Dr.WEB®
ATM Shield

Защити созданное

Dr.Web® ATM Shield

Версия 6.0

Методическое пособие для практических занятий по курсу DWCERT-007

«Централизованно управляемая защита банкоматов, терминалов и иных встраиваемых систем на базе решения Dr.Web ATM Shield»

Версия программного обеспечения	6.0.4
Версия документа	1.0
Дата последнего изменения	3 февраля 2014 года

Ограничение ответственности

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

Внимание! В программные продукты, выпускаемые ООО «Доктор Веб», могут вноситься изменения, не отраженные в данном документе. Со всеми изменениями, вносимыми в программные продукты ООО «Доктор Веб», можно ознакомиться на сайте http://www.drweb.com.

Содержание

1. Введение

Данный документ содержит сведения, описывающие порядок реализации (установки, развертывания и сопровождения) комплексной антивирусной защиты встраиваемых устройств с помощью Dr.Web® ATM Shield.

Обращаем ваше внимание, что данный документ не содержит сведений относительно:

- общих принципов организации антивирусной защиты,
- основных угроз в области информационной безопасности,
- принципов выбора мер и средств защиты на основе анализа актуальности угроз безопасности.

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».

Внимание! Сдача экзамена по курсу DWCERT-007 «Централизованно управляемая защита банкоматов, терминалов и иных встраиваемых систем на базе решения Dr.Web ATM Shield» воможна только после сдачи экзамена по курсу DWCERT-070-3 «Антивирусная система защиты предприятия».

Внимание! Возможности Dr.Web ATM Shield не ограничиваются функционалом, описанным в данной методике. Для ознакомления с возможностями ATM Shield используйте документацию по соответствующим программным продуктам компании «Доктор Веб».

Данный документ адресован администратору антивирусной сети — сотруднику организации, которому поручено руководство антивирусной защитой компьютеров этой сети.

Администратор антивирусной сети должен иметь полномочия системного администратора или сотрудничать с администратором локальной сети, быть компетентным в вопросах стратегии антивирусной защиты и детально знать антивирусные пакеты Dr.Web для всех используемых в сети ОС.

Ряд начальных глав будет полезен руководителю организации, принимающему решение о приобретении и установке системы комплексной антивирусной защиты.

Внимание! Перед прочтением документа убедитесь, что это последняя версия. Актуальную версию можно найти на официальном веб-сайте компании «Доктор Веб» http://download.drweb.com, а также в разделе https://training.drweb.com/external.

1.1. Назначение Dr.Web ATM Shield

Антивирус Dr.Web ATM Shield предназначен для организации и управления единой и надежной комплексной антивирусной защитой встраиваемых компьютеров вашей организации. При этом необязательно, чтобы компьютеры были объединены в локальную сеть и/или все имели доступ в сеть Интернет.

Dr.Web ATM Shield решает следующие задачи:

- централизованная (без необходимости непосредственного доступа персонала) установка и настройка антивирусных пакетов на защищаемых компьютерах,
- централизованное обновление вирусных баз и программного обеспечения на защищаемых компьютерах,
- мониторинг вирусных событий, а также состояния антивирусных пакетов и ОС на всех защищаемых компьютерах.

Dr.Web ATM Shield позволяет при необходимости сохранить либо ограничить для персонала, работающего с защищаемыми компьютерами, права на настройку и управление антивирусными пакетами данных компьютеров.

Антивирусная сеть Dr.Web ATM Shield имеет архитектуру клиент-сервер. Совокупность компьютеров, на которых установлены взаимодействующие компоненты Dr.Web ATM Shield, будем называть антивирусной сетью.

В состав антивирусной сети входят следующие компоненты:

Основные компоненты:

- **Dr.Web Enterprise Server (Enterprise Сервер).** Этот компонент устанавливается на одном из компьютеров антивирусной сети. Хранит дистрибутивы антивирусных пакетов для различных ОС защищаемых компьютеров, обновления вирусных баз, антивирусных пакетов и **Enterprise Агентов**, пользовательские ключи и настройки пакетов защищаемых компьютеров и передает их по запросу **Enterprise Агентов** на соответствующие компьютеры. **Enterprise Сервер** ведет единый журнал событий антивирусной сети.

Антивирусная сеть должна иметь в своем составе хотя бы один **Enterprise Сервер**.

Dr.Web Enterprise Server выполняет следующие задачи:

- установка антивирусных пакетов на выбранный компьютер или группу компьютеров,
- запрос номера версии антивирусного пакета, а также дат создания и номеров версий вирусных баз на каждом защищаемом компьютере,
- 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.

Enterprise Сервер обеспечивает сбор и протоколирование информации о работе антивирусных пакетов, передаваемой ему посредством ПО на защищаемых компьютерах (**Enterprise Агентов**, подробнее см. ниже).

Протоколирование производится в общем журнале событий, реализованном в виде внешней или внутренней базы данных.

Сбору и протоколированию в общем журнале событий подлежит следующая информация:

- информация о версии антивирусных пакетов на защищаемых компьютерах,
- время и дата установки и обновления ПО антивирусной рабочей станции с указанием версии ПО,
- время и дата обновления вирусных баз с указанием их версий,
- информация о версии ОС, установленной на защищаемых компьютерах, типе процессора, расположении системных каталогов ОС и т. п.,
- конфигурация и режимы работы антивирусных пакетов (использование эвристических методов, список проверяемых типов файлов, действия при обнаружении компьютерных вирусов и т. п.),
- информация о вирусных событиях, в том числе название обнаруженного компьютерного вируса, дата обнаружения, предпринятые действия, результат лечения и т. п.

Enterprise Сервер оповещает администратора антивирусной сети о возникновении событий, связанных с работой антивирусной сети. Оповещение администратора антивирусной сети производится по электронной почте или с использованием стандартных широковещательных средств операционных систем Windows. Настройка событий, вызывающих направление сообщения, и прочих параметров оповещения описана в п. «Оповещения».

Для повышения надежности и продуктивности антивирусной сети, а также для распределения нагрузки **Dr.Web ATM Shield** позволяет создать антивирусную сеть с несколькими Серверами. В таком случае серверное ПО устанавливается на несколько компьютеров одновременно.

Управление **Enterprise Сервером**, как правило, осуществляется при помощи **Центра управления**. **Центр управления Dr.Web** позволяет удаленно управлять антивирусной сетью путем редактирования настроек **Enterprise Сервера**, а также настроек защищаемых компьютеров, хранящихся на **Enterprise Сервере** и на защищаемых компьютерах.

