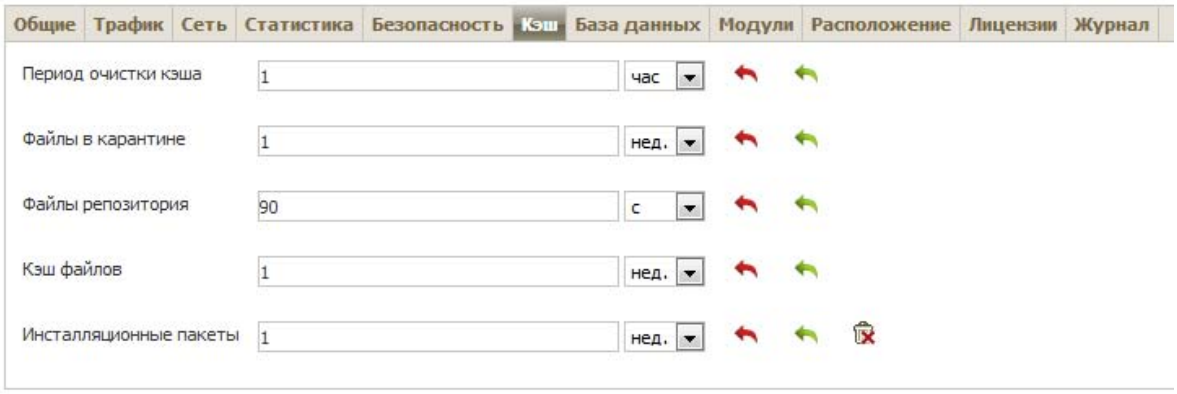
Адреса хостов в этих сетях вида: 195.136.12.*

2. Префикс 8 обозначает сети с маской 255.0.0.0

Содержит до 16387064 адресов (256*256*256).

Адреса хостов в этих сетях вида: 125.*.*.*

На вкладке **Кэш** задаются параметры очистки серверного кэша:

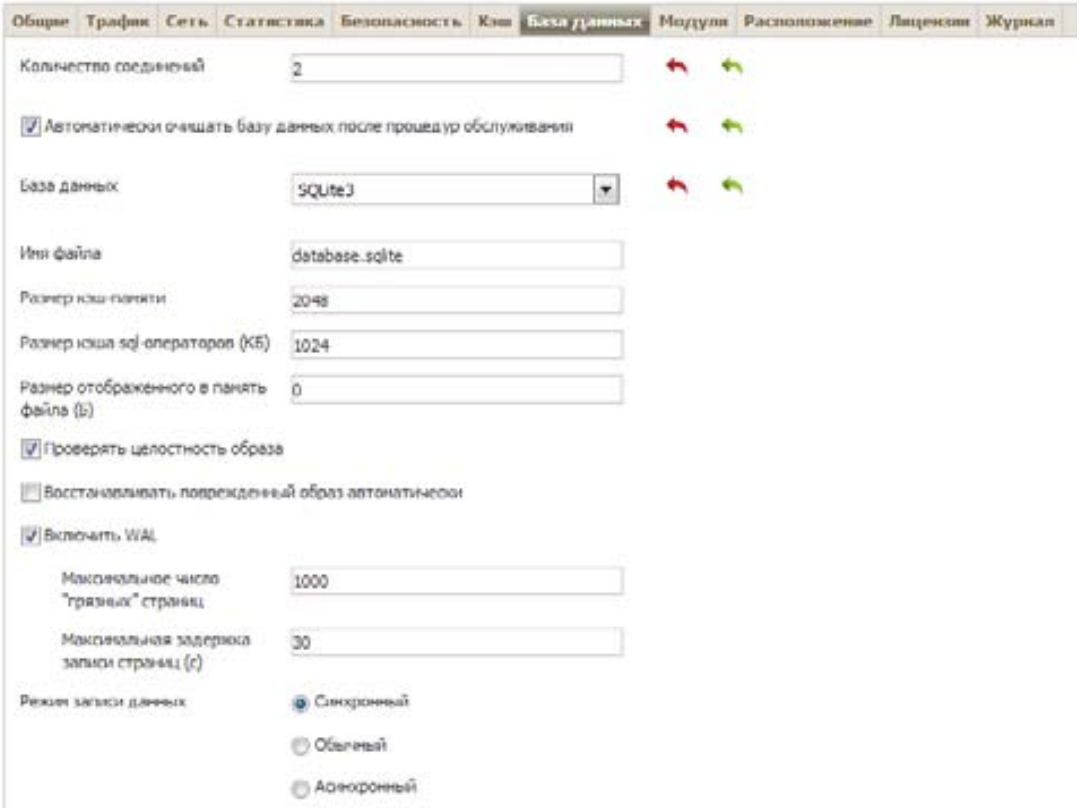


- **Период очистки кэша** — периодичность полной очистки кэша.
- **Файлы в карантине** — периодичность удаления файлов в Карантине на стороне Сервера.
- **Файлы репозитория** — периодичность удаления файлов в репозитории.
- **Кэш файлов** — периодичность очистки файлового кэша.
- **Инсталляционные пакеты** — периодичность удаления персональных и групповых инсталляционных пакетов.

Нажмите кнопку **Удалить все инсталляционные пакеты сейчас**, чтобы удалить все ранее созданные персональные и групповые инсталляционные пакеты, находящиеся в каталоге installers-cache каталога var. Обратите внимание: при обращении к данным пакетам для скачивания они будут созданы заново, что может занять некоторое время.

При задании числовых значений обратите внимание на выдающие списки с единицами измерения периодичности.

На вкладке **База данных** задается выбор СУБД, необходимой для функционирования Сервера Dr.Web.



Структуру БД Сервера Dr.Web можно получить на основе sql-скрипта init.sql, расположенного в подкаталоге etc каталога установки Сервера Dr.Web.

Чтобы задать параметры работы с базой данных:

1. В поле **Количество соединений** задайте максимально допустимое количество соединений Сервера с базой данных. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.

2. Установите флажок **Автоматически очищать базу данных после процедур обслуживания**, чтобы автоматически проводить отложенную очистку базы данных после ее инициализации, обновления и импорта. Если флажок снят, автоматическая очистка не будет выполняться. В этом случае рекомендуется настроить задание **Очистка базы данных** в расписании Сервера или выполнять очистку вручную через раздел Управление базой данных.

Для выполнения автоматической очистки создается скрытое задание в расписании Сервера. Задание выполняется ближайшей ночью после обозначенных процедур обслуживания, в 01:17 по местному времени Сервера. Задание выполняется только в том случае, если в расписании Сервера не запланировано другого задания **Очистка базы данных** в течение ближайших суток относительно обозначенных процедур обслуживания.

3. В выпадающем списке **База данных** выберите тип базы данных:

- **MySQL** — внешняя БД,
- **ODBC** — для использования внешней БД через ODBC-соединение,

При возникновении предупреждений или ошибок в работе Сервера Dr.Web с СУБД Microsoft SQL Server через ODBC следует убедиться, что вы используете последнюю доступную версию СУБД для данной редакции.

С тем, как определить наличие исправлений, вы можете ознакомиться на следующей странице компании Microsoft: https://support.microsoft.com/en-us/kb/321185.

- **Oracle** — внешняя БД для платформ, кроме FreeBSD,

При использовании внешней СУБД Oracle через ODBC-подключение необходимо установить последнюю версию ODBC-драйвера, поставляемую с данной СУБ Д. Использование ODBC-драйвера Oracle, поставляемого Microsoft, категорически не рекомендовано.

- **PostgreSQL** — внешняя БД,
- **SQLite3** — встроенная БД (компонент Сервера Dr.Web).

4. Задайте необходимые настройки для работы с БД:

- Для встроенных БД при необходимости введите в поле **Имя файла** полный путь к файлу с базой данных и задайте размер кэш-памяти и режим записи данных.
- Параметры для внешних БД описаны в документе **Приложения**, в разделе Приложение В. Настройки, необходимые для использования СУБД. Параметры драйверов СУБД.

5. Для применения заданных настроек нажмите кнопку **Сохранить**.

Дистрибутив Сервера Dr.Web содержит встроенные клиенты для поддерживаемых СУБД, поэтому:

- Если вы планируете использовать поставляемые вместе с Сервером Dr.Web встроенные клиенты СУБД, то при установке (обновлении) Сервера в настройках инсталлятора убедитесь, что разрешена установка соответствующего встроенного клиента для СУБД в разделе **Поддержка баз данных**.
- Если вы планируете использовать в качестве внешней базы данных БД Oracle через ODBC-подключение, то при установке (обновлении) Сервера в настройках инсталлятора отмените установку встроенного клиента для СУБД Oracle (в разделе **Поддержка баз данных → Драйвер базы данных Oracle**). В противном случае работа с БД через ODBC будет невозможна из-за конфликта библиотек.

Инсталлятор Сервера поддерживает режим изменения продукта. Для добавления или удаления отдельных компонентов, например, драйверов для управления базами данных, достаточно запустить инсталлятор Сервера и выбрать вариант **Изменить**.

По умолчанию предусмотрено использование встроенной СУБД. Выбор этого режима создает значительную вычислительную нагрузку на Сервер. При значительном размере антивирусной сети рекомендуется использовать внешнюю СУБД. Процедура смены типа СУБД описана в документе **Приложения**, в разделе Смена типа СУБД Dr.Web Enterprise Security Suite.

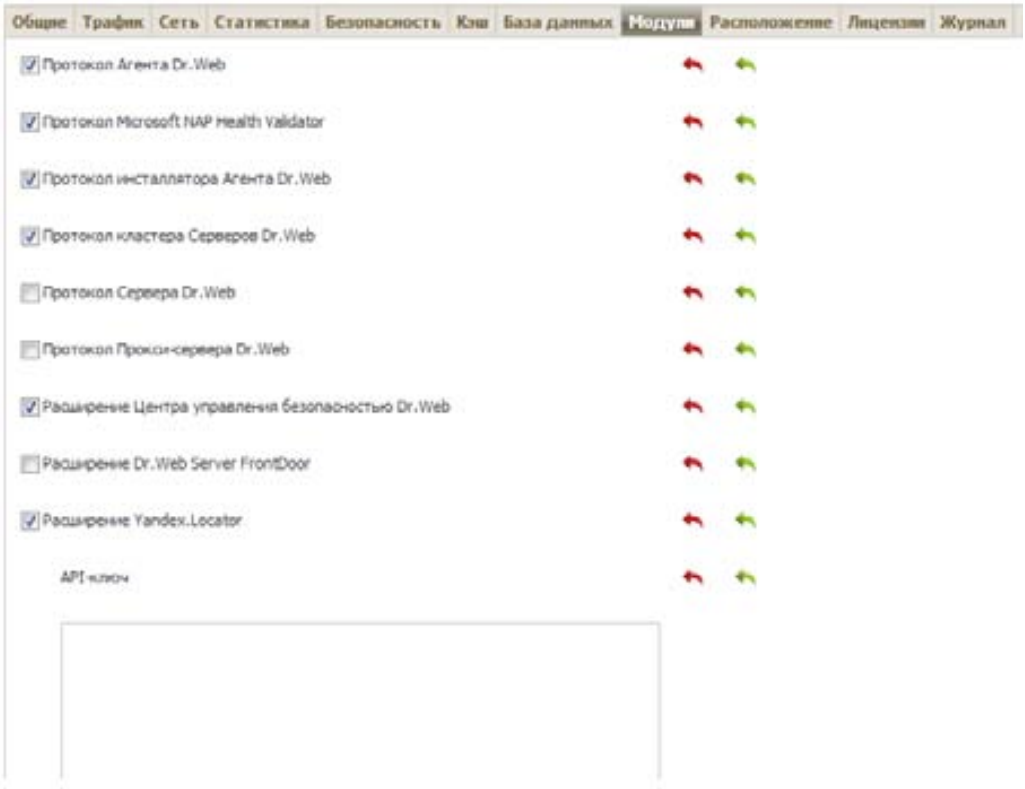
> Использование встроенной БД допустимо при подключении к Серверу не более 200–300 станций. Если позволяет аппаратная конфигурация компьютера, на котором установлен Сервер Dr.Web, и нагрузка по прочим задачам, выполняемым на данном компьютере, возможно подключение до 1000 станций.
>
> В противном случае необходимо использовать внешнюю БД.

При использовании внешней БД и подключении к Серверу более 10000 станций рекомендуется выполнение следующих минимальных требований:

- процессор с частотой 3ГГц,
- оперативная память — от 4 ГБ для Сервера Dr.Web, от 8 ГБ — для сервера БД,
- ОС семейства UNIX.

Предусмотрена возможность осуществления операций, связанных с очисткой базы данных, используемой Сервером Dr.Web, а именно: удаление записей о событиях, а также информации о станциях, не посещавших Сервер в течение определенного периода. Для очистки базы данных перейдите в раздел расписания Сервера и создайте соответствующее задание.

На вкладке **Модули** задается режим взаимодействия Сервера Dr.Web с другими компонентами Dr.Web Enterprise Security Suite:



- Установите флажок **Протокол Агента Dr.Web** для включения протокола взаимодействия Сервера с Агентами Dr.Web.
- Установите флажок **Протокол Microsoft NAP Health Validator** для включения протокола взаимодействия Сервера с компонентом проверки работоспособности системы Microsoft NAP Validator.
- Установите флажок **Протокол инсталлятора Агента Dr.Web** для включения протокола взаимодействия Сервера с инсталляторами Агентов Dr.Web.
- Установите флажок **Протокол кластера Серверов Dr.Web** для включения протокола взаимодействия между Серверами в кластерной системе.
- Установите флажок **Протокол Сервера Dr.Web** для включения протокола взаимодействия Сервера Dr.Web с другими Серверами Dr.Web. Протокол по умолчанию отключен. При задании многосерверной конфигурации сети

(см. п. Особенности сети с несколькими Серверами Dr.Web) включите этот протокол, установив флажок **Протокол Сервера Dr.Web**.

- Установите флажок **Протокол Прокси-сервера Dr.Web** для включения протокола взаимодействия Сервера Dr.Web с Прокси-Серверами Dr.Web.
- Установите флажок **Расширение Центра управления безопасностью Dr.Web** для возможности управления Сервером и антивирусной сетью через Центр управления.

При снятии флажка **Расширение Центра управления безопасностью Dr.Web**, после перезагрузки Сервера Dr.Web будет недоступен Центр управления безопасностью Dr.Web. При этом управление Сервером и антивирусной сетью будет возможно только через утилиту дистанционной диагностики, при условии что флажок **Расширение Dr.Web Server FrontDoor** установлен.

- Установите флажок **Расширение Dr.Web Server FrontDoor** для возможности использования расширения Dr.Web Server FrontDoor, позволяющего подключение утилиты дистанционной диагностики Сервера (см. также п. Удаленный доступ к Серверу Dr.Web).
- Установите флажок **Расширение Yandex.Locator**, чтобы разрешить использование расширения Yandex.Locator для определения местоположения мобильных устройств, подключенных к Серверу.
    - В поле **API-ключ** введите свой API-ключ, полученный в Яндексе.

Если вы включите расширение Yandex.Locator, но не зададите API-ключ, расширение не будет активно.

Подробную информацию по использованию и настройке расширения Yandex.Locator вы можете найти в документе **Приложения**, в разделе Автоматическое определение местоположения станции под ОС Android.

На вкладке **Расположение** вы можете задать дополнительную информацию о физическом расположении компьютера, на котором установлено ПО Сервера Dr.Web.

Также на данной вкладке вы можете просмотреть расположение Сервера на географической карте.

Для просмотра расположения Сервера на карте:

1. Задайте в полях **Широта** и **Долгота** географические координаты Сервера в формате десятичных градусов (Decimal Degrees).

2. Нажмите кнопку **Сохранить** для сохранения введенных данных в конфигурационном файле Сервера.

Для отображения карты перезагрузка Сервера не требуется. Однако для применения измененных географических координат перезагрузка Сервера потребуется.

3. На вкладке **Расположение** отобразится превью карты OpenStreetMap с меткой, соответствующей заданным координатам.

В случае если загрузка превью невозможна, отображается текст **Показать на карте**.

4. Для просмотра полноразмерной карты нажмите на превью или на текст **Показать на карте**.

На вкладке **Лицензии** задаются настройки распространения лицензий между Серверами Dr.Web.

Настройки для Сервера, выдающего лицензии

- **Период автоматического продления выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на данном Сервере. После окончания этого периода осуществляется автоматическое продление выданных лицензий на тот же самый период. Автоматическое продление будет осуществляться до тех пор, пока длится срок распространения лицензий, заданный в Менеджере лицензий на шаге 5. Данный механизм обеспечивает возвращение лицензий на главный Сервер в том случае, если подчиненный Сервер будет отключен и не сможет вернуть выданные лицензии.
- **Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами. Синхронизация лицензий позволит

определить, что количество лицензий, выданных главным Сервером и полученных подчиненным Сервером, совпадает. Данный механизм позволяет выявить сбои и случаи подлога при передаче лицензий.

- **Период отправки отчета об использовании лицензий** — периодичность, с которой подчиненный Сервер будет отправлять отчеты об использовании полученных лицензий на главный Сервер. Настройка задается на главном Сервере, но используется подчиненным Сервером при отправке отчетов.
- **Период подсчета активных станций для отчета по лицензиям** — период, в течение которого будет подсчитываться количество активных станций для отправки отчета об использовании лицензий. Настройка задается на главном Сервере, но используется подчиненным Сервером при отправке отчетов.

Настройки для Сервера, получающего лицензии

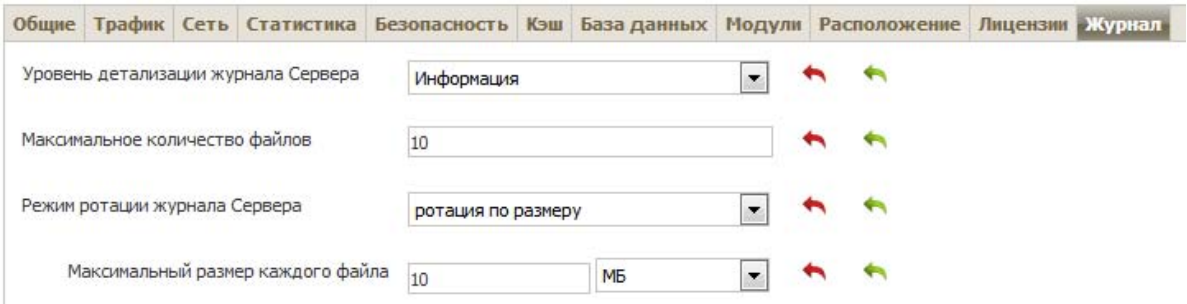
- **Интервал для предварительного продления получаемых лицензий** — промежуток времени до окончания периода автоматического продления лицензий, полученных от соседнего Сервера, начиная с которого данный Сервер запрашивает предварительное автоматическое продление этих лицензий.

Использование данной настройки зависит от типа подключения, выбранного в настройке **Параметры соединения** при конфигурации связи между Серверами (см. раздел Настройка связей между Серверами Dr.Web):

  - Для периодического типа подключения: если период переподключения, заданный в настройке связи, больше, чем **Период автоматического продления выдаваемых лицензий**, заданный на Сервере, выдавшем лицензии, то автоматическое продление этих лицензий будет инициировано раньше, чем истечет **Период автоматического продления выдаваемых лицензий**.
  - Для постоянного подключения: данная настройка не используется.

Подробную информацию о распространении лицензий между Серверами см. в разделе Распространение лицензий по межсерверным связям.

На вкладке **Журнал** задаются настройки ведения журнала работы Сервера Dr.Web:



- В выпадающем списке **Уровень детализации журнала Сервера** выберите уровень подробности для ведения журнала работы Сервера Dr.Web.
- **Максимальное количество файлов** — максимальное количество файлов журнала (включая текущий и архивные), которые будут храниться.
- **Режим ротации журнала Сервера** — режим ротации журнала работы Сервера. Выберите одно из представленных значений:

- **ротация по размеру** определяет ограничение на размер каждого из файлов журнала.

Максимальный размер каждого файла — максимально допустимый размер каждого файла журнала. Когда текущий файл достигает заданного размера, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.

- **ротация по времени** определяет длительность записи каждого из файлов журнала.

Максимальное время записи файла — максимальная длительность для записи каждого файла журнала. Когда время записи файла достигает заданной длительности, он списывается в архив с соответствующим изменением имени, и создается новый файл журнала.

Внимание! Для применения внесенных изменений необходима перезагрузка Сервера.

Перезагрузка может быть в ыполнена как через Центр управления, так и при помощи соответствующей консольной команды.

Подробная информация о журнале Сервера приведена в разделе Журнал Сервера Dr.Web.

8.2. Настройка сетевого экрана

Для возможности взаимодействия компонентов антивирусной сети необходимо, чтобы все используемые ими порты и интерфейсы были открыты на всех компьютерах, входящих в антивирусную сеть.

При установке Сервера инсталлятор позволяет автоматически добавить исключения в настройки сетевого экрана операционной системы Windows (кроме ОС Windows 2000). Для этого достаточно установить флажок **Добавить в исключения брандмауэра порты и интерфейсы сервера**.

При использовании сетевого экрана, помимо встроенного сетевого экрана ОС Windows, администратор антивирусной сети должен произвести соответствующие настройки вручную.

8.3. Настройка сетевых соединений

К **Серверу Dr.Web** могут подключаться следующие клиенты:

- **Агенты**,
- Сетевые инсталляторы **Агентов**,
- другие **Серверы Dr.Web**.

Соединение всегда устанавливается по инициативе клиента.

Возможны следующие схемы подключения клиентов к Серверу.

1. Посредством прямых соединений (direct connections). Данный подход имеет много преимуществ, но не всегда однозначно предпочтителен (также есть ситуации, когда такой подход не следует использовать).
2. При использовании **Службы обнаружения Сервера**. По умолчанию (если явно не задано иное) клиенты используют именно эту Службу. При данной схеме подключения клиенту заранее не известен адрес Сервера. Перед каждым установлением соединения

осуществляется поиск Сервера в сети. Для этого клиент посылает в сеть широковещательный запрос и ожидает ответ от Сервера с указанием его адреса. После получения отзыва клиент устанавливает соединение с Сервером. Для этого Сервер должен «прослушивать» сеть на подобные запросы.

При конфигурации антивирусной сети **Dr.Web ESS** на использование прямых соединений **Служба обнаружения Сервера** может быть отключена. Для этого в описании транспортов (**Администрирование → Конфигурация → Конфигурация Сервера Dr.Web → Сеть → Транспорт**) нужно снять флажки **Обнаружение** и **Multicasting**.

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

По умолчанию используется режим *Multicast over UDP*.

1. Сервер регистрируется в мультикаст-группе с адресом 231.0.0.1.
2. Агенты при поиске Сервера посылают в сеть мультикаст-запросы на групповой адрес 231.0.0.1.

По умолчанию для «прослушивания» Сервером устанавливаются (аналогично прямым соединениям) udp/231.0.0.1:2193. Параметр задается в настройках Сервера **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web → Сеть → Транспорт** в поле **Multicast-группа**.

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

   Возможность обращения к **Серверу** через SRV-записи реализуется следующим образом:

   1. При установке **Сервера** настраивается регистрация в домене Active Directory, инсталлятор вносит соответствующую SRV-запись на DNS-сервер. SRV-запись вносится на DNS-сервер в соответствии с RFC2782 (см. http://tools.ietf.org/html/rfc2782 и https://ru.wikipedia.org/wiki/SRV-запись).
   2. При запросе подключения к **Серверу** пользователь задает обращение через протокол srv. Например, через запуск инсталлятора **Агента** с явным указанием **Сервера**: drwinst srv/drwcs
   3. Клиент прозрачно для пользователя использует функционал протокола SRV для обращения к **Серверу**.

   Если при обращении **Сервер** явно не указан, по умолчанию в качестве имени сервиса используется drwcs.

8.3.1.1. Установка прямых соединений (Direct connection)

Данный вариант подключения следует использовать, если необходима перенастройка всей системы, в частности, если требуется перенести **Сервер Dr.Web** на другой компьютер или поменять IP-адрес машины, на которой установлен Сервер.

В настройках Сервера Dr.Web должно быть указано, какой адрес необходимо «прослушивать» для приема входящих TCP-соединений. Данный параметр задается в

настройках С ервера **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web → Сеть → Транспорт** в поле **Адрес**.

При конфигурации антивирусной сети на использование прямых соединений Служба обнаружения Сервера может быть отключена. Для этого поле **Адрес** следует оставить пустым.

По умолчанию для «прослушивания» Сервером устанавливаются tcp/0.0.0.0:2193 — при использовании порта 2193, зарегистрированного за **Dr.Web ESS** в IANA. Обозначение 0.0.0.0 означает «все сетевые интерфейсы» для данной машины, на которой установлен Сервер.

Для корректной работы антивирусной системы достаточно, чтобы Сервер «слушал» хотя бы один TCP-порт, который должен быть известен всем клиентам.

Для того чтобы Агент Dr.Web использовал прямые соединения, при его установке нужно явно указать адрес Сервера Dr.Web, к которому необходимо подключиться (IP-адрес или сетевое имя машины, на которой запущен **Сервер**) в параметрах установки: drwinst <*Адрес_Сервера*> (по умолчанию команда drwinst, запущенная без параметров, будет сканировать сеть на наличие **Серверов** Dr.Web и попытается установить Агент с первого найденного Сервера в сети (режим Multicasting с использованием Службы обнаружения Сервера). Таким образом, адрес **Сервера** становится известен Агенту при установке.

В дальнейшем адрес Сервера может быть изменен вручную в настройках Агента. Просмотр и редактирование настроек соединения осуществляется при помощи пункта контекстного меню значка Агента **Настройки → Основные → Сервер → Изменить настройки**.

При установке Агента рекомендуется использовать имя Сервера, предварительно зарегистрированное в службе DNS. Это упростит процесс настройки антивирусной сети, связанный с процедурой переноса **Сервера** Dr.Web на другой компьютер.

Альтернативным способом является редактирование конфигурационного файла.

8.3.2. Использование шифрования и сжатия трафика

Антивирусная сеть **Dr.Web ESS** позволяет зашифровать трафик между всеми компонентами сети. Шифрование применяется, чтобы избежать возможной утечки лицензионных ключей, а также сведений об оборудовании и пользователях антивирусной сети.

Политика использования шифрования настраивается отдельно на каждом из компонентов антивирусной сети, но эти настройки должны быть согласованы с настройками шифрования на Сервере Dr.Web.

Антивирусная сеть **Dr.Web Enterprise Security Suite** использует криптографически устойчивые алгоритмы шифрования и цифровой электронной подписи, основанные на концепции пар открытых и закрытых ключей.

Чтобы задать политики сжатия и шифрования для Сервера **Dr.Web**, необходимо сделать следующее:

1. В Центре управления выберите пункт **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**.
2. На вкладке **Сеть → Транспорт** выберите в выпадающих списках **Шифрование** и **Сжатие** один из вариантов:

- **Да** — шифрование (или сжатие) трафика со всеми компонентами обязательно (устанавливается по умолчанию для шифрования, если при установке **Сервера** не было задано другое).
- **Возможно** — шифрование (или сжатие) будет выполняться для трафика с теми из компонентов, настройки которых этого не запрещают. По умолчанию **Агент** устанавливается с настройками шифрования **Возможно**. Данное сочетание означает, что по умолчанию шифрование будет производиться, но может быть отменено редактированием настроек **Сервера Dr.Web**.
- **Нет** — шифрование (или сжатие) не поддерживается (устанавливается по умолчанию для сжатия, если при установке **Сервера** не было задано другое).

При согласовании настроек политики шифрования на **Сервере** и другом компоненте (**Агенте** или **Сетевом инсталляторе**) следует иметь в виду, что ряд сочетаний настроек является недопустимым и их выбор приведет к обрыву соединения между **Сервером** и компонентом.

В таблице ниже собраны сведения о том, при каких установках соединение между Сервером и компонентом будет шифрованным (+), при каких — нешифрованным (–) или соединение не будет установлено (Ошибка).

Настройки сервера / настройки компонента	Да	Возможно	Нет
Да	+	+	Ошибка
Возможно	+	+	—
Нет	Ошибка	—	—

Использование шифрования трафика создает заметную вычислительную нагрузку на мощности компьютера, поэтому если аппаратная конфигурация станции близка к минимально необходимой, от шифрования имеет смысл отказаться, если установленные на предприятии требования к информационной безопасности допускают это. Шифрование также не рекомендуется использовать в крупных сетях (от 2000 станций). При этом следует последовательно переключать Сервер и компоненты сначала в режим **Возможно**, не допуская создания несовместимых пар Сетевой инсталлятор — Сервер и Агент — Сервер. Несоблюдение этой последовательности может привести к потере управляемости компонента и необходимости его переустановки.

Ввиду того, что трафик между компонентами антивируса (особенно соседними Серверами) может быть весьма значительным, зачастую имеет смысл использовать сжатие трафика сетевого трафика антивируса. Настройка политики сжатия и совместимость таких настроек на разных компонентах полностью аналогичны описанным выше для шифрования, с тем отличием, что для Сервера настройкой сжатия по умолчанию является **Нет**.

Использование сжатия уменьшает трафик, но, даже в большей мере чем шифрование, увеличивает вычислительную нагрузку на компьютеры, что стоит принимать во внимание.

8.3.3. Ведение серверного протокола

Сервер Dr.Web ведет протокол событий, связанных с его работой. Имя файла протокола — *drwcsd.log*. Протокол Сервера используется для отладки, а также устранения неполадок в случае нештатной работы компонентов антивирусной сети.

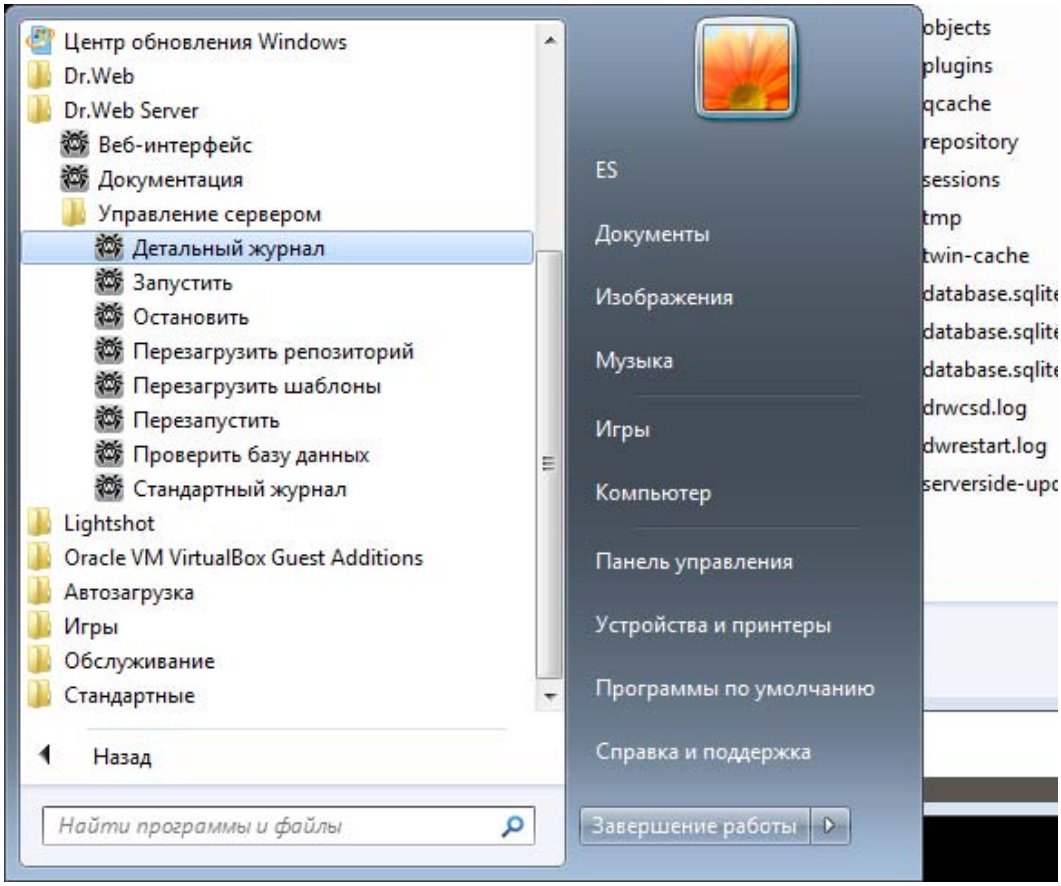
По умолчанию размещение файла протокола:

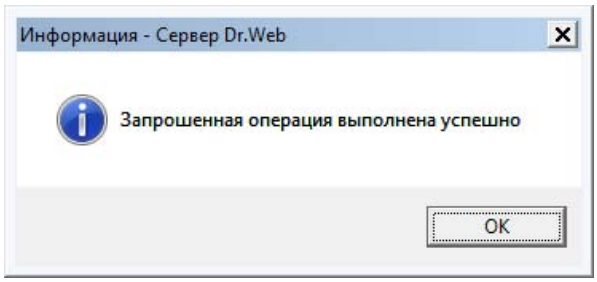
- Под ОС UNIX:
  - для Linux: `/var/opt/drwcs/log/drwcsd.log`;

- для FreeBSD: `/var/drwcs/log/drwcsd.log`.
- Под ОС Windows: в подкаталоге var каталога установки Сервера.

Файл имеет простой текстовый формат.

Для изменения уровня детализации серверного протокола нажмите кнопку **Пуск**, и в группе **Dr.Web Server → Управление сервером** выберите **Детальный журнал**.





Настройка параметров логирования ротации файлов журнала Сервера Dr.Web по времени (час, день, неделя) задается при установке сервера (для ОС Windows) или через параметры командной строки при запуске Сервера на любой системе.

Для просмотра журнала работы Сервера через Центр управления:

1. Выберите пункт **Администрирование → Журналы → Журнал Сервера Dr.Web**.
2. Откроется окно со списком журналов работы **Сервера**. Согласно настройкам режима ротации используется следующий формат именования файлов журнала работы **Сервера**:

   `<file_name>.<N>.log` или `<file_name>.<N>.log.gz`, где <N> — порядковый номер: 1, 2, и т. д.

3. Например, при названии файла drwcsd, список файлов журнала работы будет следующий:
   a. drwcsd.log — текущий файл (в который идет запись),
   b. drwcsd.1.log.gz — предыдущий,
   c. drwcsd.2.log.gz и так далее — чем больше число, тем более старая версия.

4. Для управления файлами журнала установите флажок напротив нужного файла или нескольких файлов. Для выбора всех файлов журнала установите флажок в заголовке таблицы. На панели инструментов станут доступны следующие кнопки:
   a. **Экспортировать выбранные файлы журнала** — сохранить локальную копию выбранных файлов журнала. Сохранение копии журнала может использоваться, например, для просмотра содержимого файла журнала с удаленного компьютера.
   b. **Удалить выбранные файлы журнала** — для удаления выбранных файлов журнала без возможности восстановления.

8.3.4. Управление репозиторием Dr.Web Enterprise Server

Репозиторий **Сервера Dr.Web** предназначен для хранения эталонных образцов антивирусного ПО и обновления их с серверов ВСО Dr.Web.

Для этой цели репозиторий оперирует наборами файлов, которые относятся к соответствующим компонентам антивируса (так называемым продуктам). Каждый продукт размещается в отдельном подкаталоге каталога репозитория (repository), расположенного в каталоге var, который при установке по умолчанию является подкаталогом корневого каталога Сервера. Функции репозитория и управление ими осуществляются для каждого продукта независимо.

Для управления обновлением репозиторий использует понятие *ревизии* продукта. Ревизия представляет собой корректное на определенный момент времени состояние файлов продукта (включает имена файлов и контрольные суммы) и характеризуется уникальным номером.

Репозиторий производит синхронизацию ревизий продукта в следующих направлениях:

a) на Сервер Dr.Web с сайта обновления продукта (по протоколу HTTP),

b) между различными Серверами Dr.Web в многосерверной конфигурации (в соответствии с заданной политикой обмена),

c) с Сервера Dr.Web на рабочие станции.

Репозиторий предоставляет Администратору антивирусной сети возможность настраивать следующие параметры:

- перечень сайтов обновления при операциях типа **a)**;
- ограничение состава продуктов, нуждающихся в синхронизации типа **a)** (таким образом, пользователю предоставляется возможность отслеживать только нужные ему изменения отдельных категорий продуктов);
- ограничение частей продукта, нуждающихся в синхронизации типа **c)** (пользователь может выбрать, что именно подлежит установке на рабочие станции);
- контроль перехода на новые ревизии (возможно самостоятельное тестирование продуктов перед внедрением);
- добавление в продукты собственных компонентов;
- самостоятельное с оздание новых продуктов, для которых также будет выполняться синхронизация.

В настоящее время в поставку входят следующие продукты:

- Сервер Dr.Web,
- Агенты Dr.Web (ПО Агента, антивирусное ПО рабочей станции для соответствующих операционных систем),
- Прокси-сервер Dr.Web,
- Вирусные базы Dr.Web,
- Базы SpIDer Gate,
- Модуль обновления Dr.Web,
- Данные безопасности сервера Dr.Web,
- Базы Антиспама Dr.Web,
- Новости компании «Доктор Веб».

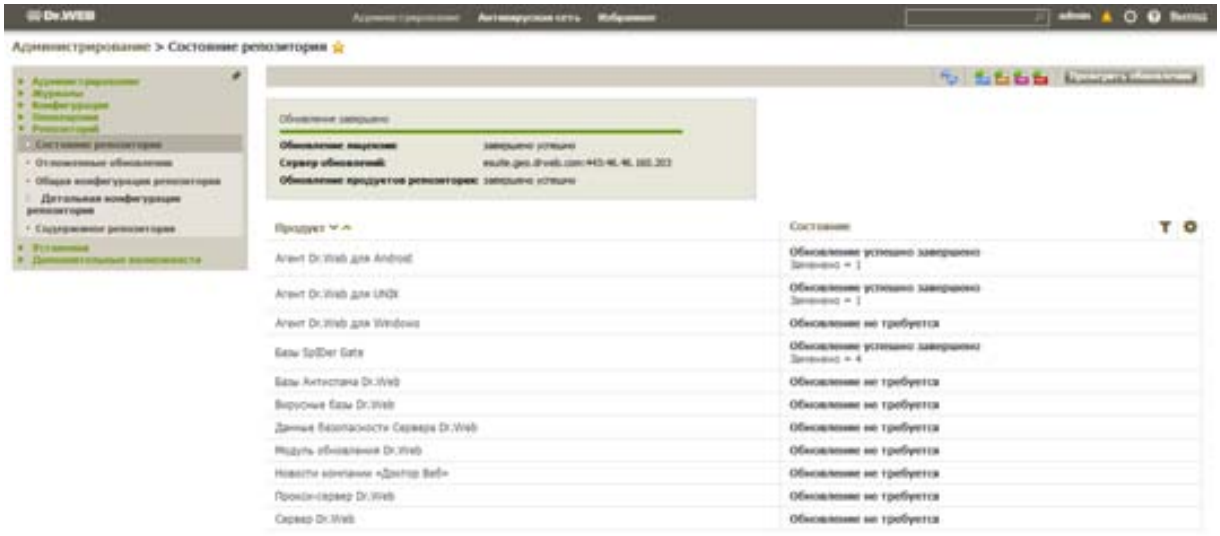
1. Выберите пункт **Администрирование** в главном меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**.

2. В открывшемся окне приведен список продуктов репозитория, дата используемой в данный момент ревизии, дата последней загруженной ревизии и состояние продуктов.

В столбце **Состояние** указано состояние продуктов в репозитории Сервера на момент последнего обновления.

3. Для управления содержимым репозитория используйте следующие кнопки:

- Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО. Если проверяемый компонент устарел, то его обновление произойдет автоматически в процессе проверки. При этом прогресс обновления с указанием адресов ВСО выводится на экран в режиме реального времени.

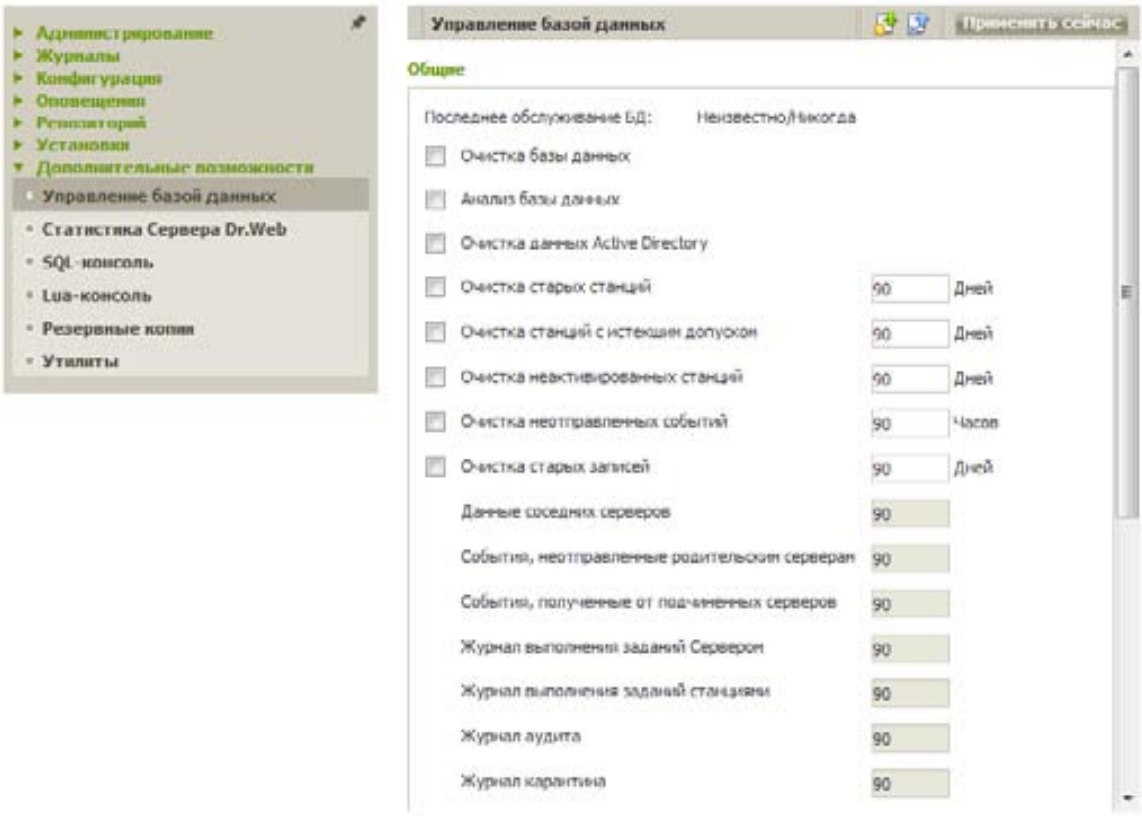


- Нажмите кнопку **Перезагрузить репозиторий с диска**, чтобы произвести перезагрузку текущей версии репозитория с диска. Этот пункт используется, если сервер долго не перезагружался и в памяти находится устаревшая версия репозитория или в находящейся в ОС копии репозитория произошел сбой. В этом случае после перезагрузки репозитория с диска в память будет помещена его обновленная или рабочая версия.

При запуске Сервер загружает содержимое репозитория в память, и если в процессе работы Сервера содержимое репозитория было изменено администратором в обход Центра управления, например, при обновлении содержимого репозитория при помощи внешней утилиты или вручную, для использования загруженной на диск версии репозитория также необходимо осуществить его перезагрузку.

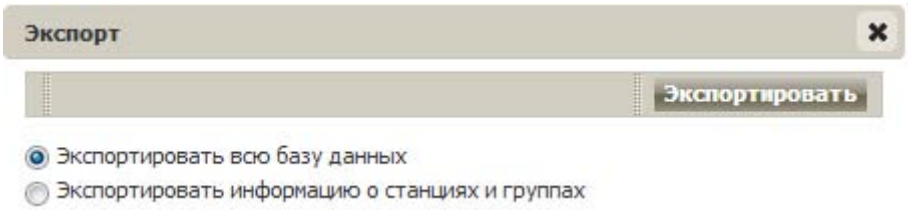
8.3.4.1. Управление базой данных Сервера Dr.Web через Центр управления

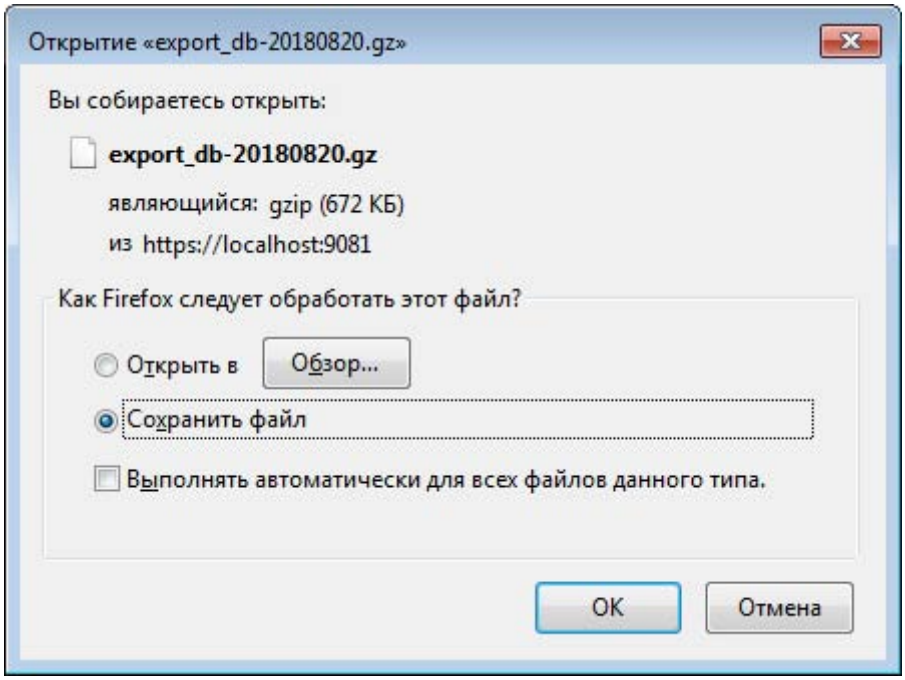
Администратор антивирусной сети имеет возможность выполнения ряда действий по управлению базой данных через Центр управления, например анализ и очистку БД от устаревших записей. Для этого выберите пункт **Администрирование → Дополнительные возможности → Управление базой данных**.



Любое из перечисленных в окне действий можно выполнить, отметив его флажком и нажав **Применить сейчас** — отмеченное действие или несколько действий будут выполнены немедленно. Кроме общей очистки БД или удаления определенных неактуальных данных, можно провести обслуживание и оптимизацию структуры и содержимого базы данных, выбрав пункт **Анализ базы данных**.

Также администратор имеет возможность импорта ( ) и экспорта ( ) информации из базы данных.





Если есть необходимость выполнить какой-либо произвольный запрос к БД, который не имеет соотнесенной команды в интерфейсе Центра управления, воспользуйтесь SQL-консолью, позволяющей работать с БД вручную из Центра управления. Доступ к консоли регулируется правами администратора.

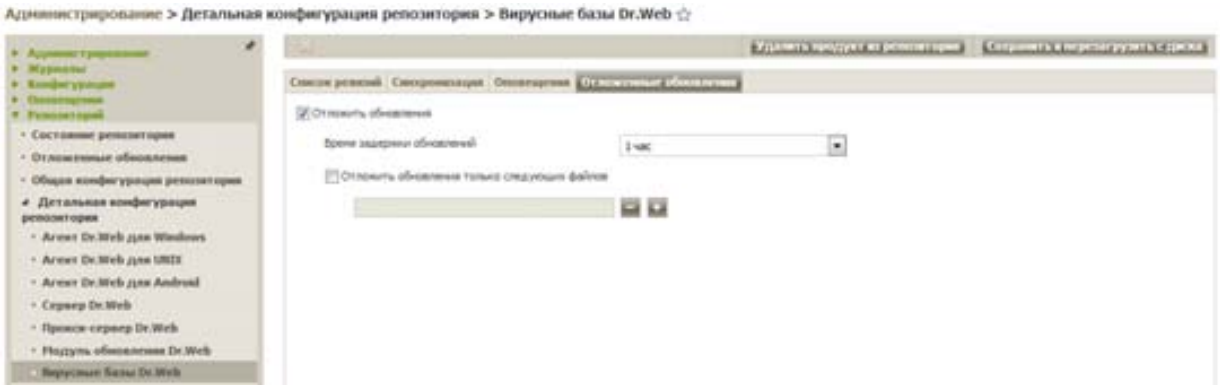
Для выполнения произвольного скрипта выберите **Администрирование → Дополнительные возможности → SQL-консоль,** в текстовом поле введите текст скрипта (служебные слова будут автоматически выделяться цветом) и нажмите Выполнить для запуска скрипта или Очистить для удаления введенных символов. Если скрипт необходимо сохранить для дальнейшего использования, например, на другом сервере, это можно сделать, сохранив его в один из форматов: CSV HTML XML PDF.

8.3.4.2. Отложенные обновления

Функционал отложенных обновлений может использоваться, если необходимо временно заблокировать распространение последней ревизии продукта на все станции антивирусной сети. Н апример, при необходимости предварительного тестирования данной ревизии на ограниченном количестве станций.

Чтобы настроить отложенные обновления:

1. В разделе **Администрирование → Репозиторий → Детальная конфигурация репозитория** выберите продукт (например, Вирусные базы Dr.Web) и перейдите на вкладку **Отложенные обновления**.



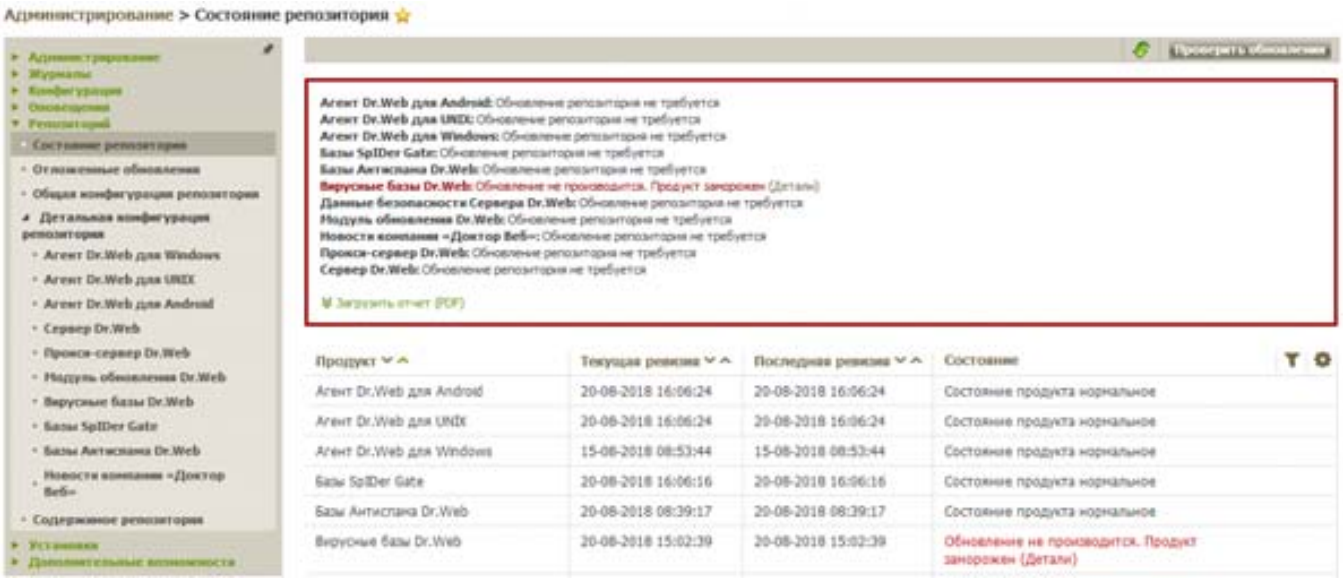
2. Установите флажок **Отложить обновления**, чтобы временно о тменить распространение уже загруженных обновлений данного продукта, полученных с серверов ВСО (за исключением станций, для которых установлен флажок **Получать все последние обновления**).
3. В выпадающем списке **Время задержки обновлений** выберите время, на которое откладывается загрузка обновлений на станции антивирусной сети (за исключением станций, для которых установлен флажок **Получать все последние обновления**). Начало времени заморозки считается с момента получения ревизии с **ВСО**.

   Если над замороженным продуктом не было задано действие по его разморозке, то по истечении времени, заданного в списке **Время задержки обновлений**, ревизия будет автоматически размморожена и включена в список ревизий с распространением на станции по общей процедуре.

4. При необходимости ус тановите флажок **Отложить обновления только следующих файлов**, чтобы отложить распространение обновлений, содержащих файлы, которые соответствуют маскам, заданным в списке ниже. Список масок задается в формате регулярных выражений. Если флажок не установлен, будут заморожены все обновления, приходящие с ВСО.
5. Чтобы изменения вступили в силу, нажмите 

.

   После очередного получения обновлений на странице **Состояние репозитория** будет выведено сообщение о наличии в репозитории замороженного обновления.



Выбрав в разделе **Детальная конфигурация репозитория** продукт, для которого ранее настраивался порядок обновлений, и перейдя на вкладку **Список ревизий**, можно получить информацию обо всех ревизиях выбранного продукта, доступных на данном **Сервере —** включая замороженные.

В столбце **Распространяемая** могут стоять два типа маркеров:

- Распространяемая ревизия. Ревизия используется для обновлений **Агентов** и антивирусного ПО на станциях.
- Замороженная ревизия. Данная ревизия не распространяется на станции, новые ревизии не скачиваются с **Сервера**.

Ревизия для распространения выбирается следующим образом:

1. Распространяется ревизия, отмеченная маркером в столбце **Текущая**. Отмечена может быть только одна ревизия. При откате Агента к более старой ревизии станция будет принудительно перезагружена с интервалом задержки 5 минут.
2. Если в столбце **Текущая** ревизия не отмечена, распространяется последняя ревизия, отмеченная маркером в столбце **Хранимая**.
3. Если в столбцах **Текущая** и **Хранимая** не отмечена ни одна ревизия, распространяется самая последняя ревизия.

Автоматический маркер всегда указывает на распространяемую ревизию.