- **Dr.Web Enterprise Agent (Enterprise Агент).** Этот компонент устанавливается на защищаемом компьютере, после чего уже он производит установку компонентов антивирусной защиты.

Dr.Web Enterprise Agent выполняет следующие функции:

- выполнение заданий, сформированных **Enterprise Сервером** (таких как установка и регулярное обновление антивирусного пакета, запуск сканирования и т. п.); при необходимости через специальный интерфейс вызываются на выполнение файлы антивирусного пакета;
- передача результатов выполнения заданий **Enterprise Серверу**;
- передача установленному антивирусному ПО команд и настроек с **Enterprise Сервера**;
- передача **Enterprise Серверу** сообщений о возникновении заранее оговоренных событий (в том числе вирусных) в работе антивирусного пакета.

Каждый **Enterprise Агент** подключен к **Enterprise Серверу** и входит в состав одной или нескольких зарегистрированных на этом Сервере групп (подробнее см. п. «Группы станций и их использование. Предустановленные группы»). Передача информации между Агентом и указанным Сервером осуществляется по протоколу, используемому в локальной сети (TCP/IP, IPX или NetBIOS).

В дальнейшем защищаемый компьютер с установленным Агентом, в соответствии с его функциями в антивирусной сети, будет именоваться рабочей станцией антивирусной сети. Необходимо помнить, что по своим функциям в локальной сети такой компьютер может быть как рабочей станцией, так и сервером локальной сети.

Запущенный **Enterprise Агент** в среде ОС Windows выводит в панель задач значок  . Через контекстное меню этого значка доступны некоторые функции управления антивирусной защитой, при этом список параметров, доступных через контекстное меню Агента, зависит от конфигурации рабочей станции, заданной средствами антивирусной сети. Состав параметров **Enterprise Агента** и описание соответствующих им функций для управления рабочей станцией приведены в справке **Enterprise Агента**.

Внимание! Команда **Выход** только удаляет значок из области уведомлений панели задач. Агент при этом продолжает работу. Чтобы остановить саму программу, введите в командной строке `net stop drwagntd`.

Вид значка зависит от того, установлено ли соединение рабочей станции с Сервером, и от других параметров.

Возможные варианты и соответствующие им состояния компонентов приведены в таблице.

Знак	Описание	Значение
	черный рисунок на зеленом фоне	**Агент** работает нормально и связывается с **Сервером**.
	красные стрелки на фоне значка	Отсутствует подключение к **Серверу**.
	восклицательный знак в желтом треугольнике на фоне значка	**Агент** запрашивает перезагрузку компьютера, либо отключены компоненты **SelfPROtect** или **Spider Guard**.
	фон значка меняет цвет с зеленого на красный	Произошла ошибка при обновлении компонентов пакета.
	фон значка постоянно красного цвета	**Агент** остановлен или не работает.
	фон значка желтого цвета	**Агент** работает в мобильном режиме (подробнее см. в п. Обновление мобильных Агентов Dr.Web Enterprise Agent).

Останавливать Агент не рекомендуется, так как из-за этого ПО антивирусного пакета не обновляется, а Сервер не получает информацию о состоянии рабочей станции, хотя постоянная защита компьютера при этом и не отключается. Агент автоматически загрузится после перезапуска компьютера. Чтобы снова включить Агент без перезапуска компьютера, введите в командной строке net start drwagntd. Постоянная защита компьютера будет восстановлена.

Антивирусная защита рабочих станций осуществляется антивирусными пакетами Dr.Web, разработанными для соответствующих ОС. В составе антивируса **Dr.Web ES** эти пакеты работают под управлением компонента комплекса (**Enterprise Агента**), установленного на защищаемом компьютере и постоянно загруженного в память. Это позволяет централизовано настраивать антивирусы на рабочих станциях, удаленно запускать и прерывать антивирусное сканирование, независимо от уровня квалификации пользователей рабочих станций устанавливать оптимальную стратегию защиты от вирусов.

В случае временного отключения рабочей станции от антивирусной сети **Enterprise 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.

Дополнительные компоненты:

- **Прокси-сервер.** Этот компонент может опционально включаться в состав антивирусной сети. Основная задача Прокси-сервера – обеспечение связи **Enterprise Сервера** и **Enterprise Агентов** в случае невозможности организации прямого доступа, например, если **Enterprise Сервер** и **Enterprise Агенты** расположены в различных сетях, между которыми отсутствует маршрутизация пакетов. За счет использования функции кеширования также может быть обеспечено уменьшение сетевого трафика и времени получения обновлений **Enterprise Агентами**.
- **NAP Validator.** Позволяет использовать технологию **Microsoft Network Access Protection** (NAP) для проверки работоспособности ПО защищаемых рабочих станций на основе соответствия политикам.

Внимание! **Enterprise Сервер** можно установить на любом компьютере, а не только на компьютере, выполняющем функции сервера ЛВС. Основные требования к этому компьютеру приведены в п. «Системные требования».

Внимание! В состав антивирусной сети может входить несколько **Enterprise Серверов**. Особенности такой конфигурации в настоящем руководстве описываются в п. «Иерархия серверов».

В состав антивирусного пакета Dr.Web, устанавливаемого на защищаемые рабочие станции Windows, входят следующие компоненты.

Основные компоненты:

- **Dr.Web Сканер для Windows** входит в состав обычного продукта Dr.Web для Windows. Его исполняемый файл – `drweb32w.exe`. Настройки сканера задаются непосредственно для него (через групповые настройки или персональные для станции). Проверяет ПК по запросу пользователя или согласно локальному расписанию пользователя. Дополнительно включает в себя модуль защиты от руткитов.
- **Dr.Web Enterprise Сканер для Windows** – это одна из функций **Enterprise Агента**. Это тоже антивирусный сканер, использует те же вирусные базы, то же поисковое ядро. Но функциональность эта «встроена» в **Enterprise Агента**. Предназначение **Dr.Web Enterprise Сканера для Windows** – выполнять антивирусную проверку по запросу: либо запуском по расписанию, либо непосредственным заданием **Сканировать из Центра управления Dr.Web**. Какого-либо специального интерфейса и самостоятельных настроек работы у него нет, все задается только через **Центр управления** при запуске Сканера (при настройке запуска по расписанию или при ручном инициировании проверки).
- **SelfPROtect** – обеспечивает защиту файлов и каталогов **Dr.Web ES** от несанкционированного или невольного удаления или модификации пользователем, а также вредоносным ПО. При включенном системном мониторе доступ к указанным ресурсам имеют только программы Dr.Web.

Дополнительные компоненты:

- **Сторож SpIDer Guard** (файловый монитор) постоянно находится в памяти и проверяет «на лету» все открываемые файлы на сменных дисках и открываемые на запись файлы на жестких дисках. Кроме того, сторож постоянно отслеживает действия запущенных процессов, характерные для вирусов, и при их обнаружении блокирует процессы с выводом соответствующего сообщения пользователю.
- **Почтовый сторож SpIDer Mail** (почтовый монитор) также постоянно находится в памяти. Программа перехватывает все обращения почтовых клиентов вашего ПК к почтовым серверам по протоколам POP3/SMTP/IMAP4/NNTP и проверяет входящую (или исходящую) почту до ее приема (или отправки) почтовым клиентом.
- **HTTP-сторож SpIDer Gate** постоянно находится в памяти компьютера и перехватывает все обращения к веб-сайтам по протоколу HTTP. Программа нейтрализует угрозы в HTTP-трафике (например, в отправляемых или получаемых файлах), а также блокирует доступ к подозрительным или некорректным ресурсам.
- **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. Программа позволяет не только контролировать целостность важных файлов от случайного изменения или заражения вирусами, но и запрещает служащим доступ к нежелательной информации.

1.2. Системные требования

Для установки и функционирования Dr.Web ATM Shield требуется:

1) чтобы **Enterprise Сервер** был установлен на компьютер, имеющий доступ в Интернет, для автоматического получения обновлений с серверов ВСО (Всемирной системы обновления) Dr.Web;
2) чтобы компьютеры антивирусной сети имели доступ в Интернет для связи с **Enterprise Сервером** либо прокси-сервером или находились в одной локальной сети с ним;
3) для совместной работы антивирусных компонентов на используемых компьютерах должны быть открыты все необходимые порты и сокеты:

Номер	Протокол	Назначение
порты 2193, 2371	TCP, UDP	Для связи антивирусных компонентов с Сервером.
порт 23	NetBIOS	Для связи антивирусных компонентов с Сервером.
сокет 2371	IPX/SPX	Для связи антивирусных компонентов с Сервером.
порты 2193, 2372	UDP	Для работы Сканера Сети.
порты 139, 445	TCP, UDP	Для работы Сетевого инсталлятора.
порт 9080	http	Для работы Центра управления Dr.Web.
порт 9081	https	Для работы Центра управления Dr.Web.

Компьютеры, на которые устанавливается **Dr.Web Enterprise Server**, должны удовлетворять следующим требованиям:

Компонент	Требование
Процессор	Intel® Pentium® III с частотой 667 МГц или выше
Оперативная память	512 МБ (1 ГБ при использовании встроенной БД)

Место на жестком диске	до 12 ГБ: до 8 ГБ для встроенной базы данных (каталог установки), до 4 ГБ в системном временном каталоге (для рабочих файлов). **Внимание!** При установке Сервера необходимо, чтобы на системном диске (вне зависимости от места установки самого Сервера) было не менее 300 МБ свободной памяти для запуска инсталлятора и распаковки временных файлов.
Операционная система	▪ 32 bit: Microsoft® Windows® XP Professional (SP3)/Server 2003 (SP2)/Vista (также с SP1 и выше)/Server 2008 (также с SP1 и выше)/7/8 ▪ 64 bit: Microsoft® Windows® Server 2003 (SP2)/Vista (также с SP1 и выше)/Server 2008 (также с SP1 и выше)/Server 2008 R2/7/Server 2012/8 Полный список поддерживаемых ОС приведен в Приложении А Руководства администратора.
Прочее	MS Installer 2.0 (при установке **Enterprise Сервера** для ОС Windows). Windows Script 5.6. WindowsXP-Windows2000-Script56-KB917344-x86-enu.exe .

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 1 000 станций. В противном случае необходимо использовать внешнюю БД.

Компонент	Требование
Процессор	Intel® Pentium® III с частотой 667 МГц или выше
Оперативная память	512 МБ
Место на жестком диске	не менее 1 ГБ
Операционная система	Microsoft® Windows® XP и выше Полный список поддерживаемых ОС приведен в Приложении А Руководства администратора.
Прочее	MS Installer 2.0 (при установке Прокси-сервера для ОС Windows). Подробнее см.: http://msdn2.microsoft.com/en-us/library/aa367449.aspx. Windows Script 5.6 WindowsXP-Windows2000-Script56-KB917344-x86-enu.exe (при установке Прокси-сервера для ОС Windows).

Автоматически вместе с **Enterprise Сервером** устанавливается **Центр управления Dr.Web**.

Для работы **Центра управления** требуется веб-браузер Windows® Internet Explorer® 7 и выше или веб-браузер Mozilla® Firefox® 3.0 и выше. Также возможно использование веб-браузеров Opera® 10 и выше, Safari® 4 и выше, Chrome® 7 и выше. Однако возможность работы под данными веб-браузерами не гарантируется.

Подключаемый модуль Dr.Web Browser-Plugin для полноценной работы с **Центром управления**. Модуль поставляется вместе с дистрибутивом Сервера и устанавливается по запросу браузера в процессе работы с элементами **Центра управления**, требующими подгрузку модуля (для Сканера сети, при удаленной установке антивирусных компонентов). При использовании веб-браузера Safari подключаемый модуль Dr.Web Browser-Plugin доступен только для версий, работающих под ОС Windows. При использовании веб-браузеров Mozilla Firefox, Opera и Chrome подключаемый модуль Dr.Web Browser-Plugin доступен только для версий, работающих под ОС Windows.