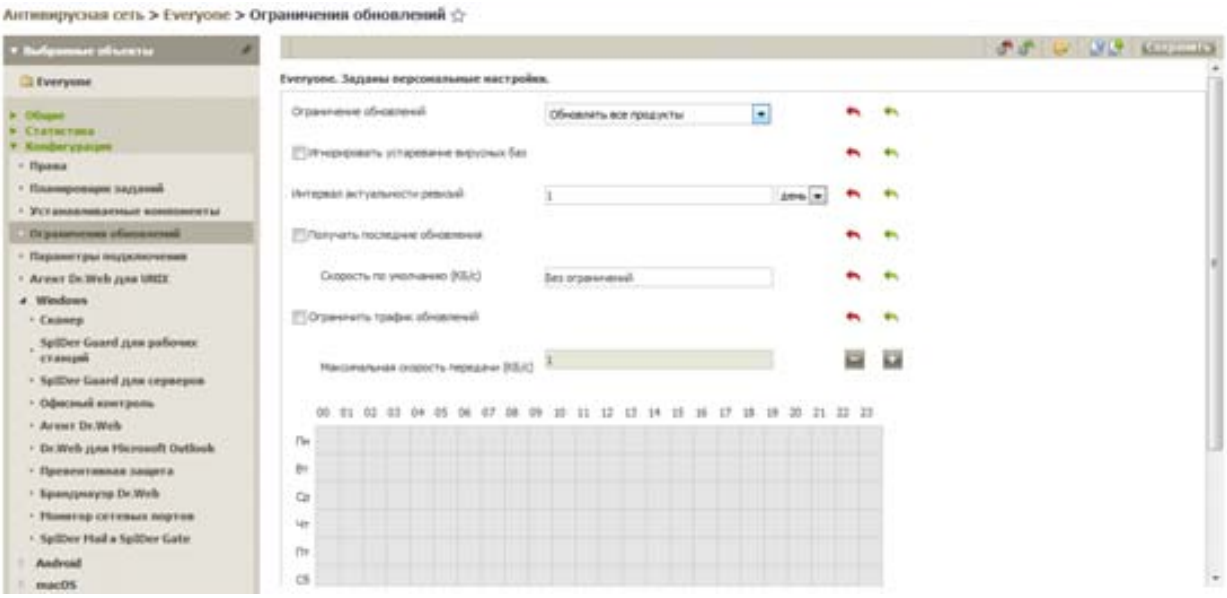
При наличии замороженной ревизии ревизия для распространения выбирается следующим образом:

1. Если маркер в столбце **Текущая** установлен, станциям раздается текущая ревизия.
2. Если маркер в столбце **Текущая** не установлен, станциям раздается ревизия, предшествующая замороженной.

В столбце **Текущая** установите маркер, чтобы задать ревизию продукта, которая будет использоваться для обновлений **Агентов** и антивирусного ПО на станциях. Может быть установлена только одна текущая ревизия. Маркер, задающий текущую ревизию, может быть не установлен.

6. После настройки параметров работы с отложенными обновлениями, необходимо выбрать группу или отдельную станцию в разделе **Антивирусная сеть → Конфигурация → Ограничения обновлений**.

Настройка отложенных обновлений осуществляется для каждой группы или станции отдельно.



Для группы или станции, на которые будет автоматически распространяться последняя ревизия, установите флажок **Получать все последние обновления —** обновления будут приходить на эти станции в обход режима заморозки ревизии. Таким образом, эти станции могут использоваться д ля тестирования обновлений, пока на остальные станции будет распространяться ревизия, которую вы отметили в качестве текущей.

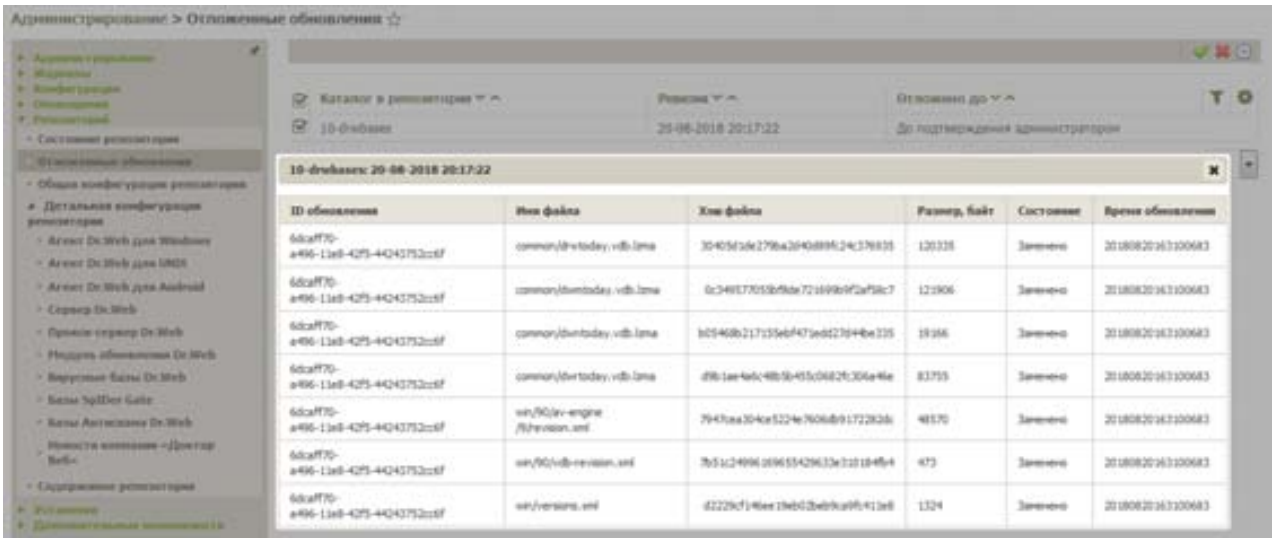
7. Следующая загруженная с **ВСО** ревизия, которая удовлетворяет условиям опции **Отложить обновления только следующих файлов**, будет заморожена и отложена на срок, выбранный в списке **Время задержки обновлений**.

В меню **Администрирование → Репозиторий → Отложенные обновления** приводится список замороженных обновлений в виде таблицы продуктов, для которых был настроен порядок задержки обновлений.

Таблица содержит следующую информацию:

- **Каталог в репозитории —** название каталога замороженного продукта в репозитории:
  - 05-drwmeta — данные безопасности Сервера Dr.Web,
  - 10-drwgatedb — базы **SpIDer Gate**,
  - 10-drwbases — антивирусные базы,
  - 10-drwspamdb — базы **AntiSpam**,
  - 10-drwupgrade — модуль обновления Dr.Web,
  - 20-drwagent — Агент **Dr.Web** для Windows,
  - 20-drwandroid11 — Агент **Dr.Web** для Android,
  - 20-drwcs — Сервер **Dr.Web**,
  - 20-drwunix — Агент **Dr.Web**,
  - 40-drwproxy — Proxy-сервер Dr.Web,
  - 80-drwnews — новости компании «Доктор Веб».
- **Ревизия** — номер замороженной ревизии.
- **Отложено до** — время, до которого были отложены обновления данного продукта.

При нажатии на строку таблицы замороженных продуктов (имеющих отложенную ревизию) выводится подробная информация о замороженной ревизии данного продукта.



Чтобы снять заморозку с ревизии, необходимо:

1. Установите флажок напротив тех продуктов, для которых вы хотите разморозить ревизии. Для выбора всех продуктов установите флажок в заголовке таблицы замороженных продуктов.

2. На панели инструментов выберите ✔ **(Выполнить немедленно).** Будет снята заморозка продукта, и данная ревизия включится в список ревизий с распространением на станции по общей процедуре.

Также доступны следующие действия:

✖ **Отменить обновление** — снять заморозку продукта и запретить данную ревизию. Процесс получения обновлений с ВСО будет восстановлен. Размороженная ревизия будет удалена из списка ревизий продукта. При приходе следующей ревизии размороженная ревизия будет также удалена с диска.

Изменить время задержки обновлений — задать время, на которое ревизия данного продукта откладывается. Начало времени заморозки считается с момента получения ревизии с ВСО.

3. Если над замороженным продуктом не было задано действие по его разморозке, то по истечении времени, заданного в списке **Время задержки обновлений**, ревизия будет автоматически разморожена и включена в список ревизий с распространением на станции по общей процедуре.

Вы также можете отменить распространение последней ревизии, если установите в качестве текущей ревизии одну из предыдущих ревизий на вкладке **Список ревизий** в разделе **Детальная конфигурация репозитория** → <*Продукт*>.

8.3.4.3. Редактор конфигурации репозитория

Редактор конфигурации репозитория позволяет задать общие параметры конфигурации репозитория для всех продуктов.

После изменения настроек репозитория необходимо произвести успешное обновление ПО компонентов антивирусной сети для изменения состояния репозитория в соответствии с выбранными вами настройками.

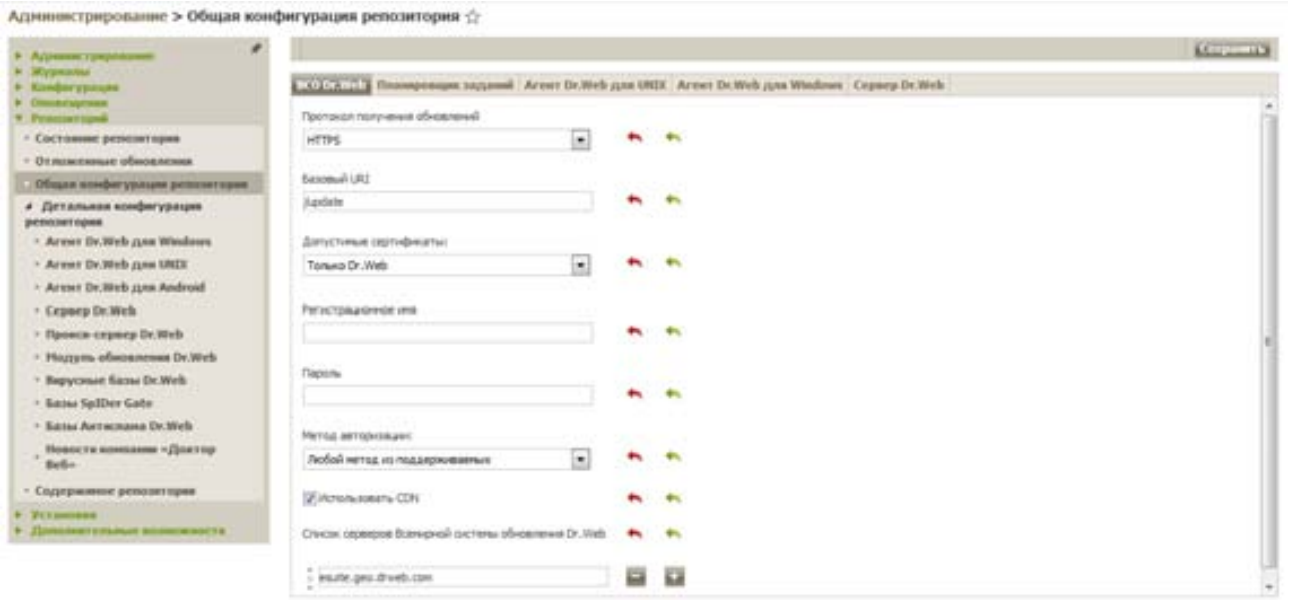
Чтобы отредактировать конфигурацию репозитория, выберите пункт **Администрирование** главного меню Центра управления, в открывшемся окне выберите пункт управляющего меню **Общая конфигурация репозитория**.

Если в процессе редактирования параметров необходимо отменить все внесенные изменения, используйте следующие кнопки на панели инструментов:

Установить все параметры в начальные значения — сбросить значения всех параметров данного раздела в значения, которые они имели до текущего редактирования. Для аналогичного действия над отдельными параметрами используйте кнопки напротив каждого параметра.

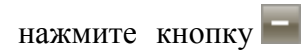
Установить все параметры в значения по умолчанию — сбросить значения всех параметров данного раздела в значения, сохраненные в конфигурационном файле Сервера. Для аналогичного действия над отдельными параметрами используйте кнопки напротив каждого параметра.

Настроив все необходимые параметры, нажмите Сохранить.



На вкладке **BCO Dr.Web** осуществляется настройка параметров подключения к Всемирной системе обновлений Dr.Web.

Для редактирования подключения к BCO используются следующие настройки:

- В выпадающем списке **Протокол получения обновлений** выберите тип протокола для получения обновлений с серверов обновлений. Для всех протоколов загрузка обновлений осуществляется согласно настройкам в разделе **Список серверов Всемирной системы обновления Dr.Web**.
- **Базовый URI** — каталог на серверах обновлений, содержащий обновления продуктов Dr.Web. При обновлении с серверов BCO Dr.Web не следует менять данную настройку без необходимости.
- Если в списке **Протокол получения обновлений** выбран один из защищенных протоколов, поддерживающий шифрование, то в выпадающем списке **Допустимые сертификаты** выберите тип TLS-сертификатов, которые будут автоматически приниматься при установке соединения по выбранному протоколу.
- Если в списке **Допустимые сертификаты** выбран вариант **Пользовательский**, то необходимо задать путь до файла с вашим TLS-сертификатом в поле **Сертификат**.
- **Регистрационное имя** — регистрационное имя пользователя для аутентификации на сервере обновлений, если сервер требует авторизации.
- **Пароль** — пароль пользователя для аутентификации на сервере обновлений, если сервер требует авторизации.
- В выпадающем списке **Метод авторизации** выберите метод авторизации на сервере обновлений.
- Установите флажок **Использовать CDN**, чтобы разрешить использование Content Delivery Network при загрузке репозитория.
- При необходимости отредактируйте список серверов BCO, с которых осуществляется обновление репозитория, в секции **Список серверов Всемирной системы обновления Dr.Web**:
  - Чтобы добавить сервер BCO в список серверов, используемых для обновления, нажмите кнопку  и введите адрес сервера BCO в добавленное поле.
  - Чтобы удалить сервер BCO из списка используемых, нажмите кнопку  напротив сервера, который необходимо удалить.
  - Порядок серверов BCO в списке определяет порядок обращения Сервера Dr.Web при обновлении репозитория. Для изменения порядка серверов BCO перетащите требуемый сервер, захватив строку сервера за корешок слева.

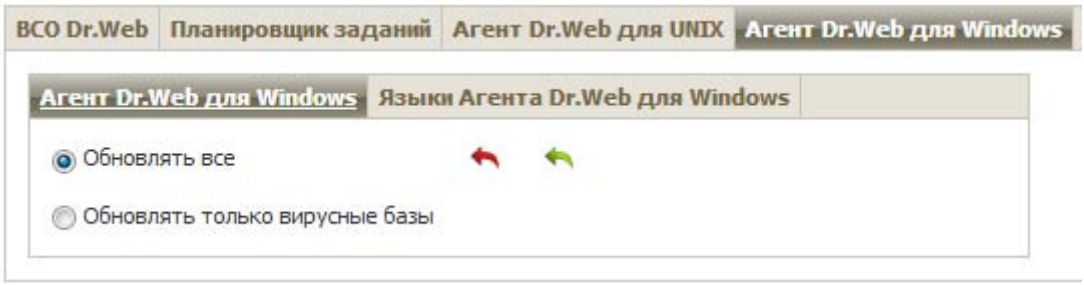
При установке Сервера Dr.Web в список входят только серверы обновлений компании «Доктор Веб». При необходимости вы можете настроить собственные зоны обновлений и внести их в список серверов для получения обновлений.

На вкладке **Планировщик заданий** приведены все задания из расписания Сервера Dr.Web на обновление репозитория.

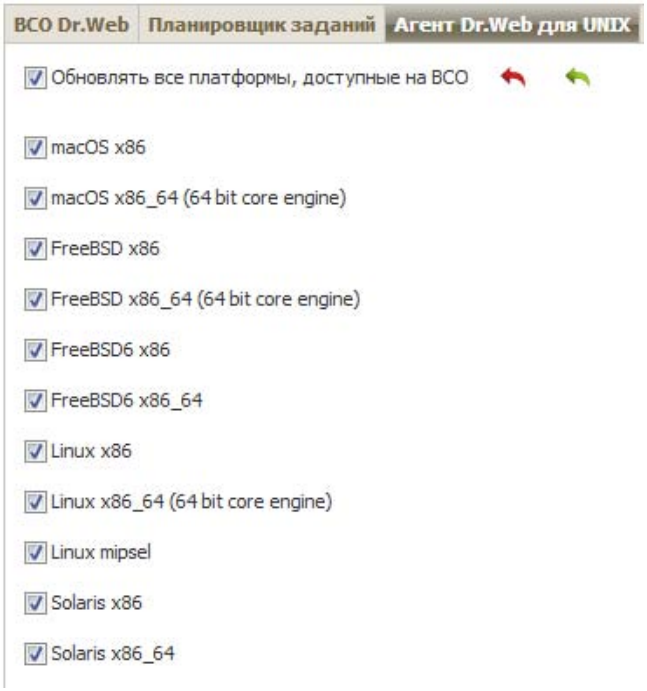
Создание, удаление и редактирование заданий на обновление репозитория осуществляется в разделе **Планировщик заданий Сервера Dr.Web**.

Для того чтобы настроить обновления репозитория для **Агента** и антивирусного пакета для различных версий ОС, сделайте следующее:

- На вкладке **Агент Dr.Web для Windows** на внутренней вкладке **Агент Dr.Web для Windows** укажите, требуется ли обновление всех компонентов, устанавливаемых на рабочие станции под ОС Windows, или только вирусных баз, а также набор доступных языков на вкладке **Языки Агента Dr.Web для Windows**.



- На вкладках Агент **Dr.Web для Unix** и **Сервер Dr.Web Server** укажите, для каких ОС требуется обновление компонентов, устанавливаемых на рабочие станции.

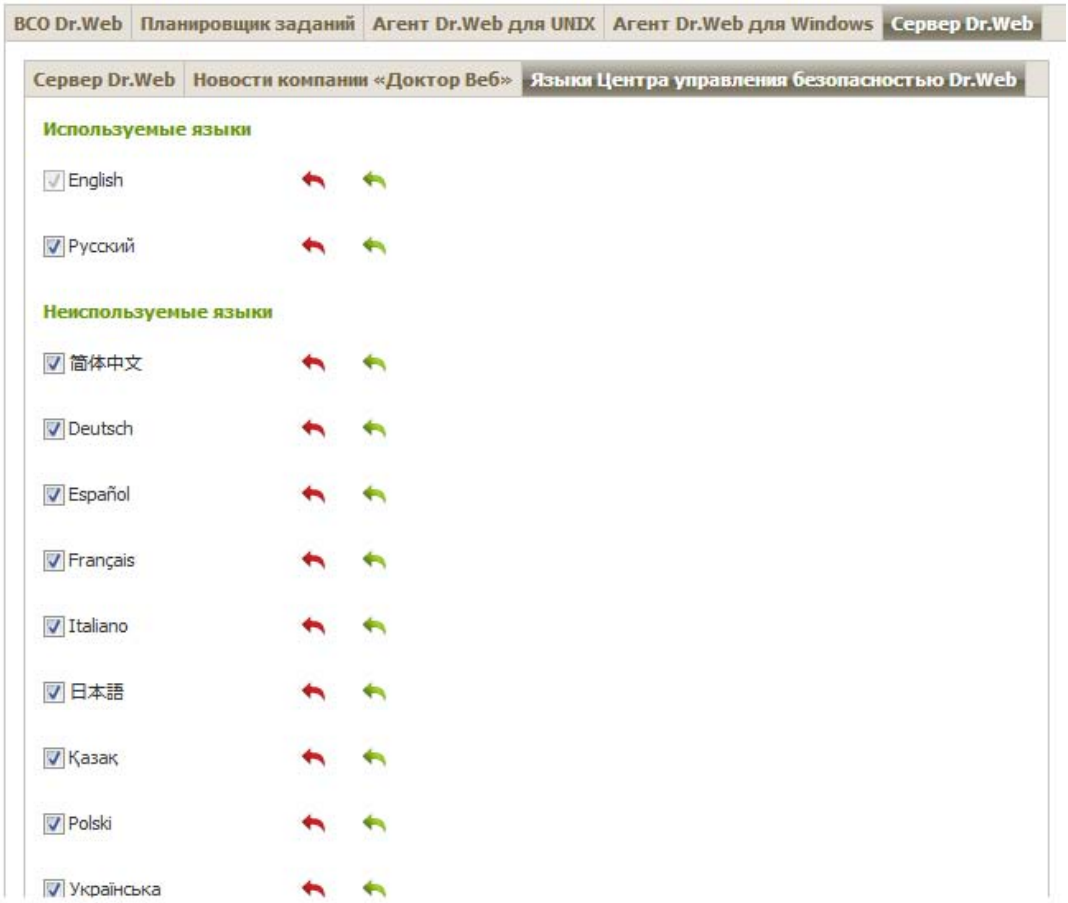


Чтобы получать обновления для **Серверов** под всеми поддерживаемыми ОС, установите флажок **Обновлять все платформы, имеющиеся на ВСО**.

Чтобы получать обновления для **Сервера** только под некоторыми из поддерживаемых ОС, установите флажки только напротив названий этих ОС.

Для Сервера Dr.Web также настраиваются получение новостей компании «Доктор Веб» на различных языках и перечень загружаемых языковых пакетов для антивируса. На вкладке **Новости компании «Доктор Веб»** задайте список языков, на которых будет скачиваться новостная лента. Подробно настройка параметров получения и просмотра новостей компании «Доктор Веб» описана в разделе **Просмотр новостей компании «Доктор Веб» из Центра управления**.

На вкладке **Языки Dr.Web Агента для Windows** задайте список языков интерфейса **Агента** и антивирусного пакета для ОС Windows, которые будут скачиваться с **ВСО**.



Чтобы полностью отключить получение обновлений с **BCO** для **Агента Dr.Web для UNIX** или для **Сервера Dr.Web**, перейдите в раздел **Детальная конфигурация репозитория**, пункт Агент **Dr.Web для Unix** (или Сервер **Dr.Web** соответственно), и на вкладке **Синхронизация** установите флажок **Отключить обновление продукта**.

Раздел **Детальная конфигурация репозитория** позволяет настроить конфигурацию ревизий для каждого продукта репозитория в отдельности. Для этого:

1. В главном меню **Центра управления** выберите пункт **Администрирование → Репозиторий**.

2. В открывшемся меню **Детальная конфигурация репозитория** выберите пункт, соответствующий продукту, который вы хотите настроить.

3. Задайте все необходимые параметры репозитория выбранного продукта, описанные ниже.

4. Нажмите кнопку на панели инструментов **Сохранить и перезагрузить с диска**, чтобы сохранить все внесенные изменения. При этом осуществляется перезагрузка текущей версии репозитория с диска.

На вкладке **Список ревизий** приведена информация обо всех ревизиях выбранного продукта, доступных на данном **Сервере**.

В столбце **Распространяемая** могут стоят два типа маркеров:

- Распространяемая ревизия. Ревизия используется для обновлений **Агентов** и антивирусного ПО на станциях.
- Замороженная ревизия. Данная ревизия не распространяется на станции, новые ревизии не скачиваются с **Сервера**.

В столбце **Хранимая** установите маркер, чтобы сохранять данную ревизию при автоматической очистке репозитория. Маркер может быть установлен для нескольких ревизий одновременно. Также ни один маркер может быть не установлен.

Сервер хранит на диске определенное количество ревизий продукта, задаваемое на вкладке **Синхронизация**. При достижении максимально допустимого количества временно хранимых ревизий, для сохранения новой скачанной с **ВСО** ревизии самая старая временно хранимая ревизия удаляется.

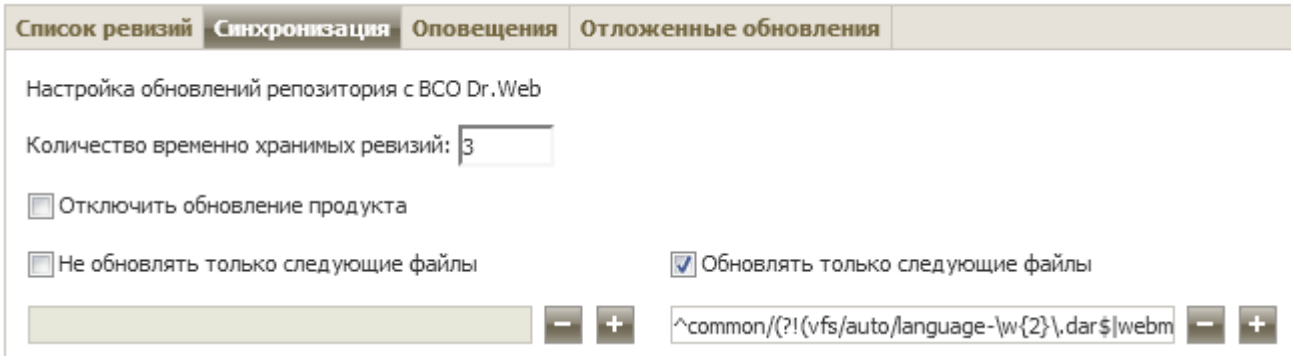
Автоматический маркер **Удерживаемая** определяет, что компоненты из данной ревизии установлены на станциях с ограничением обновлений (в разделе Ограничения обновлений установлены опции **Обновлять только базы** или **Запретить все обновления**).

Такая ревизия не удаляется при автоматической очистке репозитория и может быть использована, если будет необходимо переустановить сбойные компоненты на станции или установить дополнительные компоненты из этой ревизии.

При автоматической очистке репозитория не удаляются ревизии, отмеченные маркером в столбце **Хранимая** и маркером в столбце **Текущая**. Если ревизия продукта работает стабильно, ее можно отметить как хранимую, и в случае возникновения проблем с более новыми — откатиться на предыдущую.

В столбце **Ревизия** указана дата получения ревизии продукта. Если ревизия заморожена, в данном столбце дополнительно выводится статус блокировки.

На вкладке **Синхронизация** настраиваются параметры обновления репозитория **Сервера** с **ВСО**.



В поле **Количество хранимых ревизий** задается количество ревизий продукта, временно хранимых на диске, не считая ревизий, помеченных как **Текущая** и **Хранимая**. В случае если пришла новая ревизия, а количество ревизий продукта уже достигло заданного значения, то удаляется самая старая ревизия. Ревизии, помеченные как **Текущая** и **Хранимая**, не подлежат удалению.

- Установите флажок **Отключить обновление продукта**, чтобы отключить получение обновлений данного продукта с серверов **BCO**. Агенты при этом будут обновляться до текущей ревизии на Сервере (или согласно процедуре выбора распространяемой ревизии).
- Установите флажок **Отключить обновление продукта**, чтобы отключить получение обновлений данного продукта с серверов BCO. Агенты при этом будут обновляться до текущей ревизии на Сервере (или согласно процедуре выбора распространяемой ревизии).

Для некоторых продуктов также доступны следующие настройки:

- Установите флажок **Обновлять только следующие файлы**, чтобы получать обновления с BCO только указанных ниже файлов.
- Установите флажок **Не обновлять только следующие файлы**, чтобы отключить обновление с BCO только указанных ниже файлов.

Списки файлов задаются в формате регулярных выражений.

Если установлены оба флажка, то выборка файлов осуществляется следующим образом:

1. Из полного списка файлов продукта выбираются файлы по спискам **Обновлять только следующие файлы**.

2. Из списка, полученного на шаге 1, удаляются файлы по спискам **Не обновлять только следующие файлы**.

3. С BCO обновляются только файлы, полученные в результате выборки на шаге 2.

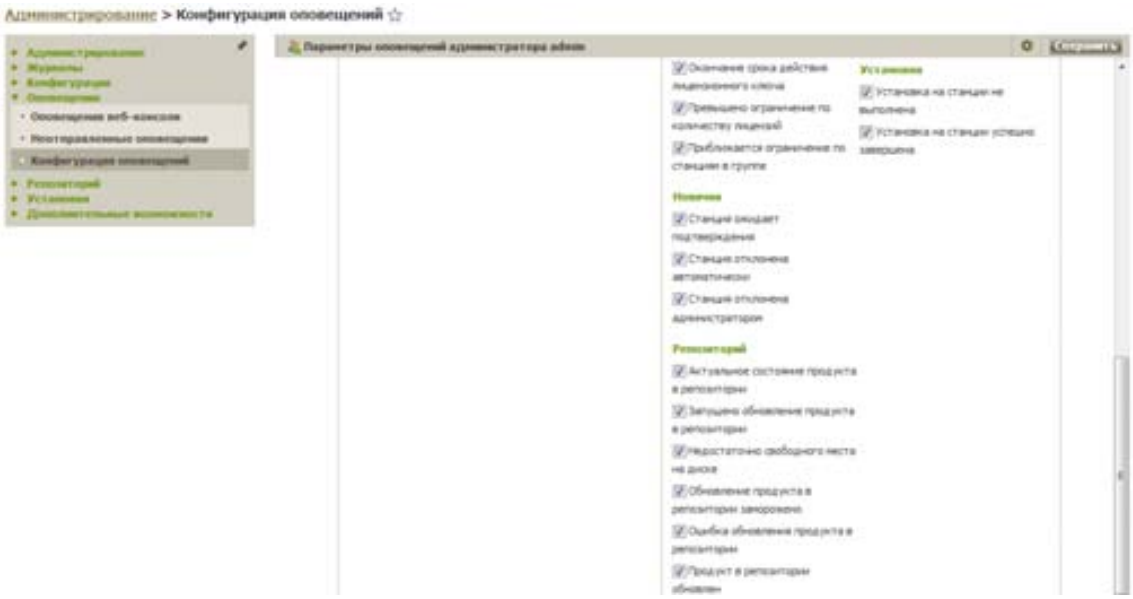
На вкладке **Оповещения** настраиваются оповещения об обновлениях репозитория:

- Установите флажок **Не оповещать только о следующих файлах**, чтобы отключить отправку уведомлений только на события, связанные с файлами, которые заданы в списке ниже.
- Установите флажок **Оповещать только о следующих файлах**, чтобы отправлять уведомления только на события, связанные с файлами, которые заданы в списке ниже.

Списки файлов задаются в формате регулярных выражений.

Если списки исключений не заданы, то будут отправляться все оповещения, включенные на странице **Конфигурация оповещений**.

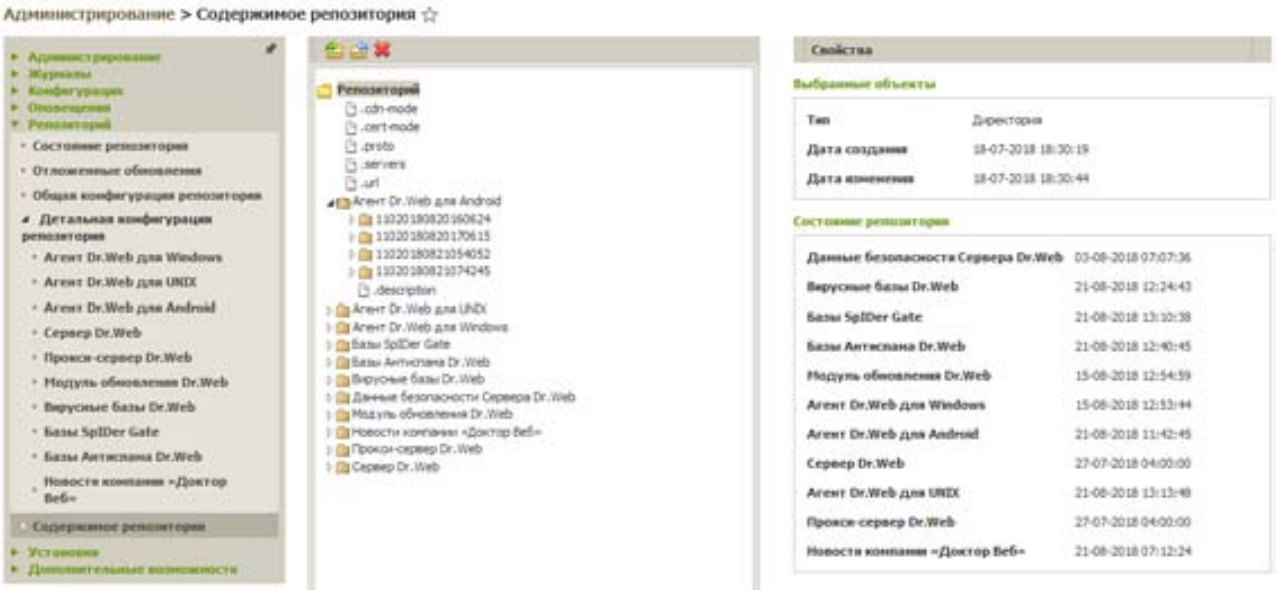
Параметры оповещений об обновлениях репозитория настраиваются на странице конфигурации оповещений в подразделе **Репозиторий**.



На вкладке **Отложенные обновления** вы можете отложить распространение обновлений на станции на определенный срок. Отложенная ревизия считается *замороженной*.

Данный функционал может использоваться, если необходимо временно отменить распространение последней ревизии продукта на все станции антивирусной сети, например при необходимости предварительного тестирования данной ревизии на ограниченном количестве станций.

Раздел **Содержимое репозитория** позволяет просматривать и управлять текущим содержимым репозитория на уровне каталогов и файлов репозитория.



Главное окно раздела **Содержимое репозитория** содержит иерархическое дерево содержимого репозитория, отражающее все каталоги и файлы в текущей версии репозитория со списком всех имеющихся ревизий каждого продукта.

Для управления содержимым репозитория используйте следующие кнопки на панели инструментов:

- **Экспортировать файлы репозитория в архив**,
- **Импортировать архив с файлами репозитория**,
- **Удалить отмеченные объекты —** удалить объекты, выбранные в дереве содержимого репозитория, без возможности восстановления.

После изменения содержимого репозитория, например при удалении или импорте объектов, для использования **Сервером** измененных данных необходимо перезагрузить репозиторий (кнопка в разделе **Состояние репозитория**).

Чтобы сохранить файлы репозитория в zip-архив:

1. В иерархическом дереве содержимого репозитория выберите продукт, отдельную ревизию продукта или весь репозиторий. Весь репозиторий будет экспортирован, если ничего не выбрано в дереве или выбран заголовок дерева — **Репозиторий**. Для выбора нескольких объектов используйте клавиши CTRL или SHIFT.

При экспорте объектов репозитория обратите внимание на основные типы экспортируемых объектов:

a. Zip-архивы продуктов репозитория. Такие архивы содержат один из следующих типов объектов репозитория: **Весь репозиторий целиком**, **Весь продукт целиком** или **Вся отдельная ревизия продукта целиком**.

   Архивы, полученные при экспорте данных объектов, могут быть импортированы через раздел **Содержимое репозитория**. Название таких архивов содержит префикс *repository_*.

b. Zip-архивы отдельных файлов репозитория.

   Архивы, полученные при экспорте отдельных файлов и каталогов, находящиеся в иерархическом дереве ниже объектов из предыдущего пункта, не подлежат импорту через раздел **Содержимое репозитория** (при попытке импорта будет выдаваться ошибка). Название таких архивов включает префикс *files_*.

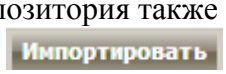
   Такие архивы могут использоваться в качестве резервных копий файлов для ручной замены. Однако не рекомендуется осуществлять замену файлов репозитория вручную, в обход раздела **Содержимое репозитория**.

2. Нажмите кнопку **Экспортировать файлы репозитория в архив** на панели инструментов. Задание пути для сохранения zip-архива с выбранным объектом репозитория осуществляется в соответствии с настройками веб-браузера, в котором открыт **Центр управления**.

Чтобы загрузить файлы репозитория из zip-архива***:***

1. Нажмите кнопку  (**Импортировать архив с файлами репозитория)** на панели инструментов.
2. В открывшемся окне в разделе **Выбор файла** задайте zip-архив с файлами репозитория.

   Импорту подлежат только zip-архивы, которые были получены при экспорте одного из следующих типов объектов репозитория: **Весь репозиторий целиком**, **Весь продукт целиком** или **Вся отдельная ревизия продукта целиком**. Название таких архивов при экспорте содержит префикс repository_.

3. В разделе **Настройки импорта** задайте следующие параметры:
   a. **Только добавить отсутствующие ревизии** — в данном режиме импорта осуществляется только добавление тех ревизий репозитория, которые отсутствуют в текущей версии. Остальные ревизии остаются без изменений.
   b. **Заменить весь репозиторий** — в данном режиме импорта осуществляется полная замена текущего репозитория на импортируемый.
   c. Установите флажок **Импортировать конфигурационные файлы**, чтобы при импорте репозитория также импортировать конфигурационные файлы.
4. Нажмите кнопку 

для запуска процесса импорта.

8.4. Запуск и останов антивирусного сервера

По умолчанию антивирусный сервер запускается автоматически после установки и после каждой перезагрузки операционной системы. Необходимость перезагрузки Сервера может возникнуть после внесения значимых изменений в его конфигурацию.

Запустить, перезапустить или остановить антивирусный сервер можно следующими способами:

- В разделе **Администрирование** Центра управления: перезапуск при помощи кнопки  , останов при помощи кнопки  .
- При помощи соответствующей консольной команды
  - Запуск:

    для ОС FreeBSD: # /usr/local/etc/rc.d/drwcsd.sh start

    для ОС Linux: # /etc/init.d/drwcsd start

  - Перезапуск:

    для ОС FreeBSD: # /usr/local/etc/rc.d/drwcsd.sh restart

    для ОС Linux: # /etc/init.d/drwcsd restart

  - Останов:

    для ОС FreeBSD: # /usr/local/etc/rc.d/drwcsd.sh stop

    для ОС Linux: # /etc/init.d/drwcsd stop

  Для ОС Windows соответствующие операции выполняются при помощи консольных команд, выполненных из подкаталога bin каталога установки антивирусного сервера:

  drwcsd start — запуск **Сервера**,

drwcsd restart — полный перезапуск службы **Сервера**,

drwcsd stop — нормальное завершение работы **Сервера**.

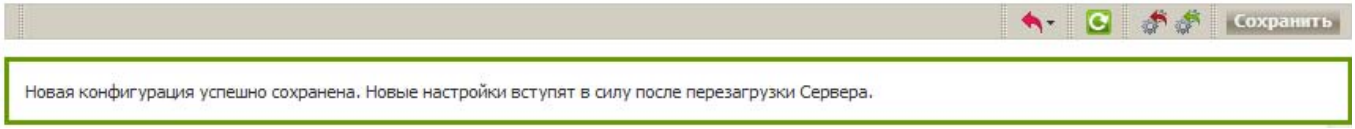
8.5. Утилита дистанционной диагностики антивирусного сервера

Модуль Dr.Web Server FrontDoor предназначен для подключения утилиты дистанционной диагностики антивирусного с ервера, позволяющей осуществлять основные операции по управлению антивирусным сервером (в том числе изменение уровня логирования), а также получать статистику антивирусного сервера сервера.

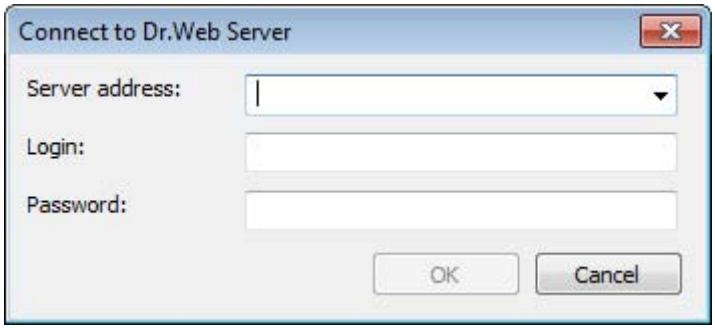
Пример подключения утилиты: drwcntlui.exe ssl://127.0.0.1

Для работы плагина необходимо настроить сервер, разрешив подключение к нему с помощью данной утилиты.

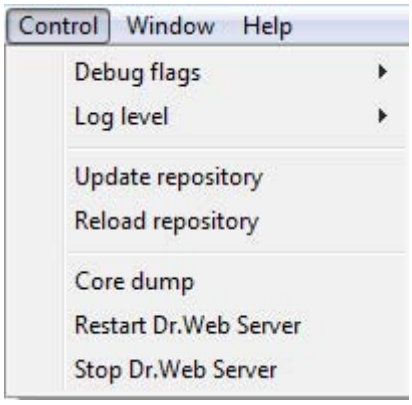
В разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** на вкладке **Модули** установите флажок Расширение Dr.Web Server Front Door для возможности использования соответствующего подключаемого модуля, позволяющего подключение утилиты дистанционной диагностики **Сервера**. Нажмите **Сохранить** и перезапустите Сервер, нажав 



Утилита находится в подкаталоге bin каталога установки антивирусного сервера, также е е можно сохранить в любую папку через раздел **Администрирование → Дополнительные возможности → Утилиты**. При запуске утилиты необходимо указать адрес Сервера Dr.Web, а также логин и пароль администратора, от имени которого будет осуществляться управление.

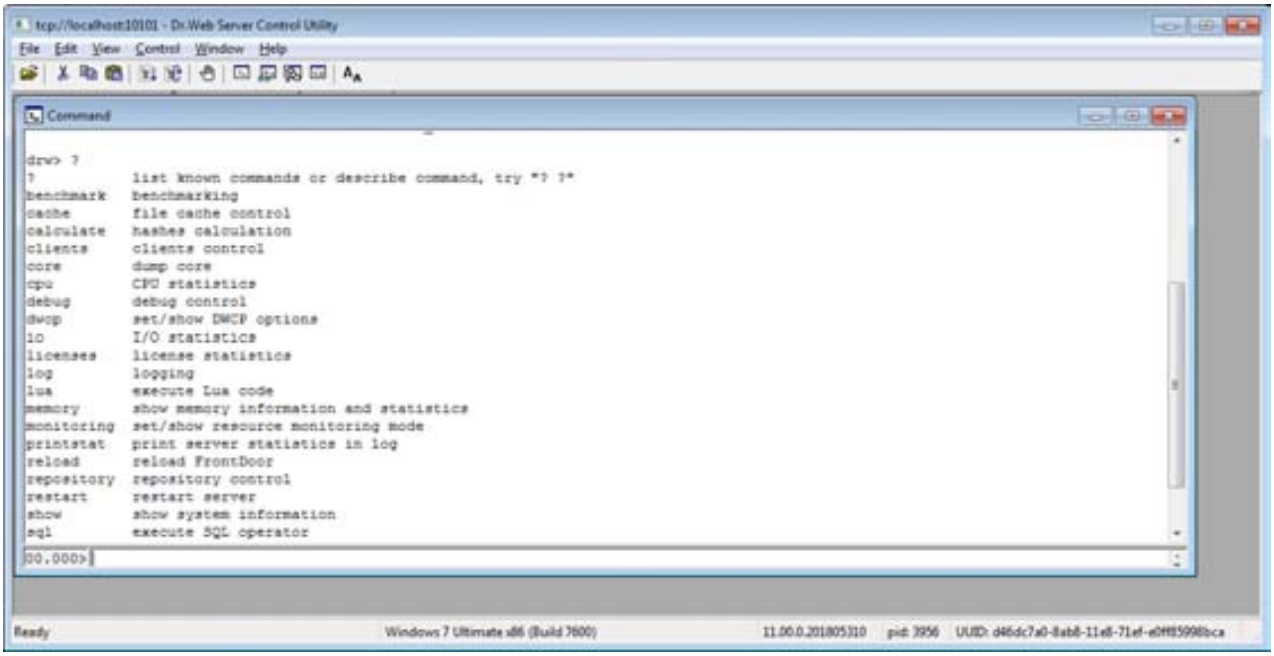


Часть функционала утилиты доступна не только в виде консольных команд, но и напрямую из графического интерфейса. С его помощью удобно обновлять/перезагружать репозиторий, перезагружать/останавливать Сервер, получать дамп памяти ядра Сервера, а также настраивать флажки диагностики и параметры журнала.

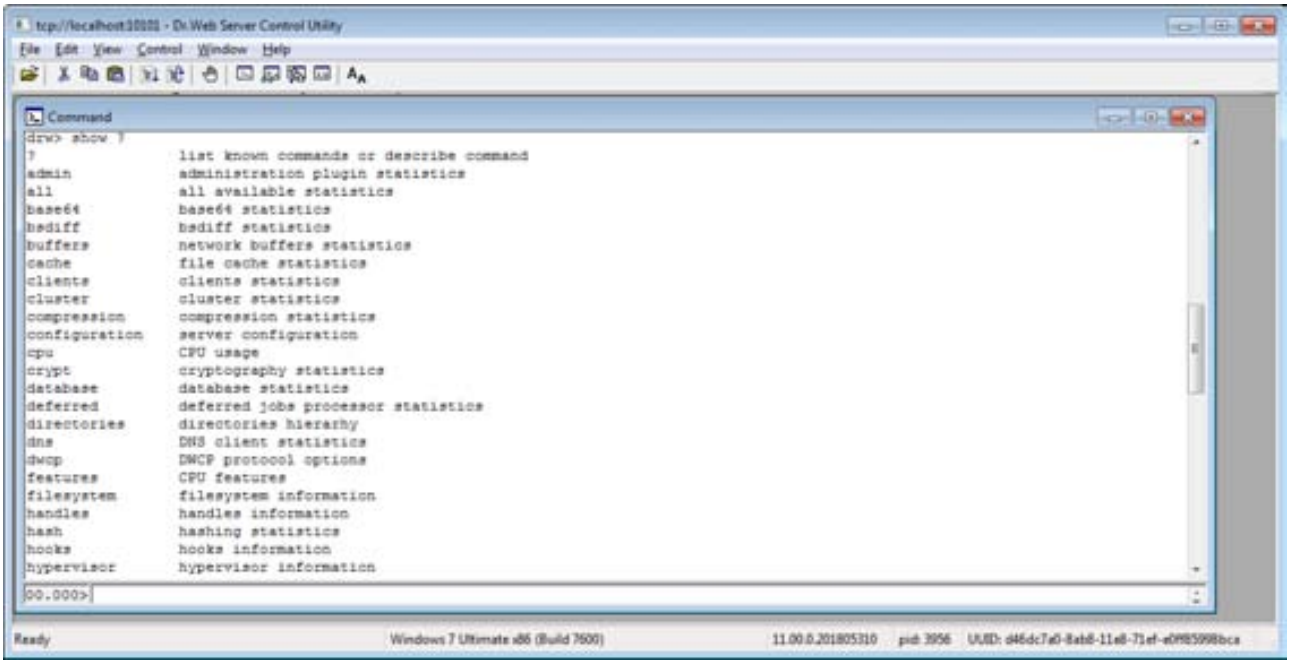


Внимание! После удаленной остановки Сервера, вы потеряете возможность для дальнейшего взаимодействия с ним, так как связь утилиты с Сервером оборвется, а удаленный запуск Сервера с ее помощью невозможен!

Кроме возможностей, которые предоставляет GUI утилиты, с ее помощью можно отправить серверу целый набор команд, с писок которых можно получить, введя команду «?» без кавычек.



Информацию о формате необходимой команды можно также узнать, введя «команда ?» без кавычек.

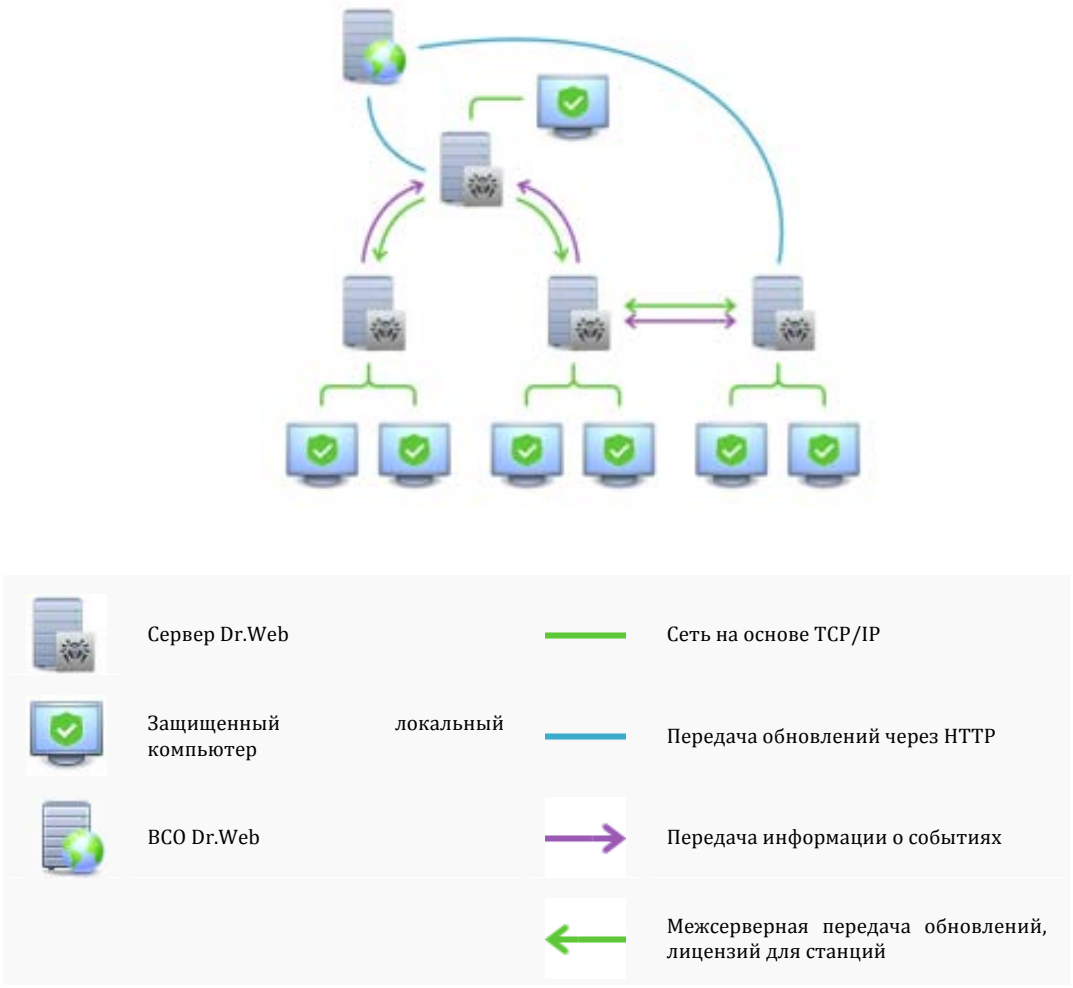


8.6. Иерархия серверов

Поскольку в антивирусной сети может использоваться несколько Серверов Dr.Web, то у администратора может возникнуть задача организовать иерархическую систему серверов, которая позволит не только экономить трафик, но и распределять нагрузку между серверами. Экономия трафика осуществляется за счет получения обновлений с ВСО только одним из Серверов, в то время как остальные получают обновления уже с него. Баланс нагрузки в свою очередь достигается распределением Агентов по Серверам Dr.Web, поскольку каждый Агент может одновременно присоединяться только к одному Серверу.

При планировании структуры антивирусной сети следует обратить внимание на особенности лицензирования сети с несколькими Серверами — при передаче части лицензий соседнему Серверу они будут недоступны остальным Серверам.

Для обмена информацией между Серверами (обновлениями файлов компонентов и сведениями о работе Серверов и подключенных к ним станций) используется специальный протокол межсерверной синхронизации. Важнейшей особенностью этого протокола является оперативность передачи обновлений.



В рамках иерархической сети могут быть реализованы два типа связей между Серверами:

- связь типа главный — подчиненный, при которой главный передает подчиненному обновления и получает обратно информацию о событиях,
- связь между равноправными, при которой направления передачи и типы информации настраиваются индивидуально.

Основные преимущества антивирусной сети с несколькими Серверами Dr.Web:

- обновления распространяются немедленно при их получении;
- возможность получения обновлений с серверов ВСО Dr.Web через один Сервер Dr.Web с последующей передачей на остальные Серверы напрямую или через промежуточные звенья. Серверы, принимающие обновления от вышестоящего Сервера, не принимают обновления с ВСО, даже при наличии такого задания в расписании, однако, на тот случай, если главный Сервер будет временно недоступен, рекомендуется оставить в расписании подчиненного Сервера задание на обновление с серверов ВСО. Это позволит Агентам, подключенным к подчиненному Серверу, получать обновление вирусных баз и программных модулей;
- отпадает необходимость в настройке расписания обновления на Сервере (кроме тех Серверов, которые получают обновления с серверов ВСО Dr.Web с использованием протокола http);
- возможность распределения защищаемых рабочих станций по нескольким Серверам с уменьшением нагрузки на каждый из них;
- объединение информации от нескольких Серверов на одном; возможность получения ее в сеансе Центра управления на этом Сервере в консолидированном виде — **Dr.Web ES**

самостоятельно отслеживает и не допускает возникновения циклических путей передачи информации.

8.6.1. Соединение главного и подчиненного ES-серверов

Чтобы настроить связь между двумя Серверами Dr.Web,один из которых будет выбран в качестве главного, а второй — подчиненного, необходимо выполнить следующие действия:

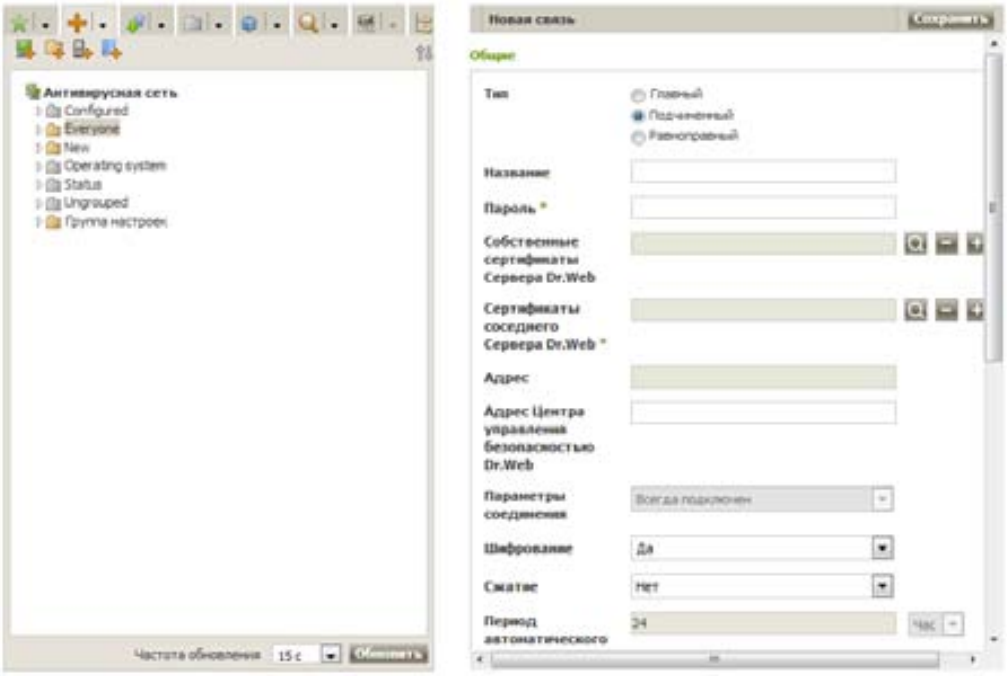
1) Убедитесь, что оба **Сервера Dr.Web** запущены и нормально функционируют.
2) Включите на обоих серверах сетевой протокол, по которому будет осуществляться связь. Для этого в пункте **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** перейдите на вкладку **Модули** и отметьте флажком пункт **Протокол Сервера Dr.Web**. Нажмите **Сохранить**.

Если серверный протокол не включен, при создании новой связи в Центре управления будет выведено сообщение о необходимости включения данного протокола и дана ссылка на соответствующий раздел настроек.

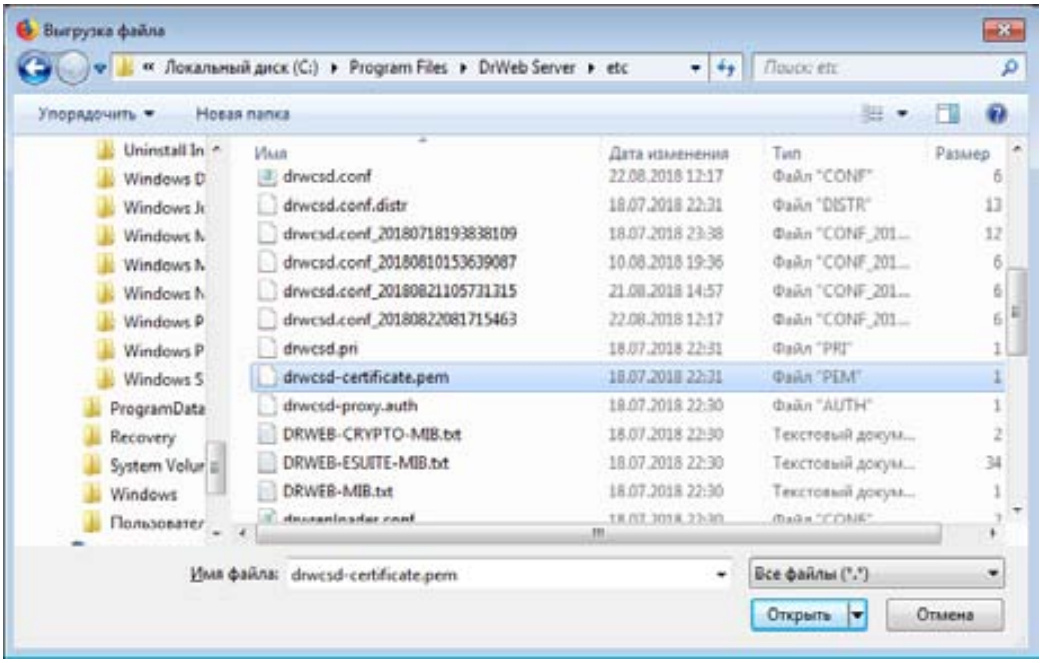
3) Убедитесь, что соединяемым серверам даны «говорящие» имена, по которым их будет удобно идентифицировать лично вам, например *MAIN* для главного и AUXILIARY для починенного. Для того чтобы дать серверу имя, в пункте **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** перейдите на вкладку **Общие** и заполните поле **Название Сервера**. Нажмите **Сохранить.**

4) Перезапустите оба сервера, чтобы применить внесенные изменения, используя значок .
5) Через Центр управления подчиненного Сервера (AUXILIARY) добавьте главный Сервер (MAIN) в список соседних Серверов. Для этого выберите пункт **Антивирусная сеть** в главном меню. Откроется окно, содержащее иерархический список антивирусной сети. Для того чтобы добавить соседний Сервер, на панели инструментов выберите **Добавить объект сети → Создать связь**.

Откроется окно настройки связи между текущим и добавляемым Сервером. Задайте следующие параметры:



- **Тип** создаваемой связи — **Главный**.
- **Название** — название главного Сервера (MAIN).
- **Пароль*** — произвольный пароль для доступа к главному Серверу.
- **Собственные сертификаты Сервера Dr.Web** — список SSL-сертификатов настраиваемого Сервера. Нажмите кнопку и выберите файл сертификата drwcsd-certificate.pem, относящийся к текущему Серверу. Для добавления еще одного сертификата нажмите и добавьте сертификат в новое поле.



- **Сертификаты соседнего Сервера Dr.Web*** — список SSL-сертификатов подключаемого главного Сервера. Нажмите кнопку и выберите файл сертификата drwcsd-certificate.pem, относящийся к главному Серверу. Для добавления еще одного сертификата нажмите и добавьте сертификат в новое поле.

- **Адрес*** — сетевой адрес главного Сервера и порт для подключения. Задается в формате <*адрес_Сервера*>:<*порт*>.

Возможен поиск списка Серверов, доступных в сети. Для этого:

a) Нажмите стрелку справа от поля **Адрес**.

b) В открывшемся окне укажите перечень 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).

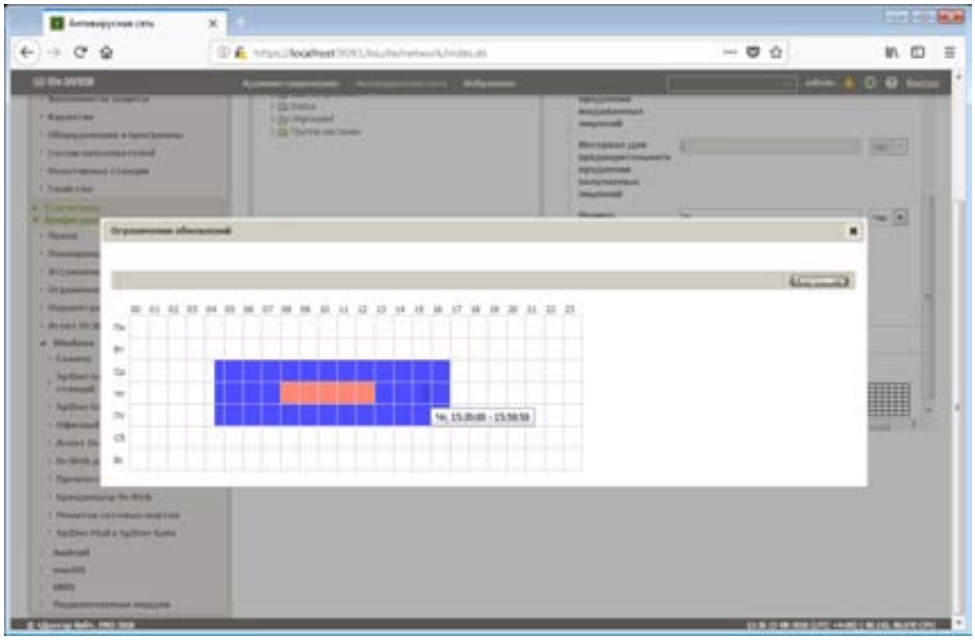
c) Нажмите кнопку . Начнется обзор сети на наличие доступных Серверов.

d) Выберите Сервер в списке доступных Серверов. Его адрес будет записан в поле **Адрес** для создания связи.

Примечание. При создании равноправной связи между Серверами рекомендуется указывать адрес подключаемого Сервера в настройках только одного из них. Это не повлияет на взаимодействие между Серверами, однако позволит избежать записей типа Link with the same key id is already activated в журнале работы Серверов.

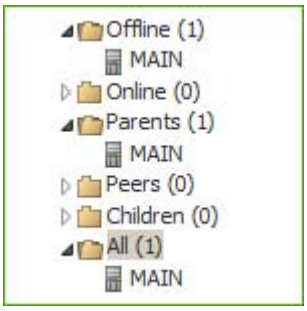
- **Адрес Центра управления безопасностью Dr.Web** — можете указать адрес начальной страницы Центра управления главного Сервера (см. п. Центр управления безопасностью Dr.Web).
- В выпадающем списке **Параметры соединения** задается принцип соединения Серверов создаваемой связи.
- В выпадающих списках **Шифрование** и **Сжатие** задайте параметры шифрования и сжатия трафика между соединяемыми Серверами (см. п. Использование шифрования и сжатия трафика).
- **Срок действия выдаваемых лицензий** — период времени, на который выдаются лицензии из ключа на главном Сервере. Настройка используется, если главный Сервер будет выдавать лицензии текущему Серверу.
- **Период для продления получаемых лицензий** — настройка не используется при создании связи до главного Сервера.
- **Период синхронизации лицензий** — периодичность синхронизации информации о выдаваемых лицензиях между Серверами.
- Флажки в разделах **Лицензии**, **Обновления** и **События** установлены в соответствии с принципом связи *главный — подчиненный* и не подлежат изменению:
  - главный Сервер отправляет лицензии на подчиненный Сервер;
  - главный Сервер отправляет обновления на подчиненный Сервер;
  - главный Сервер принимает информацию о событиях от подчиненного Сервера.

- В разделе **Ограничения обновлений → События** можете задать расписание передачи событий от текущего Сервера главному (редактирование таблицы **Ограничения обновлений** осуществляется аналогично редактированию таблицы расписания в разделе Ограничение обновлений рабочих станций).

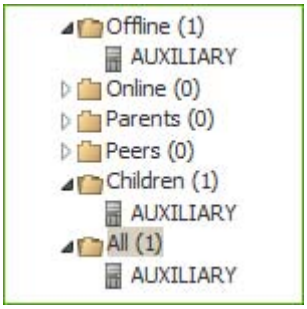


Нажмите кнопку **Сохранить**.

В результате главный Сервер попадет в папки **Parents** и **Offline**.



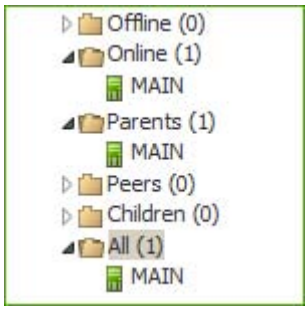
Аналогично добавьте подчиненный сервер в список соседних серверов главного сервера через его Центр управления. Поле **Адрес** заполнять не нужно. Пароль должен быть указан тот же, что и в первом случае, ключ drwcsd.pub должен относиться к подчиненному серверу. В результате подчиненный сервер будет включен в папки **Children** и **Offline**.



Дождитесь установления соединения между Серверами (обычно это занимает не более минуты). Для проверки периодически обновляйте список Серверов с помощью клавиши F5.

После установления связи подчиненный Сервер (AUXILIARY) перейдет из папки **Offline** в папку **Online**.

Откройте Центр управления подчиненного Сервера (AUXILIARY) и убедитесь в том, что главный Сервер (MAIN) подключен к подчиненному (AUXILIARY).



Просмотреть информацию и работе других серверов можно, используя пункт **Статистика → Суммарный отчет** для группы **Neighbors** меню **Антивирусная сеть**. Выведенная таблица содержит сведения об обнаруженных инфекциях, ошибках сканирования, статистики, сетевых инсталляциях, запуске и завершении заданий.

Установка соединения между Серверами **Dr.Web Enterprise Server** невозможна в следующих случаях:

- Проблемы связи по сети.
- При настройке связи задан неверный адрес главного Сервера.
- Заданы неверные открытые сертификаты на одном из Серверов.
- Задан неверный пароль доступа на одном из Серверов (заданы несовпадающие пароли на соединяемых Серверах).

Если необходимо установить новую межсерверную связь между Серверами 10 и 11 версий, дополнительно выполните следующие действия:

1. При создании связи укажите открытый ключ Сервера версии 11 на Сервере версии 10.

2. Сгенерируйте сертификат из закрытого ключа Сервера версии 10 при помощи утилиты drwsign (команда gencert) из состава Сервера версии 11 (см. документ **Приложения**, п. H9.1. Утилита генерации цифровых ключей и сертификатов). Укажите этот сертификат при создании связи на Сервере версии 11.

8.6.2. Использование антивирусной сети с несколькими антивирусными серверами

Особенностью сети с несколькими Серверами является получение обновлений с серверов ВСО Dr.Web через часть Серверов Dr.Web (как правило, один или несколько главных Серверов). При этом только на этих Серверах следует настраивать расписание, содержащее задание на обновление (см. п. Настройка расписания Сервера Dr.Web). Любой Сервер, получивший обновления с серверов ВСО Dr.Web или от другого Сервера, немедленно передает его всем Серверам, для которых у него настроена такая возможность (то есть всем связанным подчиненным, а также тем из равноправных, для которых в явном виде указана возможность получать обновления).

Dr.Web Enterprise Security Suite автоматически отслеживает ситуации, когда из-за несовершенного планирования топологии сети и настройки Серверов на один и тот же Сервер повторно поступает уже принятое из другого источника обновление, и не проводит обновление повторно.

Администратор может также получать сводную информацию о наиболее важных вирусных событиях на сегментах сети, связанных с каким-либо Сервером через межсерверные связи (например, в вышеописанной конфигурации «один главный, остальные подчиненные» такая информация консолидируется на главном Сервере).

Чтобы просмотреть информацию о вирусных событиях на всех Серверах Dr.Web, связанных с данным:

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления. В дереве антивирусной сети, в группе **Neighbors** выберите соседний Сервер, информацию которого хотите просмотреть.

2. В разделе управляющего меню **Таблицы** выберите пункт **Суммарный отчет** для просмотра сведений об общем количестве записей о событиях на соседних Серверах. В таблице со статистикой по соседним Серверам отображаются данные по следующим разделам:

- **Инфекции** — инфекции, обнаруженные на станциях, подключенных к соседним Серверам.
- **Ошибки** — ошибки сканирования.
- **Статистика** — статистика по обнаруженным инфекциям.
- **Запуск/завершение** — запуск и завершении заданий на сканирование станций.
- **Состояние** — состояние антивирусного ПО на станциях.
- **Все сетевые инсталляции** — сетевые инсталляции Агентов.

3. Для перехода к странице с подробной табличной информацией о событиях на соседних Серверах нажмите на цифру в таблице раздела **Суммарный отчет** с количеством записей по требуемому событию.

4. Также для перехода к табличным данным о событиях на соседних Серверах выберите соответствующий пункт (см. шаг 2) раздела **Таблицы** управляющего меню.

5. Для отображения данных за определенный период либо укажите диапазон времени относительно сегодняшнего дня из выпадающего списка, либо задайте произвольный диапазон дат на панели инструментов. Для задания произвольного диапазона введите требуемые даты или нажмите на значки календаря рядом с полями дат. Для просмотра данных нажмите кнопку **Обновить**.

6. При необходимости сохранить таблицу для распечатки или дальнейшей обработки, на панели инструментов нажмите

Сохранить данные в CSV-файл,

Сохранить данные в HTML-файл,

Сохранить данные в XML-файл,

Сохранить данные в PDF-файл.

Для того чтобы перейти с помощью Центра управления на Центр управления иного антивирусного сервера иерархической сети, нажмите выпадающий список на панели управления.

8.6.3. Работа нескольких Серверов Dr.Web Enterprise Server с одной БД

При создании антивирусной сети с несколькими **Серверами Dr.Web** и одной БД необходимо придерживаться следующих правил:

1. На всех Серверах должны быть одинаковые ключи шифрования *drwcsd.pub, drwcsd .pri*, сертификаты *certificate.pem, private-key.pem* и агентский ключ *agent.key*.
2. В конфигурационном файле Центра управления *webmin.conf* для всех Серверов должно быть прописано одинаковое DNS-имя Сервера в параметре **server-name**.
3. На DNS-сервере в сети регистрируется общее имя кластера для каждого отдельного Сервера и задается метод балансировки нагрузки.
4. В конфигурационных файлах Серверов *drwcsd.conf* для всех Серверов должна быть прописана одна внешняя БД.
5. В серверном расписании задания **Очистка старых записей**, **Создание статистического отчета**, **Резервное копирование критичных данных сервера, Очистка старых станций, Очистка неотправленных событий** должны быть только на одном из Серверов (наиболее производительном, если конфигурации различаются).

8.6.4. Контроль состояния серверов иерархической сети

Контроль подключений соседних Серверов иерархической сети производится с помощью стандартного задания **Соседний Сервер давно не подключался** в разделе **Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web**.

8.7. Использование антивирусных кластеров

Антивирусные Серверы для повышения надежности могут быть объединены в кластер. После этого администратор антивирусной сети получает возможность управлять параметрами защиты станций сети с любых Серверов, вне зависимости от того, к какому серверу кластера подсоединены эти станции. При этом реализация кластера не исключает вхождения серверов кластера в иерархическую сеть Серверов.

Для создания кластера и его нормального функционирования необходимо выполнение следующих условий:

- Все антивирусные серверы кластера должны работать с единой базой данных, и, соответственно, в конфигурационных файлах drwcsd.conf всех серверов кластера должна быть прописана одна внешняя БД.

  Как и в случае простого использования базы данных (без организации кластера), каждый из серверов обращается к базе данных независимо, и все данные серверов хранятся раздельно. Везде, где это актуально, сервер «забирает» из БД только записи, привязанные к его ID, который является уникальным для каждого Сервера. Использование единой базы данных само по себе позволяет одним Серверам работать с Агентами, подключенными к другим Серверам, но организация кластера дает возможность Агентам получать изменения не только при следующем подключении.

  Общая база данных должна быть создана до установки первого антивирусного Сервера кластера или до момента присоединения первого сервера к БД.

  Зайдите в меню **Пуск → Все программы → PostgreSQL 10.4 →** P**SQL** (или запустите консоль управления PostgreSQL командой **Пуск → Программы → PostgreSQL 10.4 → Командная строка** и выполните команду *psql -U postgres*). В появившемся окне на вопросы Server [localhost], Database [postgres], Port [5432], Username [postgres] следует ответить нажатием на клавишу ENTER либо ввести актуальные данные, если они отличаются от предложенных по умолчанию, затем следует ввести пароль, который был задан при установке PostgreSQL. После успешной авторизации можно вводить команды:

```
create user drwcs;

alter user drwcs password 'xxxx';
create database drwcs with owner=drwcs;
```

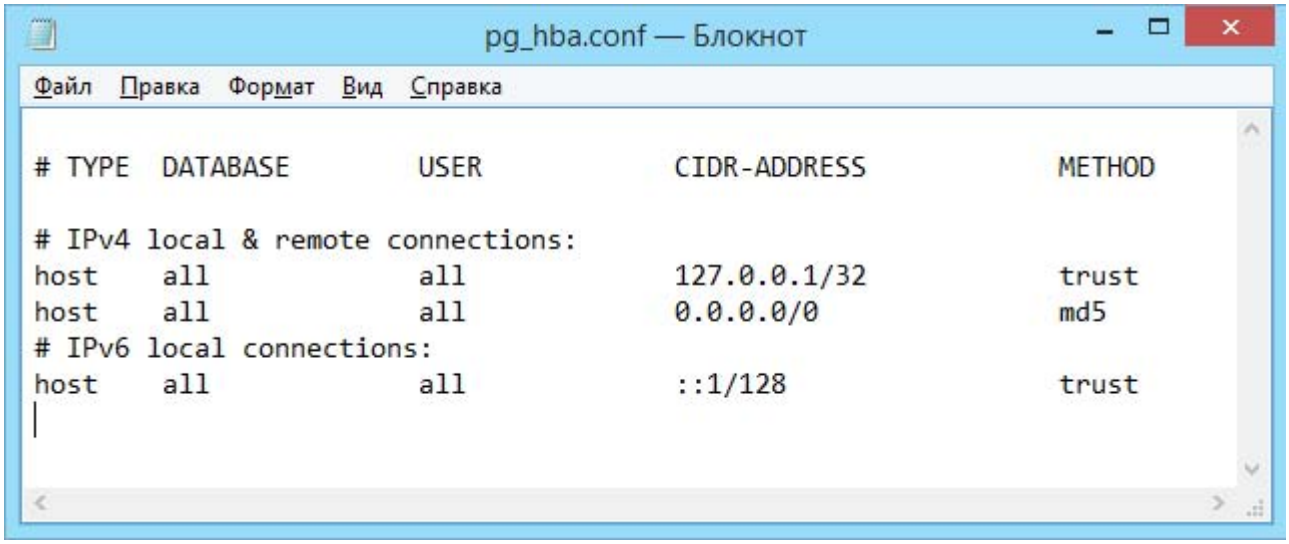
```
Server [localhost]:
Database [postgres]:
Port [5432]:
Username [postgres]:
Password for user postgres:
psql (9.3.5)
postgres=# create user drwcs;
CREATE ROLE
postgres=# alter user drwcs password 'root';
ALTER ROLE
postgres=# create database drwcs with owner=drwcs;
CREATE DATABASE
```

  По умолчанию Dr.Web Enterprise Suite 11.0 предполагает использование кодировки UTF8, поэтому можно создать базу данных с указанием данной кодировки:

  create database drwcs owner=drwcs encoding='UTF8';

  Внимание! Все серверы кластера должны иметь доступ к базе данных. В случае PostgreSQL для выполнения этого условия необходимо в конфигурационном файле

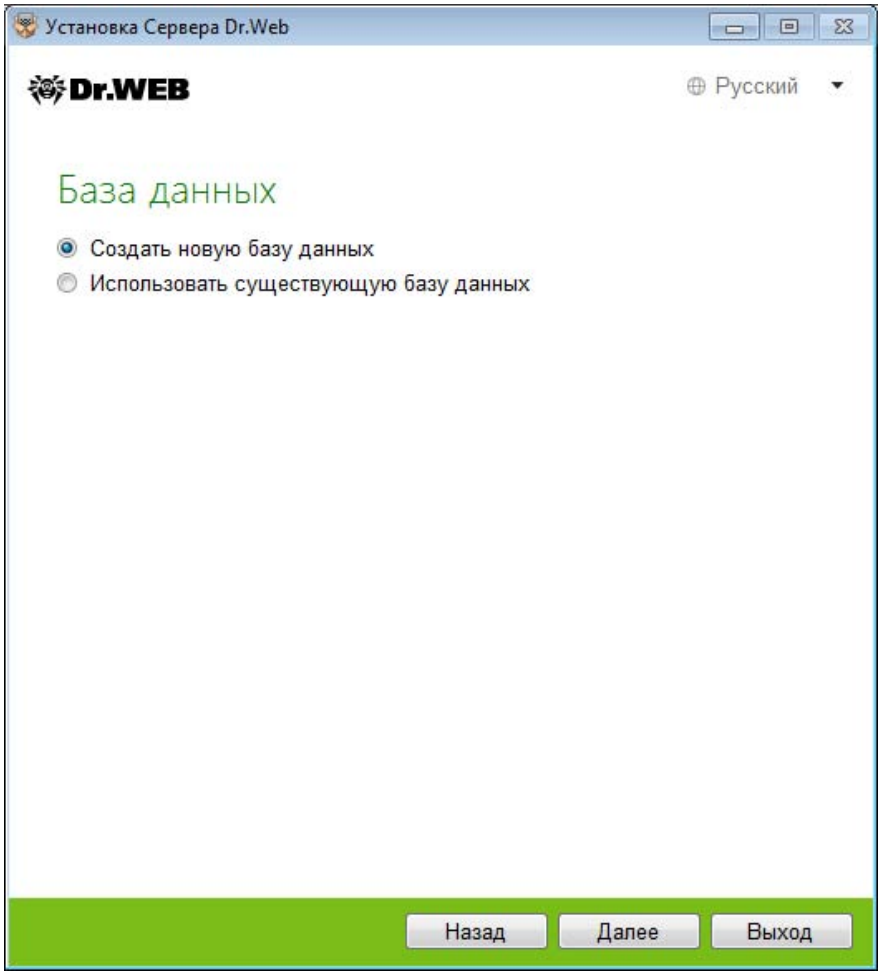
pg_hba.conf (по умолчанию расположен в каталоге *C:\PostgreSQL\data\pg10*) разрешить доступ к базе данных со всех машин кластера и после внесения изменений перезапустить сервис базы данных.



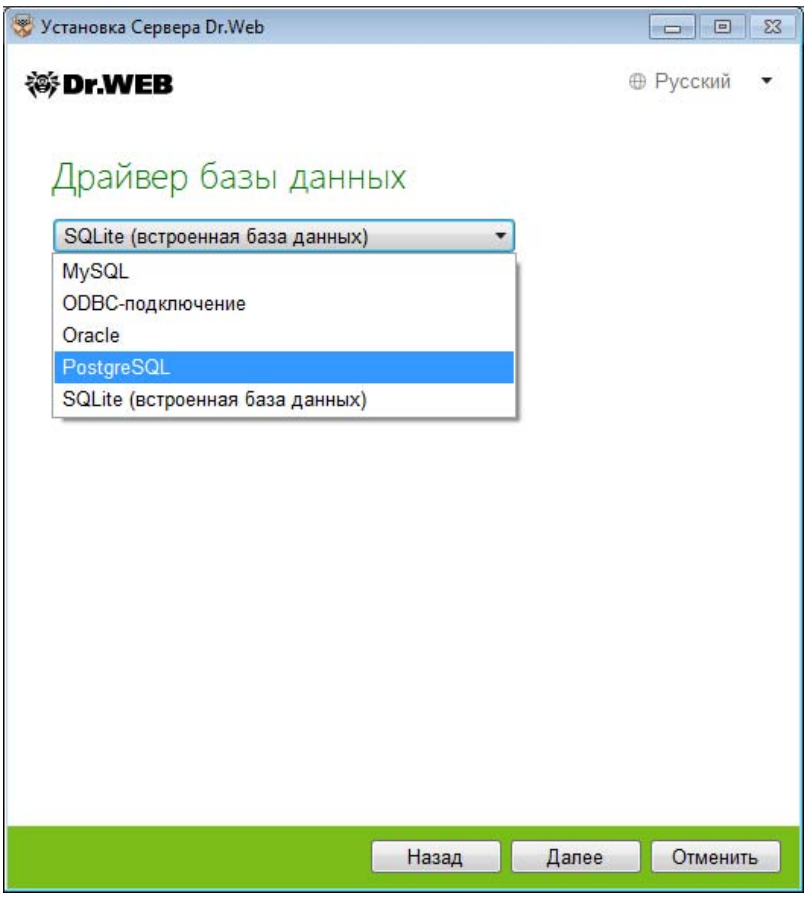
База данных может быть установлена как на отдельный компьютер, так и на ПК, где уже установлен один из антивирусных Серверов кластера.

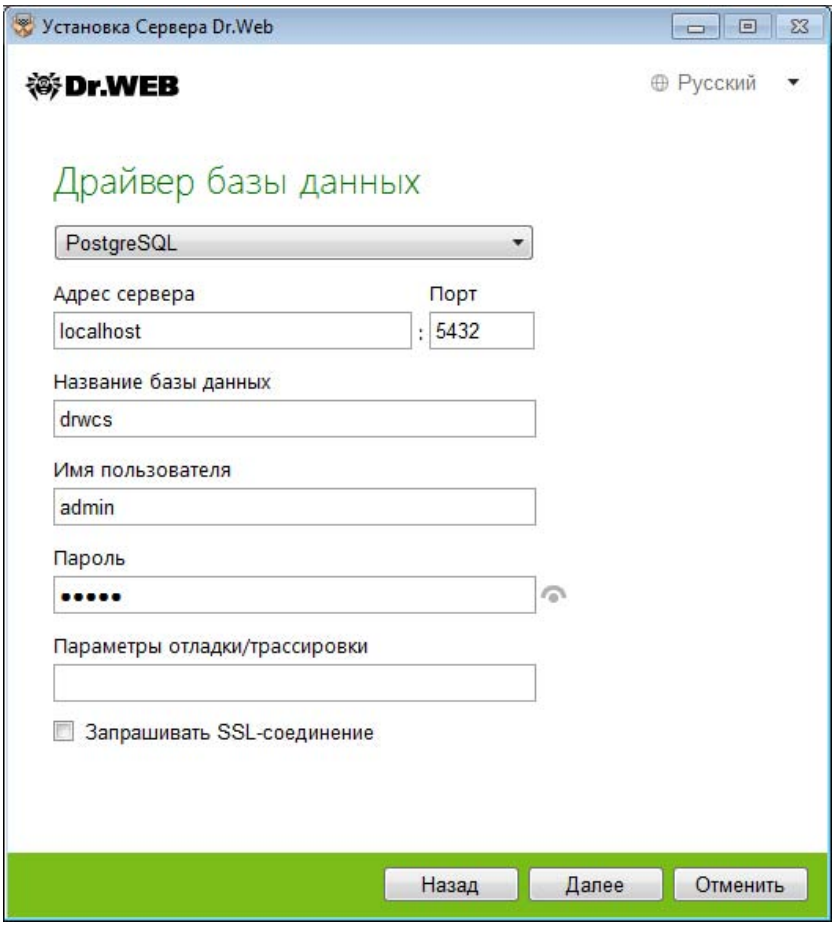
Если установка антивирусных серверов осуществляется под ОС Windows, то в ходе установки сервера необходимо сделать следующее:

- На шаге База данных укажите **Создать новую базу данных**;



- Выберите нужную БД и укажите параметры доступа.



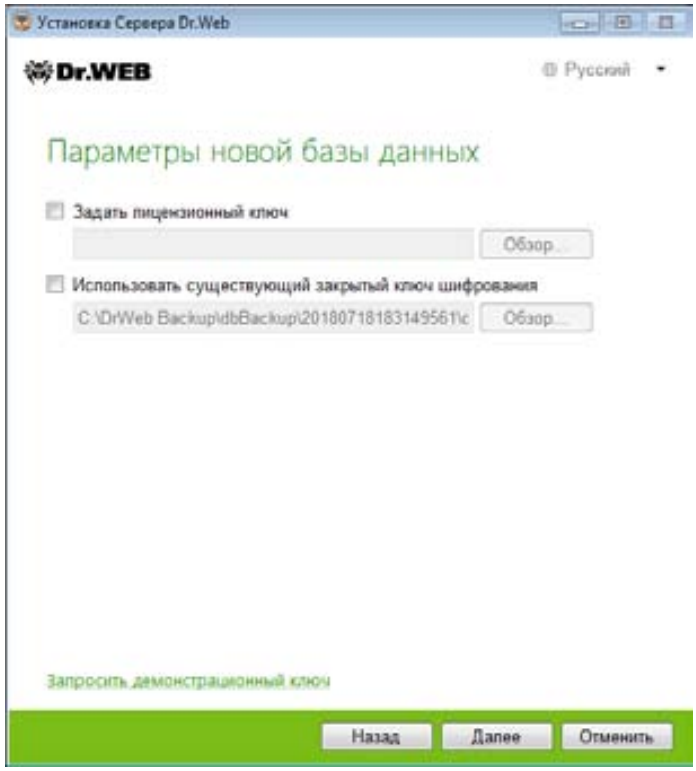


Если в ходе подключения к БД какой-то из параметров был указан неверно, причину проблем можно будет найти в файле *initdb.log* подкаталога var каталога установки Сервера Dr.Web (для ОС MS Windows в зависимости от битности дистрибутива это по умолчанию *C:\Program Files (x86)\DrWeb Server* или *C:\Program Files\DrWeb Server*).

В других случаях рекомендуется выбирать вариант с использованием внутренней базы данных, что позволит избежать потенциальных проблем с инициализацией уже существующей БД. Поэтому сразу после установки необходимо перейти в разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** на вкладку **База данных**, ввести необходимые параметры и перезагрузить Сервер.

Внимание! За исключением первого Сервера кластера, **недопустимо вводить уже использующиеся в работе С ерверы в кластер, который использует другую внешнюю или внутреннюю базу данных** — это приведет как минимум к потере данных (информации о станциях, статистике, настройках, за исключением настроек, хранящихся в конфигурационных файлах), так как при импорте данные, имеющиеся в базе, полностью затираются. Максимум, что можно сделать в таком случае — импортировать часть настроек.

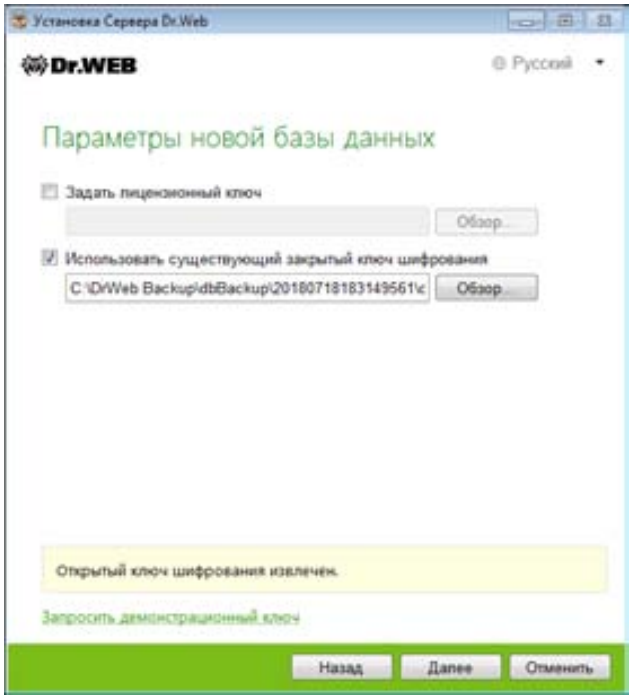
- Для обеспечения возможности работы с одной базой данных, все антивирусные Серверы кластера должны иметь одну и ту же версию. Обновлять Серверы в пределах кластера следует только из установочных пакетов, при этом требуется остановить все Серверы и осуществить их обновление по очереди. Обновление через Центр управления (переход на новую ревизию) применять не следует, поскольку при использовании общей базы данных после обновления первого Сервера все оставшиеся Серверы не смогут продолжить функционирование и обновление.
- Для функционирования кластера необходимо, чтобы на всех серверах использовались одинаковые ключи шифрования *public_key.pub* и *private_key.pri*. Если ключи ранее не создавались, то в ходе установки первого сервера кластера ключи шифрования не задаются — они будут сформированы автоматически.



Получить необходимые для продолжения развертывания ключи шифрования можно, экспортировав их в разделе **Администрирование → Администрирование → Ключи шифрования**. При этом в зависимости от того, как в дальнейшем будет развертываться кластер, могут потребоваться или оба ключа, или только *drwcsd.pri*.

Внимание! В интерфейсе Центра управления открытый и закрытый ключи получают имена private_key.pri и public_key.pub соответственно, также при экспорте к их имени добавляется номер идентификатора.

Ранее экспортированный *private_key.pri* может быть указан в ходе установки антивирусных серверов. В этом случае второй ключ формируется автоматически.



Если не указать данный ключ при установке, то сразу после установки сервера необходимо заменить оба ключа вручную. Ключ *drwcsd.pub* находится в папках Installer и webmin\install каталога установки, а *drwcsd.pri* в папке etc. После замены ключей Сервер нужно перезапустить.

- Для а втоматического применения настроек в кластере необходимо использование специального протокола, позволяющего Серверам обмениваться информацией быстрее, чем в случае, когда они связаны посредством обычных связей.

  Для включения протокола по завершении установки необходимо в разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** на вкладке **Модули** установить флажок **Протокол кластера Серверов Dr.Web**.

Для настройки параметров взаимодействия антивирусных Серверов кластера на каждом из Серверов необходимо на вкладке **Сеть → Кластер** (раздел **Конфигурация Сервера Dr.Web**) задать необходимые параметры:

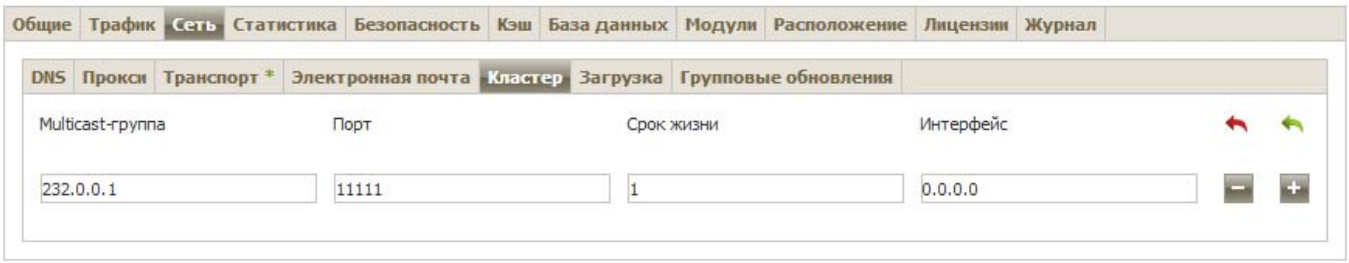
- **Multicast-группа** — IP-адрес multicast-группы, через которую серверы кластера будут осуществлять обмен информацией (по сути, мультикаст-группа тождественна мультикастному IP-адресу, на который отправляются датаграммы и, соответственно, получаются всеми узлами, которые добавились в эту группу). Возможно использование нескольких мультикаст-групп, но в этом случае каждый из Серверов должен входить только в одну мультикаст-группу. Пересечения мультикаст-групп недопустимы.
- **Порт** — номер порта сетевого интерфейса, к которому привязывается транспортный протокол для передачи информации в multicast-группу. В качестве **Порта** выбирается любой свободный порт.

- **Срок жизни** — срок жизни датаграммы при передаче данных в кластере Серверов Dr.Web.
- **Интерфейс** — IP-адрес сетевого интерфейса, к которому привязывается транспортный протокол для передачи обновлений в multicast-группу. В качестве Интерфейса используется любой сетевой адрес, по которому сервер видит остальные серверы (например, интерфейс VPN, если серверы связываются между собой посредством VPN), совпадения его с адресом Центра управления не требуется.

  Например

  •Multicast-группа: 232.0.0.1
  •Порт: 11111
  •Интерфейс: 0.0.0.0

  В данном примере для всех Серверов кластера настраиваются транспорты для всех интерфейсов. В иных случаях, например когда одна из сетей является внешней для кластера и через нее подключаются Агенты, а вторая сеть является внутрикластерной, то кластерный протокол лучше открывать только для интерфейсов внутренней сети. В этом случае в качестве интерфейсов необходимо задавать адреса вида 192.168.1.1, ..., 192.168.1.N.



Введя нужные параметры, нажмите **Сохранить** и перезапустите Сервер.

В целях исключения дублирования запросов к БД рекомендуется в серверном расписании задания **Очистка старых записей**, **Создание статистического отчета**, **Резервное копирование критичных данных сервера, Очистка старых станций, Очистка неотправленных событий** выполнять только на одном из Серверов. Если один из Серверов расположен на том же ПК, что и база данных, то эти задания необходимо выполнять именно на нем.

Важным требованием к Серверам кластера является необходимость прописать в конфигурационном файле Центра управления *webmin.conf* одинаковое DNS-имя Сервера для всех Серверов. Для этого в разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** на вкладке **Общие** заполните поле **Название Сервера**.

В случае реализации системы балансировки запросов Агентов между Серверами на DNS-сервере в сети регистрируется общее имя кластера для каждого отдельного Сервера и задается метод балансировки нагрузки.

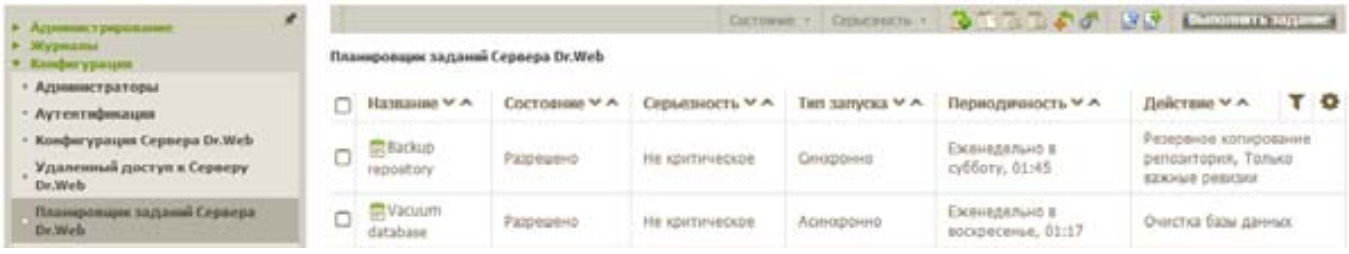
Внимание! Если запросы станций динамически распределяются при каждом подключении согласно логике динамического распределения нагрузки, то в случайный момент на каждом из Серверов может оказаться занято по одной лицензии на одного и того же Агента, что приведет к превышению числа доступных лицензии и сбою в работе Агента. В связи с этим при динамическом распределении запросов не рекомендуется использовать **Менеджер лицензий** для распространения лицензий по отдельным Серверам, в таком случае желательно использовать отдельные ключи на каждом Сервере. Однако в случае, когда динамическое распределение не используется и Агенты постоянно присоединены к одному Серверу, можно использовать Менеджер лицензий и одинаковый ключ для всех серверов.

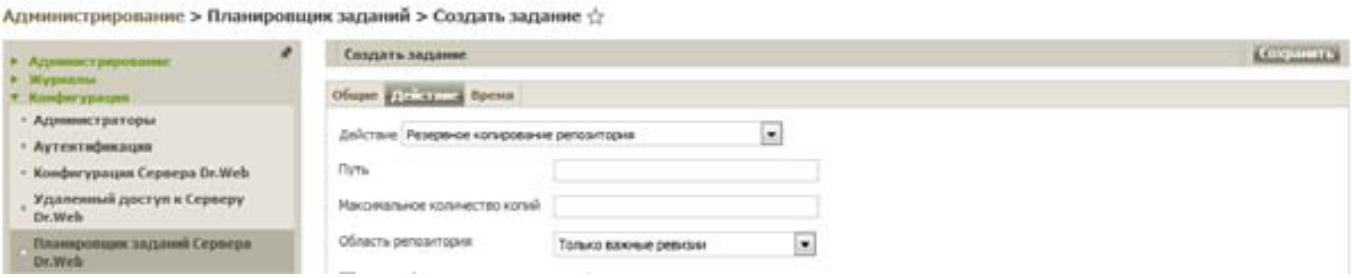
После того как на новом Сервере сети будут указаны необходимые параметры на закладке **Кластер,** можно посмотреть его статистику в разделе **Администрирование → Дополнительные возможности → Статистика Сервера Dr.Web** в подразделе **Кластер**.

Для того чтобы убедиться в работоспособности кластера, на любом из серверов кластера выберите станцию, подключенную к другому серверу, внесите изменения в ее настройки и проверьте, что изменения применились на станции сразу, без необходимости переподключения или инициации нового запроса.

8.8. Резервное копирование критичных данных сервера

Перед началом эксплуатации антивирусного ПО рекомендуется изменить настройку каталога резервного копирования критичных данных Сервера. Данный каталог желательно разместить на другом локальном диске, чтобы уменьшить вероятность одновременной потери файлов ПО Сервера и резервной копии.





Сервер регулярно сохраняет резервные копии важной информации: лицензионного ключа, содержимого базы данных, ключа шифрования, конфигурации **Сервера** и **Центра управления**. Резервные копии сохраняются в следующих каталогах относительно рабочего каталога **Сервера**:

- для ОС **Windows**: \var\Backup
- для ОС **Linux**: /var/opt/drwcs/backup
- для ОС **FreeBSD**: /var/drwcs/backup

Для этого в расписание включено ежедневное задание, выполняющее эту функцию. Если такое задание в расписании отсутствует, рекомендуется создать его.

Также рекомендуется хранить на другом ПК копии следующих файлов: ключей шифрования drwcsd.pri и drwcsd.pub, лицензионных ключей enterprise.key и agent.key, сертификата для SSL certificate.pem, закрытого ключа RSA private-key.pem и периодически сохранять там же резервные копии содержимого базы данных **Сервера** database.gz, конфигурационного файла **Сервера** drwcsd.conf и **Центра управления** webmin.conf. Таким образом, вы сможете избежать потери данных при повреждении ПК, на котором установлен **Dr.Web Сервер**, и полностью восстановить данные и функциональность **Сервера**. В случае утраты лицензионных ключей их можно запросить заново.

Резервная копия критичных данных Сервера (содержимого базы данных, лицензионного ключевого файла Сервера, закрытого ключа шифрования, конфигурационного файла и Центра управления) создается с помощью следующей команды:

drwcsd -home=<путь> backup [<каталог> [<количество>]]

При этом критичные данные копируются в указанный каталог. Параметр **home** задает каталог установки сервера, **<количество>** — количество сохраняемых копий одного и того же файла.

Пример для Windows

C:\Program Files\DrWeb Enterprise Server\bin>drwcsd -home="C:\Program Files\DrWeb Enterprise Server" backup C:\a

Резервные копии сохраняются в формате *.dz*, совместимом с *gzip* и другими архиваторами. После распаковки все файлы, кроме содержимого БД, готовы к использованию. Содержимое БД, сохраненное в резервной копии, нужно импортировать в другую БД Сервера при помощи ключа *importdb* или с помощью кнопки импорта () в интерфейсе Центра управления, и таким образом восстановить данные.

Пример для Unix:

Для сохранения базы данных необходимо остановить сервер, после чего осуществляется экспорт базы данных в файл:

для FreeBSD:
```
# /usr/local/etc/rc.d/drwcsd.sh stop

# /usr/local/etc/rc.d/drwcsd.sh exportdb
/var/drwcs/etc/dbbackup.avd
```

для Linux:
```
# /etc/init.d/drwcsd stop

# /etc/init.d/drwcsd exportdb
/var/opt/drwcs/etc/dbbackup.avd
```

После того как БД экспортирована, необходимо сохранить все конфигурационные файлы сервера, лицензионные ключи и ключи шифрования. В зависимости от используемой ОС это можно сделать командой:

для FreeBSD:
```
# cp –r /var/drwcs/etc /root/avdesk_backup
```

для Linux:
```
# cp –r /var/opt/drwcs/etc /root/avdesk_backup
```

Публичный ключ **drwcsd.pub** расположен в каталоге установки сервера *webmin\install*, его также необходимо сохранить:

для FreeBSD:
```
# cp /usr/local/drwcs/webmin/install/drwcsd.pub
/root/avdesk_backup/
```

для Linux:
```
# cp /opt/drwcs/webmin/install/drwcsd.pub
/root/avdesk_backup/
```

8.9. Восстановление ПО сервера из резервной версии

Важным нововведением 11-й версии Dr.Web ESS стала возможность использования актуальной версии Сервера для восстановления Серверов более старых версий. При этом после вынужденной работы по восстановлению Сервера вы одновременно получите актуальную версию Сервера Dr.Web со всеми ее преимуществами перед ранними версиями. Это стало возможно за счет того, что начиная с версии 11.0, Сервер Dr.Web поддерживает импорт резервных копий, созданных в более старых версиях. Для восстановления данных после падения Сервера, сделайте следующее.

1. Выберите компьютер, на который будет устанавливаться новый Сервер Dr.Web. Изолируйте данный компьютер от работающих Агентов: отключите его от сети, в которой установлены Агенты, или временно измените его IP-адрес, или воспользуйтесь любым другим наиболее удобным для вас способом.

2. Установите новый Сервер Dr.Web.

3. В разделе **Администрирование → Менеджер лицензий** добавьте лицензионный ключ от предыдущей установки Сервера и распространите его на соответствующие группы, в частности на группу **Everyone**. Шаг обязателен, если при установке Сервера не был задан лицензионный ключ.

4. Обновите репозиторий установленного Сервера с ВСО:

a) Откройте раздел Центра управления **Администрирование → Состояние репозитория**.

b) Нажмите кнопку **Проверить обновления** для проверки наличия обновлений всех продуктов на ВСО и загрузки имеющихся обновлений с серверов ВСО.

5. При наличии новых версий ПО Сервера произведите обновление до последней версии:

a) Откройте раздел Центра управления **Администрирование → Сервер Dr.Web**.

b) Для перехода к списку версий Сервера нажмите на текущую версию Сервера или на кнопку **Список версий**. Откроется раздел **Обновления Сервера Dr.Web** со списком доступных обновлений и резервных копий Сервера.

c) Для перехода к новой версии Сервера установите опцию напротив последней версии в списке **Все версии**. Нажмите кнопку **Сохранить**.

d) Дождитесь завершения процесса обновления Сервера.

6. Остановите Сервер.

7. Для получения открытого ключа шифрования из резервной копии закрытого ключа воспользуйтесь утилитой drwsign, находящейся в подкаталоге \bin каталога установки Сервера:

drwsign extract [-private-key=<*закрытый_ключ*>] <*открытый_ключ*>

В качестве <*закрытый ключ*> и <*открытый ключ*> укажите соответствующие пути, по которым расположен закрытый ключ, а также куда следует разместить созданный открытый ключ.

8. Замените критичные данные Сервера на данные, полученные из резервной копии:

Операционная система	**Открытый ключ шифрования**	**Конфигурационные файлы**
Windows	webmin\install в каталоге установки Сервера	etc в каталоге установки Сервера
Linux	/opt/drwcs/webmin/install	/var/opt/drwcs/etc
FreeBSD	/usr/local/drwcs/webmin/install	/var/drwcs/etc

9. Настройте базу данных.

a) Внешняя база данных:

Дальнейших действий по подключению базы данных к Серверу не требуется (при условии, что сохранен конфигурационный файл Сервера).

Если версия Сервера, установленная из последних обновлений, новее версии утраченного Сервера, произведите обновление внешней базы данных при помощи команды upgradedb:

- для ОС Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" upgradedb
```

- для ОС Linux:

```
/etc/init.d/drwcsd upgradedb
```

- для ОС FreeBSD:

```
/usr/local/etc/rc.d/drwcsd.sh upgradedb
```

b) Резервная копия базы данных внешней или встроенной:

При использовании внешней базы данных предварительно произведите ее очистку при помощи команды cleandb (см. Приложение H4.3).

Импортируйте базу данных из соответствующего файла резервной копии с об новлением формата базы данных до версии установленного Сервера при помощи команды upimportdb:

- для ОС Windows:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all upimportdb "<путь_к_бэкап_файлу>\database.gz"
```

- для ОС Linux:

```
/etc/init.d/drwcsd upimportdb "<путь_к_бэкап_файлу>/database.gz"
```

- для ОС FreeBSD:

```
/usr/local/etc/rc.d/drwcsd.sh upimportdb "<путь_к_бэкап_файлу>/database.gz"
```

На все замененные файлы Сервера необходимо установить те же системные права, что были выбраны при предыдущей (утраченной) установке Сервера.

Для ОС семейства UNIX: rw для drwcs:drwcs.

10. Запустите Сервер.

11. Убедитесь в сохранности и актуальности данных, полученных из резервной копии базы данных: настроек Агентов, состояния дерева антивирусной сети и т. п.

12. Восстановите доступность Сервера для Агентов, исходя из способа изоляции Сервера, выбранного на шаге 1.

Если какие-либо Агенты были установлены после создания последней резервной копии, они не смогут подключиться к Серверу после восстановления базы данных из этой резервной копии. Такие станции можно дистанционно перевести в режим новичков. В разделе **Администрирование → Конфигурация Сервера Dr.Web** на вкладке **Общие** установите флажок **Переводить неавторизованных в новички**. В выпадающем списке **Режим регистрации новичков** выберите вариант **Автоматически разрешать доступ**. Нажмите **Сохранить** и перезагрузите Сервер.

После того как все станции благополучно подключатся к новому Серверу, измените данные настройки Сервера на настройки, принятые в соответствии с политикой вашей компании.

8.10. Восстановление утерянного пароля администратора Сервера Dr.Web

В случае если пароль администратора для доступа к Серверу Dr.Web был утерян, существует возможность его просмотра или изменения с использованием прямого доступа к базе данных Сервера:

a) При использовании встроенной базы для просмотра и смены пароля администратора используется утилита **drwidbsh**, входящая в дистрибутив Сервера (см. п. H9.2. Утилита администрирования встроенной базы данных).

b) Для внешней БД используйте соответствующий sql-клиент.

Примечание. Параметры учетных записей администраторов хранятся в таблице admins.

Примеры использования утилиты drwidbsh

1. Запустите утилиту **drwidbsh3** с указанием пути до файла БД:

- Для встроенной БД под ОС Linux:

```
/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
```

- Для встроенной БД под ОС Windows:

```
"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb Server\var\database.sqlite"
```

Если используется встроенная база данных старого формата IntDB, например, в случае обновления Сервера с версии 6, то имя базы данных по умолчанию — **dbinternal.dbs**, а утилита для управления базой данных — **drwidbsh**.

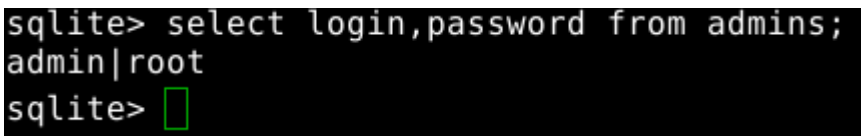
2. Для просмотра всех данных, хранящихся в таблице **admins**, выполните команду:

```
select * from admins;
```

3. Для просмотра имен и паролей для всех учетных записей администраторов выполните команду:

```
select login,password from admins;
```

4. Результат для варианта, когда существует только одна учетная запись с именем admin и у нее пароль root, приведен на скриншоте:



5. Для изменения пароля используйте команду update. Пример команды, изменяющей пароль от учетной записи admin на qwerty:

```
update admins set password='qwerty' where login='admin';
```

6.Для выхода из утилиты выполните команду:

```
.exit
```

Описание работы утилиты drwidbsh приведено в приложении Н9.2. Утилита администрирования встроенной базы данных.

8.11. Восстановление связей с Агентами после переустановки Сервера

Ключевой момент в клиент-серверном взаимодействии Агентов и Сервера состоит в том, что они по умолчанию поддерживают шифрование передаваемых между ними данных.

Приватный (drwcsd.pri) и публичный (drwcsd.pub) ключи шифрования создаются при установке сервера. При установке Агента с Сервера из каталога C:\Program Files\DrWeb Server\Installer публичный ключ копируется на рабочую станцию. Приватный ключ всегда остается исключительно на сервере.

Если эта пара ключей не совпадает, то есть публичный ключ агента не подходит к приватному ключу сервера, то сервер обрывает соединение, считая ключ скомпрометированным. При этом Агент выдает пользователю сообщение, что подключиться к серверу не удалось.

Самая частая причина такой проблемы — это переустановка сервера, при которой автоматически генерируется новая пара ключей, делая старый публичный ключ непригодным к использованию. Далее есть два варианта действий:

1) Если планируется переустановка сервера с сохранением резервной копии ключей шифрования, то их можно указать как непосредственно в момент установки нового сервера, так и после нее. Для загрузки сохраненных ключей в уже установленный сервер, необходимо сделать следующее:

1) Остановить службу Сервера через меню **Пуск** или Центр управления.