Для работы NAP требуется:

Для сервера — ОС Microsoft® Windows Server® 2008

Для агентов — ОС Windows XP SP3, ОС Windows Vista, ОС Windows Server 2008

Компьютер, на который устанавливается **Dr.Web Enterprise Agent** и полный антивирусный пакет **Enterprise Security Suite 6.0.4**, должен удовлетворять следующим требованиям:

Компонент	Требование
Процессор	Минимальные требования: Intel® Pentium® IV с частотой 1,6 ГГц
Оперативная память	Рекомендуемые требования: Intel® Pentium® IV с частотой 2,4 ГГц и выше
Место на жестком диске	Минимальные требования: 512 МБ
Операционная система	▪ 32 bit: Microsoft® Windows® XP Professional (также с SP1 и выше)/ XP Home (также с SP1 и выше)/XP Embedded/Server 2003 (также с SP1 и выше)/Vista (также с SP1 и выше)/7/7 Embedded /8/8 Embedded ▪ 64 bit: Microsoft® Windows® Vista (также с SP1 и выше)/7/7 Embedded/8/8 Embedded При этом ▪ SpIDer Gate, SelfPROtect, Офисный контроль: Windows 2000 с SP4 и выше. ▪ SpIDer Guard NT4, Dr.Web Сканер NT4 — Windows 2000 с SP4 без Update Rollup1, Windows XP без SP, а также с SP1, Windows 2003 без SP. ▪ SpIDer Guard G3, Dr.Web Сканер — Windows 2000 с SP4 и Update Rollup1, Windows XP с SP2 и выше, Windows 2003 с SP1 и выше, Windows Vista и выше.
Прочее	Для корректной работы контекстной справки Dr.Web Агент для Windows необходимо наличие Windows® Internet Explorer® 6.0 и выше.

На рабочих станциях антивирусной сети, управляемой с помощью **Dr.Web**, не должно использоваться другое антивирусное ПО (в том числе ПО других версий антивирусных программ Dr.Web).

1.3. Комплект поставки

Дистрибутив Dr.Web ATM Shield поставляется:

1) Для установки под управлением ОС Windows — в виде исполняемых файлов мастера установки для следующих компонентов:

- **Dr.Web Enterprise Server**, в составе
  - антивирусного Сервера **Dr.Web Enterprise Server** для соответствующей ОС,
  - Агентов **Dr.Web Enterprise Agent** и антивирусных пакетов для поддерживаемых ОС,
  - **Центра управления Dr.Web**.

  Кроме этого, в состав дистрибутива входят вирусные базы, документация, шаблоны и примеры.
- Прокси-сервер для соответствующей ОС,
- NAP Validator — компонент проверки допустимости системы при использовании технологии NAP.

1.4. Схема взаимодействия компонентов антивирусной сети

При запуске Dr.Web Enterprise Server выполняется следующая последовательность действий:

1) Загрузка файлов **Enterprise Сервера** 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 **Enterprise Агентов** и команд от Центров управления.

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

Между Сервером и рабочими станциями по одному из поддерживаемых сетевых протоколов (TCP/IP, IPX или NetBIOS) 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 ATM Shield** предусматривает возможность 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.

От веб-сервера обновлений к **Enterprise Серверу** 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 ATM Shield** и антивирусных пакетов) обеспечивается использованием механизма контрольных сумм: поврежденный при пересылке или подмененный файл не будет принят Сервером. Между Сервером и **Центром управления** 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.

2. Развертывание антивирусной сети Dr.Web ATM Shield

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 **Enterprise Сервера**.
5) Установите ПО **Enterprise 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 **Enterprise 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 **Enterprise Сервера**. **Enterprise 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 **Enterprise Серверов**. Особенности такой конфигурации описаны в п. «Иерархия серверов».

Внимание! На время установки **Enterprise Сервера** и **Enterprise 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 **Enterprise Серверам** или рабочим станциям.

2.1. Подготовка локальной сети (разрешение портов, брандмауэров и т. д.)

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

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

2.2. Установка и настройка сервера Dr.Web Enterprise Security Suite

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 все 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.

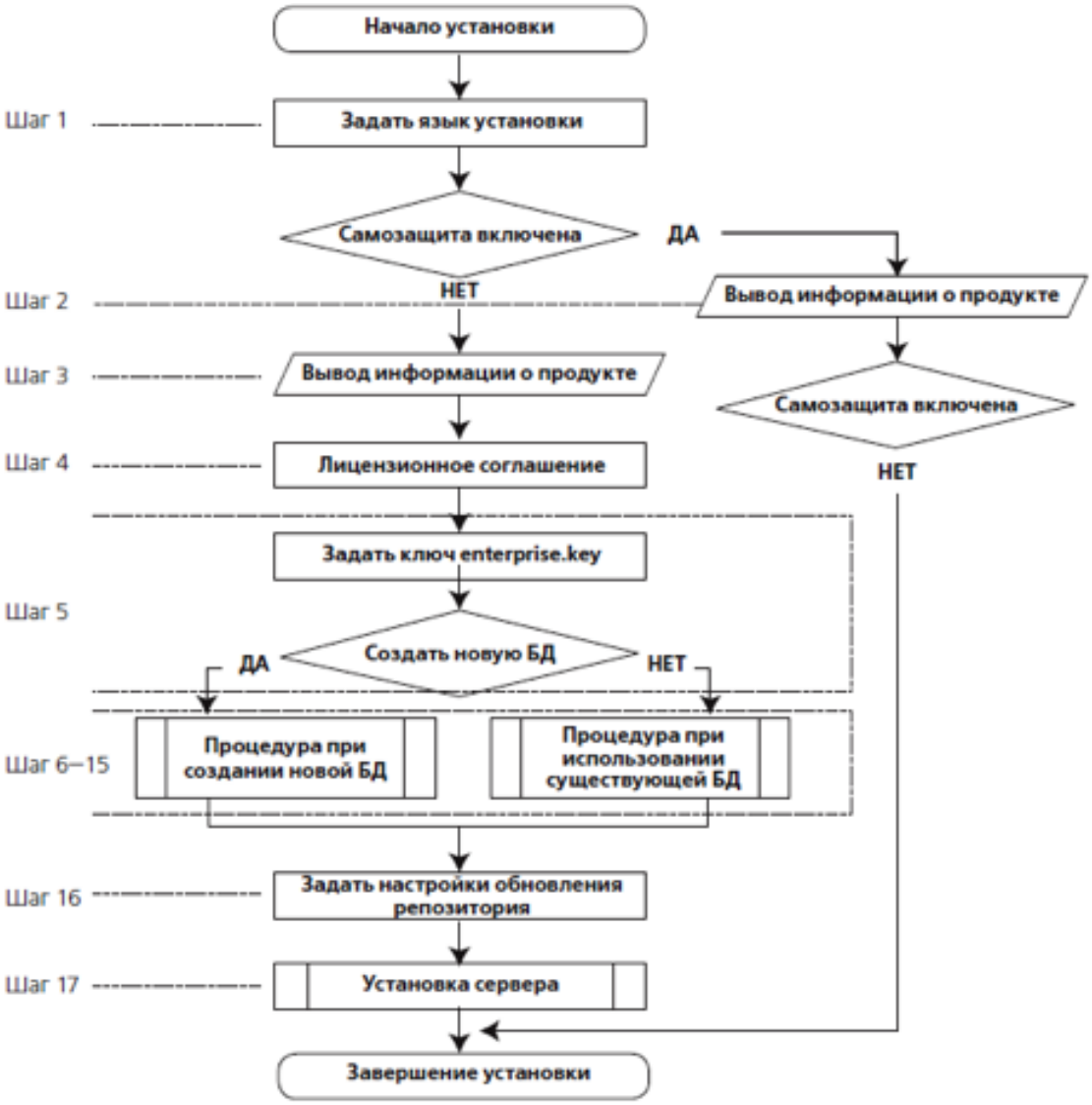
2.2.1. Установка сервера Dr.Web Enterprise Security Suite под ОС Windows NT4/2000/XP/2003/Vista/2008/2012