2) В папку установки сервера (по умолчанию C:\Program Files\DrWeb Server\Installer) скопировать с заменой ранее сохраненный публичный ключ drwcsd.pub.

3) В папку настроек сервера (по умолчанию C:\Program Files\DrWeb Server\etc скопировать с заменой ранее сохраненный приватный ключ drwcsd.pri.

4) Вновь запустить службу Сервера.

2) Если старые ключи не сохранялись, то на вновь установленном Сервере необходимо сгенерировать новую пару ключей, после чего вручную установить их на Агенты. Для этого потребуется:

1) Сохранить приватный ключ drwcsd.pri и сервисную утилиту drwsign.exe на сменный носитель или сетевой ресурс, куда имеют доступ все ПК Агентов.

2) Загрузить указанные выше файлы на компьютер Агента, либо передав через сменный носитель, либо скачав по локальной сети.

3) На ПК агента через командную строку (запускать cmd.exe необходимо от имени Администратора) выполнить следующую команду:

**путь_к_файлу*\drwsign.exe extract -private-key=*путь_к_файлу*\drwcsd.pri "c:\program files\DrWeb\drwcsd.pub"*

4) Перезагрузить компьютер и подождать несколько минут, чтобы убедиться, что Агент корректно подключился к Серверу.

5) Повторить действия 2–4 для всех агентских ПК.

Примечание. Использование шифрования соединения Агентов и Сервера можно отключить, активировав на Сервере параметр **Разрешить работу без открытого ключа**. Но делать это крайне не рекомендуется, так как при этом резко упадет защищенность передачи данных. Также использование этого параметра не поможет решить проблему, если старый приватный ключ уже удален с Сервера — Агенты не смогут подключиться к нему, чтобы «принять» этот параметр.

8.12. Восстановление утраченного пароля администратора Сервера Dr.Web

В случае если пароль администратора для доступа к Серверу Dr.Web был утерян, существует возможность его просмотра или изменения с использованием прямого доступа к базе данных Сервера:

a) При использовании встроенной базы для просмотра и смены пароля администратора используется утилита drwidbsh, входящая в дистрибутив Сервера (см. п. H9.2. Утилита администрирования встроенной базы данных).

b) Для внешней БД используйте соответствующий sql-клиент.

Параметры учетных записей администраторов хранятся в таблице admins.

Примеры использования утилиты drwidbsh

1. Запустите утилиту drwidbsh3 с указанием пути до файла БД:

- Для встроенной БД под ОС Linux:

/opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite

- Для встроенной БД под ОС Windows:

"C:\Program Files\DrWeb Server\bin\drwidbsh3" "C:\Program Files\DrWeb Server\var\database.sqlite"

Если используется встроенная база данных старого формата IntDB, например в случае обновления Сервера с версии 6, то имя базы данных по умолчанию — dbinternal.dbs, а утилита для управления базой данных — drwidbsh.

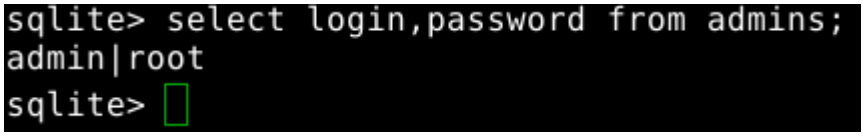
2. Для просмотра всех данных, хранящихся в таблице admins, выполните команду:

*select * from admins;*

3. Для просмотра имен и паролей для всех учетных записей администраторов выполните команду:

select login,password from admins;

4. Результат для варианта, когда существует только одна учетная запись с именем admin и у нее пароль root, приведен на скриншоте:



5. Для изменения пароля используйте команду update. Пример команды, изменяющей пароль от учетной записи admin на qwerty:

update admins set password='qwerty' where login='admin';

6. Для выхода из утилиты выполните команду:

.exit

Описание работы утилиты drwidbsh приведено в приложении Н9.2. Утилита администрирования встроенной базы данных.

8.12.1. Оптимизация работы сервера антивирусной защиты для работы в условиях повышенной нагрузки

8.12.1.1. Настройка БД PostgreSQL

Если эксплуатация Серверов Dr.Web планируется в условиях высокой нагрузки (более 10000 Агентов), то для нормальной работы антивирусной сети необходимо использовать внешнюю БД типа **PostgreSQL.** Поэтому важно правильно сконфигурировать данную БД, настроив ее параметры в файле *postgresql.conf*.

Внимание! Настройки в примере ниже приводятся для сервера/БД, обслуживающего около 200000 агентов, из которых 40000 находятся в режиме онлайн. Предполагается, что сервер, на котором размещена БД, установлено как минимум 4 ГБ ОЗУ.

Файл postgresql.conf:

```
shared_buffers = 1000MB

temp_buffers = 32MB

work_mem = 64MB

maintenance_work_mem = 128MB

max_stack_depth = 4MB

max_fsm_pages = 350000

max_fsm_relations = 1000

fsync = off

full_page_writes = off
```

```
effective_cache_size = 20000

constraint_exclusion = on

autovacuum = off

datestyle = 'iso, dmy'

standard_conforming_strings = on
```

8.12.1.2. Организация резервного копирования таблиц БД

Начиная с пяти тысяч уникальных рабочих станций (записей типа ID), содержащихся в БД, рекомендуется отказаться от использования встроенных средств Сервера Dr.Web, предназначенных для резервного копирования базы данных. Нужно использовать стандартную утилиту копирования/восстановления записей, входящую в состав пакета поставки СУБД. При этом необходимо отключить стандартное задание на резервирование, выполняемое Сервером по расписанию. Для этого в окне **Администрирование → Конфигурация → Расписание Сервера Dr.Web** отметьте флажком запись **Резервное копирование критичных данных сервера (Backup sensitive data)** и с помощью кнопки **Состояние** укажите **Запретить выполнение**. Нажмите **Да** в появившемся окне запроса подтверждения действия.

Для автоматизации процесса резервного копирования записей БД целесообразно использовать скрипт, который будет запускаться по расписанию операционной системы (например, *cron*) и выполнять следующие процедуры: 1) временный останов Сервера Dr.Web; 2) дамп содержимого требуемой БД; 3) запуск Сервера Dr.Web.

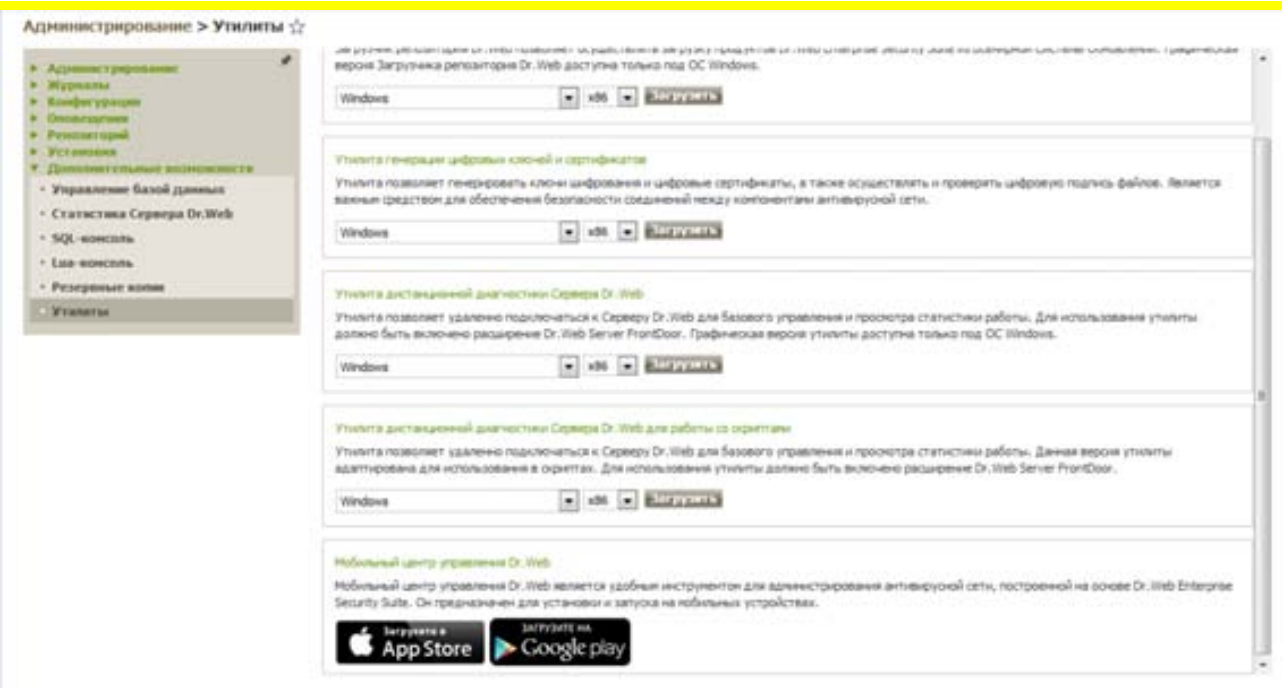
Остановка Сервера необходима для предотвращения изменения таблиц БД в процессе ее копирования.

Дамп базы данных выполняется следующей командой:
```
# pg_dump -E UTF-8 -F t -U postgres -f /var/drwcs/backup/current.dump drwcs_db
```

Пользователь, от имени которого производится подключение к БД (опция -U), и путь к папке с дампами могут меняться в зависимости от операционной системы.

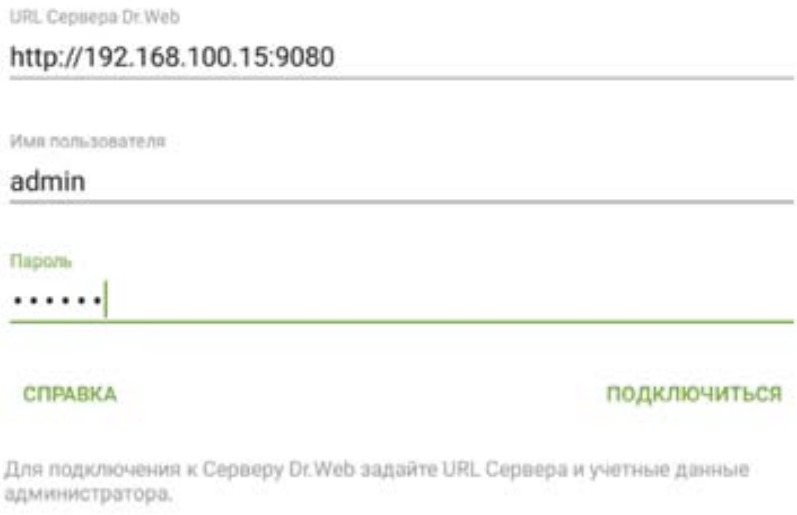
8.13. Управление антивирусной сетью из Мобильного центра управления

Мобильный центр управления доступен для установки на мобильные устройства с iOS и Android. Для того чтобы загрузить Мобильный центр управления, необходимо зайти на страницу **Администрирование → Дополнительные возможности → Утилиты.**



Внимание! Мобильный центр управления должен быть установлен только на личное или рабочее устройство администратора антивирусной сети или лица, его замещающего.

Для запуска Мобильного центра управления нажмите на его иконку (), в появившемся окне введите параметры подключения и нажмите Подключиться.



Внимание! Для обеспечения возможности подключения к Серверу Dr.Web с помощью мобильного центра управления необходимо выполнить ряд условий:

1) Подключение должно осуществляться по протоколу http на порт 9080 Сервера.
2) Сервер должен иметь «белый» IP-адрес и быть доступным из сети Интернет. В случае использования NAT и «серых» IP подключение будет невозможно.
3) Флажок **Перенаправлять на защищенное соединение** (вкладка **Безопасность** раздела **Конфигурация веб-сервера**) должен быть снят.
4) Адрес Сервера, к которому будет происходить подключение, должен быть указан в следующих разделах Центра управления:
    1) на вкладке **Общие** и **Транспорт** в разделе **Конфигурация веб-сервера** ;
    2) на вкладке **Общие** в разделе **Удаленный доступ к Серверу Dr.Web**.

После подключения автоматически открывается окно с информацией о станциях сети, статистикой сканирования и актуальности антивирусной защиты.

Используя возможности Мобильного центра управления, администратор может произвести сканирование групп и отдельных станций.

Также можно произвести их обновление, перезагрузку или отправить сообщение.

Кроме того, Мобильный центр управления позволяет:

1) просматривать и управлять Карантином,
2) обновлять репозиторий,
3) просматривать полученные Сервером уведомления,
4) просматривать статистику антивирусной сети,
5) подтверждать, назначая первичную группу и отклонять новые станции.

9. Обновление антивирусной сети Dr.Web Enterprise Security Suite

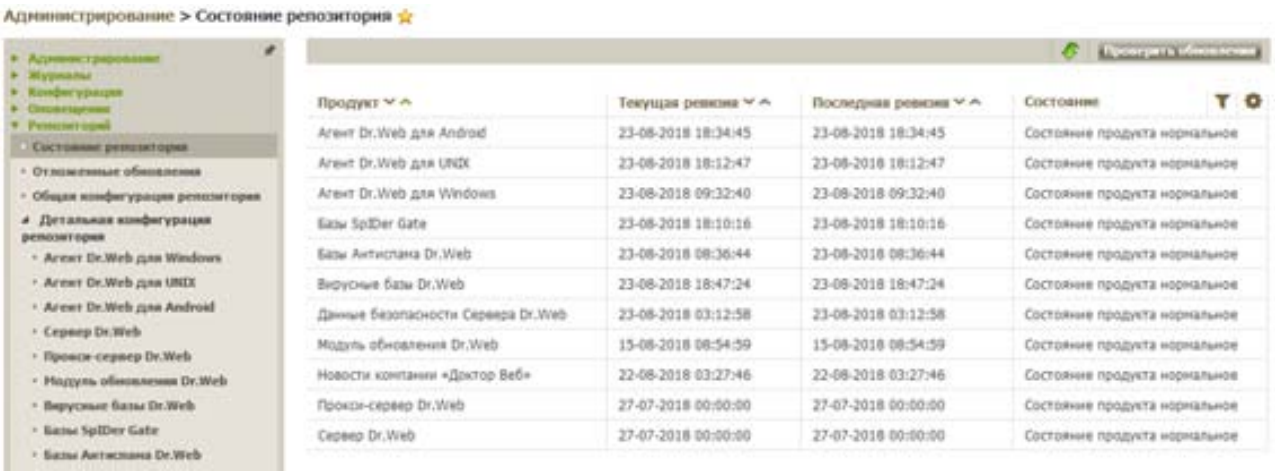
9.1. Обновление антивирусного ПО на защищаемых узлах сети

Внимание! Служба обновления может не запускаться, если установленный язык системы для программ, не поддерживающих Unicode, не соответствует языку, используемому в путях установки Агента и антивирусного пакета. Проблема устраняется при установке соответствующего языка системы для программ, не поддерживающих Unicode.

9.1.1. Проведение обновлений автоматически и вручную

Перед началом обновления антивирусной системы **Dr.Web ESS** в целом и е е отдельных компонентов настоятельно рекомендуем проверить корректность настроек протокола TCP/IP для возможности доступа в Интернет всех компонентов антивирусной сети. В частности, должна быть включена и корректно настроена служба DNS.

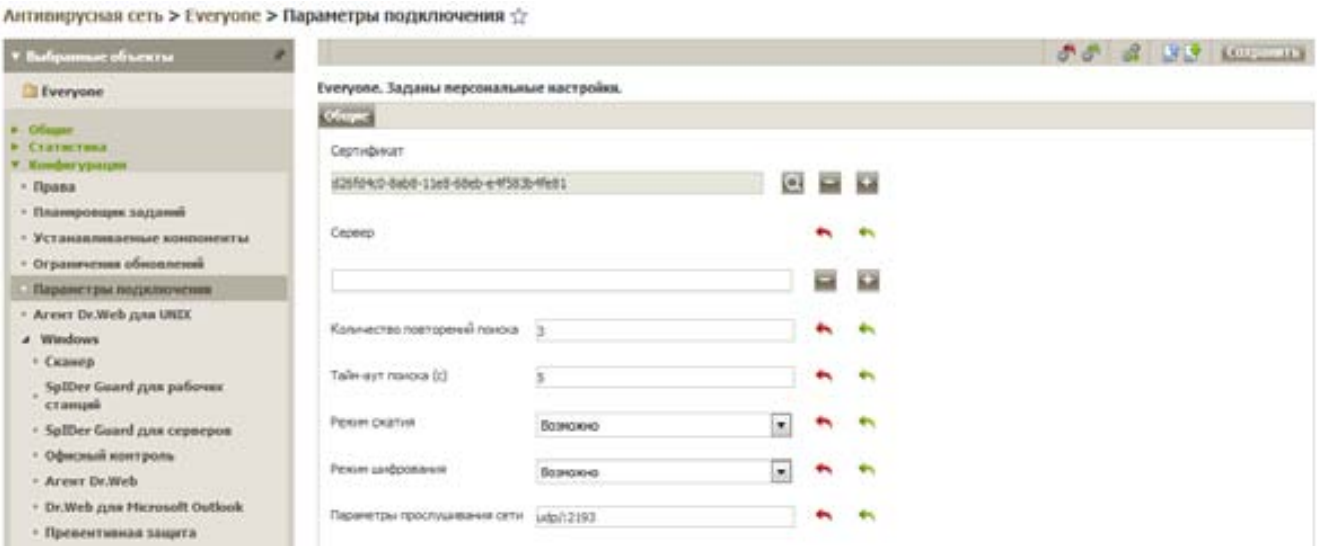
Чтобы проверить наличие обновления продуктов Dr.Web Enterprise Security Suite на сервере обновлений ВСО , выберите пункт **Администрирование → Репозиторий → Состояние репозитория.** В открывшемся окне отображается информация обо всех продуктах в репозитории, а также дата их последней ревизии и ее текущее состояние. Для проверки наличия обновлений нажмите **Проверить обновления**. Если какой-либо продукт устарел, то его обновление произойдет автоматически в процессе проверки.



После обновления репозитория Сервера Dr.Web обновления компонентов на рабочих станциях будут проведены автоматически, за исключением тех станций и групп, для которых настроены отложенные обновления.

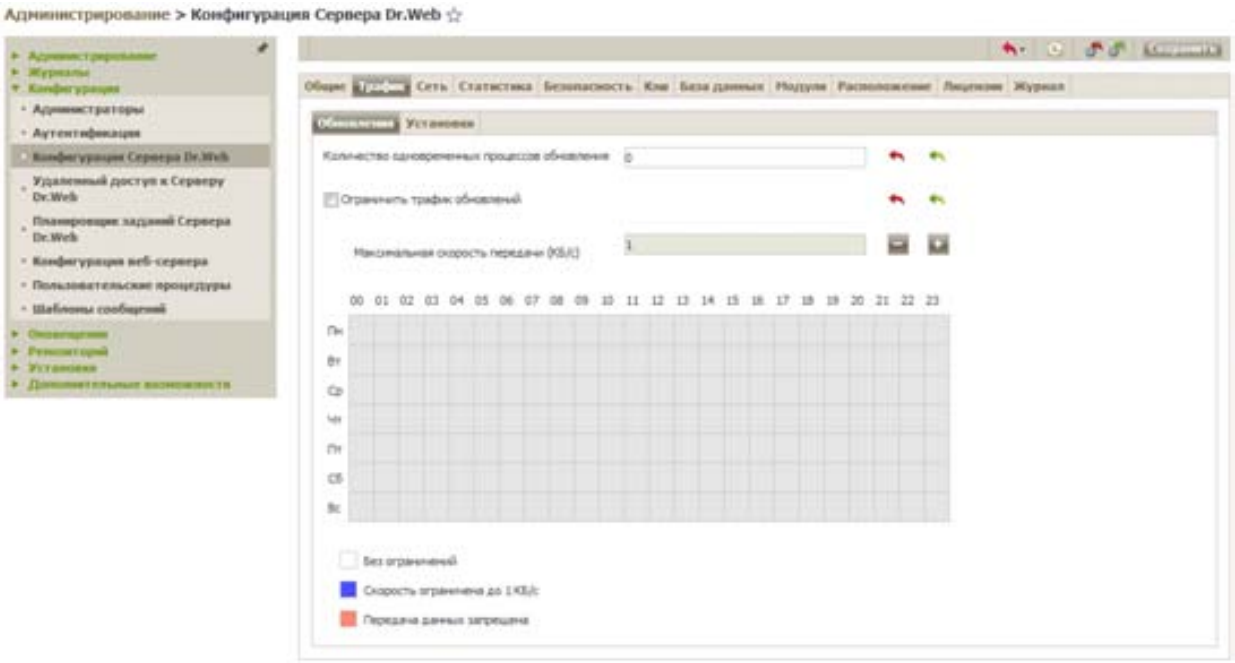
9.1.2. Настройка параметров обновлений рабочих станций и серверов

Для того чтобы задать источник обновлений (по умолчанию установленный Агент работает в multicast-режиме и ищет ближайший доступный сервер), выберите рабочую станцию или группу в меню **Антивирусная сеть**, после чего в разделе **Конфигурация → Параметры подключения** задайте адрес источника обновлений.



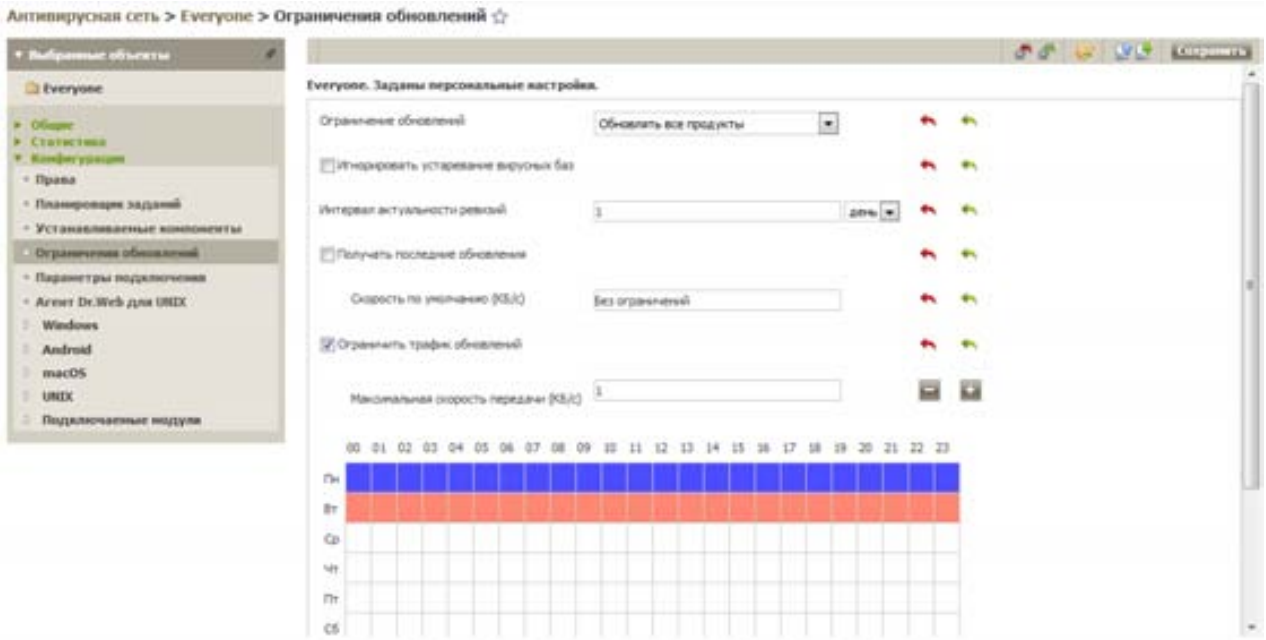
В антивирусной сети **Dr.Web Enterprise Security Suite** существует возможность ограничить скорость передачи обновлений между **Сервером** и **Агентами**.

Для ограничения общей скорости передачи обновлений для всех станций настройка ограничений осуществляется с помощью параметра **Ограничить трафик обновлений**, вкладки **Трафик → Обновления** раздела **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**.



Персональное ограничение скорости передачи обновлений для конкретных станций или групп станций осуществляется в разделе настройки станций. Выберите рабочую станцию или группу в меню **Антивирусная сеть**, после чего в разделе **Конфигурация → Ограничения обновлений** отметьте флажком пункт **Ограничить трафик обновлений.**

В обоих случаях вы можете настроить время, когда скорость обновлений снижена до указанного максимального значения (синие поля), когда — обновления запрещены (красные поля), а когда ограничения не действуют (белые поля).



Для рабочих станций в выпадающем списке **Ограничение обновлений** можно выбрать режим ограничений:

- **Обновлять все продукты** — не устанавливать ограничения на распространение обновлений на станции.
- **Запретить все обновления** — запретить распространение всех обновлений на станции в промежутках времени, заданных ниже в таблице **Расписание обновления станций**.
- **Обновлять только базы** — запретить распространение только обновлений программных модулей в промежутках времени, заданных ниже в таблице **Расписание обновления станций**. Обновление вирусных баз будет осуществляться без изменений в штатном режиме.

Установите флажок **Игнорировать устаревание вирусных баз**, чтобы снизить серьезность состояний станций с устаревшими вирусными базами. Если флажок установлен, то станции с устаревшими вирусными базами будут отображаться в антивирусной сети с общим значком, а в разделе **Состояние** у станций будет серьезность **Низкая**. Если флажок снят, то станции с устаревшими вирусными базами будут отображаться в антивирусной сети со значком (если включена опция на панели инструментов **Настройки вида дерева** → **Показывать серьезность состояния станций**), а в разделе **Состояние** у станций будет серьезность **Максимальная** или **Высокая**.

В поле **Интервал актуальности ревизий** задается временной интервал, в течение которого ревизии продуктов, установленных на станциях, будут считаться актуальными при появлении более новых ревизий в репозитории Сервера.

Установите флажок **Получать последние обновления**, чтобы станция получала все обновления компонентов, вне зависимости от ограничений, заданных в разделе Детальная конфигурация репозитория.

Если флажок снят, станция будет получать только обновления, помеченные в качестве текущих обновлений для распространения.

Установите флажок **Ограничить трафик обновлений**, чтобы ограничить объем сетевого трафика при передаче обновлений между Сервером и Агентами.

Если флажок снят, обновления для Агентов передаются без ограничения полосы пропускания сетевого трафика.

Если флажок установлен, задайте следующие поля:

- В поле **Скорость по умолчанию** задается значение максимальной скорости передачи обновлений, используемое по умолчанию, т. е. если не задано никакое другое ограничение (пустые белые ячейки в таблице расписания). Также значение скорости по умолчанию применяется для периодов, когда передача данных запрещена, но процесс обновления уже был запущен (см. ниже).
- В поле **Максимальная скорость передачи (КБ/с)** задается значение максимальной скорости передачи обновлений. При этом обновления будут передаваться в пределах заданной полосы пропускания совокупного сетевого трафика обновлений всех Агентов.
  Допускается задание до пяти ограничений на скорость передачи обновлений. Для добавления еще одного поля ограничения скорости нажмите кнопку  . Для удаления ограничения нажмите кнопку  напротив ограничения, которое нужно удалить.

Для значений полей **Скорость по умолчанию** и **Максимальная скорость передачи (КБ/с)** существуют следующие ограничения:

- Запрещено задавать значение 0. Минимальное допустимое значение ограничения — 1 КБ/с.
- Пустое значение (поле не заполнено) снимает все ограничения на трафик обновлений для соответствующего периода времени.

В таблице расписания задается режим ограничения на передачу данных отдельно на каждые 30 минут каждого дня недели.

Для изменения режима ограничений передачи данных нажмите на соответствующий блок таблицы. Также поддерживается выбор нескольких временных блоков по принципу drag-and-drop.

Цвет ячеек изменяется циклически согласно цветовой схеме, приведенной под таблицей в зависимости от количества вариантов ограничения скорости.

В периоды времени, которые соответствуют значению **Передача данных запрещена**, запрещено начинать передачу обновлений. Если при наступлении данного периода передача обновлений уже была запущена, она не будет прервана, но максимальная скорость передачи будет ограничена значением, заданным в поле **Скорость по умолчанию**.

После завершения редактирования нажмите кнопку **Сохранить** для принятия внесенных изменений.

Ограничение трафика обновлений осуществляется по следующему принципу:

1. Если включено ограничение на общую скорость передачи обновлений в настройках **Сервера**, то суммарная скорость передачи обновлений от **Сервера** всем станциям не превысит указанного значения. При этом:

a. Вне зависимости от различий в пропускной способности каналов связи между **Сервером** и станциями, скорость передачи обновлений делится поровну между всеми станциями.

b. Если пропускная способность канала между **Сервером** и станцией меньше полученного среднего значения скорости для одной станции согласно пункту **a)**, для такой станции устанавливается ограничение передачи обновлений, равное максимальной ширине канала до этой станции. Оставшееся значение общего ограничения аналогично пункту **a)** делится поровну для остальных станций.

2. Если включено персональное ограничение на скорость передачи обновлений в настройках группы или конкретной станций, то скорость передачи обновлений на эти группы или станцию не превысит указанного значения. На все остальные станции ограничение не распространяется, и передача обновлений осуществляется с максимальной скоростью.

3. Если включено ограничение на общую скорость передачи обновлений в настройках **Сервера** и персональное ограничение на группу или станцию, то:

a. Скорость передачи обновлений на персонально ограниченные группы или станции не превысит значения, заданного в разделе настроек этих групп и станций.
b. Для передачи обновлений на остальные станции, общее ограничение скорости передачи обновлений с учетом вычета ограничения станции из п. **a)** делится поровну.
c. Если пропускная способность канала между **Сервером** и станцией, не ограниченной индивидуально, меньше полученного среднего значения скорости для одной станции согласно пункту **b)**, для такой станции устанавливается ограничение передачи обновлений, равное максимальной ширине канала до этой станции. Оставшееся значение общего ограничения аналогично пункту **b)** делится поровну для остальных станций, не ограниченных индивидуально.

На панели инструментов также доступны следующие опции для управления содержимым раздела:

Установить все параметры в начальные значения — восстановить значения, которые все параметры данного раздела имели до текущего редактирования (последние сохраненные значения).

Установить все параметры в значения по умолчанию — установить для всех параметров данного раздела значения, заданные по умолчанию.

Распространить эти настройки на другой объект — скопировать настройки из данного раздела в настройки другой станции, группы или нескольких групп и станций.

Установить наследование настроек от первичной группы — удалить персональные настройки станций и установить наследование настроек данного раздела от первичной группы.

Скопировать настройки из первичной группы и установить их в качестве персональных — скопировать настройки данного раздела из первичной группы и задать их для выбранных станций. Наследование при этом не устанавливается и настройки станции считаются персональными.

Экспортировать настройки из данного раздела в файл — сохранить все настройки из данного раздела в файл специального формата.

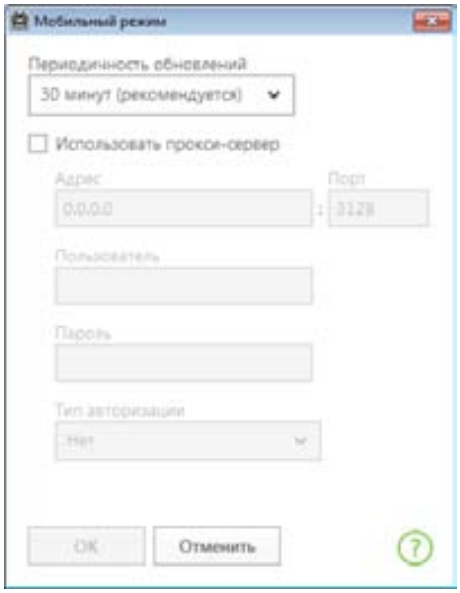
Импортировать настройки в данный раздел из файла — заменить все настройки в данном разделе настройками из файла специального формата.

9.1.2.1. Обновление мобильных Агентов Dr.Web Agent

Вариант **Мобильный режим** будет доступен настройках Агента (**Настройки → Основные → Сервер → Дополнительные настройки → Использовать Мобильный режим, если отсутствует подключение к серверу**), при условии что в правах станции

разрешен Мобильный режим использования ВСО Dr.Web (**Антивирусная сеть → Конфигурация → Windows → Агент Dr.Web**, вкладка **Мобильность**, параметр **Использовать Мобильный режим**). Использовать мобильный режим удобно, когда компьютер пользователя часто бывает вне антивирусной сети (например, это рабочий ноутбук сотрудника, часто бывающего в командировках) и не имеет связи с Сервером Dr.Web.

Чтобы задать настройки Мобильного режима работы Агента, нажмите кнопку **Настроить...** и задайте нужные параметры в открывшемся окне.



В Мобильном режиме Агент пытается подключиться к Серверу, делает три попытки и, если это не удалось, выполняет HTTP-обновление напрямую с ВСО. Попытки найти Сервер идут непрерывно с интервалом около минуты.

При использовании прокси-сервера укажите адрес и порт прокси-сервера, а также параметры авторизации.

Во время функционирования Агента в мобильном режиме связь Агента с Сервером Dr.Web прерывается. Все изменения, которые задаются на Сервере для такой станции, вступят в силу, как только мобильный режим работы Агента будет выключен, и связь с Сервером возобновится.

В мобильном режиме производится обновление только вирусных баз.

9.2. Управление ключевыми файлами

Права пользователя на антивирусную систему Dr.Web ESS регулируются при помощи ключевых файлов, предназначенных для передачи защищаемым станциям сети. Для установки и функционирования Сервера Dr.Web лицензионный ключ не требуется.

Внимание! Ключевой файл имеет формат, защищенный от редактирования при помощи механизма электронной подписи. Редактирование файла делает его недействительным. Чтобы избежать случайной порчи ключевого файла, не следует модифицировать ключевой файл и/или сохранять его при закрытии текстового редактора.

Состав и стоимость лицензии на использование антивирусного решения **Dr.Web® ESS** зависят от количества защищаемых станций в сети (в том числе серверов и других объектов, входящих в состав сети **Dr.Web® ESS** как защищаемые станции).

Ключевые файлы поставляются пользователю в виде zip-архивов, содержащих один или несколько ключевых файлов вида *agent.key*. Их количество определяется запросами клиента, исходя из структуры его сети, по умолчанию выдается один ключ. Лицензионные ключевые файлы могут входить в комплект антивируса **Dr.Web® ESS** при покупке. Однако, как правило, поставляются только серийные номера.

Пользователь может получить ключевые файлы одним из следующих способов.

- По электронной почте. Ключевые файлы формируются в ходе регистрации серийного номера на специальном веб-сайте (адрес сайта регистрации https://products.drweb.ru/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. Вы также сможете загрузить ключевые файлы непосредственно с указанного сайта.
- Вместе с дистрибутивом продукта, если лицензионные файлы были включены в состав дистрибутива продукта при его комплектации.
- На отдельном носителе в виде файла.

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.ru/demoreq/biz/v2. Ваш запрос будет рассмотрен в индивидуальном порядке. В случае положительного решения архив с ключевыми файлами будет выслан по указанному вами адресу.

Использование полученных ключевых файлов в процессе установки программы описывается в разделах, рассказывающих о возможных вариантах установки Dr.Web Enterprise Server.

Использование ключевых файлов для уже развернутой антивирусной сети описано в разделе **Обновление антивирусной сети Dr.Web Enterprise Security Suite**.

9.2.1. Менеджер лицензий

Сам антивирусный сервер не лицензируется и может быть установлен без лицензионного ключа. Ключ может быть добавлен позднее как локально, так и получен через межсерверную связь.

UUID Сервера, который в предыдущих версиях Центра управления хранился в лицензионном ключе Сервера, начиная с версии **10.0** хранится в конфигурационном файле Сервера. При

установке Сервера генерируется новый UUID. Если при запуске инсталлятора указан аргумент -activation-key=<*ключ_сервера*>, UUID берется из указанного ключа Сервера и записывается в конфигурационный файл Сервера.

При обновлении Сервера с более ранних версий, UUID берется из ключа Сервера предыдущей версии и записывается в конфигурационный файл Сервера.

В случае обновления кластера Серверов ответственный за обновление БД Сервер получает лицензионный ключ, для остальных Серверов необходимо добавлять лицензионные ключи вручную.

Если список разрешенных антивирусных компонентов у нескольких ключей одного объекта различается, список разрешенных для станций компонентов определяется пересечением множеств компонентов в ключах. Например, если для группы станций назначены ключ с поддержкой **Антиспама** и ключ без поддержки **Антиспама**, то для станций установка **Антиспама** будет **запрещена**.

Настройки лицензирования для объекта рассчитываются исходя их всех назначенных для этого объекта ключей. Если срок действия лицензионных ключей объекта различается, то по истечении ключа с минимальным сроком действия вам необходимо заменить или удалить истекший ключ вручную. Если истекший ключ накладывал ограничения на установку антивирусных компонентов, необходимо произвести корректировку настроек объекта лицензирования в разделе **Устанавливаемые компоненты**.

Управление ключами на **Сервере Dr.Web** осуществляется с помощью **Менеджера лицензий**, доступного в разделе **Администрирование → Администрирование** Центра управления.

Главное окно **Менеджера лицензий** содержит иерархический список, узлами которого являются лицензионные ключи, а также станции и группы, для которых назначены лицензионные ключи.

Для управления лицензионными ключами используются элементы Панели инструментов:

Панель инструментов содержит следующие элементы управления:

Опция	Описание	Зависимость от объектов в дереве ключей
Добавить лицензионный ключ	Добавить новую запись о лицензионном ключе.	Опция всегда доступна. Особенности функционала зависят от того, выбран ли объект в дереве ключей или нет

Опция	Описание	Зависимость от объектов в дереве ключей
		(см. Добавление нового лицензионного ключа).
Удалить выбранные объекты	Удалить связь между ключом и объектом лицензирования.	Опция доступна, если в дереве выбран объект лицензирования (станция, группа или политика) или лицензионный ключ.
Распространить ключ на группы и станции	Заменить или добавить выбранный ключ к объекту лицензирования.	Опция доступна, если в дереве выбран лицензионный ключ.
Экспортировать ключ	Сохранить локальную копию файла лицензионного ключа.	
Проверить наличие обновлений и заменить лицензионные ключи	Проверить наличие обновлений, располагаемых на ВСО, для всех ключей. При наличии обновлений скачать ключи и провести замену (см. Автоматическое обновление лицензий).	Опция всегда доступна. Действие распространяется на все лицензионные ключи в дереве.
Распространить ключ на соседние Серверы	Передать лицензии из выбранного ключа соседним Серверам.	Опция доступна, если в дереве выбран лицензионный ключ.

Настройки вида дерева позволяют изменять вид иерархического дерева:

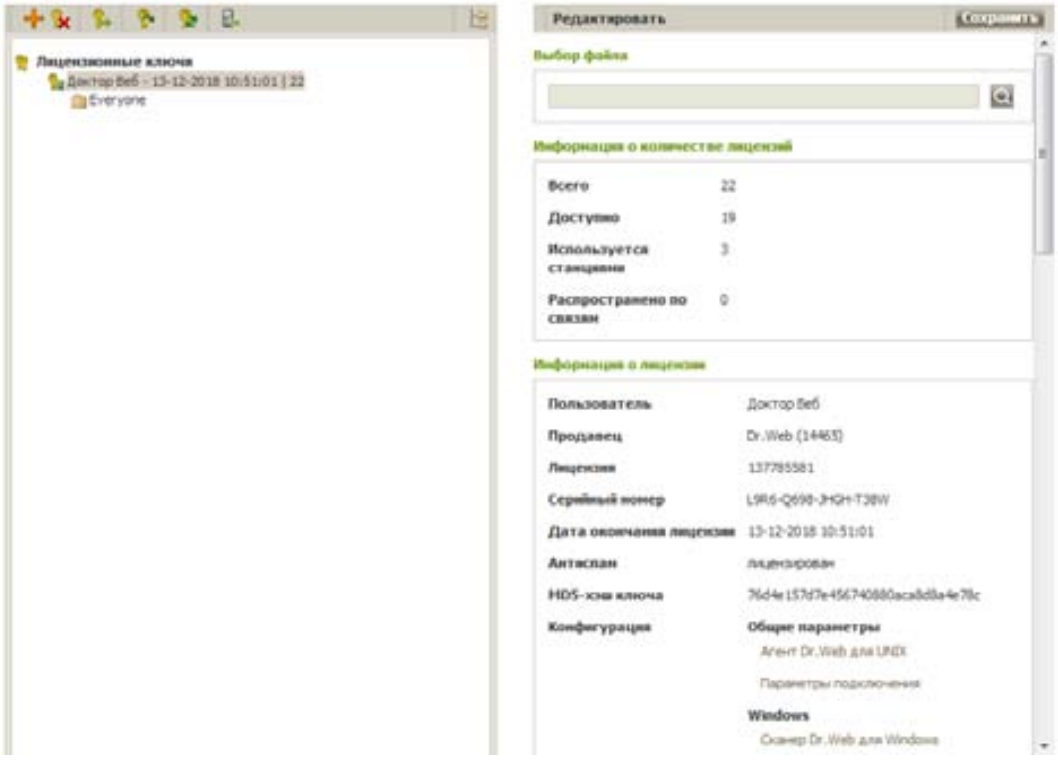
- Флажок **Показывать количество лицензий** включает/отключает отображение в дереве ключей общего количества лицензий, предоставляемых лицензионными ключевыми файлами.
- Для изменения структуры дерева используйте следующие опции:
  - Опция **Ключи** предписывает отображать все лицензионные ключи антивирусной сети в качестве корневых узлов иерархическое дерева. При этом вложенными элементами лицензионных ключей являются все группы, станции и политики, для которых назначены эти ключи. Данное представление дерева является основным и позволяет управлять объектами лицензирования и лицензионными ключами.
  - Опция **Группы** предписывает отображать в качестве корневых узлов иерархического дерева группы, содержащие объекты, для которых непосредственно назначены лицензионные ключи. При этом вложенными элементами групп являются станции и политики, входящие в данные группы, и лицензионные ключи, которые назначены для этих объектов. Данное представление дерева служит для удобства визуализации информации о лицензировании и не позволяет управлять объектами дерева.
- Для изменения внешнего вида дерева используйте следующие опции:
  - **Показывать идентификаторы клиентов** — включает/отключает отображение уникальных идентификаторов станций.
  - **Показывать названия клиентов** — включает/отключает отображение имен (названий) станций.
  - **Показывать адреса клиентов** — включает/отключает отображение IP-адресов станций.

- **Показывать описания** — включает/отключает отображение описаний станций и групп станций.

При помощи **Менеджера лицензий** вы можете осуществлять следующие действия над лицензионными ключами Dr.Web Enterprise Server.

1) Просматривать информацию о лицензии. Для того чтобы просмотреть сводную информацию о лицензионном ключе, выберите в главном окне Менеджера лицензий учетную запись ключа, информацию о котором вы хотите просмотреть (нажмите на название учетной записи ключа). В открывшейся панели будет выведена такая информация, как:

- предоставляемое и используемое количество лицензий из данного лицензионного ключевого файла,
- пользователь лицензии,
- продавец, у которого была приобретена данная лицензия,
- идентификационный и серийный номера лицензии,
- дата окончания срока действия лицензии,
- включает ли данная лицензия поддержку модуля Антиспам,
- MD5-хэш лицензионного ключа,
- список антивирусных компонентов, которые позволяет использовать данная лицензия.



2) Добавление нового лицензионного ключа. Для того чтобы добавить новый лицензионный ключ:

1. В главном окне Менеджера лицензий нажмите кнопку **Добавить лицензионный ключ** на панели инструментов.

2. На открывшейся панели нажмите кнопку и выберите файл с лицензионным ключом.

3. Установите флажок:

- **Назначить лицензионный ключ группе Everyone**, если это первый лицензионный ключ в антивирусной сети. Добавляемый ключ будет автоматически назначен группе **Everyone**.
- **Заменить лицензионный ключ группы Everyone**, если это не первый лицензионный ключ в антивирусной сети. Текущий лицензионный ключ группы **Everyone** будет заменен добавляемым лицензионным ключом.

Если для группы **Everyone** назначено несколько лицензионных ключей, то будет заменен первый в списке.

Если вы хотите заменить определенный лицензионный ключ группы **Everyone**, воспользуйтесь процедурой Обновление лицензионного ключа.

4. Нажмите кнопку **Сохранить**.

5. Лицензионный ключ будет добавлен в дерево ключей.

Если на шаге 3 вы не установили соответствующий флажок, то добавленный лицензионный ключ не будет привязан ни к одному из объектов. В этом случае для задания объектов лицензирования выполните процедуры Замена лицензионного ключа или Расширение списка лицензионных ключей объекта, описанные ниже.

3) Обновление лицензионного ключа. При обновлении лицензионного ключа новый лицензионный ключ будет назначен для тех же объектов лицензирования, для которых был назначен обновляемый ключ.

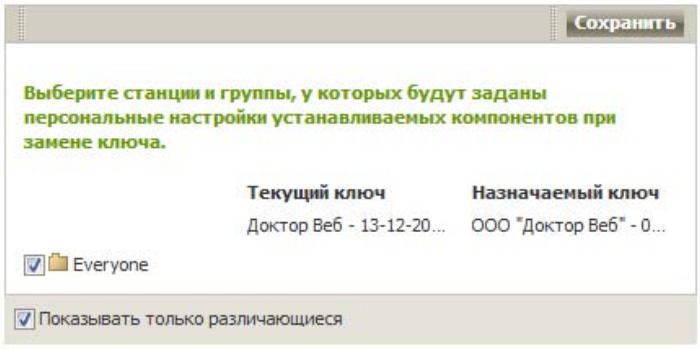
Воспользуйтесь процедурой обновления ключа для замены ключа с истекшим сроком действия или для замены на ключ с другим списком устанавливаемых компонентов с сохранением структуры дерева ключей.

Для того чтобы обновить лицензионный ключ:

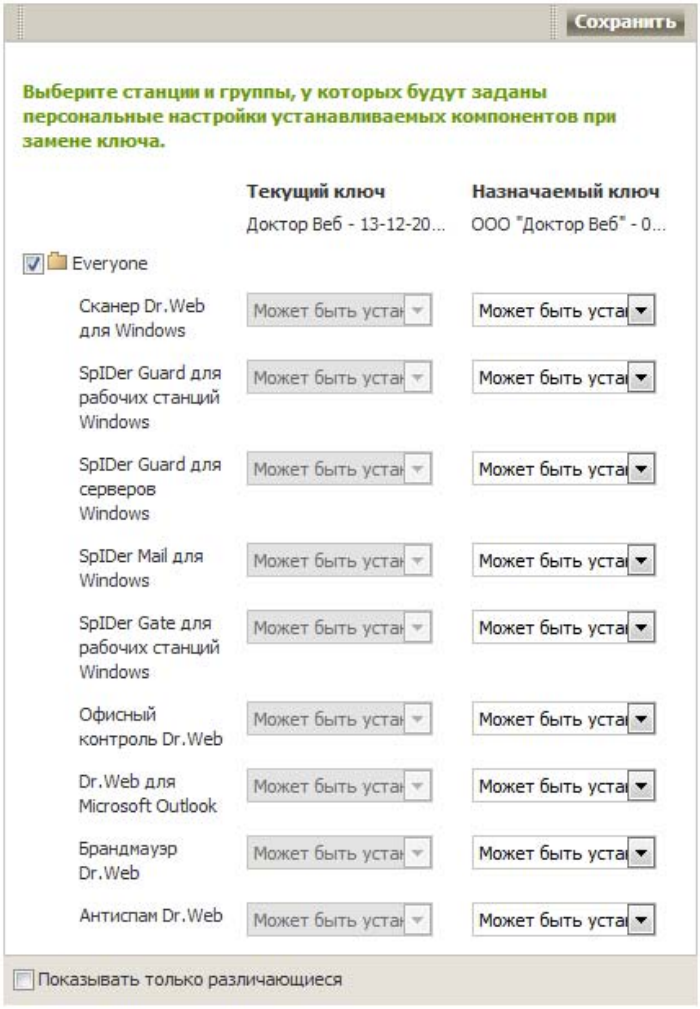
1. В главном окне Менеджера лицензий в дереве ключей выберите ключ, который хотите обновить.

2. На открывшейся панели свойств ключа нажмите кнопку  и выберите файл с лицензионным ключом.

3. Нажмите кнопку **Сохранить**. Откроется окно настроек устанавливаемых компонентов, описанное ниже:



При установленном флажке **Показывать только различающиеся** в списке отображаются только компоненты, настройки которых в текущем и назначаемом (наследуемом) ключах различаются.



1. В окне настроек устанавливаемых компонентов в списке объектов приведены:

- Станции, группы и политики со своими списками устанавливаемых компонентов.
- В столбце **Текущий ключ** приведен список ключей объекта и настройки устанавливаемых компонентов, актуальные для объекта на данный момент.
- В столбце **Назначаемый ключ** приведен ключ и настройки устанавливаемых компонентов, заданные в ключе, который будет назначен для выбранных объектов.
- При необходимости установите флажок **Показывать только различающиеся**, чтобы в списке отображались только те компоненты, настройки которых в текущем и назначаемом ключах различаются.

2. Для настройки списка устанавливаемых компонентов:

a) В столбце **Назначаемый ключ** вы можете настроить результирующий список устанавливаемых компонентов.

- Настройки устанавливаемых компонентов в столбце **Назначаемый ключ** рассчитываются исходя из того, разрешено ли использование компонента в текущих настройках и новом ключе (+) или не разрешено (–), следующим образом:

Текущие настройки	Настройки назначаемого ключа	Результирующие настройки
+	+	+
–	+	+
+	–	–
–	–	–

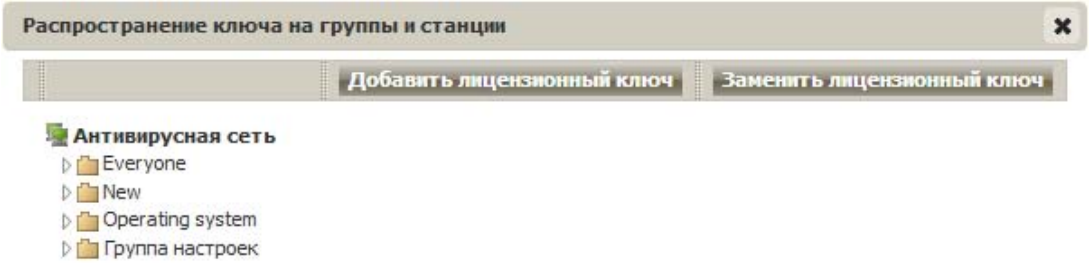
- Вы можете изменить настройки устанавливаемых компонентов (понизить права на установку) только если в настройках, полученных в столбце **Назначаемый ключ**, разрешено использование этого компонента.

b) Установите флажки для тех объектов (станций, групп и политик), для которых будет разорвано наследование настроек и заданы настройки устанавливаемых компонентов из столбца **Назначаемый ключ** в качестве персональных. Для остальных объектов (для которых флажки не установлены) будет установлено наследование изначальных настроек из столбца **Назначаемый ключ**.

Нажмите кнопку **Сохранить** для обновления лицензионного ключа.

4) Замена лицензионного ключа, расширение списка лицензионных ключей объекта. При замене лицензионного ключа, для объекта лицензирования удаляются все текущие лицензионные ключи и добавляется новый ключ. При добавлении лицензионного ключа сохраняются все текущие ключи и в список добавляется новый лицензионный ключ. Для того чтобы з аменить текущий лицензионный ключ или добавить лицензионный ключ к списку лицензионных ключей объекта:

1) В главном окне **Менеджера лицензий** в дереве ключей выберите ключ, который хотите назначить объекту лицензирования, и на панели инструментов нажмите кнопку  (**Распространить ключ на группы и станции)**. Откроется окно с иерархическим списком станций и групп антивирусной сети.



2) Выберите в списке объекты лицензирования. Для выбора нескольких станций и групп используйте кнопки CTRL и SHIFT.

3) Нажмите кнопку Заменить лицензионный ключ или Добавить лицензионный ключ соответственно. Откроется окно настроек устанавливаемых компонентов, аналогичное описанному выше.
4) Нажмите кнопку **Сохранить** для замены или добавления лицензионного ключа.

5) Удаление лицензионного ключа и удаление объекта из списка лицензирования

Внимание! Нельзя удалить лицензионный ключ **Everyone**, если он является единственным.

Для того чтобы удалить лицензионный ключ или объект из списка лицензирования:

a. В главном окне **Менеджера лицензий** выберите ключ, который вы хотите удалить, или объект (станцию или группу), для которого назначен этот ключ, и нажмите кнопку  (**Удалить выбранные объекты)** на панели инструментов.

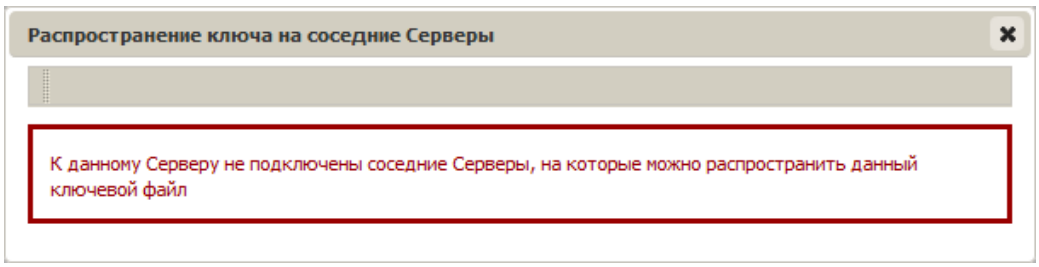
При этом:

- Если был выбран объект лицензирования, то он удаляется из списка объектов, на которых распространяется действие назначенного для него ключа. Для объекта, у которого удаляется персональный лицензионный ключ, устанавливается наследование лицензионного ключа.
- Если был выбран лицензионный ключ, удаляется учетная запись ключа из антивирусной сети. Для всех объектов, для которых был назначен данный лицензионный ключ, будет установлено наследование лицензионного ключа.

b. Откроется окно настроек устанавливаемых компонентов, аналогичное описанному выше процессу **Обновление лицензионного ключа**.
c. Нажмите кнопку **Сохранить** для удаления выбранного объекта и переключения на наследуемый ключ.

6) Передача лицензий на соседний Сервер. При передаче части свободных лицензий на соседний Сервер из лицензионного ключа на данном Сервере, переданное количество лицензий будет недоступно для использования на данном Сервере до окончания срока распространения этих лицензий. Для того чтобы передать лицензии на соседний Сервер:

a. В главном окне **Менеджера лицензий** в дереве ключей выберите ключ, свободные лицензии из которого хотите передать на соседний **Сервер**. При отсутствии серверов будет показано окно:



b. На панели инструментов нажмите кнопку  (**Распространить ключ на соседние Серверы)**. Откроется окно с иерархическим списком соседних **Серверов**.

c. Выберите в списке **Серверы**, на которые хотите распространить лицензии.

d. Напротив каждого из **Серверов** задайте следующие параметры:

- **Количество лицензий** — количество свободных лицензий, которые вы хотите передать из данного ключа на соседний **Сервер**.
- **Дата окончания лицензии** — срок действия передачи лицензий. По истечении указанного срока все лицензии будут отозваны с соседнего **Сервера** и вернутся в список свободных лицензий данного лицензионного ключа.

e. Нажмите одну из кнопок:

- **Добавить ключ** — чтобы добавить лицензии к списку имеющихся лицензий соседних Серверов.
- **Заменить ключ** — чтобы удалить текущие лицензии соседних Серверов и задать только распространяемые лицензии.

f. Нажмите кнопку **Сохранить** для распространения лицензий на соседние Серверы.

7) Редактирование лицензий, переданных на соседний Сервер. Для того чтобы отредактировать лицензии, распространенные на соседний Сервер:

Для того чтобы отредактировать лицензии, распространенные на соседний Сервер:

1. В главном окне Менеджера лицензий в дереве ключей выберите соседний Сервер, на который были распространены лицензии.

2. На открывшейся панели свойств отредактируйте следующие параметры:

- **Количество лицензий** — количество свободных лицензий, которые переданы из ключа с данного Сервера на соседний Сервер.
- **Дата окончания лицензии** — срок действия передачи лицензий. По истечении указанного срока все лицензии будут отозваны с данного Сервера и вернутся в список свободных лицензий соответствующего лицензионного ключа.

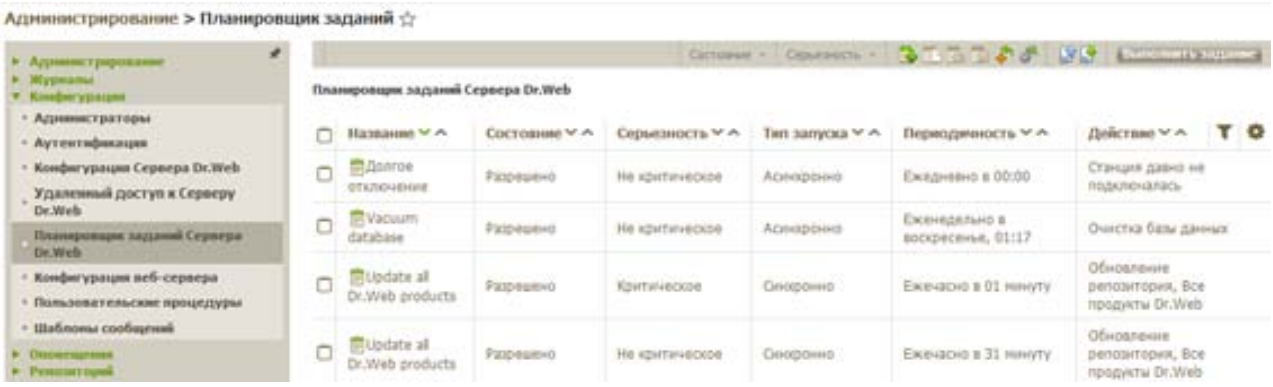
3. Нажмите кнопку **Сохранить** для обновления информации по распространяемым лицензиям.

9.3. Обновление сервера Dr.Web Enterprise Security Suite

Внимание! Администратор антивирусного сервера должен помнить о том, что после обновления серверной части все антивирусные Агенты начнут процесс обновления своих компонентов и баз сразу после подключения к Серверу, что может привести к перегрузке сети и самого С ервера. Рекомендуется постепенное обновление с ограничением доступа к серверу в пределах сегментов сети. Также целесообразно уведомить специалистов технической поддержки об обновлении антивирусного ПО.

9.3.1. Настройка обновления компонентов антивирусной сети.

Чтобы настроить расписание выполнения заданий, выберите в меню **Администрирование → Конфигурация → Планировщик заданий Сервера Dr.Web**. Откроется текущий список заданий сервера. Используя данную страницу, вы можете добавлять, удалять и настраивать любые задания, в том числе задания обновления.



В Планировщике заданий есть два предустановленных и разрешенных к выполнению задания типа «Обновление репозитория, Все продукты Dr.Web», одно из которых выполняется каждый час в 01 минуту и является критическим, второе — ежечасно в 31 минуту, но не является критическим. Как правило, этих заданий достаточно для нормального функционирования антивирусной сети и настройка расписания не требуется. Но при необходимости можно либо отредактировать одно из этих заданий, либо, что более оптимально, добавить новое аналогичное задание.

Для этого нажмите на панели инструментов кнопку  (**Создать задание**). При этом также откроется группа настроек **Создать задание**.

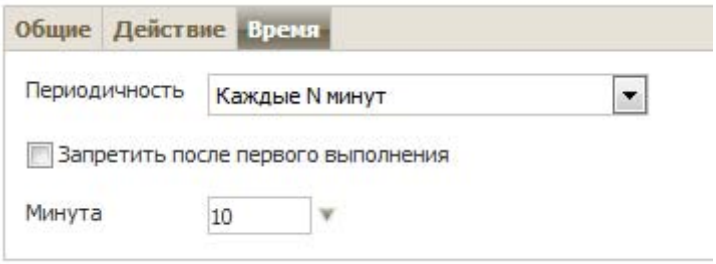
Введите в поле **Название** на вкладке **Общие** наименование задания, под которым оно будет отображаться в расписании.

С помощью флажка **Разрешить исполнение** определите, будет ли данное задание выполняться, а с помощью флажка **Критичное задание** определите, является ли данное задание критичным для выполнения, отметьте **Запускать задание асинхронно**, чтобы задание выполнялось параллельно с другими, вне общей очереди.

Перейдите на закладку **Действие** и в выпадающем меню выберите тип задания **Обновление репозитория**. При этом изменится вид нижней части окна, содержащей параметры данного типа задания. Отметьте обновляемые продукты и компоненты.

Внимание! В пункте Сервер Dr.Web речь идет об обновлении компонента в пределах той версии Сервера, которая уже используется в антивирусной сети, т. е., например, обновление с версии 10.0 на 10.1 можно установить через репозиторий, а для обновления Сервера до 11-й версии потребуется уже использование дистрибутива. Процедура обновления Сервера Dr.Web до актуальной 11-й версии подробно описана в разделах документации: Обновление Сервера Dr.Web для ОС Windows и Обновление Сервера Dr.Web для ОС семейства UNIX.

На закладке **Время** выберите в списке периодичность запуска задания и настройте время в соответствии с выбранной периодичностью.



Для того чтобы сохранить изменения настройки, нажмите на кнопку **Сохранить**.

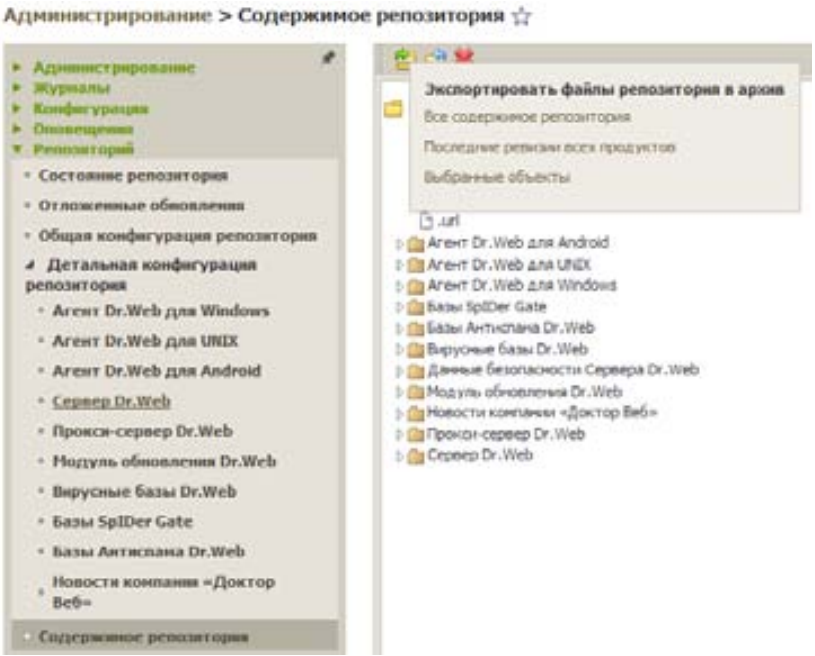
Включение авторизации на прокси-серверах MS ISA и IIS для обновления антивирусного сервера с ВСО осуществляется на вкладке **Сеть → Прокси** страницы меню **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web**. Для конфигурирования параметров доступа необходимо выбрать пункт **Использовать прокси-сервер** и указать необходимые параметры.

9.3.1.1. Обновление при отсутствии выхода в Интернет

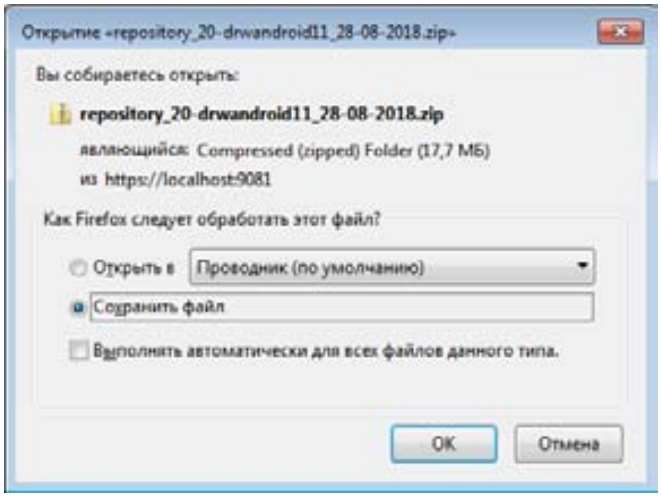
Если Сервер Dr.Web по каким-либо причинам не имеет доступа в сеть Интернет, его репозиторий можно обновить вручную, скопировав актуальный репозиторий с другого Сервера, имеющего выход в Интернет. Для этого необходимо выполнить следующие действия:

1) На подключенном к Интернету Сервере обновите репозиторий до актуального состояния, в разделе **Администрирование → Репозиторий → Состояние репозитория** нажав кнопку **Проверить обновления**.

2) Экспортируйте содержимое всего репозитория или его частей с помощью кнопки  раздела **Администрирование → Репозиторий → Содержимое репозитория.**



Например, необходимо перенести только обновления продукта Агент Dr.Web для Android. Выберите соответствующий продукт и затем — **Выбранные объекты**. Сохраните файл архива в удобном месте, например на USB-накопителе, чтобы иметь возможность перенести его на Сервер Dr.Web, где требуется обновление.

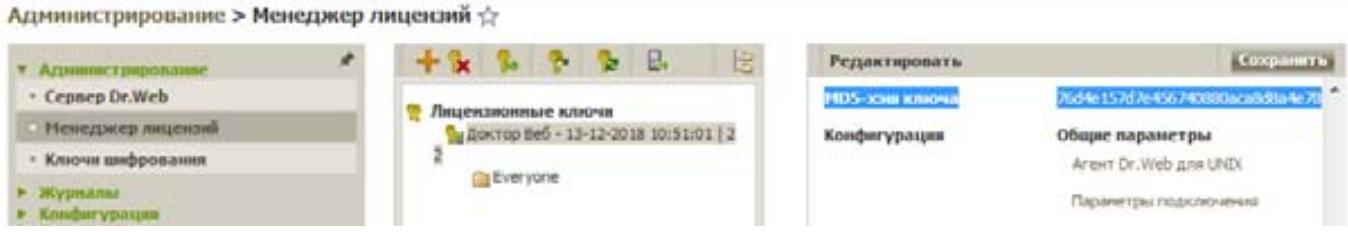


3) На обновляемом Сервере Dr.Web в аналогичном разделе управляющего меню нажмите кнопку  и укажите параметры импорта данных в репозиторий: имя импортируемого файла и настройки импорта. После чего нажмите **Импортировать**.

4) Перезагрузите репозиторий с диска в разделе **Состояние репозитория**.

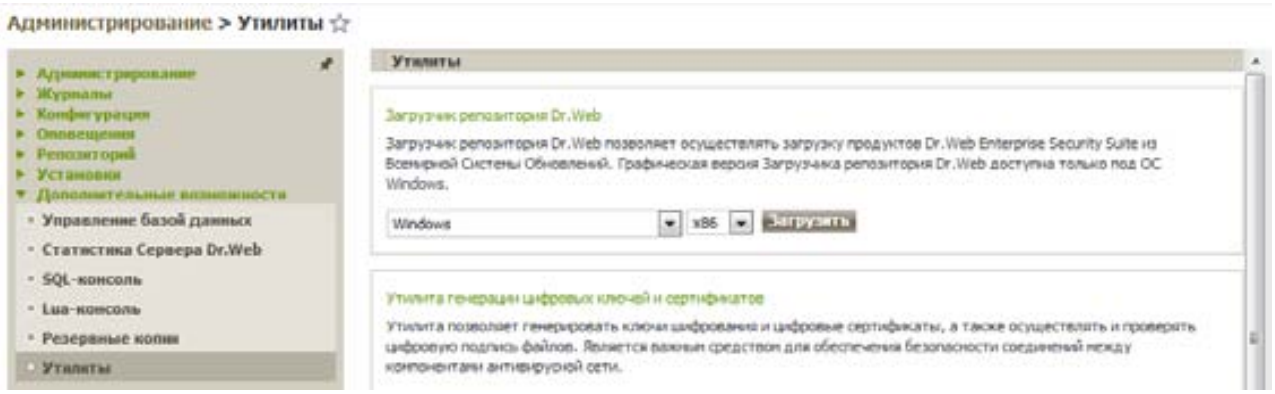
Приведенный выше метод является наиболее удобным и простым, но если по каким-то причинам его использование невозможно, то для обновления репозитория не имеющего доступа к Интернету Сервера Dr.Web можно использовать утилиту **Загрузчик репозитория Dr.Web**, доступной в виде графической (только в версии под ОС Windows) и консольной версии.

Для использования данной утилиты необходим лицензионный ключ **Dr.Web Enterprise Security Suite** либо его MD5-хэш, который доступен для просмотра в **Центре управления**, в разделе **Администрирование → Администрирование → Менеджер лицензий**.



Утилита **Загрузчик репозитория Dr.Web** может быть скачана при помощи **Центра управления**, в разделе **Администрирование → Дополнительные возможности →**

Утилиты. Укажите тип и разрядность ОС, с которой будет запускаться эта утилита, после чего нажмите Загрузить. Обратите внимание, что графическая версия утилиты доступна только для Windows (вариант **Windows UI**), для других ОС существует только консольная утилита. По умолчанию скачивается консольная версия для Windows.



Для скачивания репозитория при помощи графической версии **Загрузчика репозитория Dr.Web**:

1. Запустите графическую версию утилиты **Загрузчик репозитория Dr.Web** (`drweb-reploader-gui-windows-<версия>.exe`) на ПК, имеющем доступ к Интернету.
2. В главном окне утилиты задайте следующие параметры:

2. В главном окне утилиты задайте следующие параметры:

а) **Лицензионный ключ или MD5 ключа** — укажите файл лицензионного ключа Dr.Web. Для этого нажмите **Обзор** и выберите действующий файл лицензионного ключа или укажите его MD5-хэш.

b) **Каталог загрузки** — задайте каталог, в который будет осуществляться загрузка репозитория.

c) В списке **Режим** выберите один из режимов загрузки обновлений:

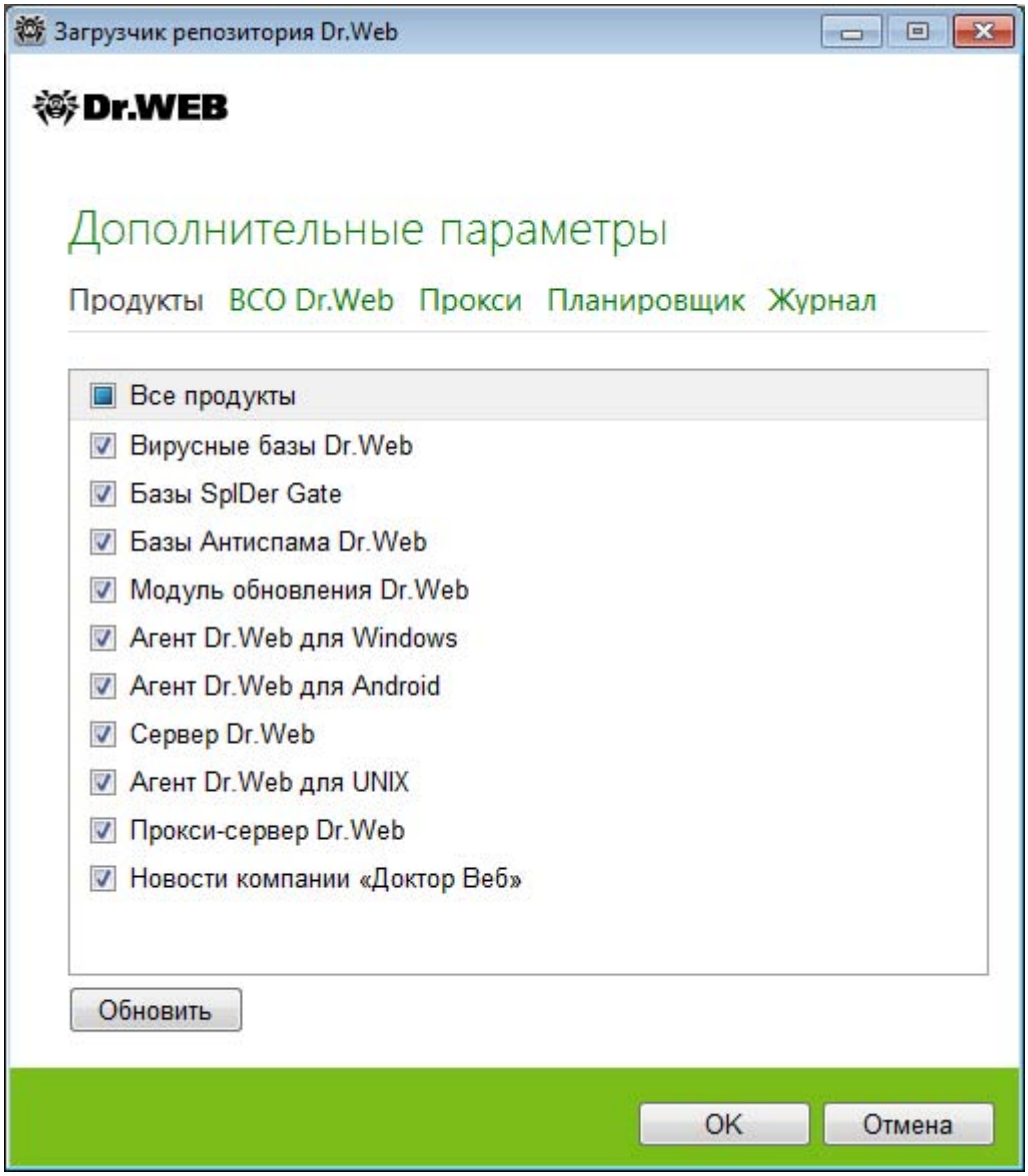
- **Загрузить репозиторий** — осуществляется скачивание репозитория в формате репозитория Сервера. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Севера.
- **Синхронизировать зеркало обновлений** — осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут выть выложены на зеркало обновлений в вашей локальной сети. В дальнейшем Серверы могут быть настроены на получение обновлений непосредственно с данного зеркала обновлений, содержащего последнюю версию репозитория, а не с серверов ВСО.

d) Установите флажок **Архивировать репозиторий**, чтобы автоматически упаковать загруженный репозиторий в zip-архив. Данная опция позволяет получить готовый архивный файл для импорта загруженного репозитория на Сервер при помощи Центра управления, из раздела **Администрирование → Содержимое репозитория**.

3. Если вы хотите изменить дополнительные настройки соединения с ВСО и загрузки обновлений, нажмите **Дополнительные параметры**. В открывшемся окне настроек доступны следующие вкладки:

a) На вкладке **Продукты** вы можете изменить список загружаемых продуктов. В окне настроек приведен список всех продуктов репозитория, доступных для загрузки с ВСО:

- Чтобы обновить список продуктов, доступных на ВСО в данный момент, нажмите кнопку **Обновить**.
- Установите флажки напротив тех продуктов, которые вы хотите загрузить с ВСО, или флажок в заголовке таблицы, чтобы выбрать все продукты из списка.



b) На вкладке **ВСО Dr.Web** вы можете настроить параметры серверов обновления:

- Порядок серверов ВСО в списке определяет порядок обращения к ним утилиты при загрузке репозитория. Для изменения порядка серверов ВСО используйте кнопки **Вверх** и **Вниз**.
- Чтобы добавить сервер ВСО в список серверов, используемых для загрузки, введите адрес сервера ВСО в поле над списком серверов и нажмите кнопку **Добавить**.
- Чтобы удалить сервер ВСО из списка используемых, выберите в списке сервер, который необходимо удалить, и нажмите кнопку **Удалить**.
- В поле **Базовый URI** указан каталог на серверах ВСО, содержащий обновления продуктов Dr.Web.
- В выпадающем списке **Протокол** выберите тип протокола для получения обновлений с серверов обновлений. Для всех протоколов загрузка обновлений осуществляется согласно настройкам списка серверов ВСО.
- В выпадающем списке **Допустимые сертификаты** выберите тип SSL-сертификатов, которые будут автоматически приниматься. Данная настройка используется только для защищенных протоколов, поддерживающих шифрование.
- **Регистрационное имя** и **Пароль** — регистрационные данные пользователя для аутентификации на сервере обновлений, если сервер требует авторизации.

- Установите флажок **Использовать CDN**, чтобы разрешить использование Content Delivery Network при загрузке репозитория.

c) На вкладке **Прокси** вы можете задать параметры подключения к BCO через прокси-сервер:

- **Адрес прокси-сервера** и **Порт** — соответственно, сетевой адрес и номер порта используемого прокси-сервера.
- **Регистрационное имя** и **Пароль** — параметры авторизации на прокси-сервере, если используемый прокси-сервер требует авторизацию.

d) На вкладке **Планировщик** вы можете настроить расписание периодических обновлений. Для выполнения расписания используется планировщик задач ОС Windows. При этом нет необходимости запускать утилиту вручную, загрузка репозитория будет осуществляться автоматически согласно заданным промежуткам времени.

e) На вкладке **Журнал** вы можете настроить параметры ведения журнала загрузок обновлений.

Нажмите **ОК** для принятия внесенных изменений и возвращения в главное окно **Загрузчика репозитория Dr.Web**.

4. После настройки всех параметров нажмите кнопку **Загрузить** в главном окне **Загрузчика репозитория Dr.Web**, чтобы начать подключение к ВСО и загрузку репозитория.

После завершения загрузки репозитория, его можно импортировать на обновляемый Сервер Dr.Web, после чего все подключенные к нему Агенты получат обновление.

Консольная версия утилиты **Загрузчик репозитория Dr.Web** имеет имя вида drweb-reploader-<ОС>-<разрядность>.exe и скачивается через интерфейс Центра управления аналогично графической утилите. Данная версия утилиты может быт запущена с любого ПК, имеющего соответствующую ОС.

Допустимые ключи утилиты:

- --archive — упаковать репозиторий в архив. По умолчанию: no.
- --auth <*аргумент*> — регистрационные данные для авторизации на сервере обновлений в формате <*пользователь*>[:<*пароль*>].
- --cert-file <*путь*> — путь к хранилищу корневых сертификатов для SSL-авторизации.

- --cert-mode [<*аргумент*>] — тип SSL-сертификатов, которые будут автоматически приниматься. Данная настройка используется только для защищенных протоколов, поддерживающих шифрование.
- <*аргумент*> может принимать одно из значений:
  - any — принимать любые сертификаты,
  - valid — принимать только проверенные сертификаты,
  - drweb — принимать только сертификаты Dr.Web,
  - custom — принимать пользовательские сертификаты.

  По умолчанию используется значение drweb.
- --config <*путь*> — путь к конфигурационному файлу Загрузчика репозитория.
- --cwd <*путь*> — путь к текущему рабочему каталогу.
- --ipc — включить передачу данных о процессе работы утилиты в поток стандартного вывода. По умолчанию: no.
- --help — вывести справку по ключам.
- --license-key <*путь*> — путь к файлу лицензионного ключа (должен быть указан ключ или его MD5).
- --log <*путь*> — путь к файлу журнала по процедуре загрузки репозитория.
- --mode <*режим*> — режим загрузки обновлений:
  - repo — осуществляется скачивание репозитория в формате репозитория Сервера. Загруженные файлы могут быть непосредственно импортированы через Центр управления в качестве обновления репозитория Севера. Используется по умолчанию.
  - mirror — осуществляется скачивание репозитория в формате зоны обновлений ВСО. Загруженные файлы могут выть выложены на зеркало обновлений в вашей локальной сети. В дальнейшем Серверы могут быть настроены на получение обновлений непосредственно с данного зеркала обновлений, содержащего последнюю версию репозитория, а не с серверов ВСО.
- --only-bases — загрузить только вирусные базы. По умолчанию: no.
- --path <*аргумент*> — загрузить репозиторий с ВСО в каталог, указанный в параметре <*аргумент*>. При упаковке репозитория в архив при помощи ключа --archive, возможно указание пути как до имени каталога, так и до имени файла архива. Если имя архива не указано, будет дано имя по умолчанию — repository.zip.
- --product <*аргумент*> — обновляемый продукт. По умолчанию загружается весь репозиторий.
- --prohibit-cdn — запретить использовать CDN при загрузке обновлений. По умолчанию: no, т.е. разрешено использование CDN.
- --proto <*протокол*> — протокол загрузки обновлений: file | ftp | ftps | http | https | scp | sftp | smb | smbs. По умолчанию: https.
- --proxy-auth <*аргумент*> — информация для аутентификации на прокси-сервере: регистрационное имя пользователя и пароль в формате <*пользователь*>[:<*пароль*>].
- --proxy-host <*аргумент*> — адрес прокси-сервера в формате <*сервер*>[:<*порт*>]. Порт по умолчанию: 3128.
- --rotate <*N*><*f*>,<*M*><*u*> — режим ротации журнала работы Загрузчика репозитория. Аналогично настройке ротации журнала Сервера.

  По умолчанию 10,10m, что означает хранить 10 файлов по 10 мегабайт, использовать сжатие.
- --servers <*аргумент*> — адреса серверов ВСО. Рекомендуется оставить значение по умолчанию: esuite.geo.drweb.com.
- --show-products — показать список продуктов на ВСО. По умолчанию: no.
- --ssh-auth <*тип*> — тип авторизации на сервере обновлений при обращении по SCP/SFTP. В качестве параметра <*тип*> допускается одно из следующих значений:

    - pwd — авторизация по паролю. Пароль задается в ключе --auth.
    - pubkey — авторизация по открытому ключу. При этом необходимо задать закрытый ключ через --ssh-prikey для извлечения соответствующего открытого ключа.
- --ssh-prikey <*путь*> — путь до закрытого ключа SSH.
- --ssh-pubkey <*путь*> — путь до открытого ключа SSH.
- --strict — остановить загрузку в случае возникновения ошибки. По умолчанию: no.
- --update-key <*путь*> — путь до открытого ключа или каталога с открытым ключом для проверки подписи обновлений, загружаемых с ВСО. Открытые ключи для проверки подлинности обновлений update-key-*.upub можно найти на Сервере Dr.Web в каталоге etc.
- --update-url <*аргумент*> — каталог на серверах ВСО, содержащий обновления продуктов Dr.Web. Рекомендуется оставить значение по умолчанию — /update.
- --verbosity <*уровень_подробности*> — уровень детализации журнала. По умолчанию TRACE3. Допустимые значения: ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. Значения ALL и DEBUG3 — синонимы.
- --version <*версия*> — версия Сервера, для которого необходимо загрузить обновления в формате <*мажорная_версия*>.<*минорная_версия*>. Например, для Сервера версии 11 параметр<*версия*> принимает значение 11.00.

При запуске утилиты **Загрузчик репозитория** обратите внимание на следующие правила:

Ключи должны быть обязательно заданы	**При условии**
--license-key	Всегда
--update-key	
--path	
--cert-file	Если следующие ключи принимают одно из значений: •--cert-mode valid | drweb | custom, •--proto https | ftps | smbs.
--ssh-prikey	Если следующие ключи принимают одно из значений: •--proto sftp | scp, •--ssh-auth pubkey.

Примеры использования

1. Создать импортируемый архив со всеми продуктами:

```
drweb-reploader-windows-x86.exe --path C:\Temp --archive --
license-key C:\agent.key --update-key "C:\Program Files\DrWeb
Server\etc" --cert-file "C:\Program Files\DrWeb Server\etc"
```

2. Создать импортируемый архив с вирусными базами:

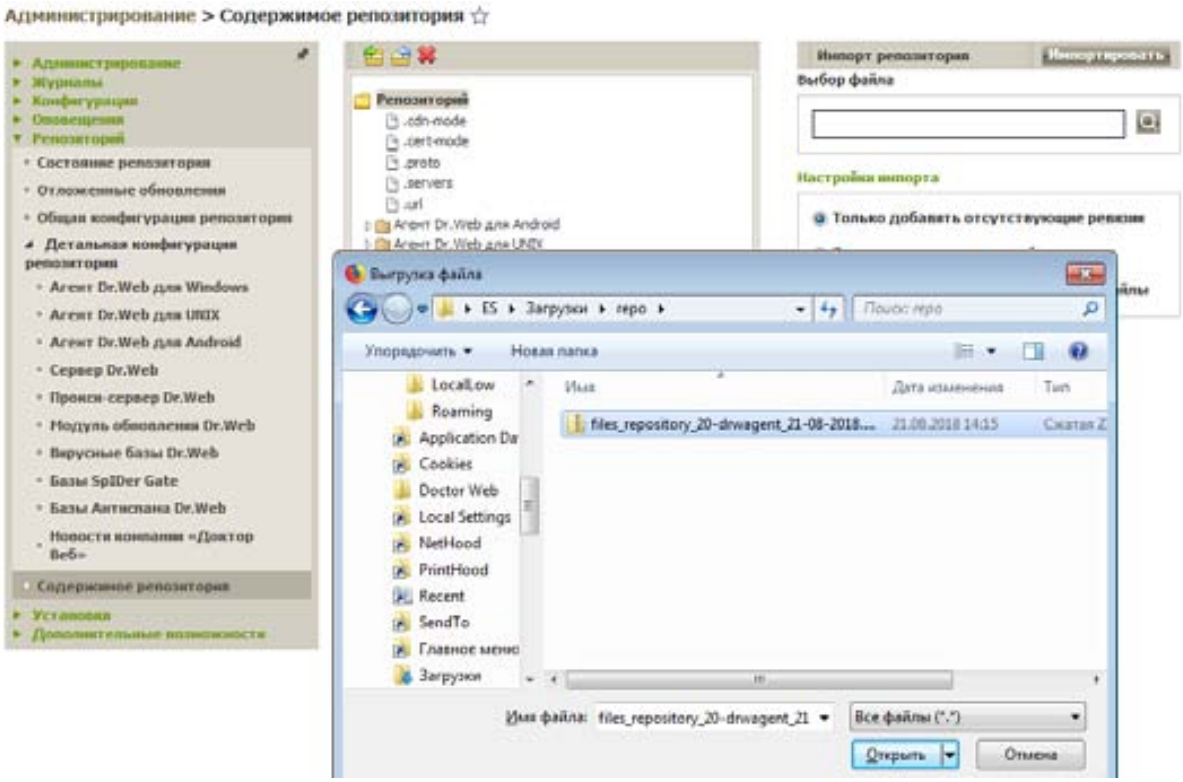
```
drweb-reploader-windows-x86.exe --path C:\Temp --archive --
license-key "C:\agent.key" --update-key "C:\Program
Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb
Server\etc" -only-bases
```

3. Создать импортируемый архив только с Сервером:

```
drweb-reploader-windows-x86.exe --path C:\Temp --archive --
license-key "C:\agent.key" --update-key "C:\Program
Files\DrWeb Server\etc" --cert-file "C:\Program Files\DrWeb
Server\etc" --product=20-drwcs
```

Рекомендуемая процедура использования консольной утилиты

1. Загрузите с ВСО репозиторий **Сервера Dr.Web** через утилиту **Загрузчик репозитория Dr.Web**, как и зложено выше. При загрузке используйте ключ *--archive* для создания архива репозитория.
2. Импортируйте загруженный репозиторий на **Сервер** при помощи **Центра управления**, из раздела **Администрирование → Содержимое репозитория**.



Процедура с ручным импортом

1. Загрузите с ВСО репозиторий **Сервера Dr.Web** через утилиту **Загрузчик репозитория Dr.Web**, как и зложено выше. При загрузке используйте ключ *--archive* для создания архива репозитория. При загрузке используйте ключ *--path* <*аргумент*> для загрузки репозитория в заданный каталог.
2. Для импорта репозитория скопируйте его содержимое, расположенное в каталоге, указанном в параметре <*аргумент*>, в каталог */repository* в каталоге установки Сервера с заменой файлов.

3. Перезагрузите репозиторий из **Центра управления**, в разделе **Администрирование → Репозиторий → Состояние репозитория** нажав кнопку  **(Перезагрузить с диска)**.

9.3.2. Обновление сервера Dr.Web Enterprise Security Suite

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

Для сохранения базы данных:

1. Остановите Сервер.

2. Экспортируйте базу данных в файл:

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

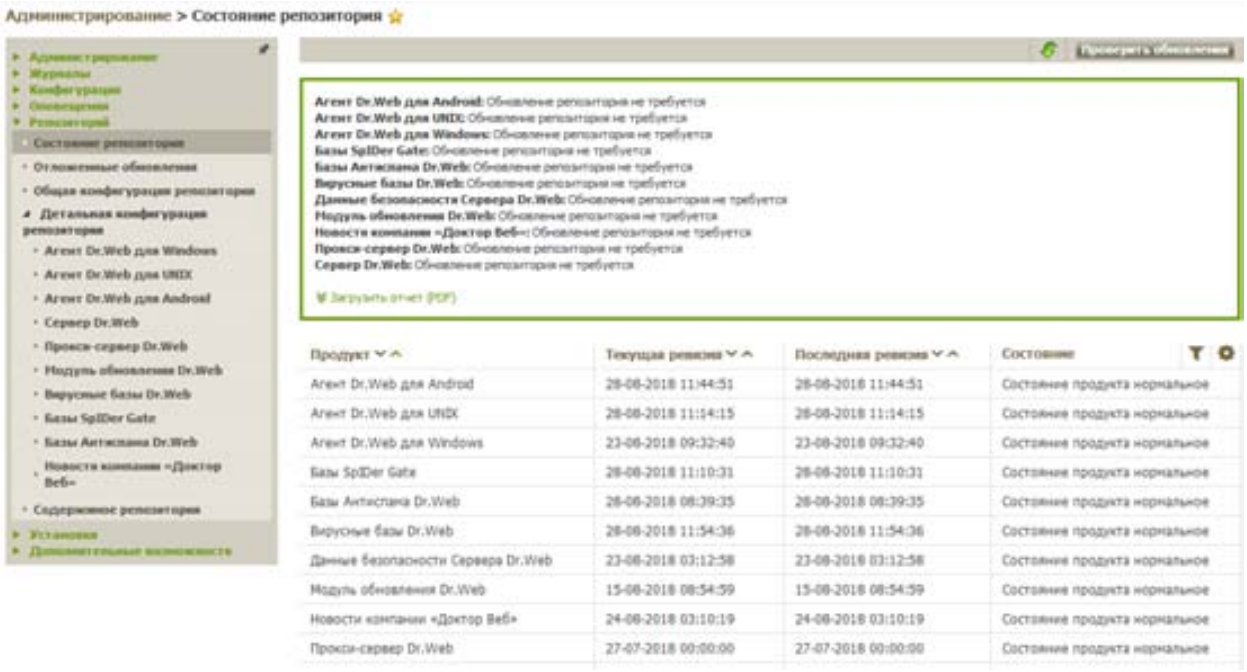
Для Серверов, использующих внешнюю базу данных, рекомендуется использовать штатные средства, поставляемые вместе с базой данных.

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

Центр управления предоставляет следующие возможности по обновлению антивирусного Сервера:

- Обновление ПО антивирусного сервера на одну из доступных версий, скачанных из ВСО и хранящихся в репозитории антивирусного сервера.
- Откат ПО антивирусного сервера к сохраненной резервной копии. Резервные копии создаются автоматически при переходе к новой версии в разделе **Обновления Сервера Dr.Web**.

Для получения новых обновлений вручную выберите раздел **Администрирование → Репозиторий → Состояние репозитория** и нажмите **Проверить обновления**.



Для перехода к списку доступных версий антивирусного сервера выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Сервер Dr.Web**. Далее нажмите на текущую версию антивирусного сервера в главном окне или на кнопку **Список версий**.

В открывшемся разделе **Обновления Сервера Dr.Web** будет представлен список доступных обновлений и резервных копий антивирусного сервера.

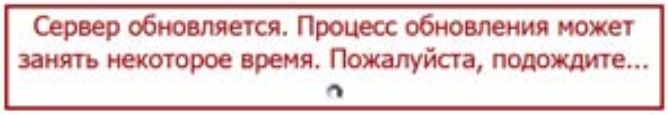
В списке **Текущая версия** указана версия **Сервера**, которая используется в данный момент, а в списке **Все версии** приведен список обновлений для данного **Сервера**, скачанных с **ВСО**. В разделе **Описание** приведен краткий список новых возможностей для каждого из обновлений.

Для версии, соответствующей первоначальной установке **Сервера** из инсталляционного пакета, в разделе **Описание** приводится ссылка на **Примечания к выпуску**, содержащие описание всех новых возможностей данной версии.

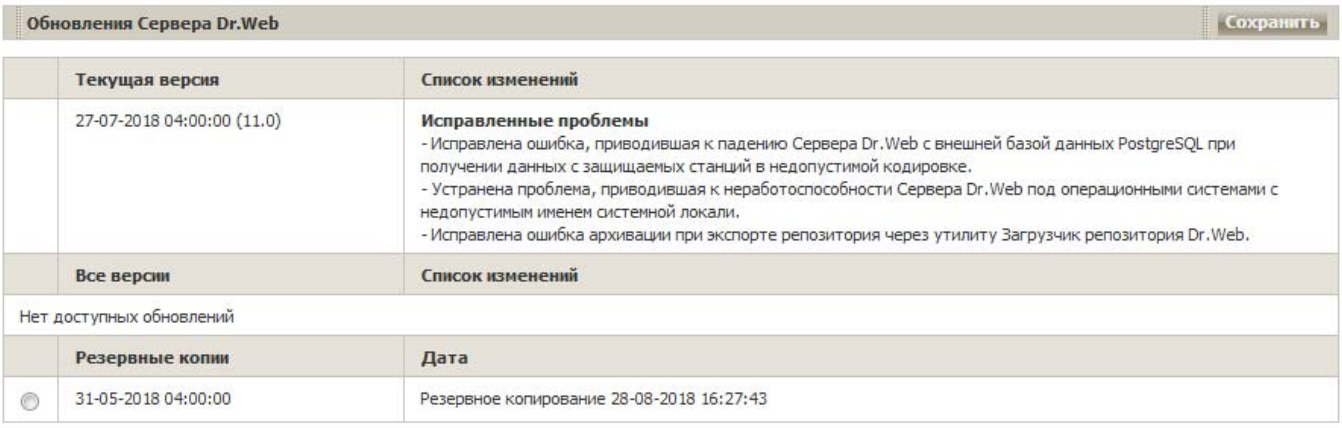
В списке **Резервные копии** приведен список резервных копий, сохраненных для данного **Сервера**. В разделе **Описание** приводится информация о дате резервного копирования.

Также информация о наличии обновлений сервера доступна на странице **Сервер Dr.Web** в меню **Администрирование**.

Для обновления ПО антивирусного сервера установите флажок напротив нужной версии в списке **Все версии** и нажмите Сохранить. Произвести обновление можно только на более позднюю версию относительно используемой в данный момент.



В процессе обновления текущая версия сохраняется как резервная копия (помещается в раздел **Резервные копии**), а версия, на которую осуществляется обновление, перемещается из раздела **Все версии** в раздел **Текущая версия**.



Резервные копии сохраняются в каталоге установки Сервера в каталоге var → update → backup → <старая_версия>_<новая_версия>. Также в процессе обновления создается или дополняется файл журнала var → *dwupdater.log*.

Для отката к сохраненной резервной копии установите флажок напротив нужной версии **Сервера** в списке **Резервные копии** и нажмите Сохранить. В процессе отката ПО **Сервера** резервная копия, на которую осуществляется переход, помещается в раздел **Текущая версия**.

Перед обновлением ПО Dr.Web Enterprise Security Suite рекомендуется выполнить резервное копирование базы данных. Для Серверов, использующих внешнюю базу данных, рекомендуется использовать штатные средства, поставляемые вместе с базой данных.

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

9.3.3. Обновление сервера Dr.Web Enterprise Security Suite под ОС Windows

При обновлении Сервера до версии 11.0 средствами инсталлятора конфигурационные файлы сохраняются в каталог, заданный для резервного копирования:

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

При обновлении Сервера с версии 6 сохраняются следующие конфигурационные файлы:

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

При обновлении Сервера с версии 10 сохраняются следующие конфигурационные файлы:

Файл	**Описание**
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ads.xml	конфигурационный файл внешней авторизации администраторов через Active Directory
auth-ldap.xml	конфигурационный файл внешней авторизации администраторов через LDAP
auth-radius.xml	конфигурационный файл внешней авторизации администраторов через RADIUS
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При

Файл	Описание
	установке нового Сервера 11.0 отсутствует
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.conf.distr	шаблон конфигурационного файла Сервера с параметрами по умолчанию
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub	открытый ключ шифрования
download.conf	сетевые настройки для формирования инсталляционных пакетов Агента
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
webmin.conf	конфигурационный файл Центра управления
openssl.cnf	сертификат Сервера для HTTPS

При обновлении Сервера в пределах версии 11.0 сохраняются следующие конфигурационные файлы:

Файл	Описание
agent.key (имя может отличаться)	лицензионный ключ Агента
auth-ads.conf	конфигурационный файл внешней авторизации администраторов через Active Directory
auth-radius.conf	конфигурационный файл внешней авторизации администраторов через RADIUS
auth-ldap.conf	конфигурационный файл внешней авторизации администраторов через LDAP
auth-ldap-rfc4515.conf	конфигурационный файл внешней авторизации администраторов через LDAP по упрощенной схеме
auth-ldap-rfc4515-check-group.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory
auth-ldap-rfc4515-check-group-novar.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме с проверкой принадлежности к группе Active Directory с использованием переменных
auth-ldap-rfc4515-simple-login.conf	шаблон конфигурационного файла внешней авторизации администраторов через LDAP по упрощенной схеме
auth-pam.conf	конфигурационный файл внешней авторизации администраторов через PAM
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует
drwcsd-certificate.pem	сертификат Сервера
download.conf	сетевые настройки для формирования инсталляционных

Файл	Описание
	пакетов Агента
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.conf.distr	шаблон конфигурационного файла Сервера с параметрами по умолчанию
drwcsd.pri	закрытый ключ шифрования
dbexport.gz	экспорт базы данных
drwcsd.pub	открытый ключ шифрования
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
openssl.cnf	сертификат Сервера для HTTPS
webmin.conf	конфигурационный файл Центра управления
yalocator.apikey	API-ключ для Расширения Yandex.Locator

Внимание!

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

1. Лицензионный ключ Сервера более не используется (см. п. Глава 2: Лицензирование).

2. Встроенная база данных обновляется, а конфигурационный файл Сервера конвертируется средствами инсталлятора. Данные файлы не подлежат замене на автоматически сохраненные копии при переходе с Сервера версии 6.

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

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

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

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

Если вы планируете использовать в качестве внешней базы данных БД Oracle через ODBC-подключение, то при установке (обновлении) Сервера в настройках инсталлятора отмените установку встроенного клиента для СУБД Oracle (в разделе **Поддержка баз данных → Драйвер базы данных Oracle**).

В противном случае работа с БД Oracle через ODBC будет невозможна из-за конфликта библиотек.

При обновлении с версии 6

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

2. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флажок **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.

3. В последующих шагах осуществляется настройка Сервера аналогично процессу Установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.

4. Для начала процесса удаления Сервера предыдущей версии и установки Сервера версии 11.0 нажмите кнопку **Установить**.

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

При обновлении с версии 10.0

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

2. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флажок **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.

3. В последующих шагах осуществляется настройка Сервера аналогично процессу Установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.

4. Для начала процесса удаления Сервера предыдущей версии и установки Сервера версии 11.0 нажмите кнопку **Установить**.

5. В процессе обновления откроется окно с настройкой резервного копирования критичных данных перед удалением Сервера предыдущей версии. Рекомендуется установить флажок **Сохранить резервную копию критических данных Сервера Dr.Web**. При необходимости можете изменить каталог для резервного копирования, заданный по умолчанию (<*диск_установки*>:\DrWeb Backup).

При обновлении с версий 10.0.1, 10.1 и в пределах версии 11.0

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

2. Откроется окно с настройкой резервного копирования критичных данных перед удалением Сервера предыдущей версии. Рекомендуется установить флажок **Сохранить резервную копию критических данных Сервера Dr.Web**. При необходимости можете изменить каталог для резервного копирования, заданный по умолчанию (<*диск установки*>:\DrWeb Backup). Для начала процесса удаления предыдущей версии Сервера нажмите **Удалить**.

3. После завершения удаления предыдущей версии Сервера начнется установка новой версии. Откроется окно с информацией о продукте и ссылкой на текст лицензионного соглашения. После ознакомления с условиями лицензионного соглашения, для продолжения обновления установите флажок **Я принимаю условия Лицензионного соглашения** и нажмите кнопку **Далее**.

4. В последующих шагах осуществляется настройка Сервера аналогично процессу Установки Сервера Dr.Web на основе файлов конфигурации от предыдущей версии. Инсталлятор автоматически определяет каталог установки Сервера, расположение конфигурационных файлов и встроенной БД от предыдущей установки. При необходимости вы можете изменять пути к файлам, которые были автоматически найдены инсталлятором.

5. Для начала процесса установки Сервера версии 11.0 нажмите кнопку **Установить**.

После завершения обновлений Серверов антивирусной сети необходимо:

1. Повторно задать настройки шифрования и сжатия у связанных Серверов (см. Руководство администратора, раздел Настройка связей между Серверами Dr.Web).

2. Очистить кэш веб-браузера, используемого для подключения к Центру управления.

9.3.4. Обновление сервера Dr.Web Enterprise Security Suite под ОС семейства UNIX

Обновление ПО Сервера поверх установленной версии возможно не для всех ОС семейства UNIX. Поэтому под ОС семейства UNIX, в которых невозможно произвести обновление поверх уже установленного пакета, необходимо удалить ПО Сервера более ранних версий, сохранив резервную копию, и установить ПО версии 10.0 на основе сохраненной резервной копии.

Для сохранения базы данных необходимо остановить сервер, после чего осуществляется экспорт базы данных в файл. В случае если используется внешняя БД PostgreSQL, рекомендуется использовать штатные средства PostgreSQL:

```
# /etc/init.d/drwcsd stop
# pg_dump -E UTF-8 -F -t -U postgres -f /root/avdesk_backup/current.dump
drwcs_db
```

Пользователь, от имени которого производится подключение к БД (опция -U), и путь к папке с дампами могут меняться в зависимости от операционной системы.

Если по каким-то причинам используется внутренняя БД, то дамп выполняется командой: для FreeBSD:

```
# /usr/local/etc/rc.d/drwcsd.sh stop
# /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/dbbackup.avd
```

для Linux:

```
# /etc/init.d/drwcsd stop
# /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/dbbackup.avd
```

Убедитесь, что экспорт базы данных сервера завершился успешно. Отсутствие резервной копии БД не позволит восстановить сервер в случае непредвиденных обстоятельств!

При обновлении и удалении Сервера автоматически сохраняются следующие файлы:

Файл	**Описание**
agent.key (имя может отличаться)	лицензионный ключ Агента
certificate.pem	сертификат для SSL
common.conf	конфигурационный файл (для некоторых ОС семейства UNIX)
dbinternal.dbs	встроенная БД
drwcsd.conf (имя может отличаться)	конфигурационный файл Сервера
drwcsd.pri	закрытый ключ шифрования
drwcsd.pub	открытый ключ шифрования
enterprise.key (имя может отличаться)	лицензионный ключ Сервера
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления

При удалении Сервера версии 10 сохраняются следующие конфигурационные файлы:

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

Файл	Описание
enterprise.key (имя может отличаться)	лицензионный ключ Сервера. Сохраняется в том случае, если присутствовал после обновления с предыдущих версий. При установке нового Сервера 11.0 отсутствует
frontdoor.conf	конфигурационный файл для утилиты дистанционной диагностики Сервера
local.conf	настройки журнала Сервера
private-key.pem	закрытый ключ RSA
webmin.conf	конфигурационный файл Центра управления
*.dbs *.sqlite	встроенная БД

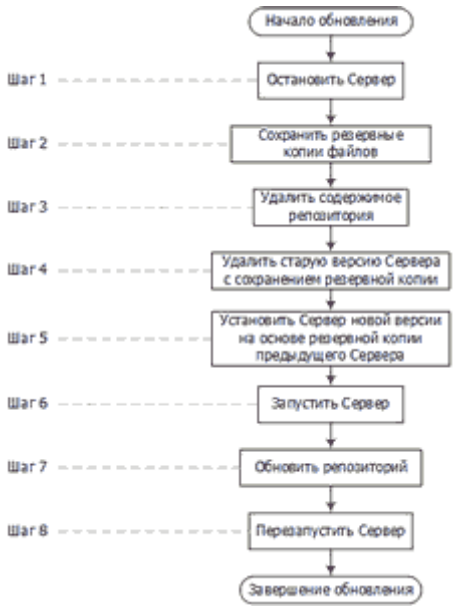
При необходимости сохраните другие важные для вас файлы.

Автоматическое обновление Dr.Web Server

Обновление Сервера до версии 11.0 зависит от исходной версии:

- Обновление с версии 6.0.4 на версию 11.0 осуществляется только вручную.
- Обновление с версии 10 на версию 11.0 автоматически поверх установленной версии возможно не для всех ОС семейства UNIX. Поэтому под ОС семейства UNIX, в которых невозможно произвести автоматическое обновление поверх уже установленного пакета, необходимо осуществить обновление вручную.
- Обновление Сервера в пределах версии 11.0 для одинаковых типов пакетов осуществляется автоматически для всех ОС семейства UNIX. При желании вы также можете осуществить обновление вручную.

Ручное обновление Dr.Web Server



Базовая блок-схема процесса переустановки Dr.Web Сервера для ОС семейства UNIX

Подробное описание шагов обновления Сервера приведено в соответствующем разделе Руководства по установке Dr.Web Enterprise Security Suite.

9.3.5. Обновление Агентов Dr.Web

Общие требования для обновления Агентов для всех ОС:

1. Агенты должны быть установлены на компьютерах, работающих под ОС, поддерживаемых для установки Агентов для Dr.Web Enterprise Security Suite версии 11.0 (см. документ **Приложения**, п. Приложение А. Полный список поддерживаемых версий ОС).

2. На станциях должны быть заданы ключи шифрования и сетевые настройки обновленного Сервера.

Если при обновлении Сервера были заданы новые ключи шифрования и сетевые настройки Сервера, после обновления ПО Сервера и автоматического обновления Агентов для возможности подключения к Серверу будет необходимо изменить настройки подключения к новому Серверу и заменить открытый ключ шифрования на станции вручную.

В зависимости от ОС обновление Агента может проходить в автоматическом (без вмешательства администратора антивирусной сети) и ручном режиме (установку придется осуществлять заново любым из доступных способов).

Обновление Агентов для Windows:

При обновлении с версии 6 или 10 обновление происходит автоматически, ручное обновление требуется только в случае возникновения ошибок или замены ключей шифрования.

Автоматическое обновление Агентов осуществляется по следующей схеме:

1. При запуске обновления удаляется старая версия Агента.

2. Осуществляется перезагрузка станции вручную.

3. Осуществляется установка новой версии Агента. Для этого автоматически создается задание в расписании Сервера.

4. После завершения обновления Агента станция автоматически подключается к Серверу. В разделе **Состояние** Центра управления для обновленной станции будет отображаться уведомление о необходимости перезагрузки. Необходимо выполнить перезагрузку станции.

Автоматическое обновление Агентов с ручной настройкой осуществляется по следующей схеме:

1. Вручную измените настройки подключения к новому Серверу и замените открытый ключ шифрования на станции.

2. После изменения настроек на станции и подключения станции к Серверу запустится процесс обновления Агента.

3. При запуске обновления удаляется старая версия Агента.

4. Осуществляется перезагрузка станции вручную.

5. Осуществляется установка новой версии Агента. Для этого автоматически создается задание в расписании Сервера.

6. После завершения обновления Агента станция автоматически подключается к Серверу. В разделе **Состояние** Центра управления для обновленной станции будет отображаться уведомление о необходимости перезагрузки. Необходимо выполнить перезагрузку станции.

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

В таком случае установка Агента должна осуществляться одним из следующих способов:

- Локально на станции.
- Удаленно через Центр управления. При этом после установки нового Агента потребуется объединить новую и старую станции в иерархическом списке антивирусной сети.

Обновление Агентов для Android, Linux и macOS осуществляется только вручную, посредством удаления старой версии Агента и установки новой.

Внимание! Если в сети присутствуют Агенты, установленные на неподдерживаемых ОС, они не смогут получать обновления (в том числе обновления вирусных баз) от нового Сервера. Если требуется наличие Агентов под неподдерживаемыми ОС, необходимо оставить в составе антивирусной сети Сервер предыдущей версии, к которому подключены эти Агенты. При этом Серверы предыдущих версий не должны быть связаны с Серверами версии 11.0. Но наилучшим решением будет использование актуальных версий операционных систем, поддерживаемых последними версиями Агента и Сервера Dr.Web.

Рекомендации по обновлению Агентов, установленных на станциях, выполняющих важные функции ЛВС, приведены в разделе «Обновление Агентов на серверах ЛВС» Приложений к документации.

10. Удаление компонентов антивирусной сети Dr.Web Enterprise Security Suite

Удаление **Агента Dr.Web** для станций под ОС Windows возможно следующими способами:

- По сети через Центр управления.