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

Перед началом установки **Dr.Web Enterprise Server** рекомендуется принять во внимание следующую информацию:

- Если в ОС Windows установлены службы **Terminal Services**, вам следует устанавливать ПО только с помощью мастера **Установка и удаление программ** на Панели управления ОС Windows.
- Файл дистрибутива 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 **Enterprise Сервера** должна выполняться пользователем с правами администратора данного компьютера.
- После установки **Enterprise Сервера** необходимо произвести обновление всех компонентов **Dr.Web ES** с помощью средств **Центра управления** (см. п. «Проведение обновлений автоматически и вручную»).
- При использовании внешней БД необходимо предварительно создать БД и настроить соответствующий драйвер.

Ниже приведена блок-схема процесса установки **Enterprise Сервера** при помощи инсталлятора. Разделение установки по шагам соответствует подробному текстовому описанию процедуры, приведенному ниже.



Блок-схема содержит три встроенные процедуры — процедуру **Установка Сервера** (шаг 17 не требует вмешательства пользователя и осуществляется непосредственно инсталлятором), а также процедуры при создании новой БД и при использовании существующей БД.

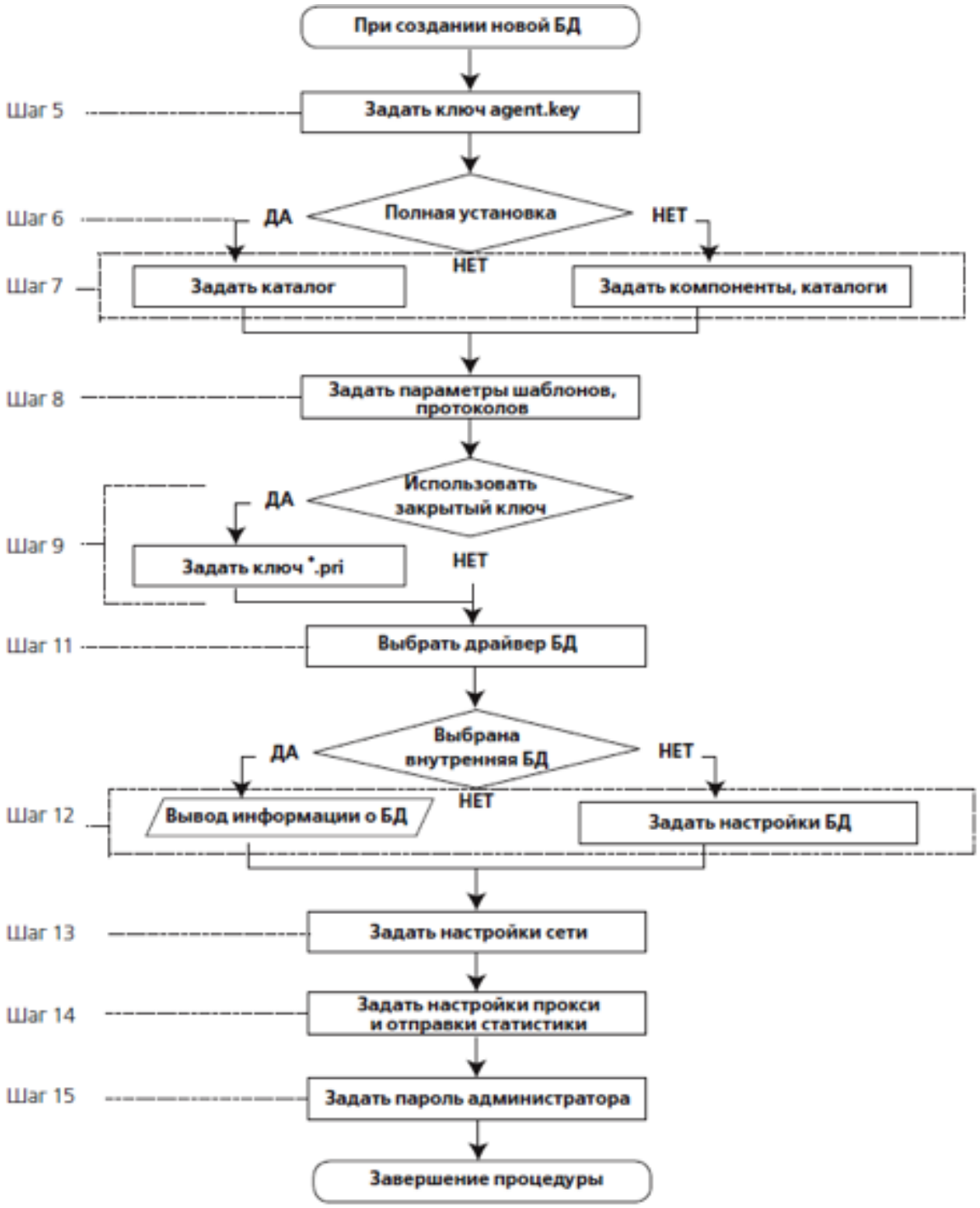


Схема процедуры инсталляции при создании новой БД

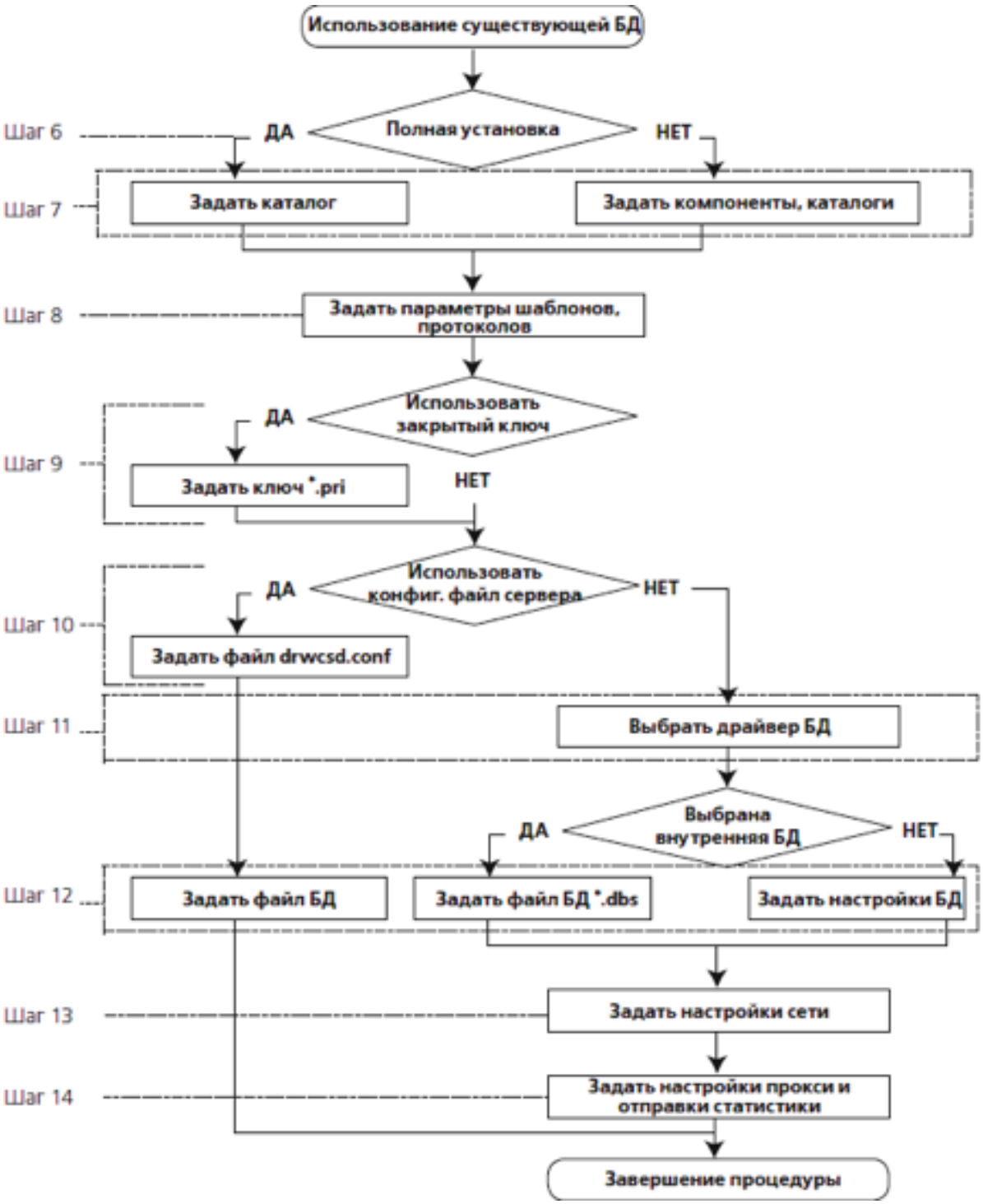
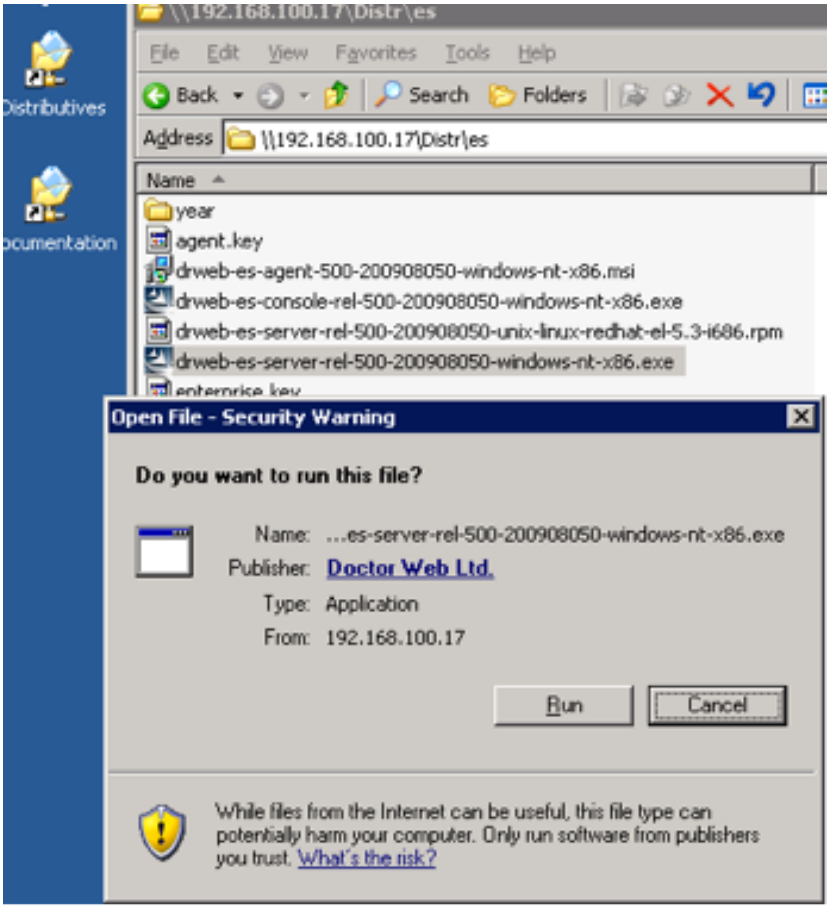


Схема процедуры установки Dr.Web Enterprise Server при использовании существующей БД

В качестве примера рассмотрим установку ESS-сервера с внутренней базой данных.

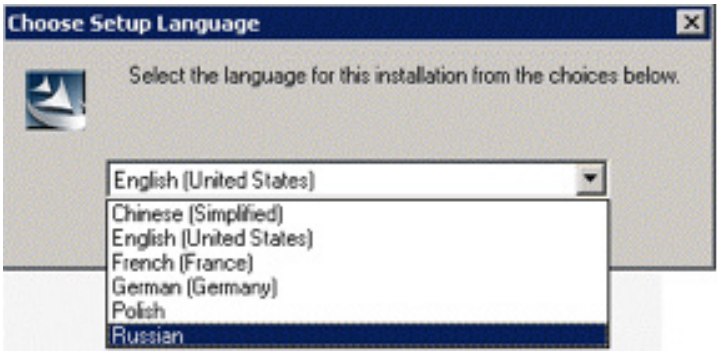
Для начала установки загрузите на сервер дистрибутив (drweb-esuite-server-se-604-201307260-windows-nt-x86.exe) и запустите его.

Внимание! Список поддерживаемых для установки антивирусного сервера и прокси-сервера операционных систем постоянно расширяется. Полный список поддерживаемых ОС приведен в документации по продукту.



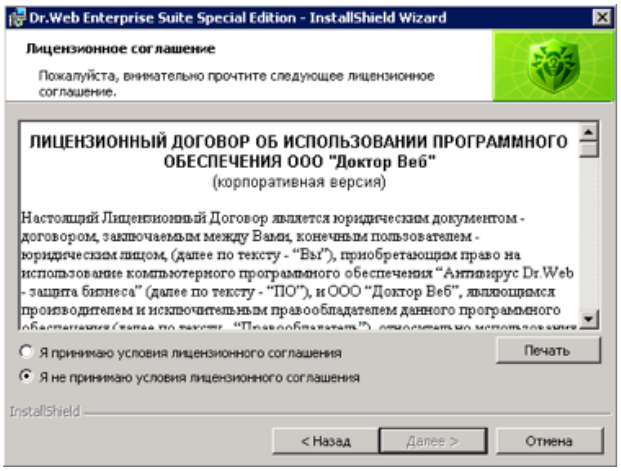
Внимание! Если установленный язык системы для программ, не поддерживающих Unicode, не соответствует языку, используемому в путях установки Сервера, — возникает ошибка чтения инсталляционного файла Сервера. Проблема устраняется установкой соответствующего языка системы для программ, не поддерживающих Unicode.

Выберите язык инсталляции.

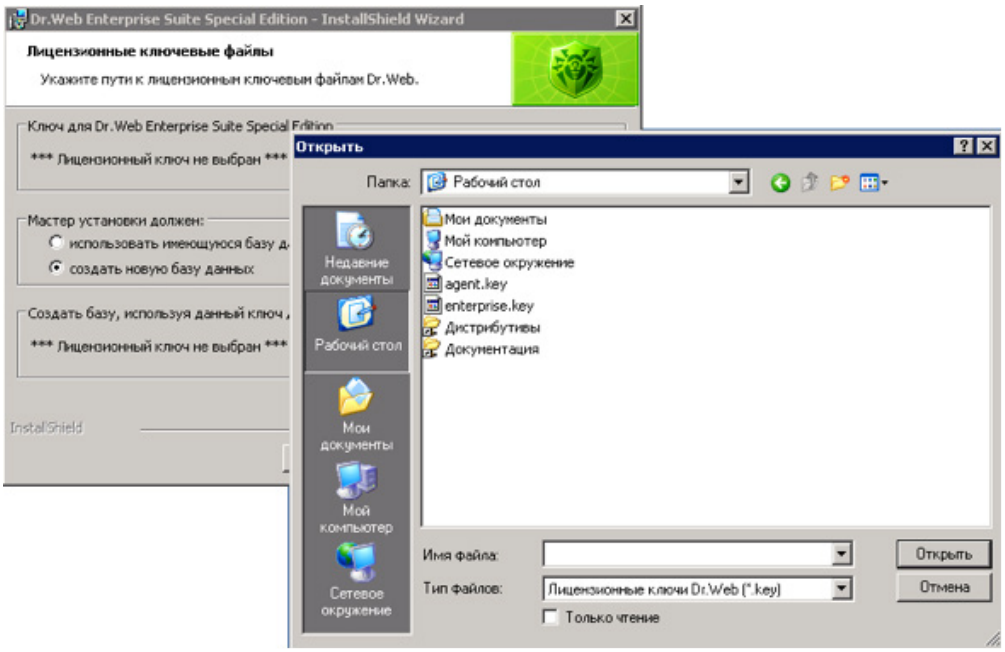


Внимание! Если на компьютере с **Enterprise Сервером** установлен **Enterprise Агент** с включенной самозащитой, то будет выдано сообщение об активности компонента самозащиты **Dr.Web**. Отключите данный компонент через настройки Агента и нажмите на кнопку **OK** для продолжения процедуры установки Сервера.

В первом окне инсталлятора необходимо принять условия лицензионного соглашения.



В появившемся окне необходимо указать используемые ключевые файлы. Укажите путь к ключам enterprise.key — для **Dr.Web Enterprise Server** и agent.key — для Dr.Web **Enterprise Agent** вручную в поле **File name** или выберите нужные файлы, нажав на кнопку **Обзор**. Если установка проводится впервые, то необходимо создать новую базу данных.



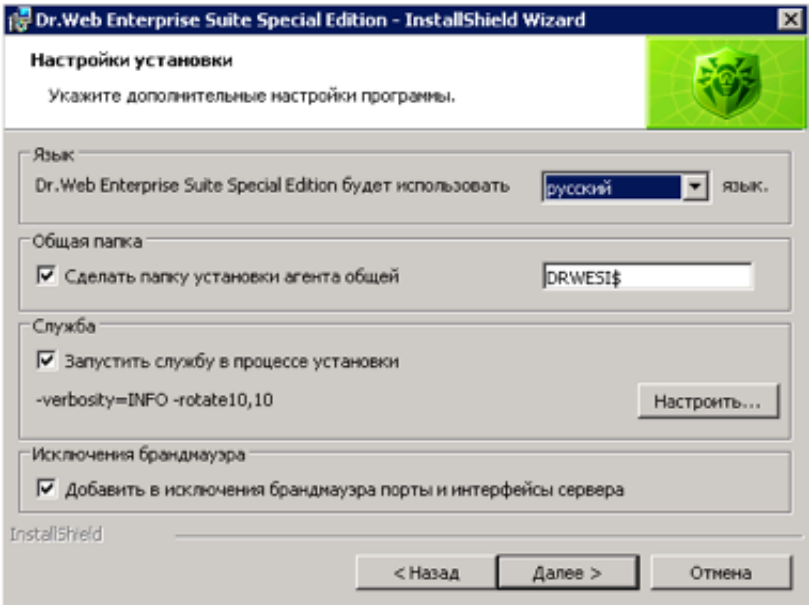
Если вы хотите сохранить базу данных Сервера от предыдущей установки, в группе кнопок выбора базы данных выберите **Использовать имеющуюся базу данных**. Файл базы данных вы сможете указать позднее.