  Удаленная установка и деинсталляция ПО **Агента** возможны только в локальной сети и требуют полномочий администратора в этой сети. Если удаление **Агента** и антивирусного пакета осуществляется при помощи **Центра управления**, то **Карантин** со станции удален не будет.

- Локально на станции.
- Через службу Active Directory, если **Агент** был установлен при помощи данной службы.

Для станций под ОС Android, Linux, macOS удаление производится локально на станции.

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

10.1. Удаление Dr.Web Agent для ОС Windows с использованием Веб-администратора Центра управления Dr.Web Enterprise Security Suite

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

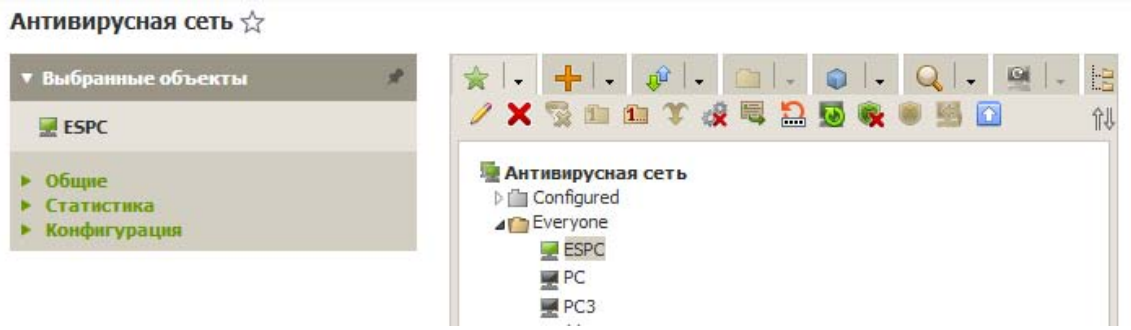
Если удаление Агента и антивирусного пакета осуществляется при помощи Центра управления, то Карантин со станции удален не будет.

Для того чтобы удалить ПО антивирусной станции удаленно:

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.

2. В открывшемся окне в каталоге антивирусной сети выберите необходимую группу или отдельные антивирусные станции.

3. На панели инструментов каталога антивирусной сети нажмите **Общие** → **Деинсталлировать Агент Dr.Web**.



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

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

При дистанционном удалении Агента (удаление на станции осуществляется в фоновом режиме) будет произведена принудительная перезагрузка станции с интервалом в пять минут. Изменение интервала, а также отмена перезагрузки невозможны. О предстоящей перезагрузке пользователям станции сообщается во всплывающем оповещении.

10.2. Удаление Агента Dr.Web и антивирусного пакета локально

Для возможности локального удаления **Агента** и антивирусного пакета данное действие должно быть разрешено на **Сервере Dr.Web** на вкладке **Общие** в разделе **Антивирусная сеть → Конфигурация → Права**.

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

1. Используя штатные средства ОС Windows.

2. При помощи инсталлятора Агента.

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

Удаление штатными средствами ОС Windows

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

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

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

Удаление при помощи инсталлятора

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

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

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

- для ОС Windows Server 2003: %ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\
- для ОС Windows Vista и старше и для ОС Windows Server 2008 и старше: %ALLUSERSPROFILE%\Doctor Web\Setup\

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

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

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

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

- **Полный инсталлятор drweb-11.05.0-<сборка>-esuite-agent-full-windows.exe**

Для того чтобы удалить ПО Агента и антивирусный пакет при помощи полного инсталлятора, запустите установочный файл drweb-11.05.0-<*сборка*>-esuite-agent-full-windows.exe той версии продукта, которая у вас установлена.

- **Сетевой инсталлятор drwinst.exe**

Для того чтобы удалить ПО Агента и антивирусный пакет при помощи сетевого инсталлятора на станции локально, необходимо в каталоге установки Агента Dr.Web (по умолчанию — C:\Program Files\DrWeb) запустить инсталлятор drwinst.exe с параметром /instMode remove. Дополнительно используйте параметр /silent no, если требуется обеспечить контроль за ходом удаления.

Например:

drwinst /instMode remove /silent no

При запуске инсталляционного пакета drweb_ess_<*ОС*>_<*станция*>.exe, полного инсталлятора drweb-11.05.0-<*сборка*>-esuite-agent-full-windows.exe и сетевого инсталлятора drwinst.exe осуществляется запуск клиентского модуля win-es-agent-setup.exe, который непосредственно осуществляет удаление.

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

10.3. Удаление Dr.Web Agent с использованием службы Active Directory

1. В Панели управления ОС Windows выберите в меню **Администрирование** элемент **Active Directory → Пользователи и компьютеры**.
2. В домене выберите созданное вами **Организационное подразделение ESS**. В контекстном меню выберите пункт **Свойства**. Откроется окно **Свойства ESS**.
3. Перейдите на вкладку **Групповая политика**. Выберите элемент списка с именем **Политики ESS**. Дважды щелкните по нему. Откроется окно **Редактор объектов групповой политики**.

4. В иерархическом списке выберите **Конфигурация компьютера → Конфигурация программ → Установка программ → Пакет**. Далее в контекстном меню пакета с дистрибутивом **Агента** выберите **Все задачи → Удалить → ОК**.
5. На вкладке **Групповая политика** нажмите **ОК**.
6. **Агент Dr.Web** будет удален с компьютеров при следующей регистрации в домене.

10.4. Удаление с использованием утилиты Drw_remover

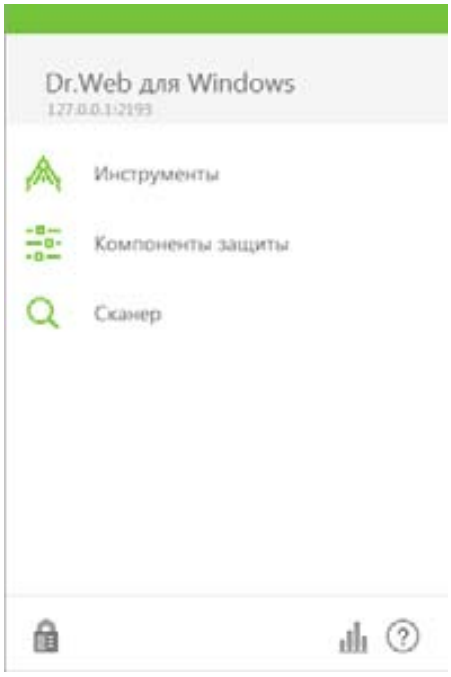
Если по какой-то причине удаление Агента штатными средствами невозможно или заканчивается ошибкой, необходимо использовать утилиту Dr.Web Remover, которую можно скачать с сайта компании «Доктор Веб».

После ее запуска на ПК с установленным продуктом Dr.Web необходимо ввести капчу (набор цифр) для подтверждения действия и после завершения удаления выполнить перезагрузку.

11. Настройка антивирусной защиты на стороне пользователя

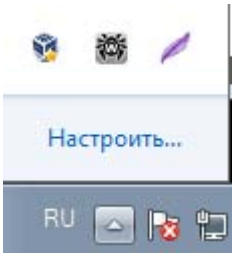
11.1. Знакомство с Агентом Dr.Web

Сразу после установки агента защиты в правом нижнем углу экрана появляется значок **Агента**  , с помощью которого можно осуществлять управление всеми настройками антивируса.



Если **Агент** не запущен и его значок отсутствует, в меню **Пуск** раскройте группу **Dr.Web** и нажмите на пункт **SpIDer Agent**.

Внимание! Если вы используете Windows 7 и выше, то для получения доступа к данному значку необходимо нажать на кнопку  (или ).



Значок **SpIDer Agent** не будет отображаться в области уведомлений в случае соответствующей настройки в Центре управления.

Значок **SpIDer Agent** отражает текущее состояние **Агент Dr.Web**:

- все компоненты, необходимые для защиты компьютера, запущены и работают правильно, соединение с сервером централизованной защиты установлено;
- Самозащита **Агент Dr.Web** или важный компонент (сторож **SpIDer Guard**, **Брандмауэр**) отключены, что ослабляет защиту антивируса и компьютера; либо ожидается соединение с сервером, но оно еще не установлено. Включите Самозащиту или отключенный компонент, дождитесь соединения с сервером;
- в процессе запуска одного из ключевых компонентов **Агент Dr.Web** возникла ошибка. Компьютер находится под угрозой заражения. Возможно, сервер отклонил подключение рабочей станции или отказал в доступе к своим ресурсам. Проверьте наличие действительного ключевого файла и при необходимости установите его или обратитесь к администратору вашей антивирусной сети.

Если настройки уведомлений не были изменены, над значком могут появляться сообщения-подсказки. Запуск и настройка компонентов антивирусного агента осуществляется с помощью контекстного меню значка модуля управления, появляющегося при нажатии на левую или правую кнопку мыши.

Внимание! Доступ к настройкам и компонентам защиты, а также отключение компонентов возможны только при работе с правами администратора.

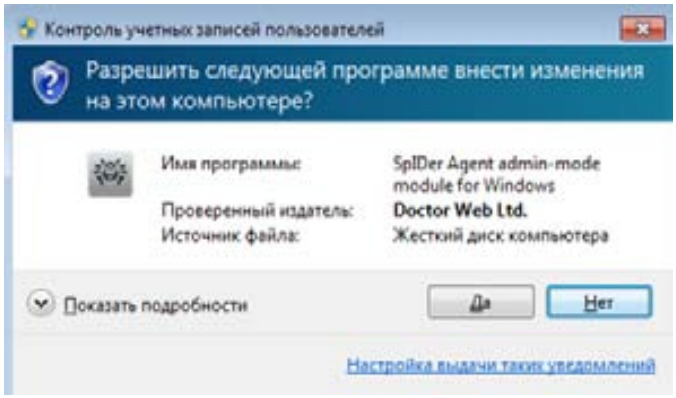
Внимание! Администратор Сервера Dr.Web имеет возможность запретить изменение любых настроек Агента Dr.Web силами локального пользователя. При полном запрете настроек у пользователя станции не будет никаких прав на изменение параметров Агента или отключение каких-либо компонентов антивируса.

Сразу после установки в меню показываются возможности, доступные обычному пользователю согласно настройкам, сделанным системным администратором в Центре управления. По умолчанию не доступны возможности настройки и останова компонентов.

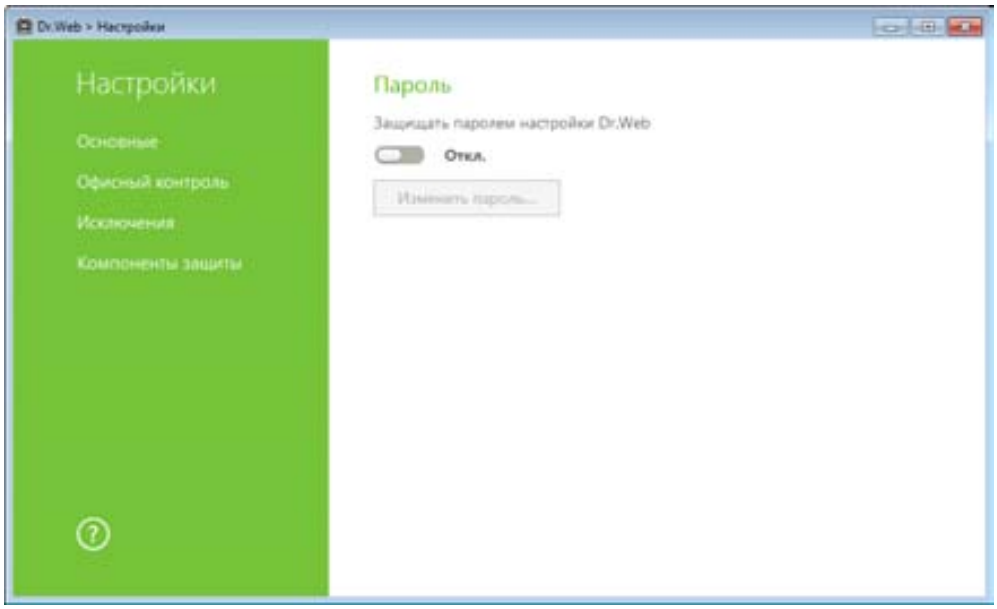
Назначение пунктов главного меню **Агента**:

- **Инструменты**. Открывает меню, предоставляющее доступ к Менеджеру карантина и разделу **Поддержка**.
- **Компоненты защиты**. Быстрый доступ к списку компонентов защиты, в котором можно при наличии прав включить или выключить каждый из компонентов.
- **Сканер**. Быстрый доступ к запуску разных типов проверки. Можно произвести быструю (проверка только наиболее часто используемых разделов памяти компьютера), полную или выборочную (только для выбранных компонентов) проверку.
- **Режим работы**. По умолчанию **Dr.Web** запускается в ограниченном режиме — режиме пользователя, в котором недоступны **Настройки** (отсутствует значок), включая возможность настройки **Компонентов защиты**. Для переключения в другой

режим необходимо щелкнуть на иконку . При включенном UAC операционная система выдаст запрос на повышение прав.



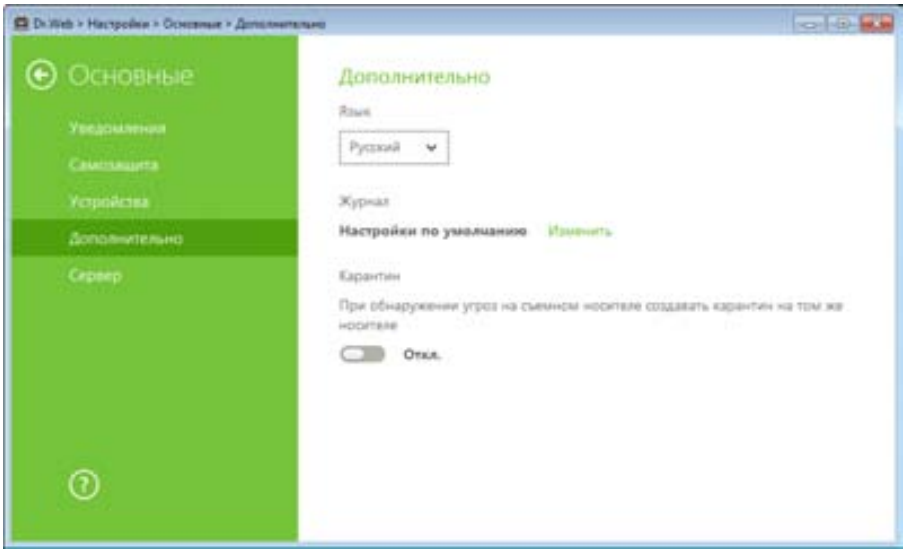
Для изменения режима работы потребуется ввести пароль, если в разделе **Настройки** была включена опция **Защищать паролем настройки Dr.Web**.



- **Статистика**. Открывает окно, содержащее сведения о работе компонентов в течение текущего сеанса (количество проверенных, зараженных и подозрительных объектов, предпринятые действия и др.).
- **Настройки**. Открывает окно с доступом к основным настройкам, настройкам компонентов защиты. Для доступа к настройкам компонентов необходимо ввести пароль, если в разделе **Настройки** была включена опция **Защищать паролем настройки Dr.Web**.
- — открывает файл справки.

11.2. Настройка языка интерфейса

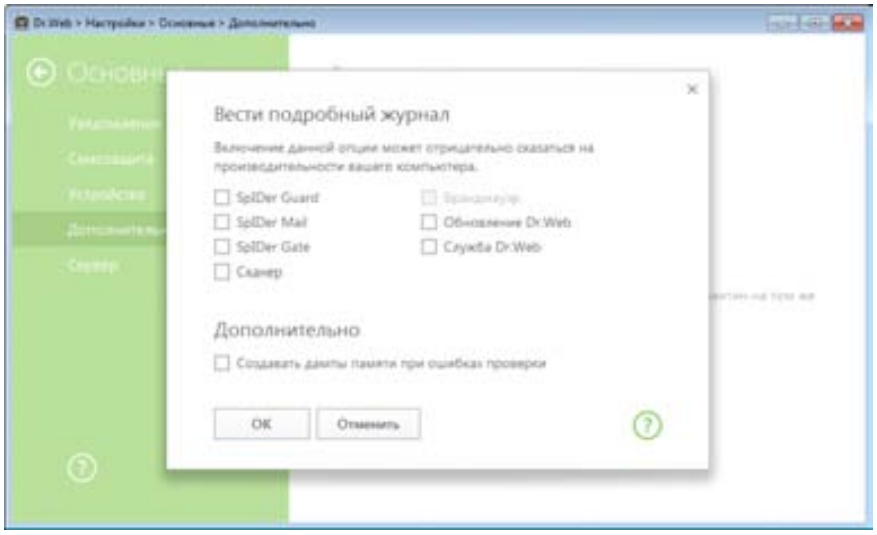
Для смены языка, щелкнув правой кнопкой мыши значок в системном трее, разблокируйте возможность изменения настроек путем нажатия значка (значок изменит вид на) и, нажав на появившийся значок , выберите в меню **Инструменты** пункт **Основные**. В открывшемся окне перейдите на пункт **Дополнительно** и в выпадающем списке **Язык** укажите необходимый язык интерфейса.



11.2.1. Изменение уровня подробности протокола событий

Для изменения уровня подробности протокола работы компонентов, щелкнув правой кнопкой мыши значок в системном трее, разблокируйте возможность изменения настроек путем нажатия значка (значок изменит вид на) и, нажав на появившийся значок , выберите в меню **Инструменты** пункт **Основные**.

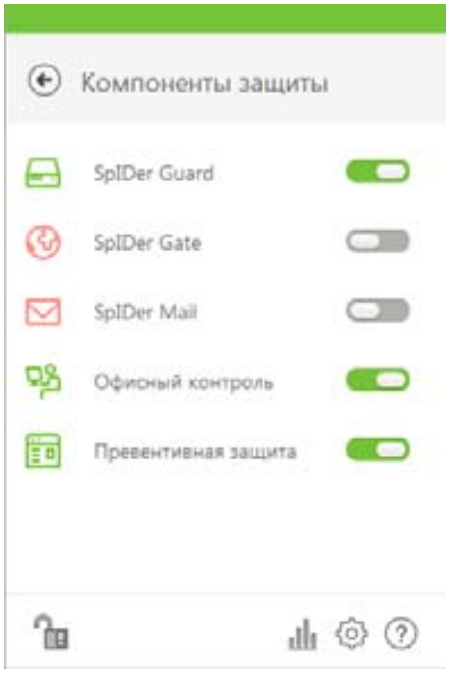
В открывшемся окне перейдите на пункт **Дополнительно** и нажмите на кнопку **Журнал → Изменить**. Отметьте компоненты, для которых уровень подробности журнала требуется изменить.



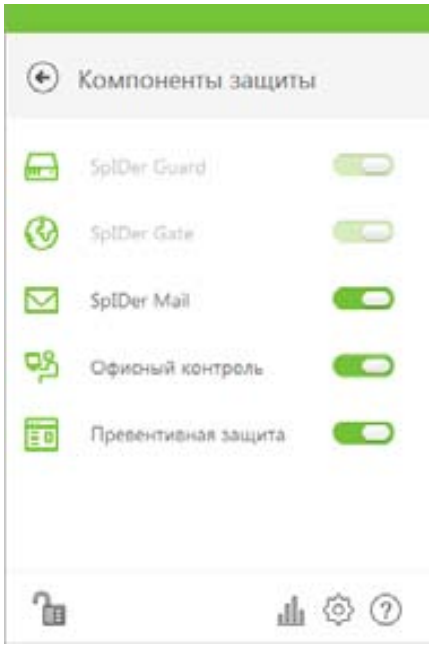
Надпись в разделе **Дополнительно** изменится на **Журнал: пользовательские настройки**.

11.3. Изменение списка разрешенных компонентов на рабочей станции

В случае наличия прав пользователь может остановить или запустить действующие у него на компьютере компоненты защиты. Для выполнения этих действий необходимо, щелкнув правой кнопкой мыши значок в системном трее, разблокировать возможность изменения настроек путем нажатия значка (значок изменит вид на) и, нажав на пункт меню **Компоненты защиты** для интересующего компонента, нажать левую или правую сторону переключателя справа от названия компонента.



Внимание! Часть пунктов может быть недоступна для изменения. Доступность настроек для редактирования определяется правами, определенными для группы или конкретной станции.



Для того чтобы настройки компонентов были доступны для пользователя, данное действие должно быть разрешено на **Сервере Dr.Web** на вкладке **Общие** в разделе **Антивирусная сеть → Конфигурация → Права**.

11.4. Антивирусная проверка станции. Выбор приоритета сканирования

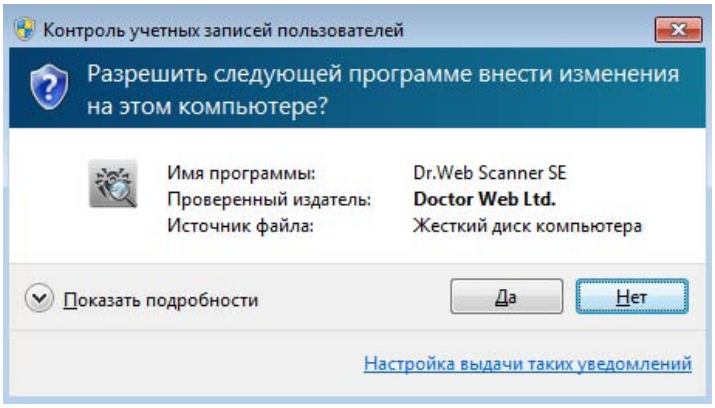
Рекомендуется сразу после инсталляции провести полную проверку системы и в дальнейшем проводить такую проверку регулярно. В частности, это необходимо в связи с тем, что проверенные файловым монитором и записанные на диск файлы (в том числе сохраненные в архивы) могут содержать вирусы, неизвестные на момент их записи на диск, а значит, при передаче их на незащищенные компьютеры (при отсутствии проверки исходящего трафика) возникает риск их заражения.

Рекомендуется запускать **Сканер** от имени пользователя, обладающего правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки), не будут подвергнуты проверке.

Для проведения проверки необходимо щелкнуть по иконке и выбрать пункт **Сканер**, либо дважды щелкнуть по иконке сканера, находящейся на рабочем столе, либо выбрать пункт меню **Сканер Dr.Web** в папке **Dr.Web** Главного меню Windows (открывается по кнопке **Пуск**).

Чтобы запустить **Сканер** с настройками по умолчанию для проверки конкретного файла или каталога, необходимо выбрать в контекстном меню значка файла или каталога (на Рабочем столе или в Проводнике операционной системы Windows) пункт **Проверить Dr.Web**.

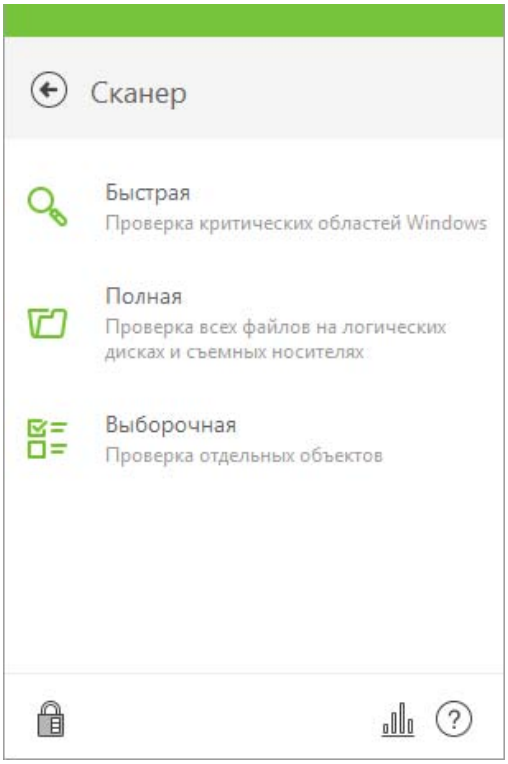
Внимание! Если вы используете ОС Windows Vista и старше (включая Windows 7/8/10) и на вашей системе включена функция контроля учетных записей Windows (UAC), то далее вам нужно будет подтвердить запуск программы, выбрав **Да**.



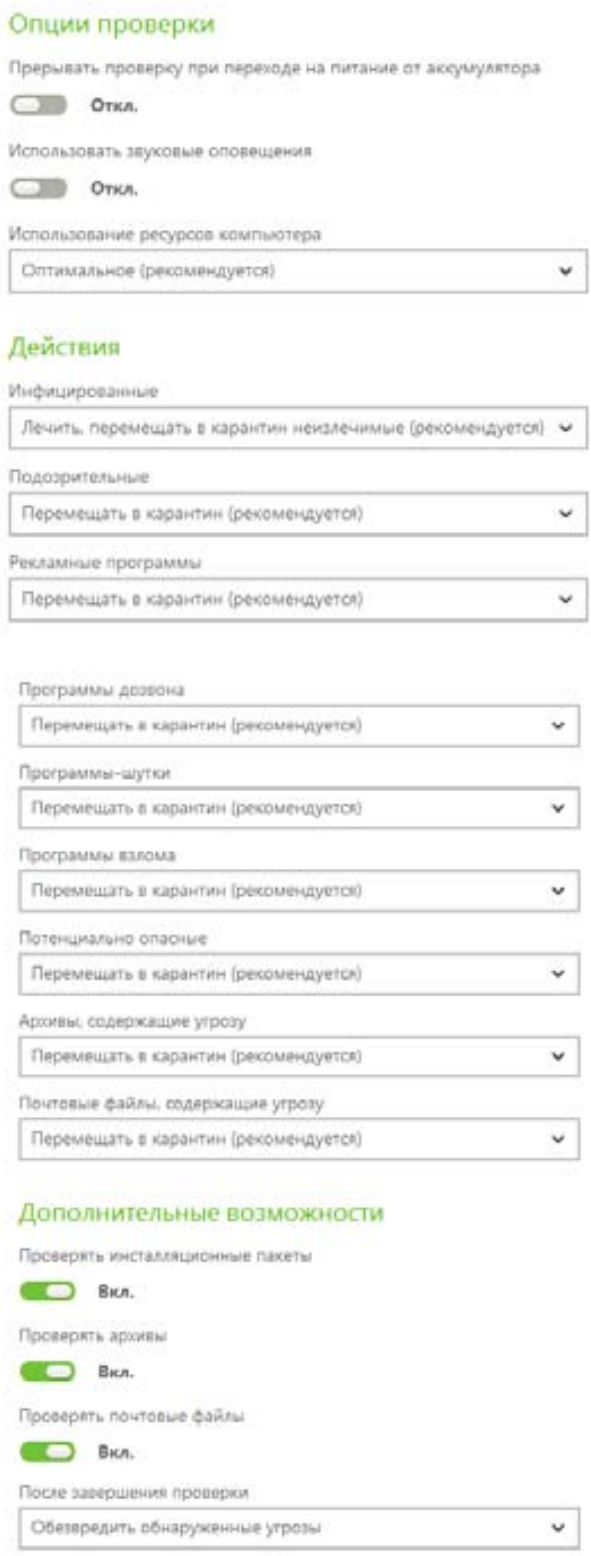
Внимание! Антивирусная проверка рабочих станций также может проводиться по расписанию Сервера Dr.Web, в таком случая у пользователя рабочей станции нет необходимости самостоятельно проводить плановую проверку.

11.4.1. Антивирусная проверка Сканером

Сильной стороной Сканера Dr.Web является возможность проверки рабочей станции не только на угрозы «верхнего» уровня, но и руткиты — вредоносное ПО «низкого» уровня загрузки. Выберите в меню Агента пункт Сканер и укажите тип проверки: быстрая, полная или выборочная.



Этот выбор влияет на проверяемые объекты, а остальные параметры сканирования задаются отдельно в настройках Сканера (**Настройки → Компоненты защиты → Сканер**).



В разделе **Действия** пользователь может определить действия, применяемые к вредоносным объектам различного типа. По умолчанию для всех объектов (кроме инфицированных) стоит действие **Перемещать в карантин**.

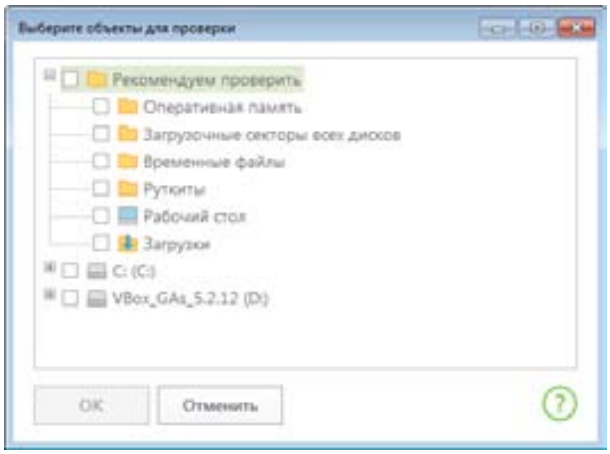
Необходимо отметить, что для различных объектов список возможных действий является различным. Так, для неизлечимых пункт **Лечить** недоступен — в отличие от инфицированных.

Ниже можно настроить список проверяемых файлов (**Архивы**, **Почтовые файлы** и **Инсталляционные пакеты)** и действие после окончания проверки.

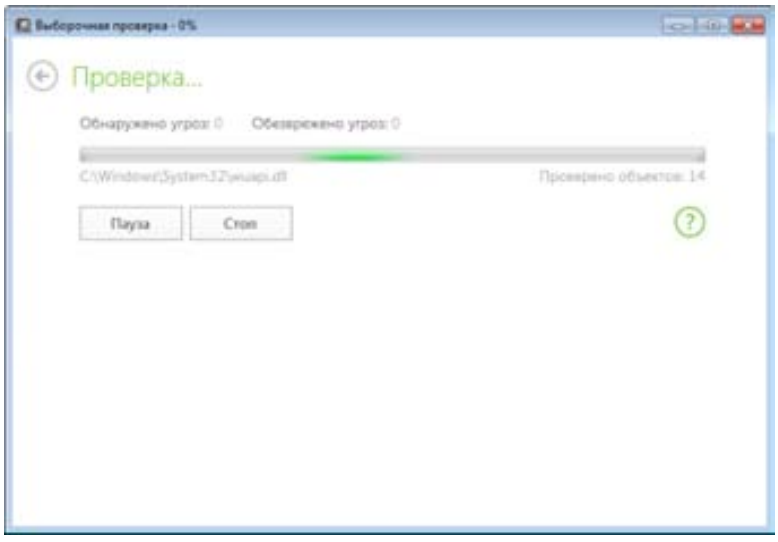
Также эти настройки могут быть заданы с Сервера Dr.Web, а также их изменение может быть запрещено администратором Сервера.

Задать исключения для проверки Сканером можно в разделе **Настройки → Исключения → Файлы и папки** для компонента **Сканер.** Подробное протоколирование проверки (ведение подробного журнала) включается с помощью соответствующего флажка в разделе **Настройки → Основные → Дополнительно → Журнал** (изменить). По аналогии с настройками, эти параметры могут быть заданы администратором Сервера Dr.Web.

В случае выборочного типа проверки пользователь может указать интересующие объекты проверки. Для проверки дисков, отдельных папок и файлов пользователь может перетащить их в окно сканера — или указать вручную.



Для запуска быстрой или полной проверки нужно в главном окне сканера нажать на пункты **Быстрая** и **Полная** соответственно. Выборочная проверка запускается из окна настроек **Выборочная проверка**.



Остановить проверку компьютера можно, нажав **Стоп**. Кнопка **Пауза** недоступна во время проверки оперативной памяти и процессов.

Если в настройках **Сканера Dr.Web** установлено действие **Обезвредить обнаруженные угрозы**, то ко всем обнаруженным угрозам будут применены соответствующие их типам действия, в противном случае по окончании проверки **Сканер** лишь информирует об обнаруженных угрозах и предлагает применить к ним наиболее оптимальные действия по обезвреживанию.

Вы можете обезвредить все обнаруженные угрозы одновременно. Для этого после завершения проверки нажмите кнопку **Обезвредить**. По нажатию кнопки **Обезвредить** к выбранным объектам в таблице применяются предопределенные действия. Если вы хотите изменить действие для части объектов, то в поле **Действие** в выпадающем списке выберите необходимое действие для каждого объекта.

По умолчанию после окончания проверки для обезвреживания выбраны все объекты, но никаких действий не предпринимается. При необходимости вы можете вручную выбрать конкретные объекты или группы объектов, для которых требуется применить действия по нажатию кнопки **Обезвредить**. Для этого используйте флажки рядом с названиями объектов или выпадающее меню.

Существуют следующие ограничения:

- лечение подозрительных объектов невозможно;
- перемещение или удаление объектов, не являющихся файлами (например, загрузочных секторов), невозможно;
- невозможны любые действия для отдельных файлов внутри архивов, инсталляционных пакетов или в составе писем — действие в таких случаях применяется только ко всему объекту целиком.

Подробный отчет о работе программы сохраняется в виде файла журнала *dwscanner.log*, который находится в папке *%USERPROFILE%\Doctor Web*.

11.4.2. Запуск антивирусной проверки из командной строки

Чтобы запустить **Сканер** с дополнительными параметрами командной строки, воспользуйтесь следующей командой:

[<*путь_к_программе*>]dwscanner [<*ключи*>] [<*объекты*>]

где:

<*объекты*> — список объектов для проверки;

<*ключи*> — параметры командной строки, которые задают настройки работы **Сканера**. При их отсутствии проверка выполняется с ранее сохраненными настройками (или настройками по умолчанию, если они не были изменены).

По умолчанию <*путь_к_программе*> — C:\Program Files\DrWeb

Список объектов для проверки может быть пуст или содержать несколько элементов, разделенных пробелами. Наиболее распространенными являются следующие варианты проверки:

/FAST — произвести быструю проверку системы.

/FULL — произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы).

/LITE — произвести стартовую проверку системы, при которой проверяются оперативная память, загрузочные секторы всех дисков, а также провести проверку на наличие руткитов.

Параметры — ключи командной строки, которые задают настройки программы. При их отсутствии проверка выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их). Ключи начинаются с символа «/» и, как и остальные параметры командной строки, разделяются пробелами.

В состав **Dr.Web** также входит **Консольный сканер**, который позволяет проводить проверку в режиме командной строки, а также предоставляет большие возможности настройки.

Чтобы запустить **Консольный сканер**, воспользуйтесь следующей командой:

[<*путь_к_программе*>]dwscancl [<*ключи*>] [<*объекты*>]

где:

<*объекты*> — список объектов для проверки;

<*ключи*> — список параметров командной строки, которые задают настройки работы **Консольного сканера**. Ключ начинается с символа «/», несколько ключей разделяются пробелами.

Список объектов проверки может быть пуст или содержать несколько элементов, разделенных пробелами.

Список ключей **Консольного сканера** содержится в Приложении к Руководству пользователя.

После выполнения **Консольный сканер** возвращает один из следующих кодов:

0 — проверка успешно завершена, инфицированные объекты не найдены;

1 — проверка успешно завершена, найдены инфицированные объекты;

10 — указаны некорректные ключи;

11 — ключевой файл не найден либо не поддерживает **Консольный сканер**;

12 — не запущен **Scanning Engine**;

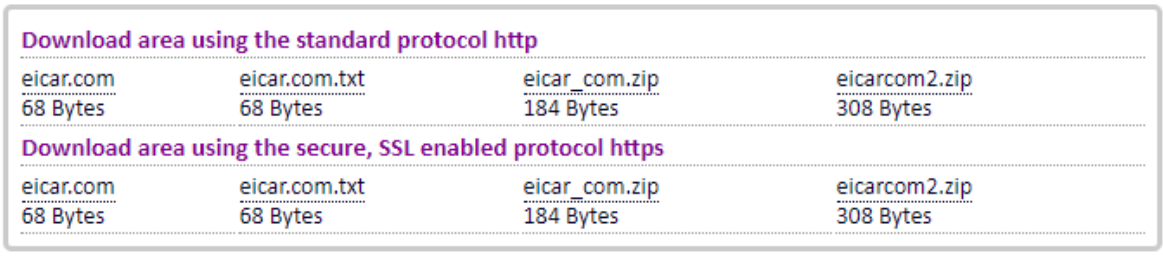
255 — проверка прервана пользователем.

11.5. Проверка работоспособности продукта

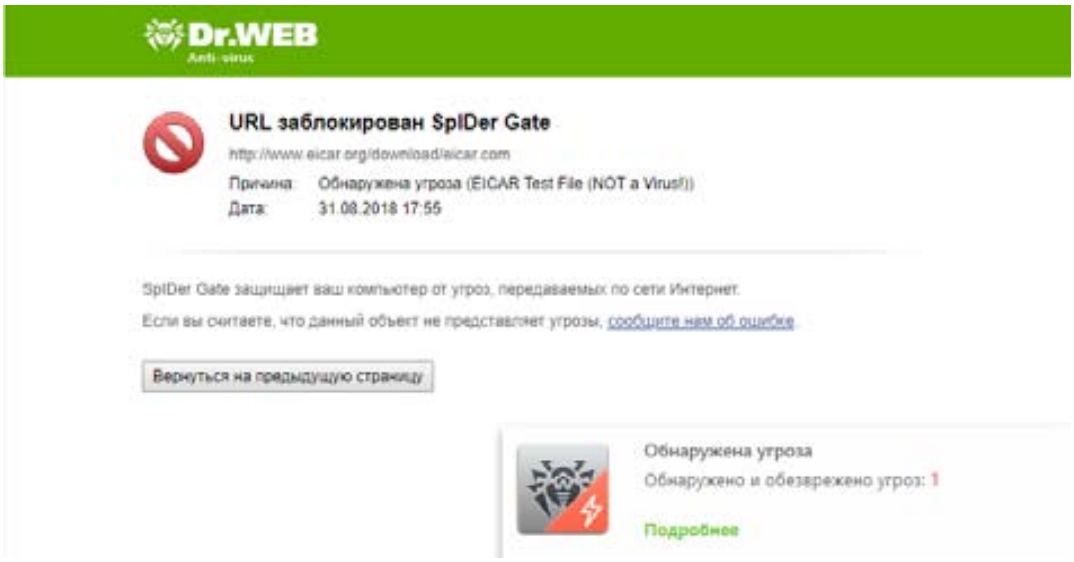
После установки антивирусного продукта, как и любой другой программы, всегда возникает желание проверить его в деле. Это можно сделать в случае, если полная проверка ничего не нашла и возникли сомнения в работоспособности антивируса. Специально для этого был разработан специальный тестовый файл *eicar.exe*, сам по себе не являющийся вирусом, но вызывающий защитную реакцию всех антивирусов.

Чтобы скачать тестовый файл откройте официальный сайт поддерживающей его некоммерческой организации: http://www.eicar.org/85-0-Download.html.

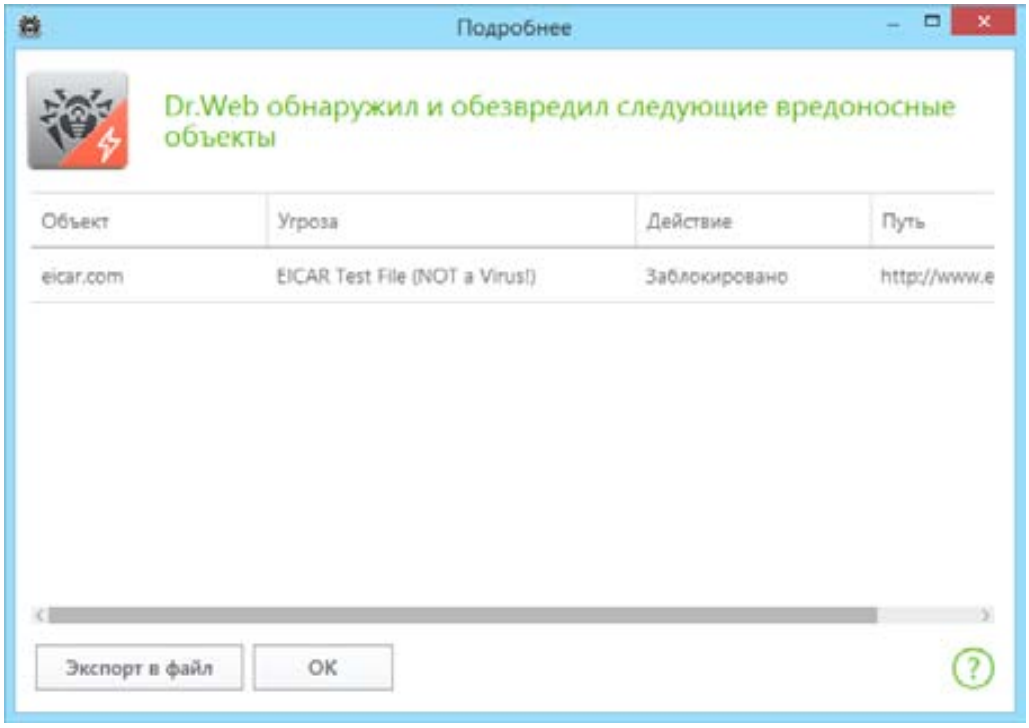
На открывшейся странице найдите раздел:



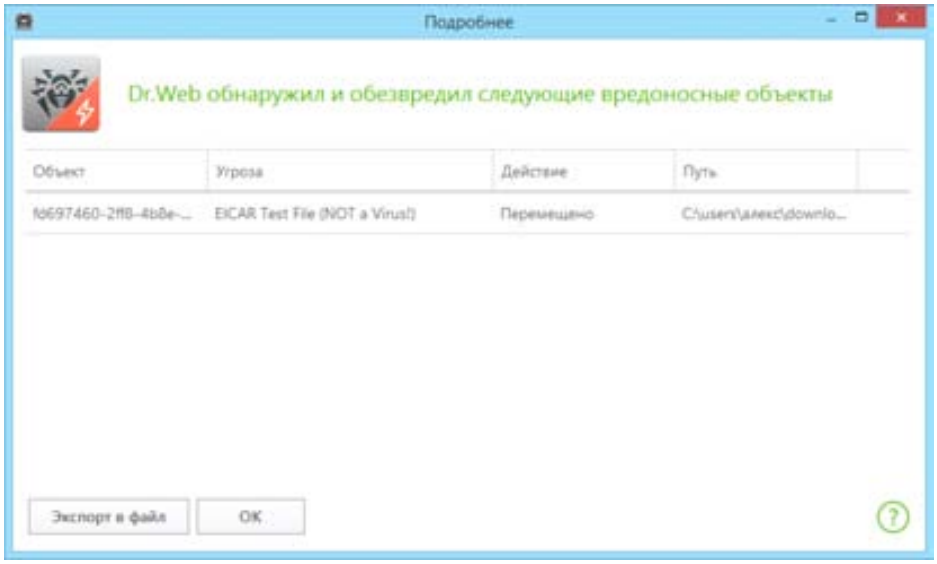
Выберите для скачивания любой из предложенных вариантов, например первый — eicar.com. В том случае, если защита работает корректно, ваш браузер должен показать следующее окно:



Нажав на кнопку **Подробнее** всплывающего окна, мы можем получить более подробную информацию и экспортировать ее.



Если вы хотите проверить работу файлового монитора, то вы должны сначала получить файл с тестовым вирусом. Для этого отключите **SpIDer Gate**, выбрав соответствующий пункт в подменю **Компоненты защиты** меню агента и нажав на переключатель справа от названия компонента. Вернитесь на сайт eicar.org и снова попытайтесь закачать тестовый вирус. Итогом попытки должно стать окно типа:



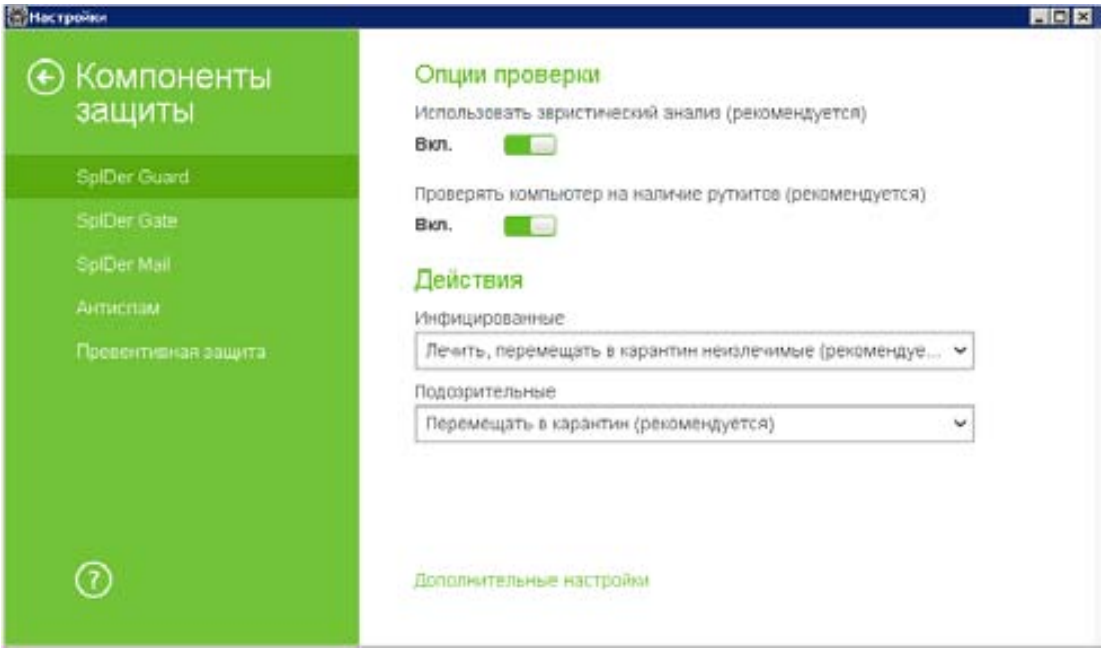
При работе в оптимальном режиме **SpIDer Guard** не прерывает запуск тестового файла EICAR и не определяет данную операцию как опасную, так как данный файл не представляет угрозы для компьютера. Однако при копировании или создании такого файла на компьютере **SpIDer Guard** автоматически обрабатывает файл как вредоносную программу и по умолчанию перемещает его в **Карантин**.

После завершения проверки не забудьте вновь включить **SpIDer Gate!**

11.6. Выбор действия по умолчанию

По умолчанию для всех типов вредоносного ПО, кроме инфицированных файлов задано действие **Перемещать в карантин**. При этом пользователь сам должен принимать решение о том, что делать с обнаруженными вредоносными объектами в дальнейшем.

Для настройки действий при обнаружении вредоносных файлов различных типов, щелкнув кнопкой мыши значок в системном трее, разблокируйте возможность изменения настроек путем нажатия значка (значок изменит вид на) и, нажав на появившийся значок , выберите в меню **Инструменты** пункт **Компоненты защиты**. В открывшемся окне **Компоненты защиты** выберите интересующий компонент. Например, пункт **SpIDer Guard**.



Существуют следующие действия, применяемые к обнаруженным объектам:

- **Лечить, перемещать в карантин неизлечимые** — восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет перемещен в карантин. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов.
- **Лечить, удалять неизлечимые** — восстановить состояние объекта до заражения. Если вирус неизлечим или попытка лечения не была успешной, то объект будет удален. Данное действие возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов.
- **Удалить** — удалить объект. Для загрузочных секторов никаких действий производиться не будет.
- **Перемещать в карантин** — переместить объект в специальную папку **Карантина**. Для загрузочных секторов никаких действий производиться не будет.
- **Игнорировать** — пропустить объект без выполнения каких-либо действий и не выводить оповещения. Данное действие возможно только для следующих вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

При этом:

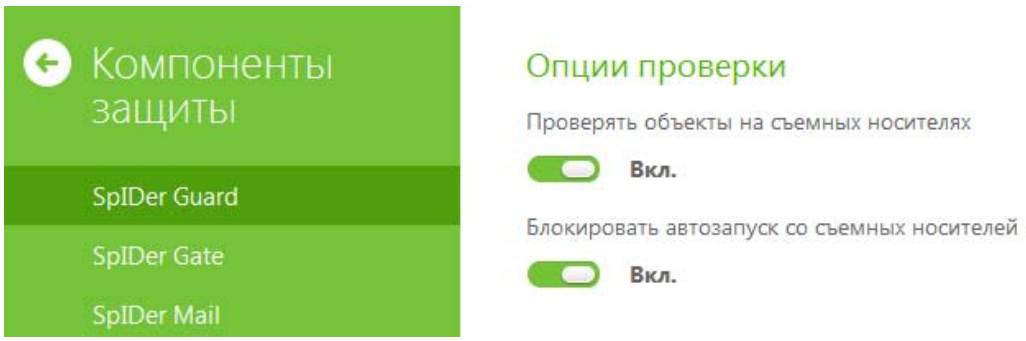
- **SpIDer Guard** не проверяет составные объекты, поэтому никакие действия над ними или входящими в их состав файлами не производятся.
- Резервные копии обработанных объектов сохраняются в **Карантине**.

Предлагаемый для компонента список действий различается для вредоносных программ различного типа. Так, для инфицированных программ на выбор предлагаются действия **Лечить…**, **Перемещать в карантин** и **Удалить**. Необходимо понимать, что для троянских программ действие **Лечить** невозможно, поскольку они сами по себе являются вредоносными программами, а не поражают изначально полезные файлы.

Для доступа к настройкам сторожа **SpIDer Guard** запрашивается пароль, если в разделе **Настройки** вы включили опцию **Защищать паролем настройки Dr.Web**.

11.7. Защита от неизвестных угроз. Превентивная защита

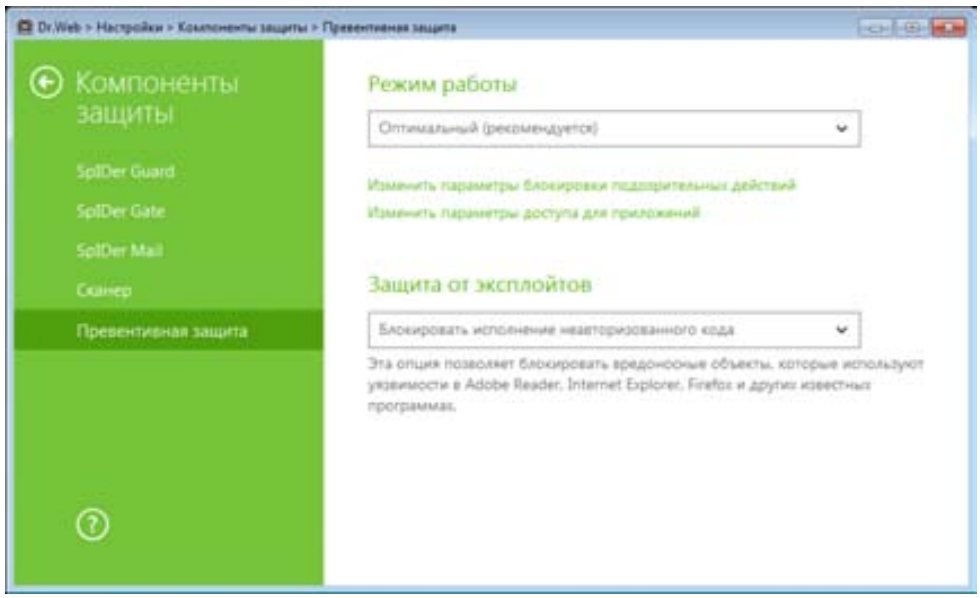
При подсоединении нового носителя информации (съемного устройства) в современных операционных системах по умолчанию срабатывает система автозапуска. Она сканирует содержимое носителя и предлагает пользователю список возможных действий. Существует целый ряд вредоносных программ, загружающихся в память ПК при установке в привод инфицированного флеш-накопителя или пораженного мобильного устройства. Чтобы предотвратить их активацию, необходимо с помощью компонента **SpIDer Gate** запретить автозапуск со всех съемных носителей.

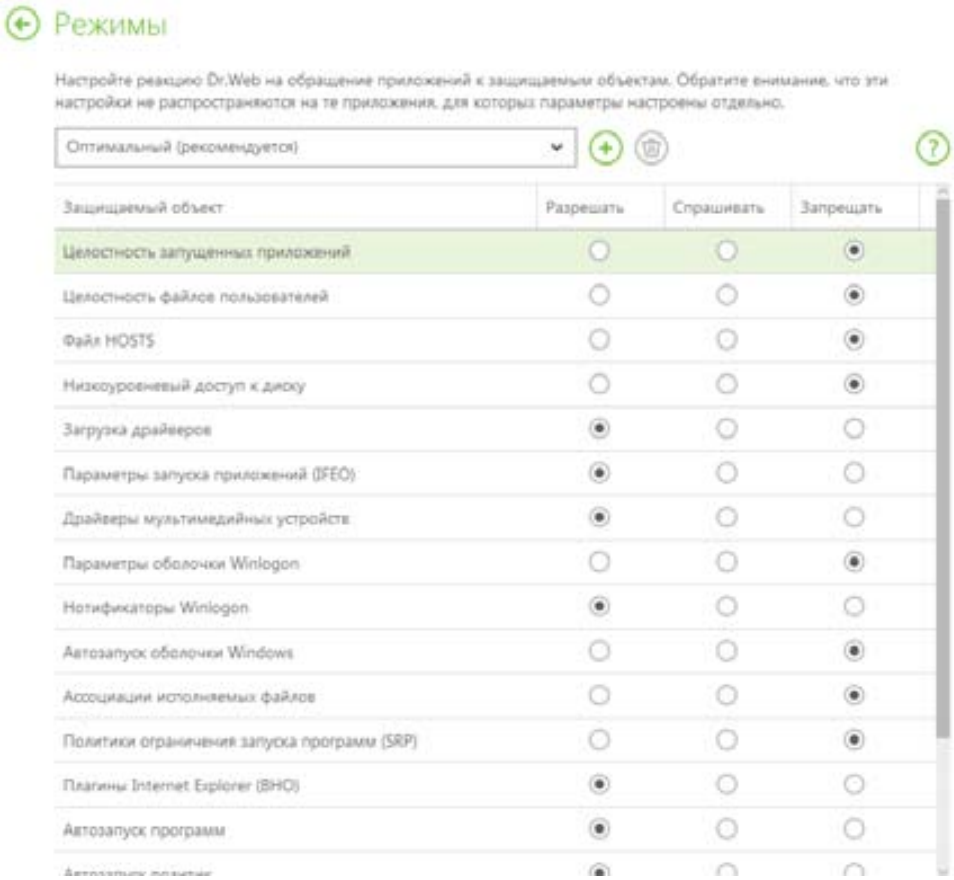


Для этого в меню Агента разблокируйте доступ к настройкам, нажав 🔒, после чего перейдите в раздел **Настройки → Компоненты защиты → SpIDer Guard** и установите переключатель **Блокировать автозапуск со съемных носителей** в положение **Вкл**.

Основным компонентов антивируса, позволяющем реагировать на еще неизвестные угрозы (отсутствующие в базах антивируса) является **Превентивная защита**. Для настройки ее параметров в меню Агента разблокируйте доступ к настройкам, нажав 🔒, после чего перейдите в раздел **Настройки → Компоненты защиты → Превентивная защита**.

В данном разделе вы можете настроить реакцию антивируса на действия сторонних приложений, которые могут привести к заражению вашего компьютера. Настройка параметров превентивной защиты позволяет держать под контролем все попытки изменения критических областей Windows. По умолчанию установлен **Оптимальный** режим проверки.





В режиме работы **Оптимальный**, установленном по умолчанию, запрещается автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещается низкоуровневый доступ к диску для защиты системы от заражения буткитами и троянцами-блокировщиками, которые заражают главную загрузочную запись диска. Для предотвращения блокировки доступа к обновлениям антивируса через Интернет и блокировки доступа на сайты производителей антивирусов запрещается модификация файла HOSTS.

При повышенной опасности заражения необходимо увеличить уровень защиты до **Среднего**. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.

Внимание! В этом режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

При необходимости полного контроля за доступом к критическим объектам Windows можно поднять уровень защиты до **Параноидального**. В данном случае будет доступен интерактивный контроль за загрузкой драйверов и автоматическим запуском программ.

Пользовательский режим позволяет гибко настроить реакцию антивируса на определенные действия, которые могут привести к заражению вашего компьютера.

Для самостоятельного задания параметров защиты выберите режим **Пользовательский** и выполните настройку, определив действия для каждого элемента списка.

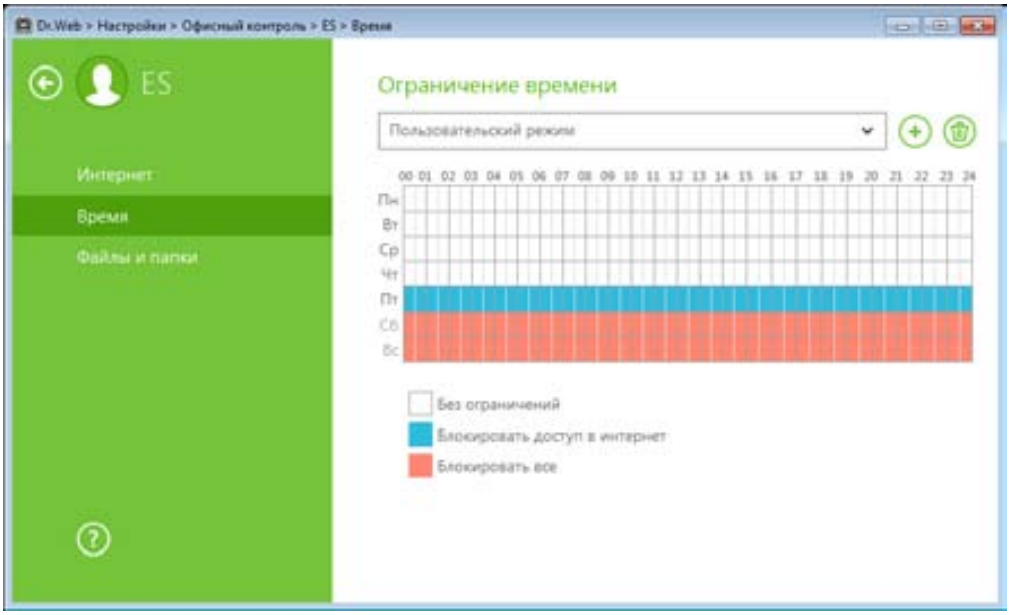
11.8. Ограничения времени доступа к Интернету и учетной записи

С помощью модуля **Офисного контроля** осуществляется ограничение доступа пользователей локального ПК к Интернету, определенным файлам и каталогам, а также компьютеру в целом. Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность и конфиденциальность важных данных и защитить файлы от заражения. Существует возможность защиты как отдельных файлов, так и каталогов целиком, при этом не важно, расположенных они на локальных дисках или на внешних носителях.

Контроль доступа к интернет-ресурсам позволяет как оградить пользователей от просмотров некоторых нежелательных сайтов (например, социальных сетей с рабочего ПК, если в этом нет производственной необходимости), так и жестко ограничить доступ в Интернет, разрешив пользователю доступ только к тем сайтам, которые определены настройками модуля **Офисного контроля —** по правилам **Белого списка.**

Параметры **Офисного контроля** распространяются одновременно на всех пользователей компьютера, на котором установлен **Агент Dr.Web**. По умолчанию для всех учетных записей разрешен неограниченный доступ к ресурсам сети Интернет и к локальным ресурсам, ограничения по времени отсутствуют.

Для ограничения времени доступа к Интернету в меню Агента разблокируйте доступ к настройкам, нажав , после чего перейдите в раздел **Настройки → Офисный контроль**. В открывшемся окне выберите пользователя, для которого будут настроены ограничения, после чего в разделе **Время нажмите** Изменить. Откроется окно **Ограничение времени**.



С помощью временной сетки настройте расписание доступа. Для этого наведите курсор на любой белый квадрат. При однократном щелчке левой клавиши мыши квадрат окрасится в голубой цвет, при двойном щелчке — в бордовый цвет, при тройном щелчке — в белый цвет. Синий цвет означает, что в заданный период времени будет заблокирован доступ в Интернет, бордовый — блокировка на пользование учетной записью (невозможно использовать компьютер под учетной записью, для которой настроена такая блокировка), белый — ограничения отсутствуют. Добившись нужного цвета квадрата, удерживайте левую клавишу мыши нажатой и проведите курсором таким образом, чтобы нужные квадраты изменили цвет. Таким образом настраивается расписание работы пользователя для конкретной учетной записи. В данном примере пользователь не сможет пользоваться компьютером по выходным, сможет работать на компьютере в будни, но не все время сможет выйти в Интернет по пятницам.

При включении ограничений времени работы за компьютером или в сети Интернет, автоматически включается опция **Запрещать изменение даты и времени системы** в разделе **Самозащита** основных настроек.

11.9. Контроль доступа к Интернет и сетевым ресурсам

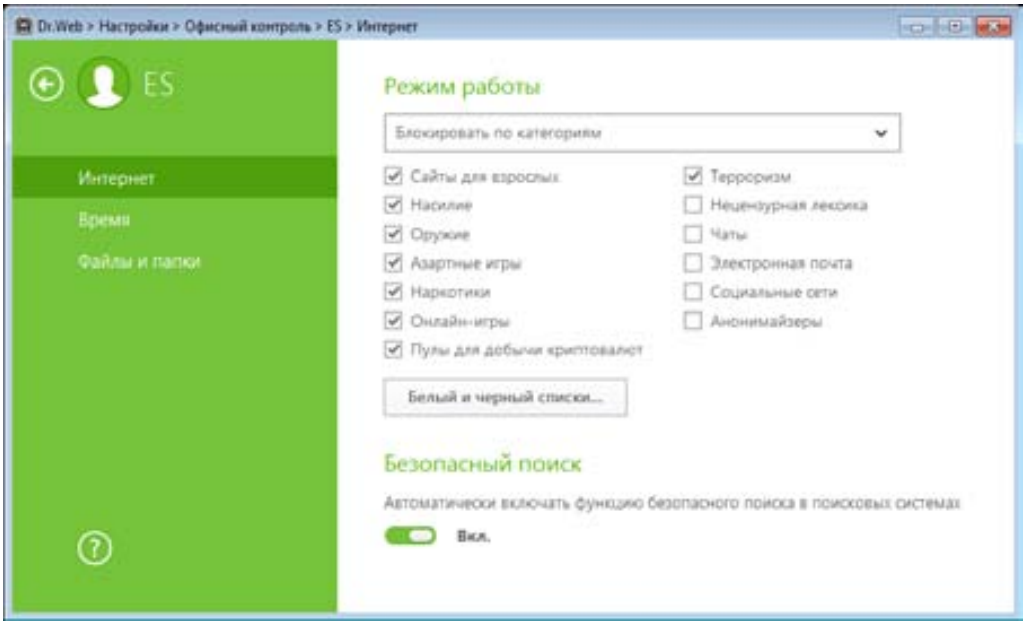
Пользователь может ограничить доступ к сменным носителям, файлам и папкам, тем самым уменьшив риск проникновения вредоносных программ.

Доступ к изменению настроек модуля может быть защищен паролем. Изменить пароль вы можете в главном окне настроек Агента.

Внимание! Все используемые пароли должны иметь достаточную длину — не менее 8 символов, в них не должны использоваться простые сочетания букв или последовательности цифр. Использование простых комбинаций делает возможным злонамеренное проникновение через перебор вариантов пароля.

Если для пользователя не установлены ограничения на посещение определенных веб-ресурсов, то в окне **Интернет Офисного контроля** будет отображено значение **Без ограничений**. Нажмите **Изменить** и выберите один из вариантов:

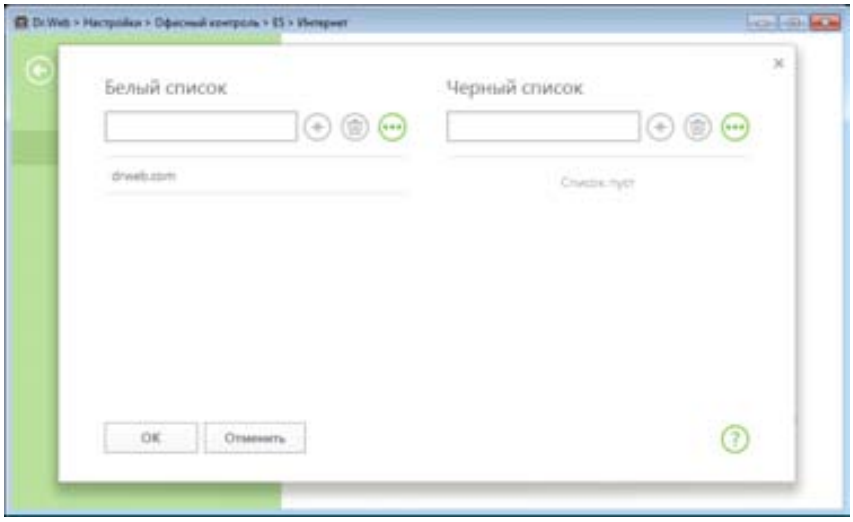
Блокировать по категориям, чтобы ограничить доступ к сайтам на основе предустановленных групп. В случае такого выбора пользователю доступен выбор групп сайтов (сайты для взрослых, насилие, оружие и т. п.), к которым необходимо ограничить доступ.



Блокировать все, кроме сайтов из белого списка — в этом режиме запрещается доступ ко всем ресурсам, кроме тех, что добавлены в Белый список Офисного контроля.

Приоритет списков выше приоритета предустановленных групп. Например, вы выбрали группу **Социальные сети**, но адрес сети «В Контакте» добавили в белый список. Тогда доступ ко всем социальным сетям, за исключением «В Контакте», будет запрещен.

Для редактирования белых и черных списков нажмите на кнопку **Белый и черный списки**.

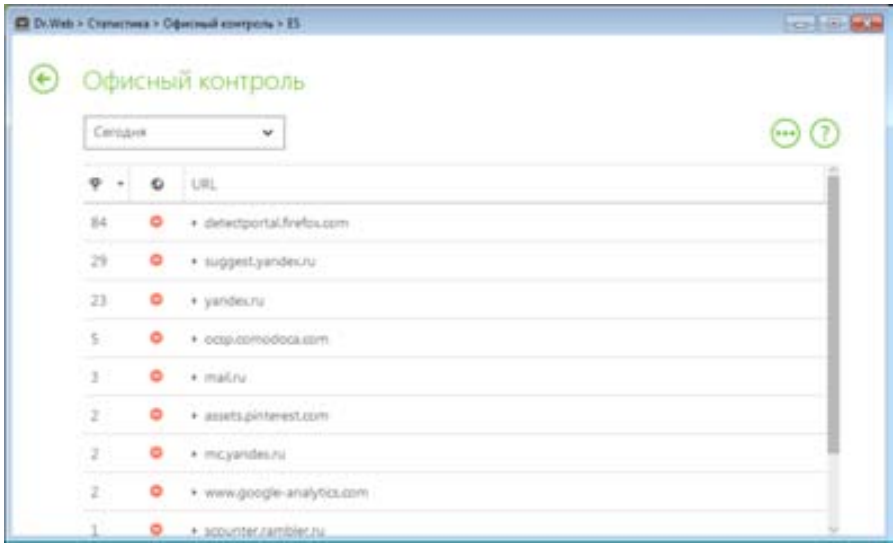


Вы можете добавить адреса веб-сайтов:

- в белый список — доступ к нему будет предоставляться вне зависимости от других настроек **Офисного контроля**;
- в черный список — доступ к нему будет блокироваться вне зависимости от других настроек **Офисного контроля**.

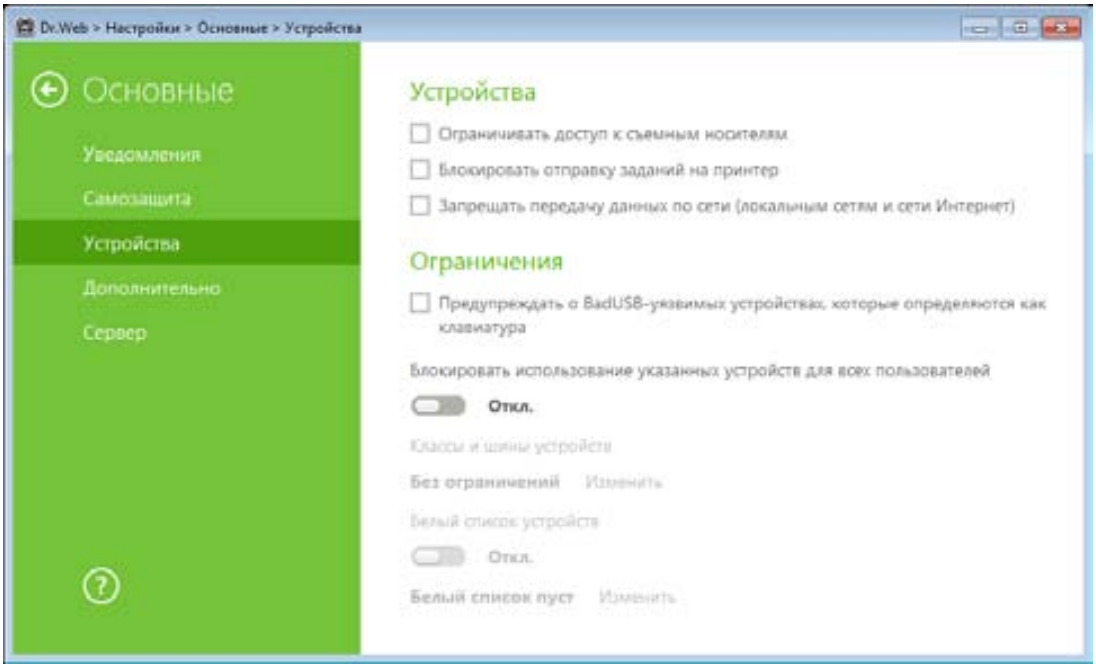
В поле **Белый список** введите адрес веб-ресурса, доступ к которому нужно разрешить. Нажмите на кнопку . Адрес ресурса будет помещен в перечень **Белый список**. Аналогично можно заполнить **Черный список**. Нажмите на кнопку **ОК** для сохранения настроек.

Просмотреть статистику обращений к различным ресурсам можно, нажав в меню Агента на значок .



11.10. Управление доступом к папкам и оборудованию ПК

С помощью функций Агента**,** задающихся в разделе **Настройка → Основные → Устройства** можно запретить запись данных на съемные носители, ограничить доступ к конкретным устройствам либо разрешить доступ только с определенных устройств, запретить передачу данных по локальным сетям и сети Интернет.



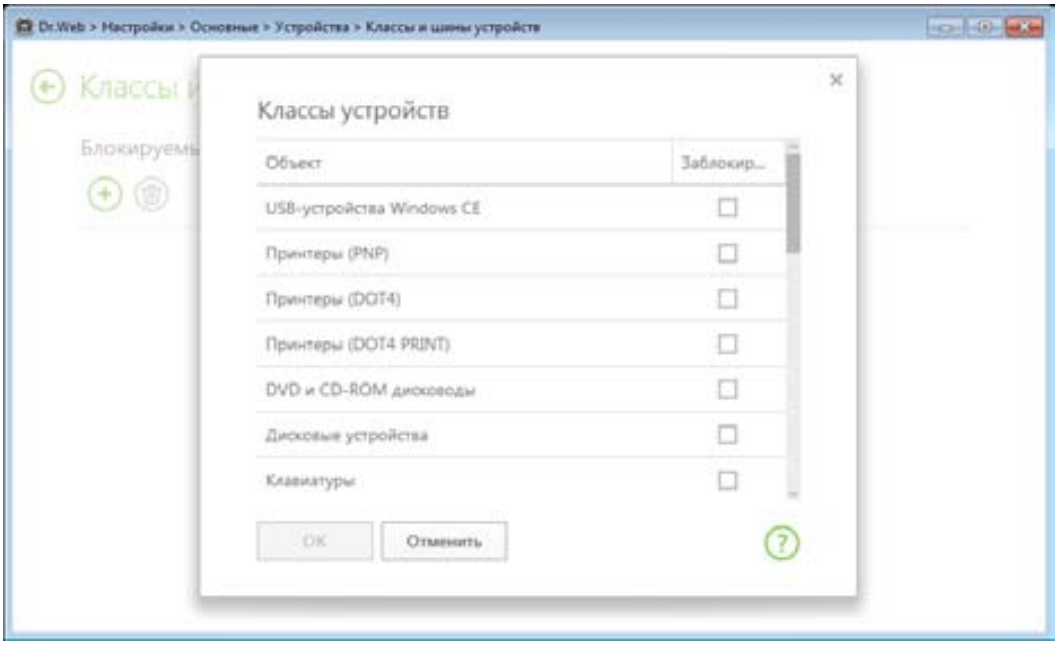
Внимание! В отличие от настроек Офисного контроля, параметры доступа устанавливаются сразу для всех учетных записей Windows.

Флажок **Ограничивать доступ к сменным носителям** запрещает доступ к любым типам накопителей, подключенным к портам USB. При этом если подключается мобильное устройство, то работа с ним будет возможна, но если при подключении указать его как съемный накопитель — доступ будет заблокирован.

Внимание! Большинство смартфонов, многие MP3-проигрыватели и некоторые другие устройства подключаются к компьютеру не по протоколу сменных носителей, а по протоколу MTP и, соответственно, не блокируются как сменные носители. Для блокировки таких устройств нужно в параметрах **Классов устройств** отметить флажком пункт **Переносные устройства Windows**.

Чтобы ограничить доступ к определенным устройствам и компонентам ПК, нажмите на переключатель **Блокировать использование указанных устройств для всех пользователей**. Для формирования списка ресурсов ограниченного доступа нажмите **Изменить**, выбрав пункт **Классы устройств** или **Шины устройств** — для ограничения доступа к конкретному устройству или целому классу устройств.

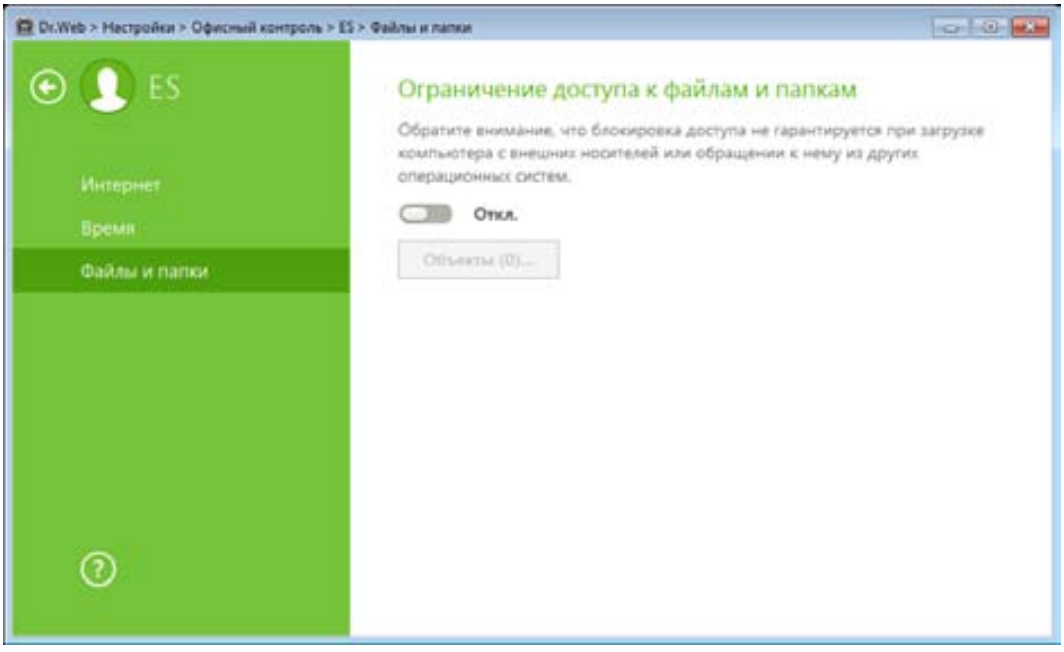
Внимание! Правила ограничения доступа классу устройств являются более приоритетными, чем отдельные правила для конкретных устройств данного типа. Например, если вы запретите доступ ко всем сменным носителям, то добавленное ранее правило для определенного флеш-накопителя перестанет действовать.



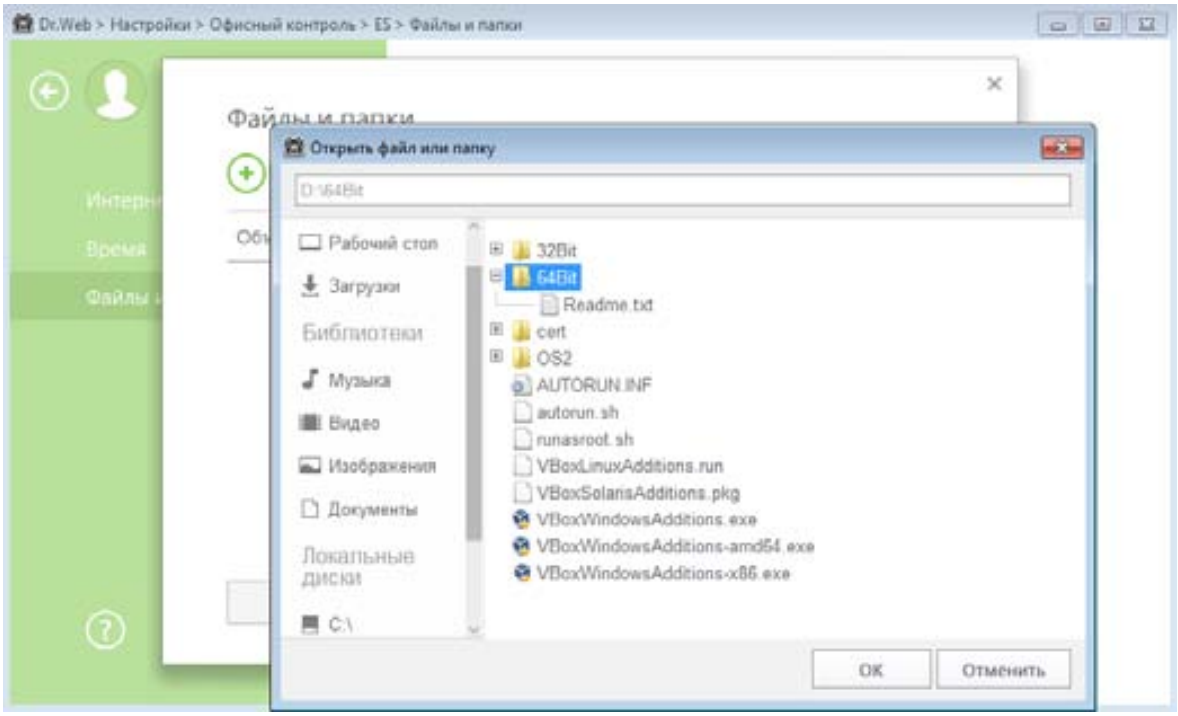
Внимание! Не ограничивайте доступ к видеоадаптерам, клавиатурам, мониторам и мышам!

Вы можете запретить пользователям использование всех видов сетей, установив флажок **Запрещать передачу данных по сети** и использование принтеров флажком **Блокировать отправку заданий на принтер**.

Также можно ограничить доступ к конкретному файлу или папке, для этого откройте настройки **Офисного контроля**, выберите пользователя, для которого настраивается доступ, после чего в разделе **Файлы и папки** нажмите **Изменить**.



В от крывшемся окне установите переключатель в положение **Вкл.**, после чего откроется окно добавления объектов. Нажмите и укажите файлы и папки, доступ к которым надо запретить, после чего нажмите **ОК**.



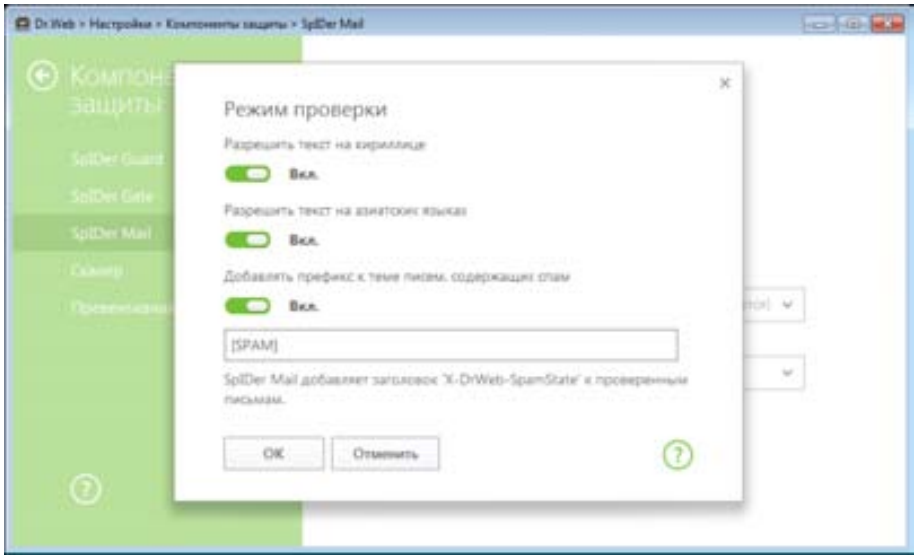
За раз может быть заблокирован доступ только к определенному файлу или папке (со всеми подпапками), для формирования списка запрещенных объектов повторите процедуру необходимое количество раз.

11.11. Защита почты

Почта являлась и является одним из основных путей проникновения вирусов на ваш компьютер. Используя возможности почтового монитора **SpIDer Mail**, пользователь может не только получать всегда чистую от вирусов почту, но и защитить свой почтовый ящик от спама.

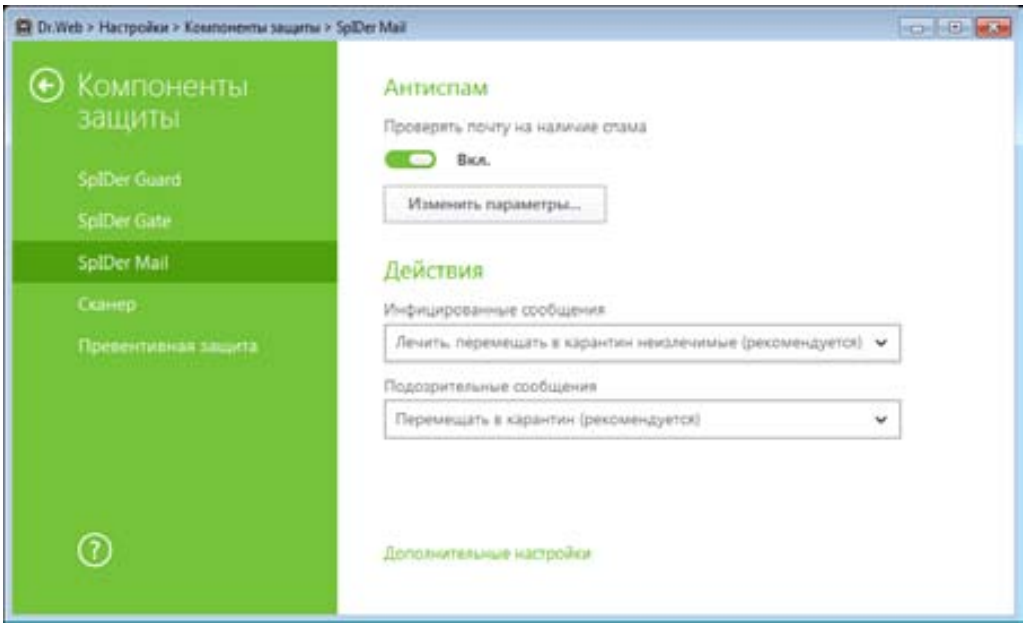
Для настройки защиты почты в меню Агента разблокируйте доступ к настройкам, нажав  , после чего перейдите в раздел **Настройки → Компоненты защиты → SpIDer Mail**.

Убедитесь, что переключатель **Проверять почту на наличие спама** установлен в положение **Вкл.** и для него заданы корректные настройки.

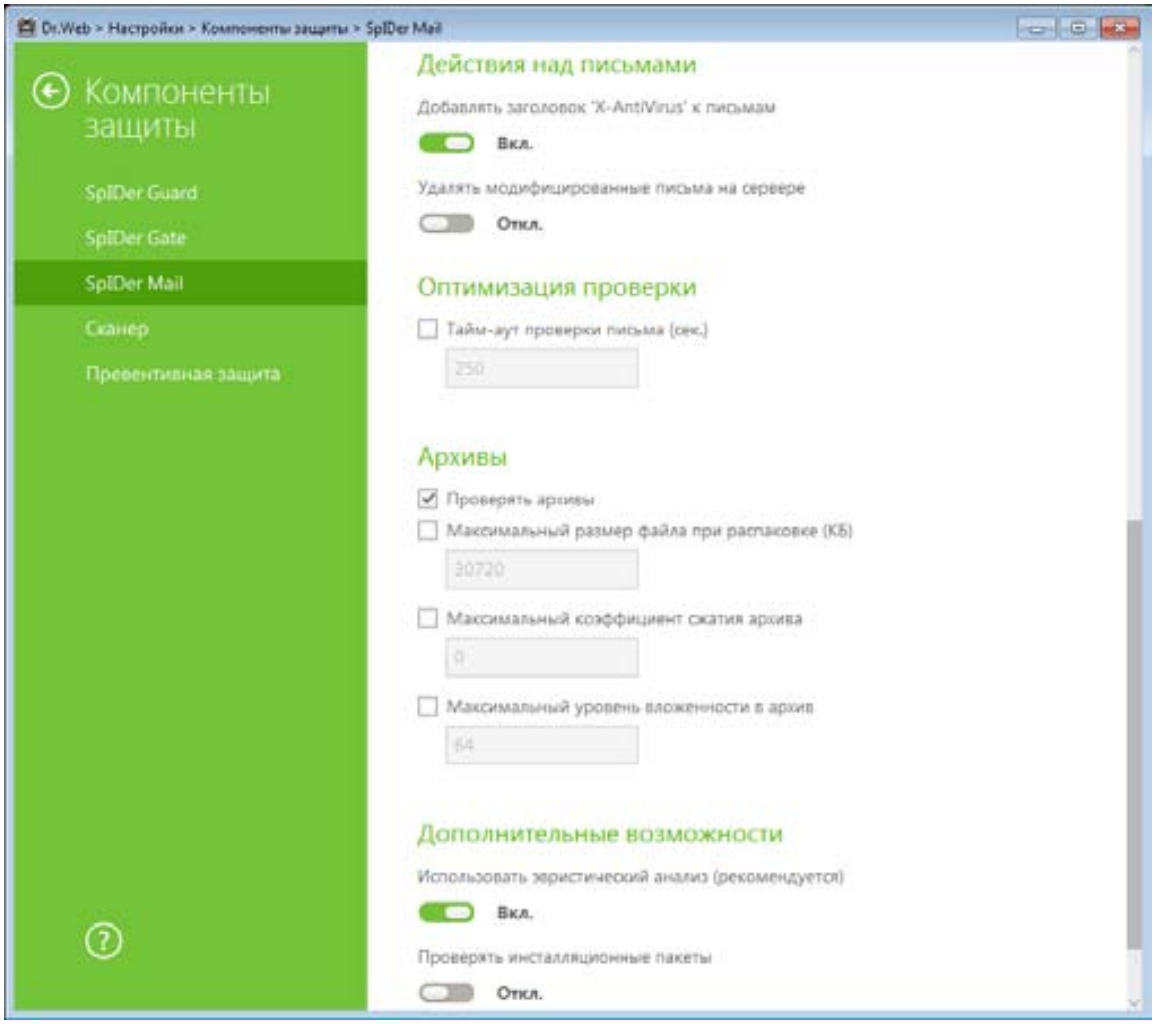


Определите, какой префикс будет присваиваться теме писем, определенных как спам-сообщения. Используя этот префикс, вы можете с помощью своего почтового клиента настроить действия со спам-сообщениями, как описано ниже.

С помощью группы настроек **Действия** вы можете указать, что следует делать в том случае, если в письме были найдены инфицированные файлы и объекты. По умолчанию для всех типов вредоносного ПО, кроме инфицированных объектов, назначено действие **Перемещать в карантин**, что позволяет их сохранять для дальнейшего анализа.



Для получения доступа ко всему перечню настроек, нажмите **Дополнительные настройки**.



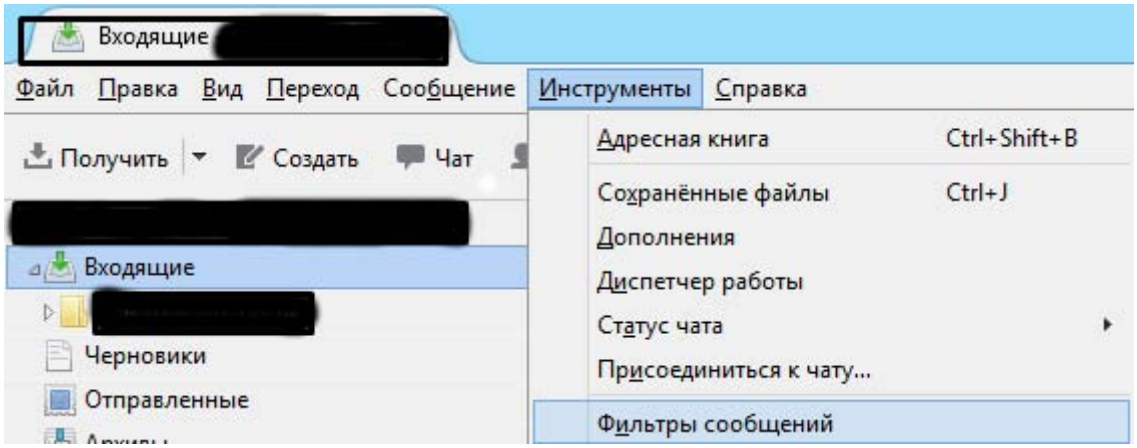
Здесь задаются параметры проверки архивов, полученных в письмах: необходимость этого действия, определение максимального времени об работки каждого письма и правила обработки архивов. Если вы хотите проверять только небольшие архивы (что увеличит скорость проверки), то можете уменьшить числа, указанные в поле справа от пунктов **Максимальный размер файла при распаковке** и **Максимальный уровень вложенности в архив**.

Отдельно настраиваются с помощью соответствующих переключателей использование эвристического анализа, проверка инсталляционных пакетов, а также удаление зараженных писем с почтового сервера.

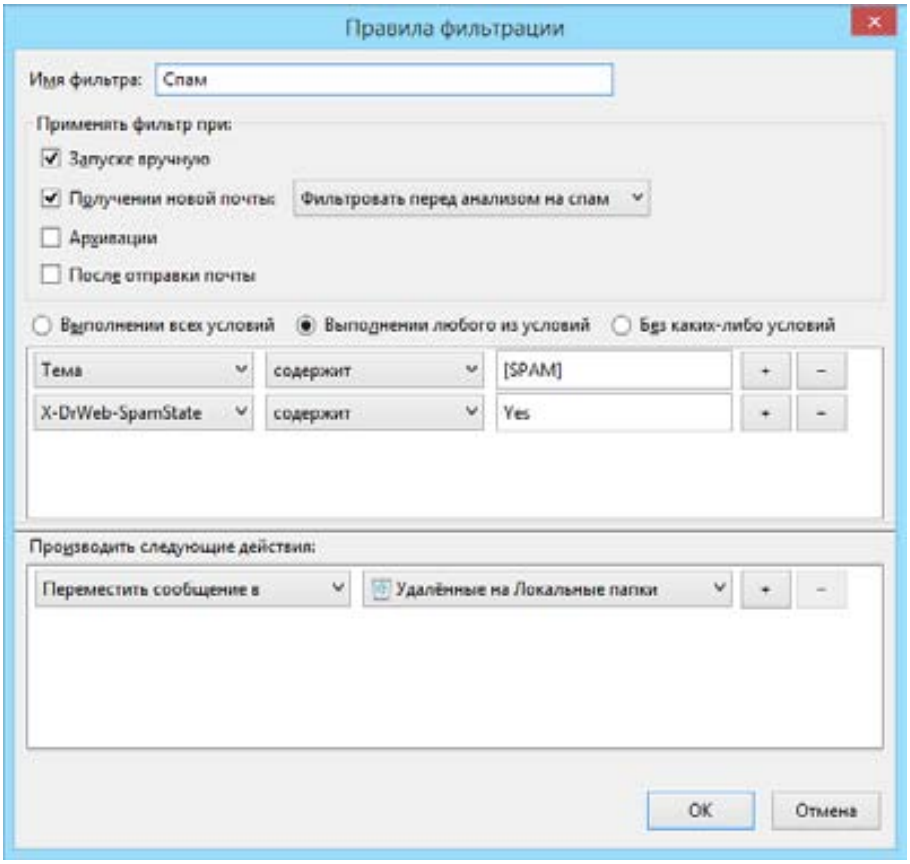
Так как **SpIDer Mail**, кроме добавления префикса к теме письма, всегда добавляет в служебные поля (скрытую в служебной области письма невидимую пользователю информацию) строку X-DrWeb-SpamState (со значениями Yes/No, где значение **Yes** показывает, что письму присвоен статус «спам»), то можно осуществлять дополнительную фильтрацию как по заголовку письма (message header), так и его теме (Subject).

Используя спам-метки, можно настроить почтовый клиент таким образом, чтобы все спам-сообщения автоматически удалялись или помещались в папку **Спам**. Для примера детальной настройки возьмем наиболее популярный почтовый клиент Thunderbird (версия 52.9.1):

В меню **Инструменты** выберите пункт **Фильтр сообщений**.

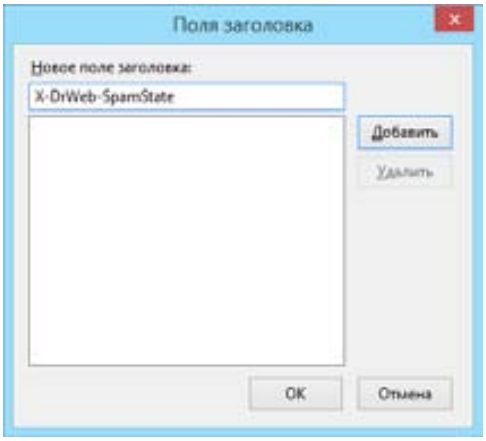


В открывшемся окне нажмите **Создать...** Задайте имя фильтра, отметьте флажком пункт **Выполнение любого из условий**, после чего установите поля следующим образом:



1) В первом условии задайте: поле **Тема содержит [SPAM]**

2) Нажмите  , чтобы добавить условие фильтрации, после чего в первом раскрывающемся списке укажите **Настроить**... и в новом окне введите в строку текст *X-DrWeb-SpamState* и нажмите **Добавить**.



3) Задайте условия: поле *X-DrWeb-SpamState* содержит *Yes*.

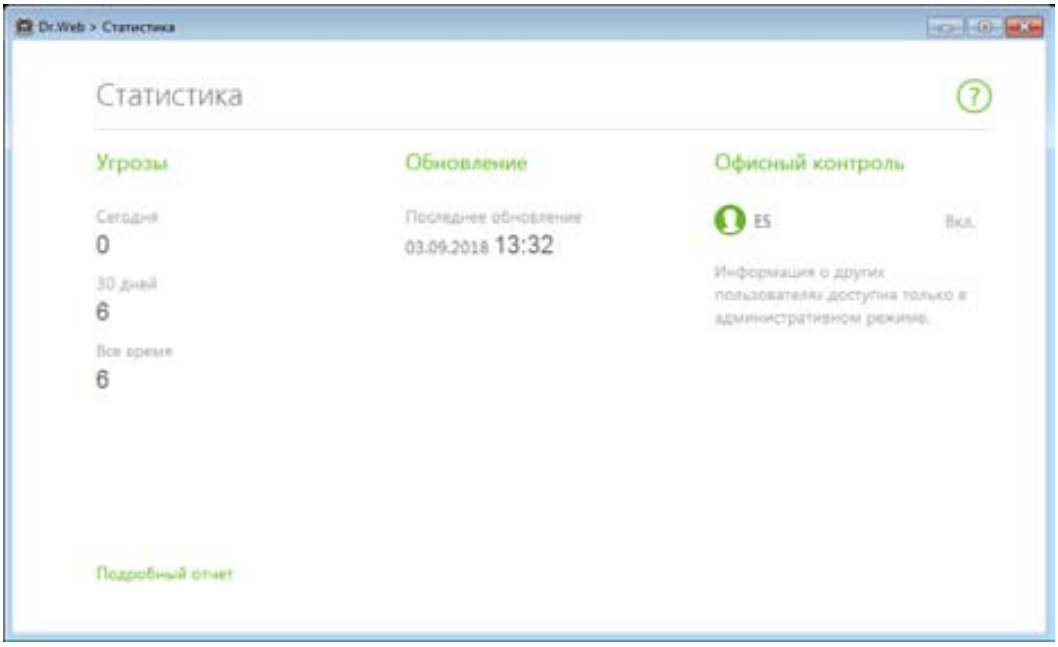
4) Нажмите **ОК**, чтобы сохранить правило.

Для завершения настройки закройте окно правил. Настройка правил фильтрации для других почтовых клиентов производится аналогично.

Для проверки правильности работы почтового фильтра создайте новое письмо и в его тело вставьте строчку: «*XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X*» без кавычек. Это так называемый GTUBE (Generic Test for Unsolicited Bulk Email) — аналог тестового вируса EICAR, применяемый для тестирования функций антиспама.

11.12. Просмотр статистики работы

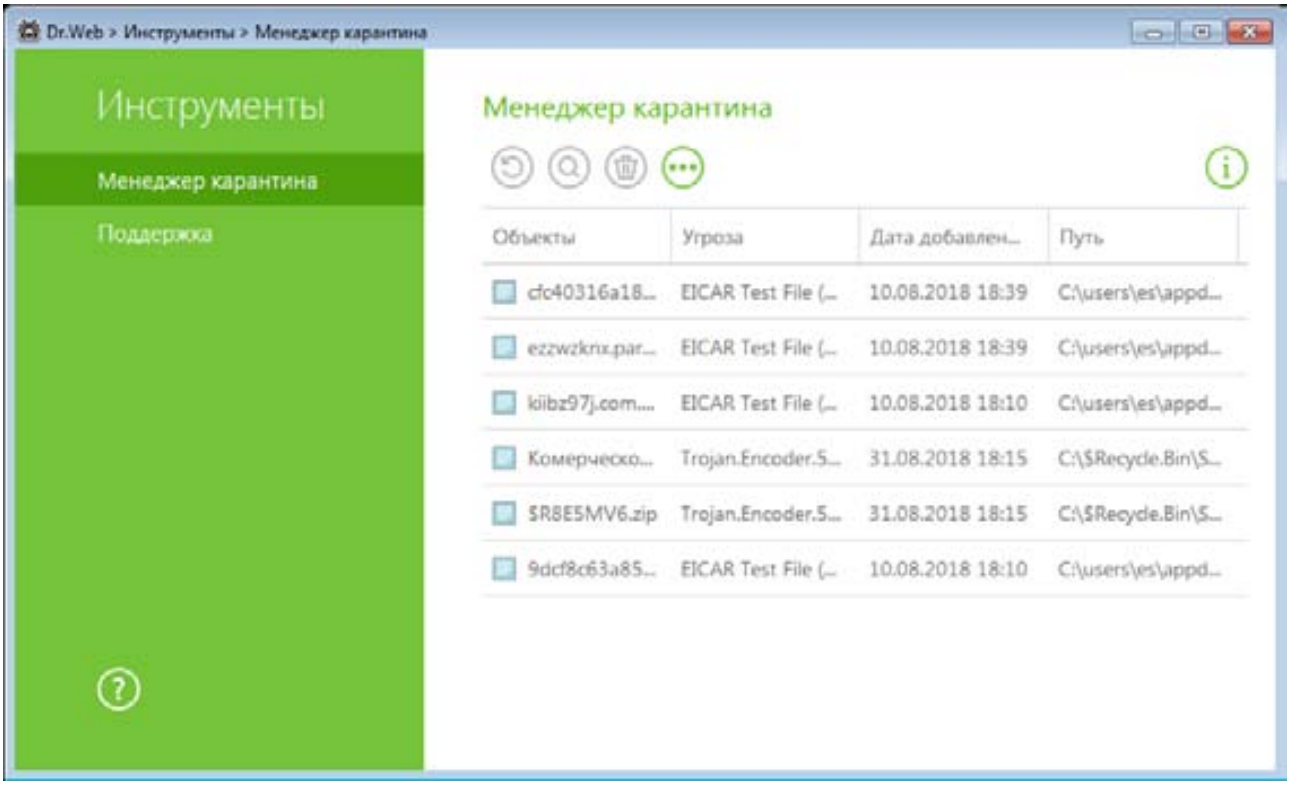
Пользователь может в любой момент времени ознакомиться со статистикой работы системы защиты. Для этого нажмите на значок  в меню Агента.



11.13. Карантин

Карантин антивируса Dr.Web служит для изоляции подозрительных файлов. Впоследствии их можно либо будет проверить повторно более новыми базами антивируса и либо удалить окончательно, либо восстановить. Также Карантин используется как временное хранилище для подозрительных файлов, которые планируется отправить на анализ в компанию «Доктор

Веб». Для управления карантином выберите пункт **Инструменты → Менеджер карантина** в меню **Агента**.



Для управления файлами в карантине нужно перейти в режим администратора, также обратите внимание, что в списке отображаются только те файлы, которые имеет право просматривать данный пользователь. Каждый файл из списка можно восстановить ( ), повторно просканировать ( ), удалить ( ), а также просмотреть его свойства ( ).

Папка **Карантина** создается отдельно на каждом логическом диске, где были обнаружены подозрительные файлы, она называется **Dr.Web Quarantine**, располагается в корне диска и имеет атрибут «скрытый». Доступ пользователей к этой папке заблокирован. Файлы карантина, размещаемые на жестком диске, хранятся в зашифрованном виде, размещаемые на съемном носителе не шифруются.

Чтобы удалить все файлы, помещенные в папку **Карантина**, нажмите и выберите **Удалить все**, после чего подтвердите действие.

Вы можете задать режим изоляции зараженных объектов, обнаруженных на съемных носителях. По умолчанию при обнаружении зараженных объектов на съемном носителе, если запись на носитель возможна, на нем создается папка **Dr.Web Quarantine**, и в нее переносится зараженный объект. Использование отдельных папок и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных.

В центральной части окна отображается таблица с информацией о состоянии карантина, включающая следующие поля:

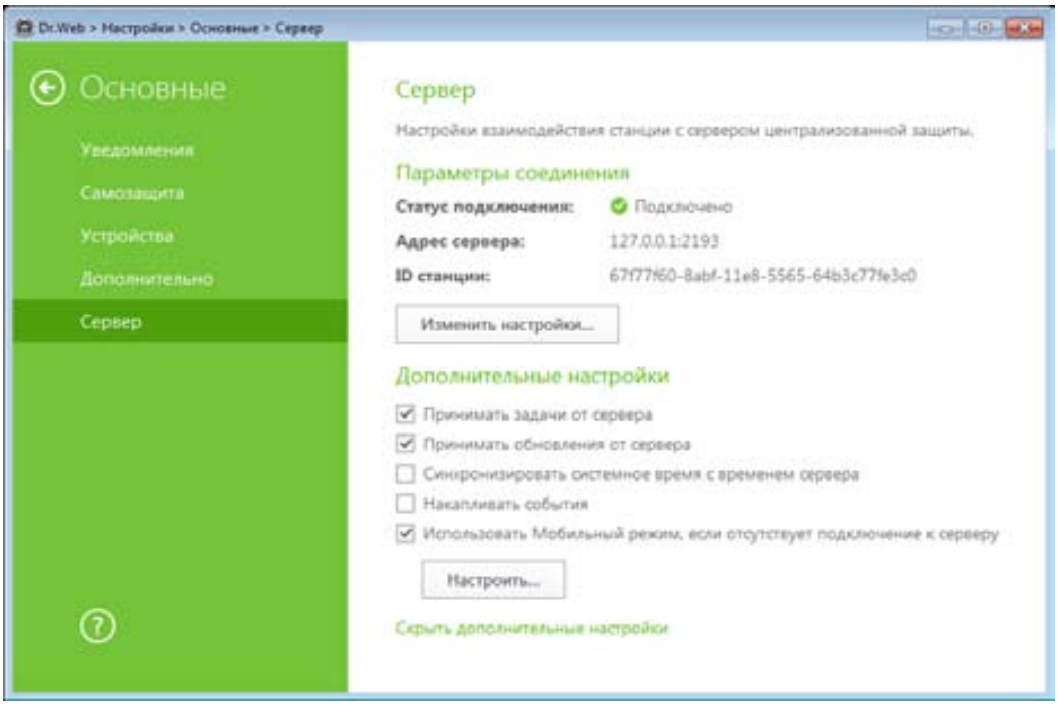
- **Объекты** — список имен объектов, находящихся в карантине;
- **Угроза** — классификация вредоносной программы, определяемая программой **Dr.Web** при автоматическом перемещении объекта в карантин;
- **Дата добавления** — дата, когда объект был перемещен в карантин;
- **Путь** — полный путь, по которому находился объект до перемещения в карантин.

В окне **Карантина** файлы могут видеть только те пользователи, которые имеют к ним доступ. Чтобы отобразить скрытые объекты, необходимо иметь права Администратора.

При переполнении диска осуществляется автоматическая очистка карантина — в первую очередь удаляются резервные копии файлов карантина, а при нехватке дискового пространства удаляются файлы карантина с истекшим сроком хранения.

11.14. Настройки мобильного режима

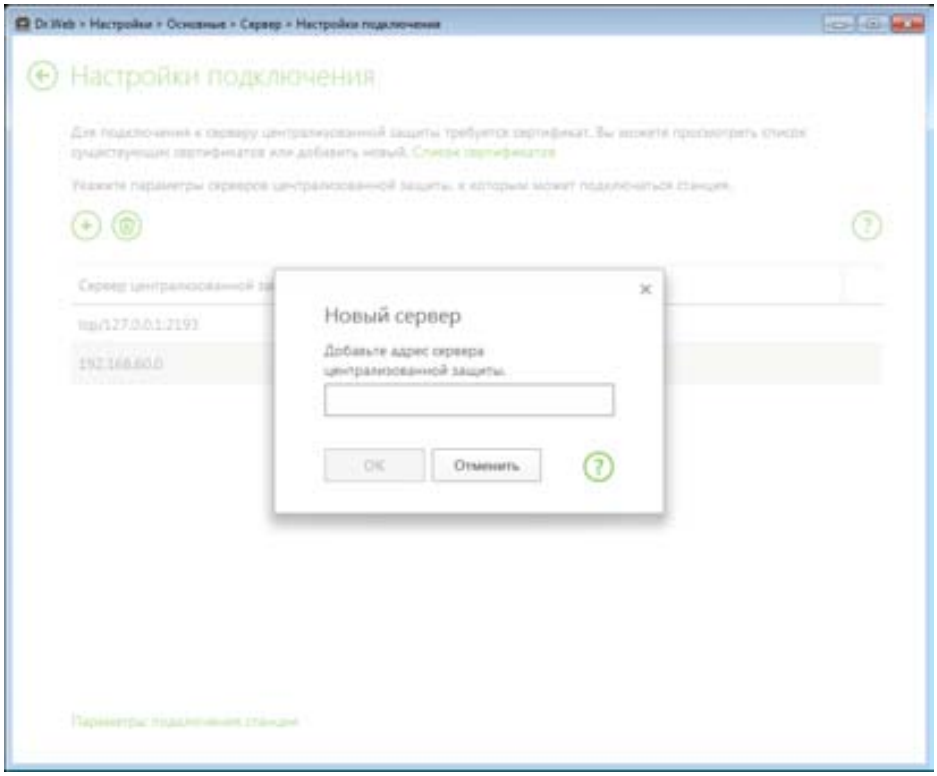
Для настройки мобильного режима в меню Агента разблокируйте доступ к настройкам, нажав , после чего перейдите в раздел **Настройки → Основные → Сервер** и нажмите **Дополнительные настройки**.



В данном разделе вы можете просматривать и редактировать параметры взаимодействия Агента **Dr.Web** с Сервером Dr.Web, а также задать настройки для Мобильного режима работы Агента. Мобильный режим доступен только в случае наличия соответствующих разрешений, выданных в Центре управления. В противном случае кнопки и флажки будут не доступны для использования.

В группе **Параметры соединения** отображается статус подключения, а также, при наличии соответствующих прав, предоставляется возможность просмотра и управления настройками соединения с сервером. Настройки подключения к серверу централизованной защиты можно менять только согласованно с администратором антивирусной сети, иначе ваш компьютер будет отключен от Сервера Dr.Web.

Для изменения настроек подключения к текущему серверу или настройки соединения с другим сервером нажмите **Изменить настройки**. Откроется окно **Настройки сервера**.

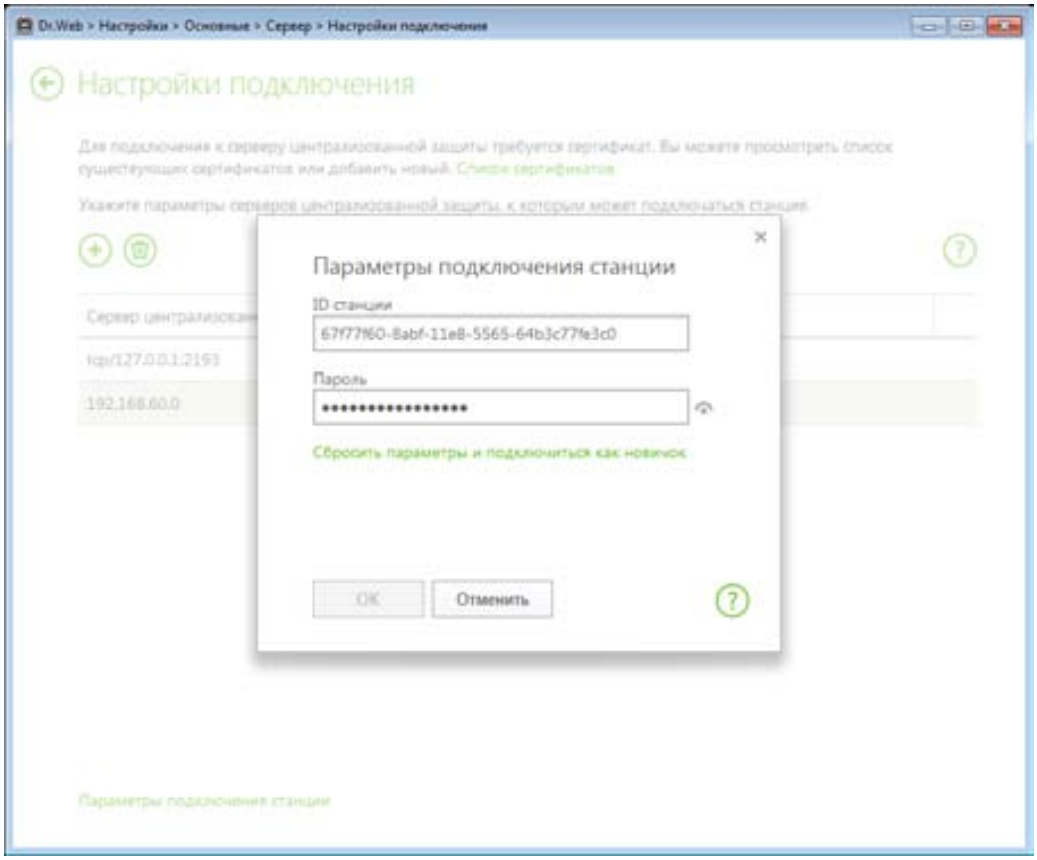


Для добавления нового Сервера нажмите , после чего укажите его адрес и порт.

При нажатии на ссылку **Параметры подключения станции** станут доступны дополнительные настройки:

- **ID станции —** укажите идентификатор **Dr.Web**, присвоенный вашему компьютеру для регистрации на сервере.
- Вы можете запросить новую регистрацию на сервере централизованной защиты, для этого нажмите **Подключиться как новичок**, либо настроить соединение с другим сервером, изменив параметры подключения к серверу (**Адрес**, **Порт** и **Открытый ключ**). После подтверждения регистрации станции на сервере централизованной защиты, **Dr.Web** получит заданные администратором настройки.

В случае необходимости укажите пароль для подключения к серверу.



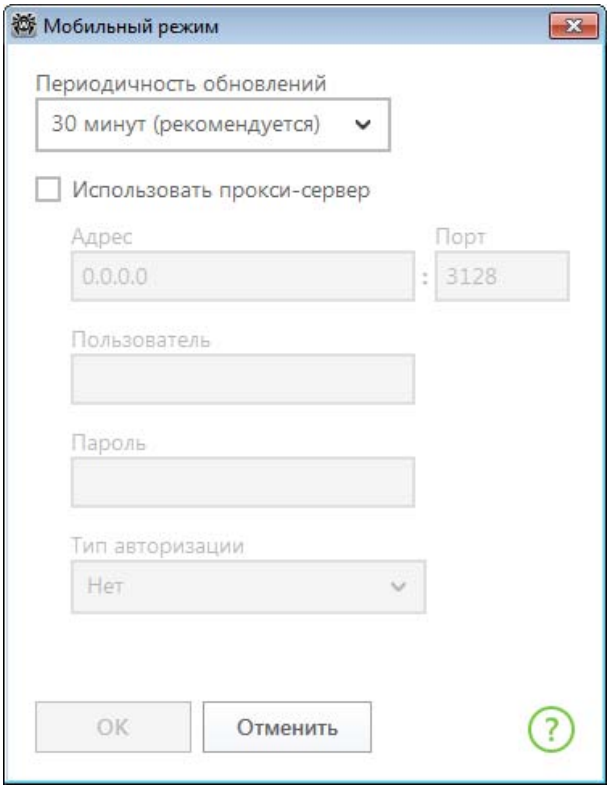
Чтобы выйти из окна **Настройки сервера** и сохранить изменения, нажмите **ОК**.

В группе **Дополнительно** вы можете выбрать следующие опции:

- **Принимать задачи от сервера** — для периодического получения заданий от администратора.
- **Принимать обновления от сервера** — для получения регулярных обновлений компонентов **Dr.Web** и вирусных баз с сервера централизованной защиты. Обновления происходят в соответствии с настройками, заданными на сервере.
- **Синхронизировать системное время с временем сервера** — для синхронизации системного времени на вашем компьютере со временем на сервере централизованной защиты.
- **Накапливать события** — для сохранения данных о произошедших событиях для последующей отправки на сервер централизованной защиты. При этом информация будет передана, как только произойдет подключение к серверу. Если флажок не установлен, а соединения с сервером нет, то важная информация (например, об обнаруженных угрозах и статистике) будет утрачена.
- **Использовать Мобильный режим, если отсутствует подключение к серверу** — для своевременного получения обновлений вирусных баз.

В Мобильном режиме **Dr.Web** пытается подключиться к серверу централизованной защиты, делает три попытки и, если не удалось, выполняет обновление вирусных баз с серверов компании «Доктор Веб». Попытки обнаружения сервера централизованной защиты идут непрерывно с интервалом около минуты.

Чтобы задать настройки Мобильного режима работы, нажмите кнопку **Настроить...** Откроется окно **Мобильный режим**.



В выпадающем списке **Периодичность обновлений** вы можете выбрать периодичность, с которой будет производиться проверка на наличие обновлений на серверах компании «Доктор Веб».

Внимание! При выборе в списке **Периодичность обновлений** опции **Вручную** автоматические обновления происходить не будут.

При использовании прокси-сервера установите соответствующий флажок и укажите данные для доступа к нему.

По окончании редактирования нажмите кнопку **ОК** для сохранения внесенных изменений.

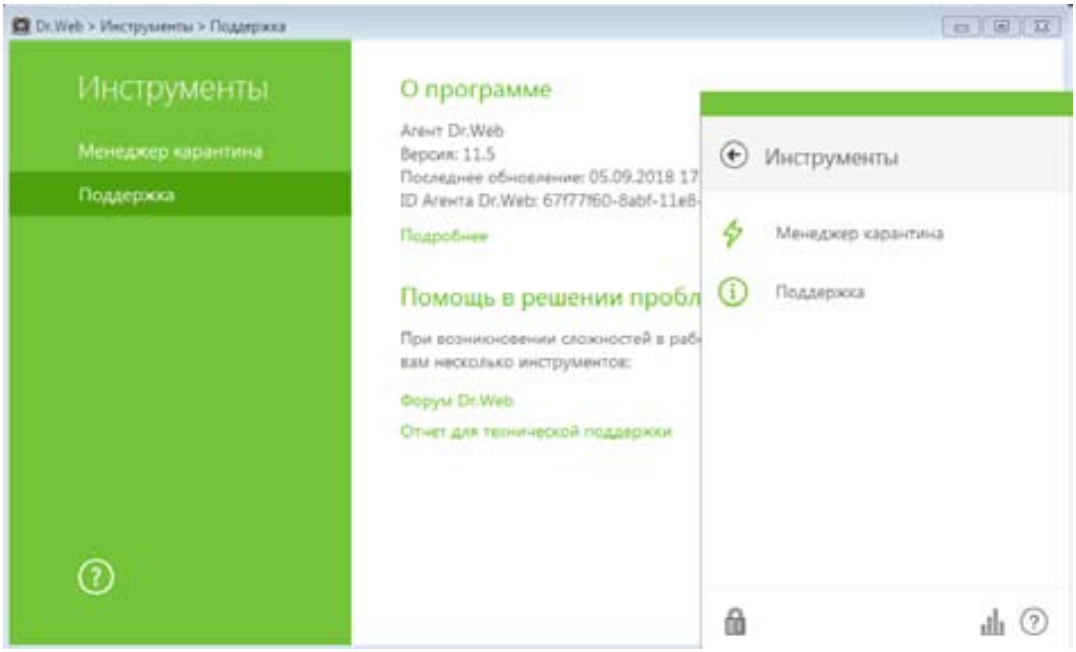
В Мобильном режиме производится обновление только вирусных баз. Если снять флажок **Использовать Мобильный режим, если отсутствует подключение к серверу** до возобновления связи с сервером централизованной защиты, то вирусные базы перестанут обновляться, но поиск сервера продолжится.

Все изменения, которые задаются для станции на сервере централизованной защиты, вступят в силу, как только связь **Dr.Web** с сервером возобновится.

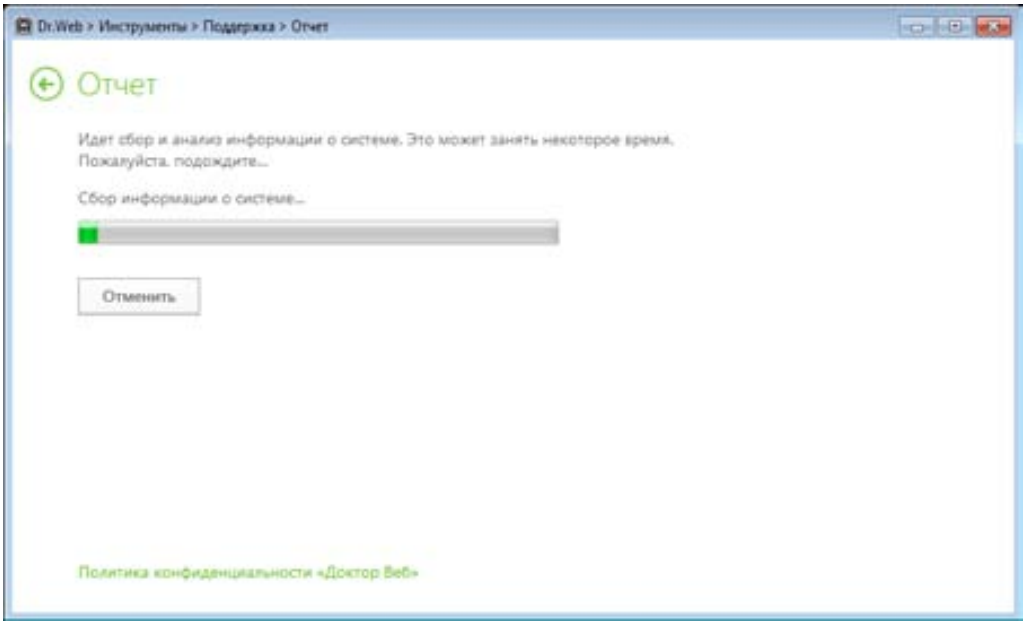
11.15. Сбор информации для служб технической поддержки

Важным преимуществом продуктов Dr.Web является автоматизированный сбор данных о работе антивируса, которые могут потребоваться при обращении в службу технической поддержки.

Для получения архива со сводной информацией необходимо, щелкнув кнопкой мыши по значку Агента, выбрать пункт **Инструменты → Поддержка**, после чего нажмите **Отчет для технической поддержки**.



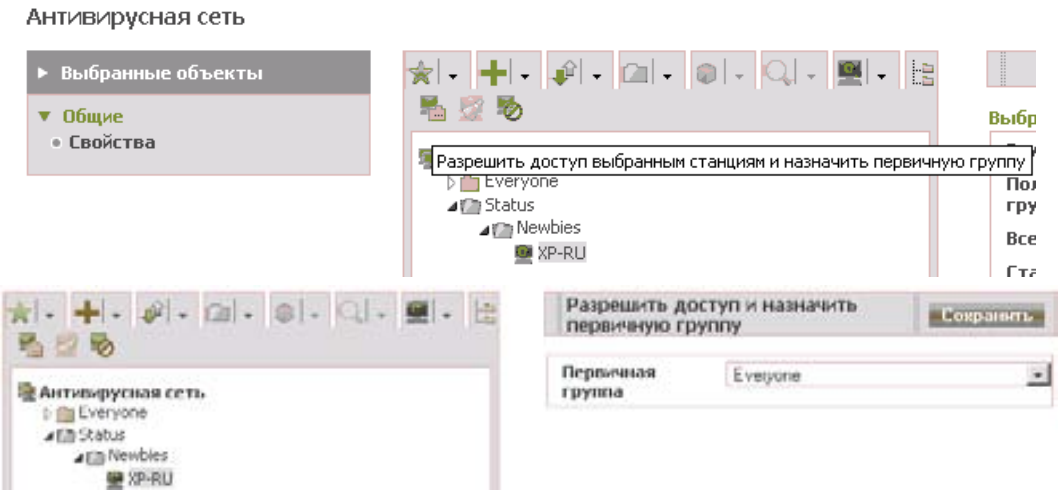
В появившемся окне нажмите **Создать отчет**. Антивирус автоматически соберет все данные и создаст в папке по умолчанию архив, который можно будет передать в службу технической поддержки либо системному администратору.



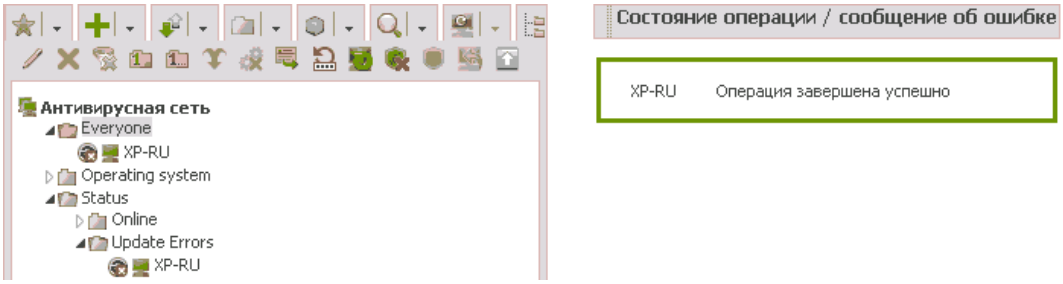
11.16. Перевод в режим централизованной защиты однопользовательских версий

Если на компьютере установлен Антивирус Dr.Web или Dr.Web Security Space, то администратор антивирусной сети может перевести эти однопользовательские версии в режим централизованной защиты. Для этого необходимо запустить любым из доступных методов инсталлятор Агента н а защищенных однопользовательскими продуктами станциях — например, найдя эту станцию через **Сканер сети**. Все изменения, которые задаются для станции на сервере централизованной защиты, вступят в силу, как только связь Агента с Сервером Dr.Web будет установлена.

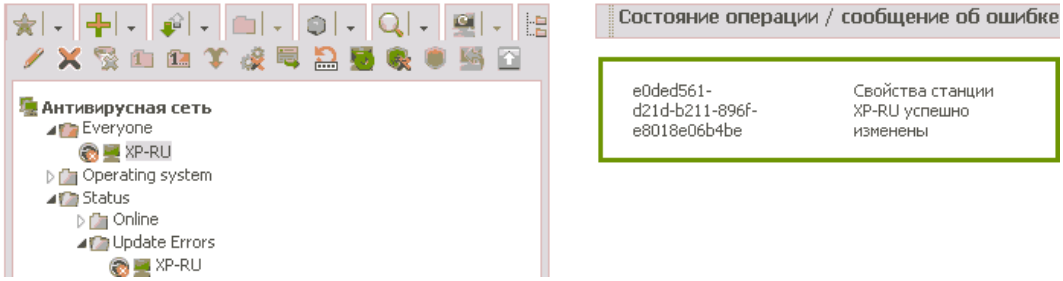
После завершения установки агента станция появится в группе новичков и для нее необходимо будет разрешить доступ и назначить первичную группу — если данное действие не выполняется автоматически.



После подтверждения статуса на станции начинается формирование репозитория, во время формирования репозитория станция имеет статус Update errors.



Начиная с появления станции в назначенной группе над ней можно выполнять требуемые администратору операции.



12. Настройка антивирусной защиты на стороне пользователя для ОС Linux

12.1. Развертывание антивирусной защиты

К сожалению, операционная система Linux не содержит стандартного механизма, позволяющего автоматически развертывать программное обеспечение. Поэтому установку антивирусной защиты в локальной сети нужно проводить в два этапа:

- Установка Антивируса Dr.Web для Linux на каждой рабочей станции
- Введение установленного антивируса в систему централизованного управления

Антивирус Dr.Web для Linux может поставляться в двух вариантах: в виде универсального пакета для UNIX-систем (run-пакета) и в виде пакетов для конкретных операционных систем (например, rpm- или deb-пакетов). Также можно использовать инсталляционный пакет, который можно создать для станций через интерфейс Центра управления Сервера Dr.Web. Далее будет рассмотрен пример установки из созданного на Сервере установочного пакета, имеющего имя вида `drweb_ess_linux_<имя_станции>_<разрядность>.run`.

Внимание! Если ранее в системе продукт или его компоненты были установлены из пакетов иных типов — необходимо убедиться, что все эти пакеты удалены.

Внимание! Для осуществления операций установки и введения в режим централизованного управления необходимы права администратора (root). Если запуск был осуществлен не с правами администратора, то инсталлятор сам попытается повысить права.

Установка и обновление **Антивируса Dr.Web для Linux** могут быть осуществлены как с помощью графического, так интерактивного консольного инсталлятора. При установке поддерживается работа с зависимостями, т. е. если для установки какого-либо из компонентов программного комплекса должен быть предварительно установлен другой компонент, то он будет установлен автоматически.

Чтобы автоматически установить компоненты **Антивируса Dr.Web для Linux**, разрешите исполнение архива, например, командой:

```
# chmod +x drweb_ess_linux_Lin_x86_64.run
```

и затем запустите его на исполнение командой:

```
# ./drweb_ess_linux_Lin_x86_64.run
```

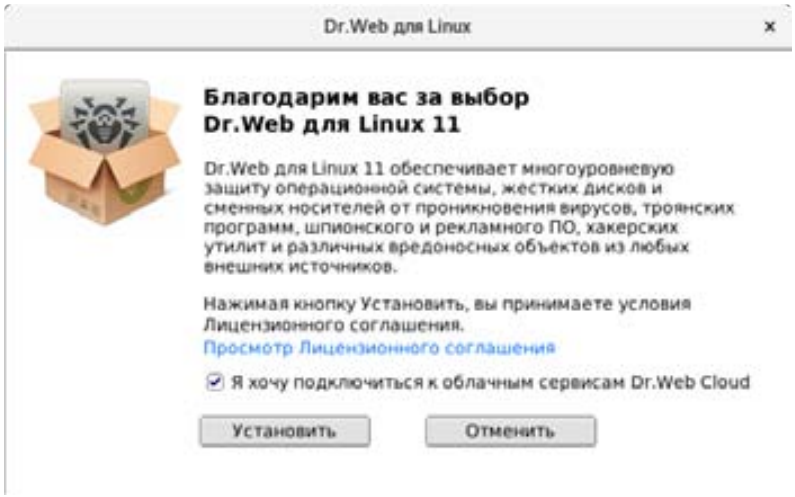
или воспользуйтесь стандартным файловым менеджером вашей графической оболочки как для изменения свойств файла, так и для его запуска.

Если запустить графический инсталлятор не удалось, то автоматически запустится интерактивный консольный инсталлятор.

Внимание! Если в процессе установки обнаруживается файл с таким же именем (например, оставшийся после неаккуратного удаления пакетов других типов), то на его место записывается новый файл, а копия старого сохраняется как *<имя_файла>.O*. Если в

директории уже имеется файл с таким именем (*<имя_файла>.O*), то он будет удален, а новый файл будет записан на его место.

При запуске графического инсталлятора командой
`drweb_ess_linux_Lin_x86_64`/install.sh открывается окно программы установки.

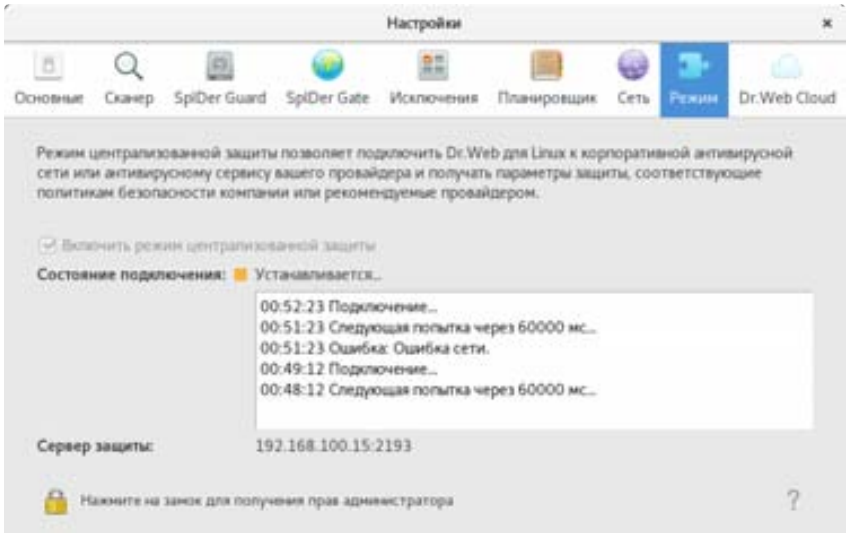


Нажмите **Установить**. Всё необходимое антивирусное ПО будет установлено автоматически.

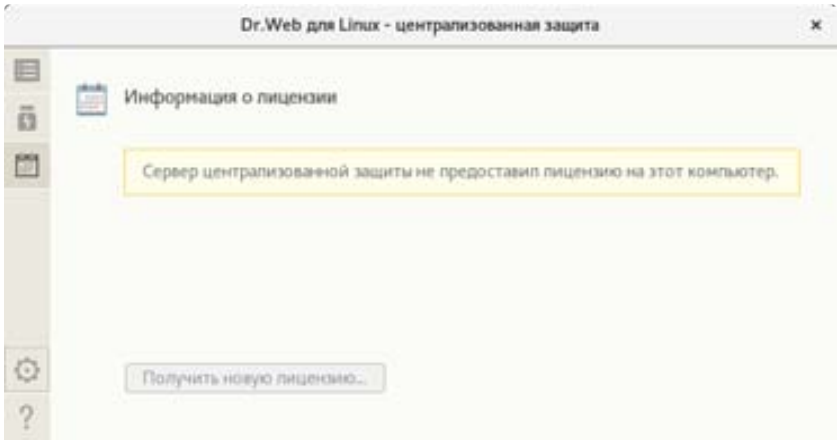
В окне **Установка** выводится отчет о процессе установки в режиме реального времени. Одновременно данный отчет копируется в файл *install.log*.

После завершения установки в меню **Приложения** появится группа **Dr.Web**, раскрыв которую вы сможете выбрать в выпадающем меню необходимый пункт для работы с **Антивирусом Dr.Web для Linux**.

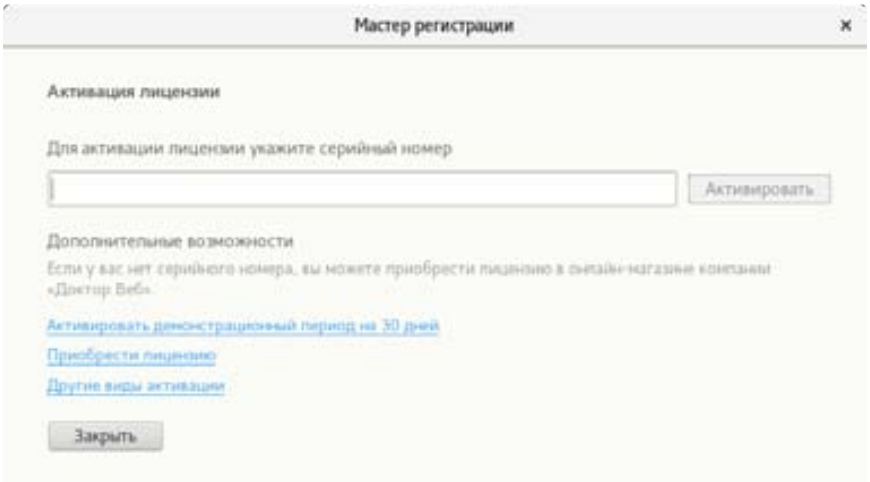
Поскольку установка производилась с дистрибутива, специально созданного для рабочих станций, связанных с существующим Сервером Dr.Web, на вкладке **Настройки → Режим** по умолчанию установлен режим централизованной защиты.



По той же причине изначально антивирус пытается связаться с сервером и получить, в том числе, данные лицензии.



При необходимости также можно указать и действующую персональную лицензию, воспользовавшись Мастером регистрации.



Настройка режима централизованной защиты

Если для установки использовался дистрибутив, полученный не от соответствующего Сервера Dr.Web, то изначально программа будет работать в автономном режиме, и использование режима централизованной защиты необходимо активировать.

В режиме централизованной защиты блокируется возможность ручного запуска и настройки обновлений. Кроме того, некоторые настройки **Антивируса Dr.Web для Linux**, в частности, возможности управления постоянной защитой и проверкой системы по требованию, могут быть изменены или заблокированы в соответствии с политикой безопасности компании. Ключевой файл для работы в таком режиме получается автоматически с сервера централизованной защиты, и ваш личный лицензионный ключ не используется.

В соответствии с политикой подключения новых станций подключить рабочую станцию к серверу централизованной защиты можно двумя способами:

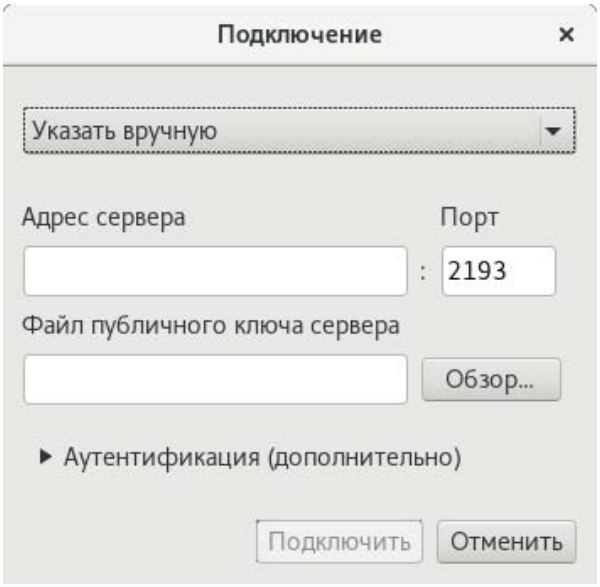
- создав учетную запись на сервере автоматически;
- создав учетную запись на сервере вручную.

Соответственно, необходимо предварительно получить у администратора антивирусной сети компании публичный ключевой файл и параметры подключения к серверу централизованной защиты.

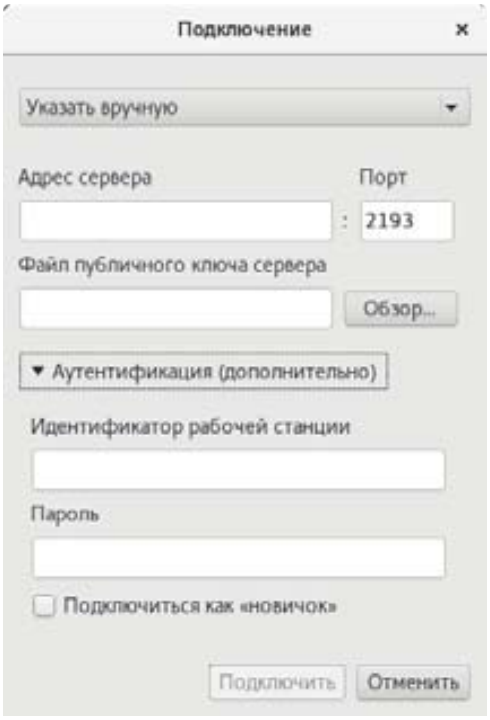
Настройка режима централизованной защиты может быть произведена как напрямую (из конфигурационных файлов), так и с помощью графического интерфейса, в последнем случае в процессе настройки необходимые изменения вносятся в конфигурационный файл **Агента** автоматически.

В меню **Настройки → Режим** отметьте флажком пункт **Включить режим централизованной защиты**. После этого будет необходимо указать данные для подключения к Серверу Dr.Web:

- IP-адрес сервера централизованной антивирусной защиты и порт, использующийся для подключения к серверу;
- путь к полученному вами ранее публичному ключу.



Если выбран режим подключения к серверу антивирусной защиты с созданием учетной записи на сервере вручную, то необходимо также указать дополнительные параметры для авторизации рабочей станции: идентификатор (логин) станции (созданный ранее и присвоенный вашему компьютеру для регистрации на сервере) и пароль, или выбрать **Подключиться как «новичок»** для получения новых учетных данных.



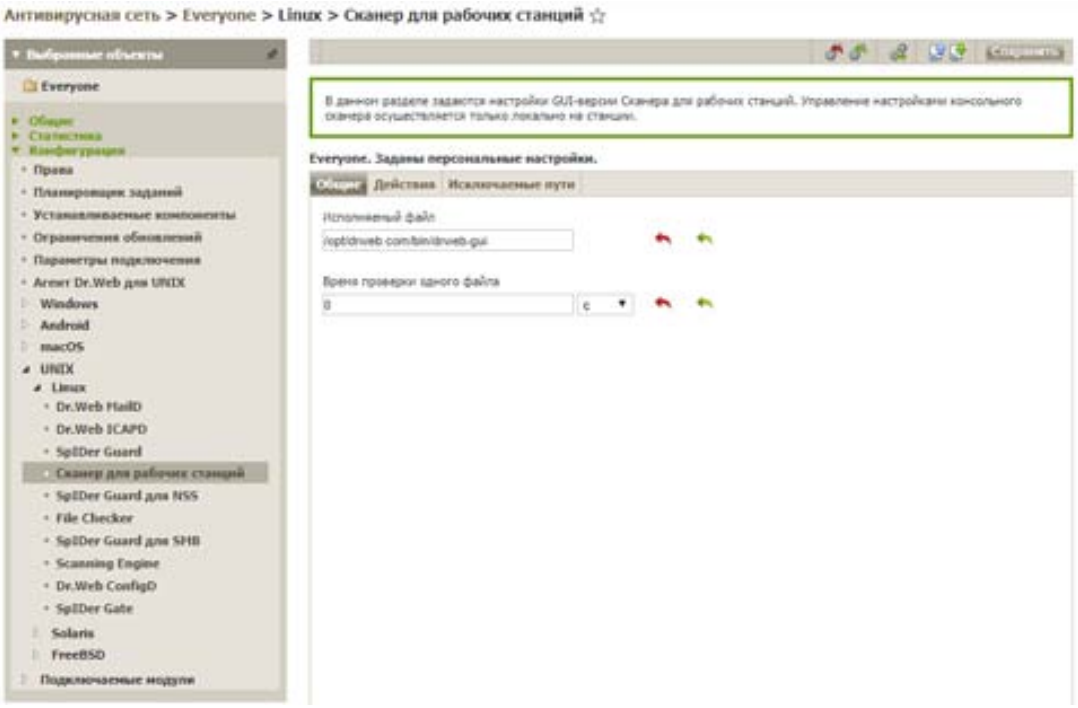
Нажмите **Подключить**. Новые параметры соединения вступят в силу и произойдет подключение к указанному антивирусному Серверу Dr.Web в качестве Агента.

В том случае, если выбран **режим подключения к серверу антивирусной защиты с автоматическим созданием учетной записи** и на сервере централизованной защиты установлен режим **Ручное подтверждение доступа**, то от администратора потребуется подтвердить регистрацию новой станции через Центр управления.

При первом запуске в режиме централизованной защиты **Агент** запрашивает регистрационные данные (идентификатор станции и пароль) у сервера. После первого подключения **Агент** записывает хеш идентификатора станции и пароля пользователя в специальном файле (по умолчанию /var/drweb/agent/pwd). Ключом шифрования является имя хоста, на котором установлен **Агент**.

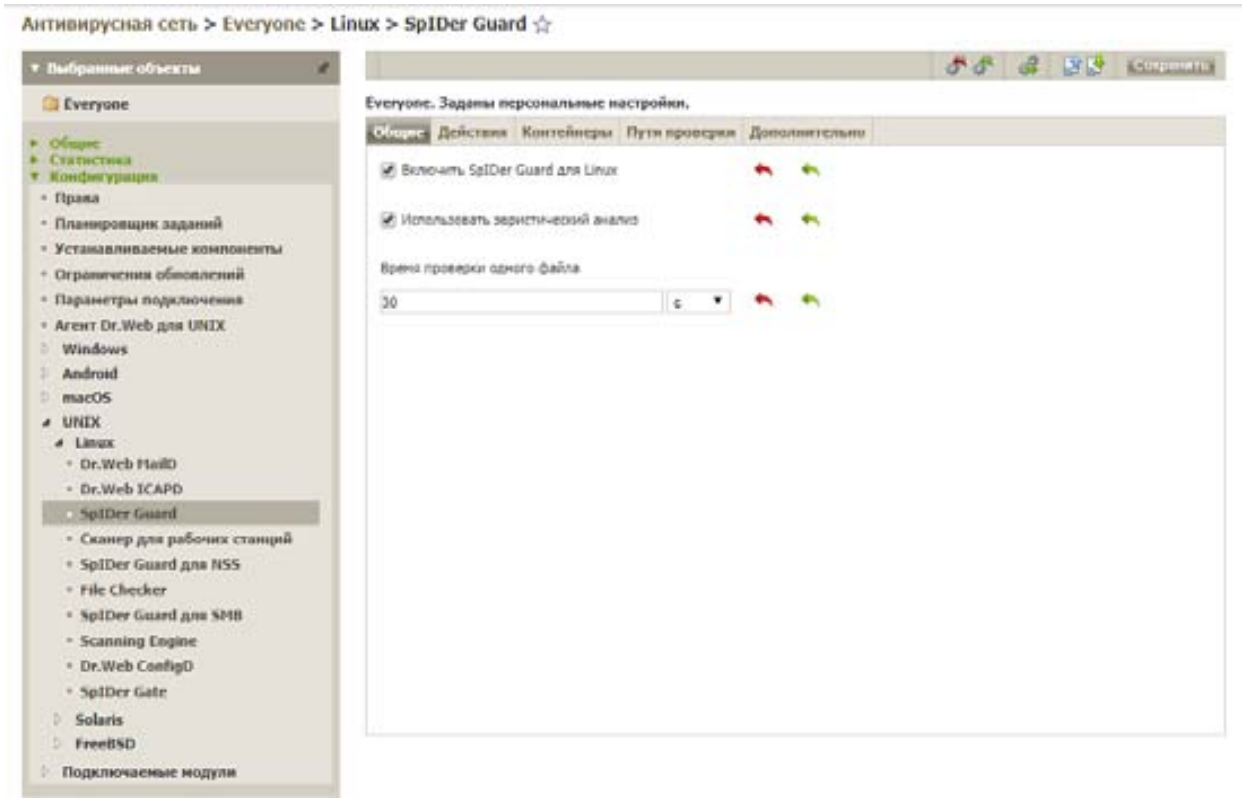
В дальнейшем данные из этого файла используются для подключения **Антивируса Dr.Web для Linux** к серверу централизованной защиты. Удаление файла с паролем приведет к повторному запросу регистрационных данных у сервера централизованной защиты при следующем запуске **Антивируса Dr.Web для Linux**.

Обратите внимание, что **Антивирус Dr.Web для Linux** в терминологии **Dr.Web Enterprise Security Suite** обозначается как Агент **Dr.Web для Linux**.



Каждый раз при запуске Агент **Dr.Web для Linux** запрашивает и получает конфигурацию антивирусных компонентов от сервера централизованной защиты. Таким образом, через Центр управления можно управлять настройкой конфигурации этих компонентов.

Если изменение настроек компонентов не запрещено администратором, то любые изменения, сделанные через интерфейс **Dr.Web для Linux**, будут автоматически сохранены на сервере централизованной защиты.



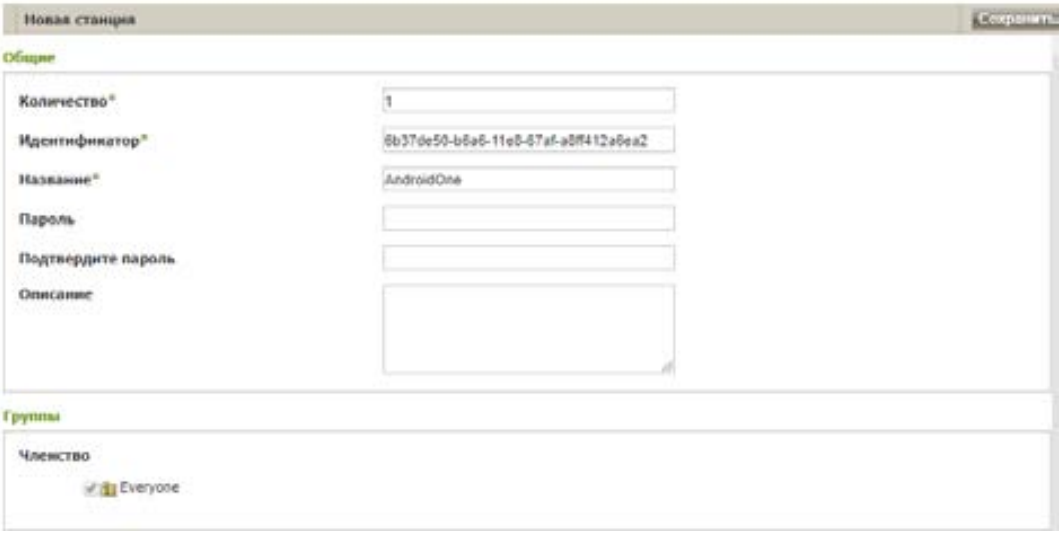
Изменения в конфигурацию рабочей станции можно вносить даже тогда, когда она временно недоступна для Сервера. Эти изменения будут приняты рабочей станцией, как только ее связь с Сервером восстановится.

13. Настройка антивирусной защиты для мобильных устройств

Подключить мобильное устройство к антивирусной сети можно двумя способами. В первом случае сначала создается станция на Сервере Dr.Web, во втором — сначала происходит установка мобильного приложения на защищаемое устройство.

Создание станции с последующим подключением Агента

1) На Сервере Dr.Web создайте новую станцию с помощью кнопки и, задав название и другие параметры, нажмите **Сохранить**.



2) Станция будет создана, и будут подготовлены ссылки на установочные файлы.

3) Вы можете передать пользователю как конфигурационный файл, так и указанные здесь данные: ID станции и пароль; также ему будет необходимо сообщить IP-адрес Сервера Dr.Web для подключения.

4) После этого пользователь, выполнив шаги 1–6 из второго варианта, подключит свое устройство к антивирусноййт сети предприятия.

Установка мобильного приложения с последующим подключением к Серверу Dr.Web

1) Пользователь самостоятельно устанавливает приложение Dr.Web Security Space для Android на свое мобильное устройство. Дистрибутив может быть скачан с сайта «Доктор Веб» или получен непосредственно от администратора антивирусной сети.

Внимание! Скачивать антивирусное ПО Dr.Web в данном случае необходимо с сайта компании «Доктор Веб» по ссылке: https://download.drweb.ru/android, а не из Google Play, так как версия из Google Play не имеет необходимой функциональности.

2) Когда приложение будет установлено, требуется принять условия лицензионного соглашения и предоставить антивирусу необходимые разрешения:

Внимание! После установки приложения мобильное устройство не будет защищено, поскольку не указан лицензионный ключ.

3) Далее нужно включить режим Агент Dr.Web, для чего в меню приложения выбрать **Настройки → Администрирование** и установить флажок **Агент Dr.Web**.

4) Откроется окно ввода данных для подключения:

5) Все поля заполняются в соответствии с данными, полученными от администратора антивирусной сети. В режиме **Подключиться как новичок** требуется указать только адрес Сервера Dr.Web, тогда при попытке подключения администратор антивирусной сети получит уведомление о новой станции и сможет подтвердить доступ и распространить на нее лицензионный ключ.

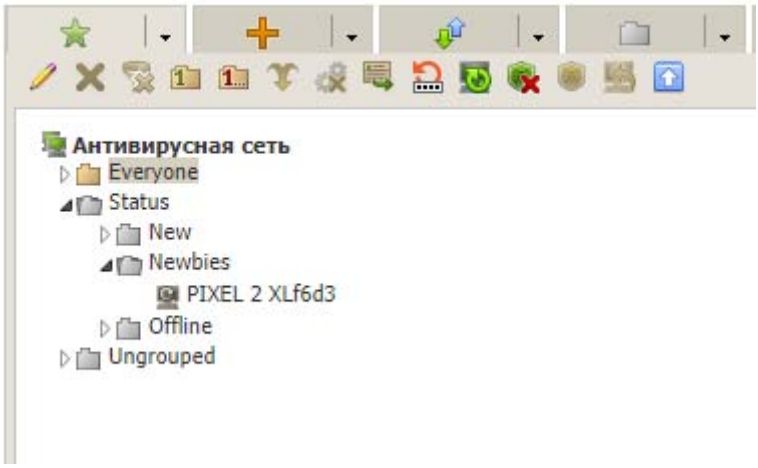
Примечание. Подключение к Центру управления возможно с помощью специально формируемого конфигурационного файла install.cfg или параметров подключения к антивирусному серверу, которые нужно задавать вручную:

1. Обратитесь к администратору антивирусной сети за параметрами подключения к серверу централизованной защиты или ссылкой на конфигурационный файл.
2. Введите полученную ссылку к конфигурационному файлу и загрузите его. Конфигурационный файл должен находиться в папке загрузке браузера или в корне SD-диска.

Если вы используете для подключения конфигурационный файл, помещенный в любой из папок первого уровня вложенности на SD- карте или в папке загрузки браузера, то поля для ввода параметров подключения к серверу будут заполнены автоматически.

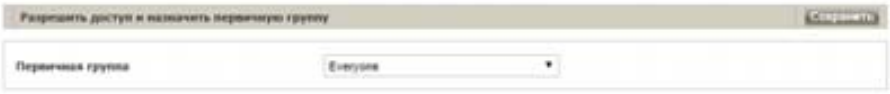
6) Нажатие кнопки **Подключить** завершает процесс подключения на стороне пользователя.

7) Одновременно с попыткой подключения мобильного Агента администратору Сервера Dr.Web будет отправлено соответствующее уведомление (Оповещение о новичках):



8) Выберите станцию-новичка и нажмите  (**Разрешить доступ выбранным станциям и назначить первичную группу**).

Выберите нужно группу из выпадающего списка и нажмите **Сохранить**.



9) После успешного подключения на станцию автоматически будет распространен лицензионный ключ, а администратор антивирусной сети получит возможность управления станцией через Центр управления Сервером Dr.Web. С этого момента пользователю больше не нужно заниматься вопросами антивирусной защиты своего мобильного устройства.

Внимание! В режиме централизованной защиты права пользователя мобильного устройства по управлению и настройкам антивируса могут быть ограничены администратором антивирусной сети. Например, может быть установлен запрет на отключение или включение компонентов или переход в мобильный режим. Ключевой файл для работы в таком режиме получается автоматически с сервера централизованной защиты, и другой лицензионный ключевой файл не используется.

Внимание! Если при подключении произошла ошибка с описанием **Неподдерживаемая опция в настройках сервера. Проверьте конфигурацию сервера и убедитесь, что параметры «Encryption» и «Compression» не равны «Yes»**, обратитесь к администратору антивирусной сети для устранения проблемы. Если вы являетесь администратором антивирусной сети, проверьте значение параметров **Сжатие** и **Шифрование** (в Центре управления настройки: **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web** на вкладке **Сеть → Транспорт**), они должны иметь значение **Нет** или **Возможно**.

Для того чтобы перейти в режим автономной работы, на главном экране вызовите меню приложения и выберите пункт **Настройки**, снимите флажок **Dr.Web Агент** в разделе **Режим**. Если снятие флажка недоступно, значит, это действие было запрещено администратором антивирусной сети.

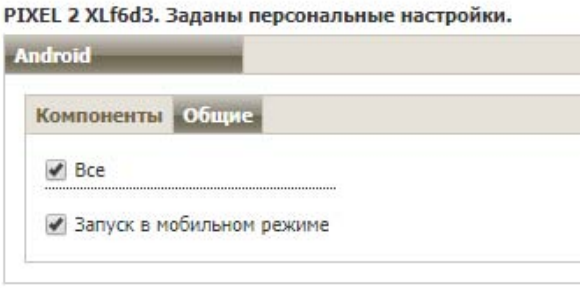
При включении режима автономной работы восстанавливаются все настройки антивируса, установленные до перехода в централизованный режим, или настройки по умолчанию. Также возобновляется доступ ко всем функциональным возможностям **Антивируса Dr.Web**.

Внимание! Для работы в автономном режиме требуется действительный персональный ключевой файл. Ключ, полученный автоматически с сервера централизованной защиты, в данном режиме использоваться не может.

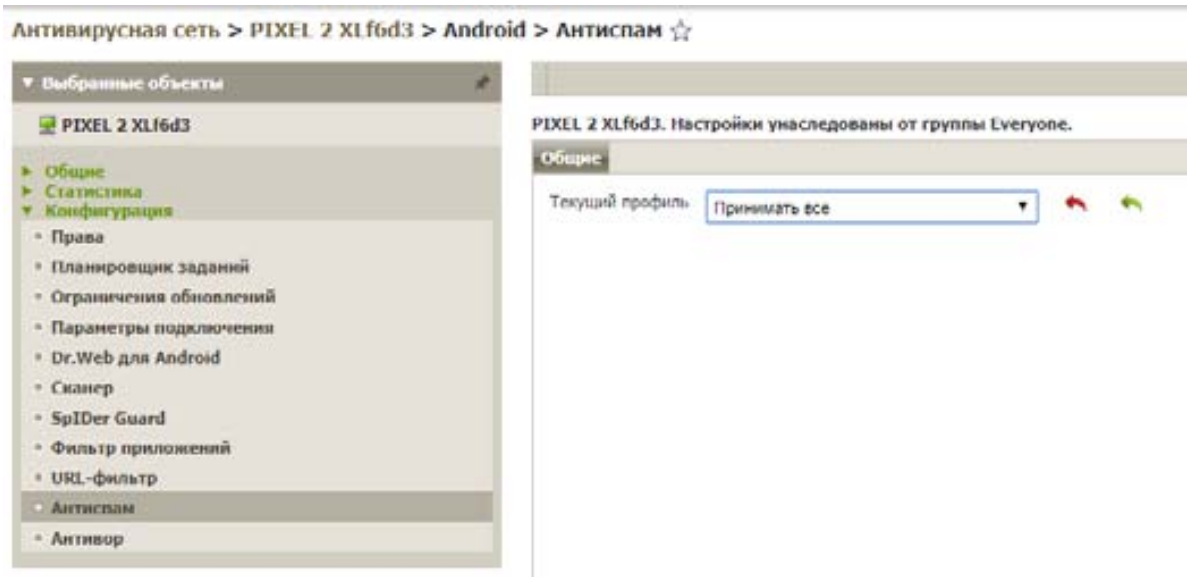
13.1. Настройка параметров защиты для мобильных устройств

Администратор антивирусной сети может практически полностью управлять антивирусной защитой мобильного устройства (исключение составляет только компонент Брандмауэр, который настраивается только локально). Выберите группу или станцию антивирусной сети и перейдите в раздел **Конфигурация → Права**.

На вкладке **Компоненты** можно настроить разрешения для действий пользователя по конфигурированию и отключению антивируса или его компонентов, а на вкладке **Общие** — разрешить перевод защищаемого устройства в мобильный (автономный) режим.



В разделах, соответствующих компонентам Антивируса, можно гибко настраивать параметры из работы. Например, для **Антиспама** можно использовать один из предустановленных профилей фильтрации:



А в Антиворе — указать действия в случае утери устройства:

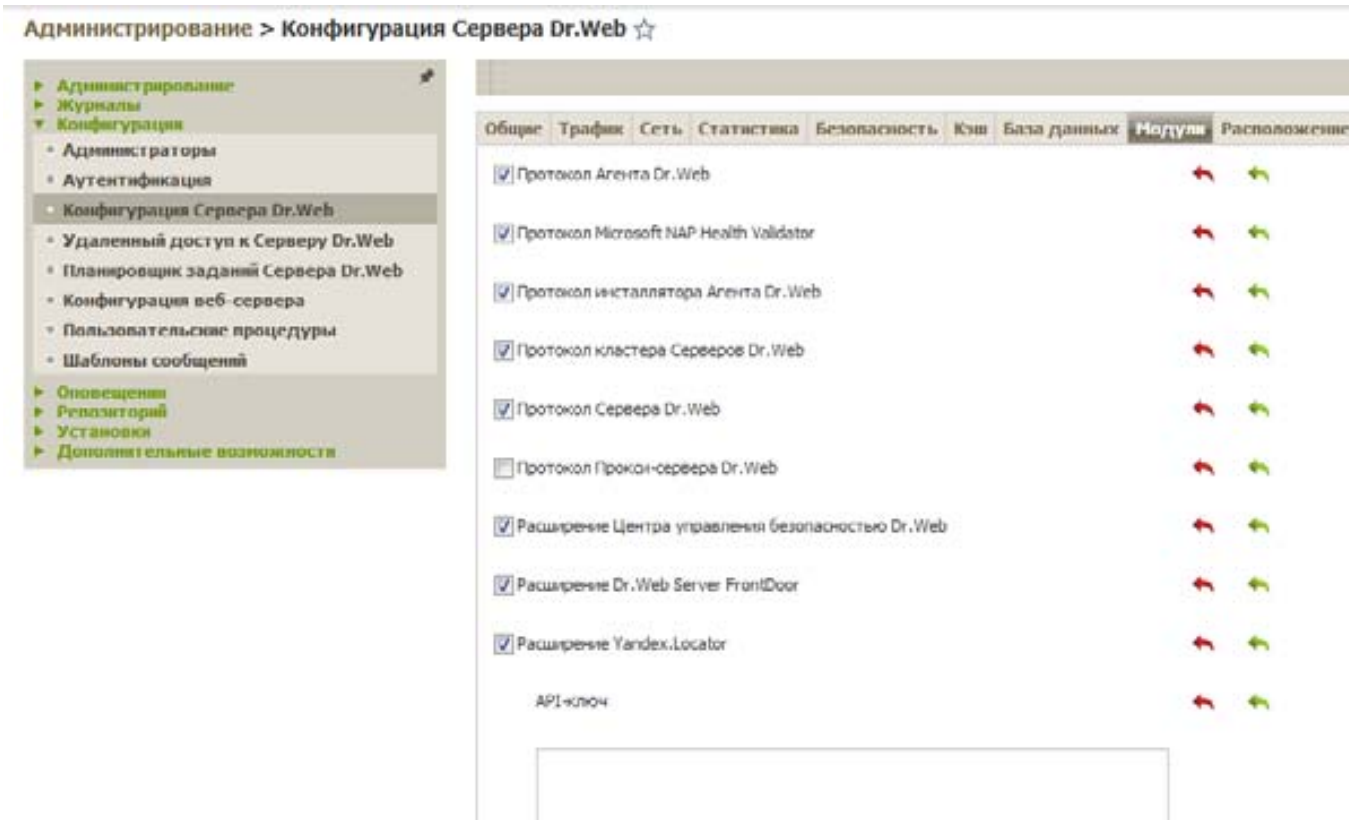
Аналогично настраиваются параметры других компонентов.

13.2. Использование Yandex.Locator для отслеживания мобильных устройств пользователей

Задача отслеживания местонахождения мобильных устройств пользователей имеет большое значение, когда речь идет об использовании корпоративных устройств и контроле «разъездных» сотрудников. Как правило, для отслеживания устройств достаточно использования ими стандартного GPS-модуля, но зачастую мобильная связь может быть или отключена пользователем устройства, или недоступна по каким-то причинам.

Для отслеживания по GPS требуется только активность телефона в сети, а для устройств, не имеющих доступа к ней, необходимо использование компонента Yandex.Locator. Для его включения необходимо сделать следующее:

1) В разделе **Администрирование → Конфигурация → Конфигурация Сервера Dr.Web → Модули** отметьте флажком пункт **Расширение Yandex.Locator**, чтобы включить его.
2) В поле API-ключ введите программный ключ, который можно получить с помощью сервиса Яндекса: https://tech.yandex.ru/maps/keys/get. Требуется регистрация.
3) Сохраните изменения и перезагрузите Сервер Dr.Web.



После настройки Yandex.Locator необходимо включить отслеживание местоположения для мобильных агентов (всех или только некоторых), установив соответствующий флажок в разделе настроек **Антивирусная сеть → Конфигурация → Dr.Web для Android → Общие**. Отслеживание будет осуществляться с помощью доступных методов — GPS-навигации или средств Yandex.Locator.

Подробнее о настройке станции с ОС Android для отслеживания е е местоположения изложено в документе **Приложения** в Главе 3, раздел Автоматическое определение местоположения станции под ОС Android.

Просмотреть текущее местонахождения мобильного агента можно в свойствах станции, нажав ссылку **Показать на карте**. Значения координат и положение на карте меняются автоматически в режиме реального времени.

14. Дополнительная информация

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу https://download.drweb.ru;
- прочитать раздел часто задаваемых вопросов по адресу https://support.drweb.ru;
- попытаться найти ответ в базе знаний Dr.Web по адресу http://wiki.drweb.com;
- посетить форумы Dr.Web по адресу https://forum.drweb.com.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела https://support.drweb.ru.

Найти ближайшее к вам представительство «Доктор Веб» и всю контактную информацию, необходимую пользователю, вы можете по адресу https://company.drweb.com/contacts/moscow.

О компании «Доктор Веб»

ООО «Доктор Веб» — российский разработчик средств информационной безопасности под маркой Dr.Web.

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

Антивирусные продукты Dr.Web разрабатываются с 1992 года, неизменно демонстрируют превосходные результаты детектирования вредоносных программ и 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!

Центральный офис «Доктор Веб» в России

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Веб-сайт: www.drweb.ru

Телефон: +7 495 789-45-87

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