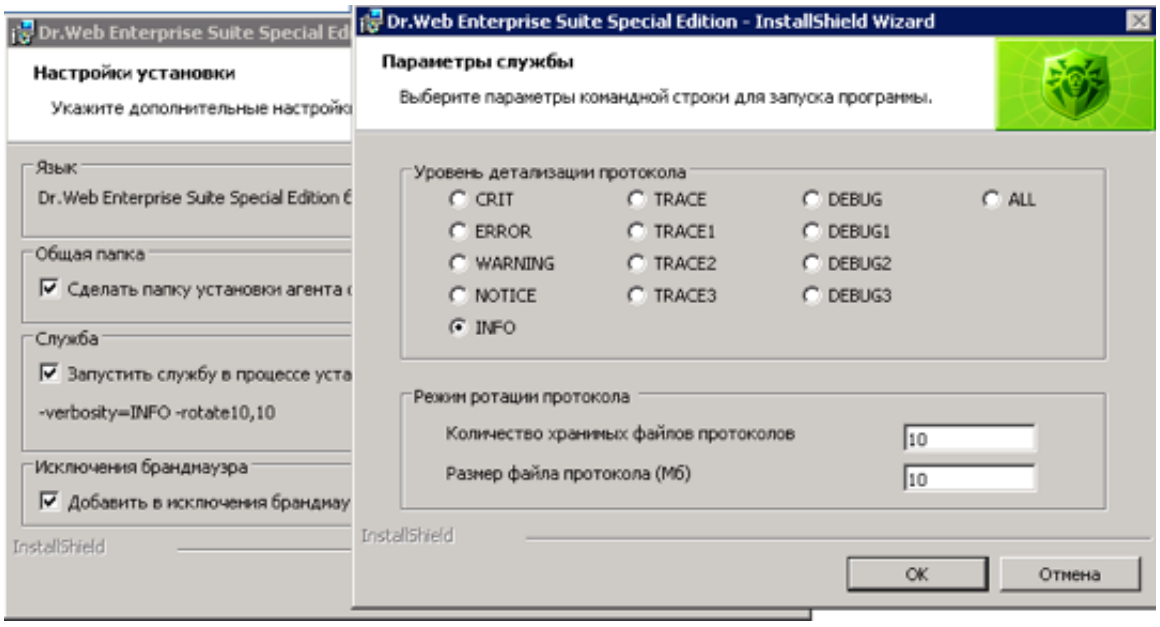
Для ознакомления с продуктом можно использовать демонстрационные ключевые файлы. Для этого необходимо перейти на веб-сайт компании «Доктор Веб» и заказать демонстрационные ключевые файлы с необходимыми параметрами.

В следующем окне необходимо выбрать тип установки — **Полная** или **Выборочная**. При выборе типа **Полная** будут установлены все компоненты **Enterprise Сервера**, при указании типа Выборочная вы сможете на следующем шаге задать компоненты, которые вы хотите установить. После выбора нажмите на кнопку **Далее**. Если на предыдущем шаге был указан тип установки **Выборочная**, то откроется окно выбора устанавливаемых компонентов и каталогов для каждого из них. В контекстном меню компонентов вы можете изменить способ их установки: установить компонент на локальной машине или для запуска по сети (доступно не для всех) или отменить установку компонента. В случае необходимости вы можете изменить каталог установки выбранного в списке компонента, для чего необходимо нажать на кнопку **Изменить** и указать новый каталог.

Если планируется использовать в качестве внешней базы данных ODBC для Oracle, выберите пункт **Выборочная** и в открывшемся окне отмените установку встроенного клиента для СУБД Oracle (в разделе **Database support — Oracle database driver**). В противном случае работа с БД Oracle будет невозможна из-за конфликта библиотек.

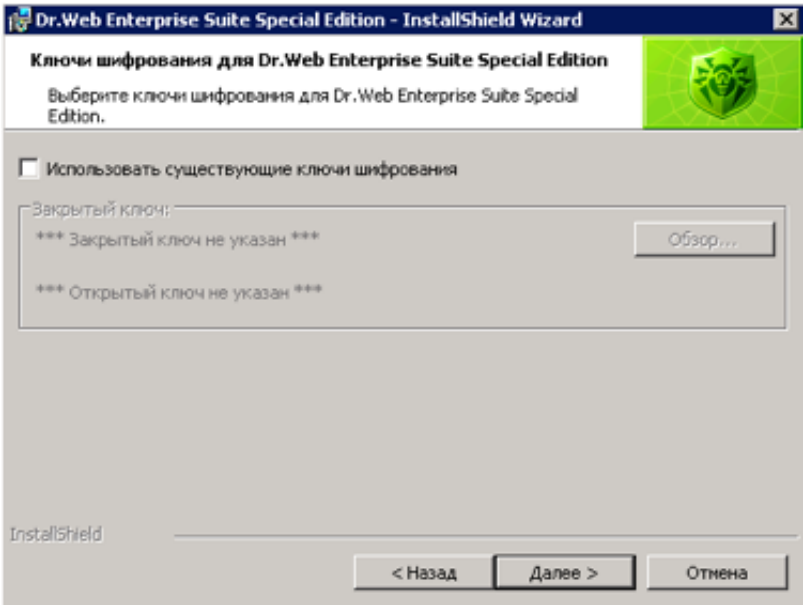
В следующем окне вы можете выбрать язык шаблонов сообщений, задать режим использования и наименование системного разделяемого ресурса для каталога установки **Агента** (по умолчанию задается скрытое имя разделяемого ресурса), задать настройки ведения файла протокола установки, нажав на кнопку **Настроить**. Если вы хотите автоматически запустить Сервер после установки, установите флаг **Запустить службу в процессе установки**. Если вы хотите добавить Сервер в исключения брандмауэра операционной системы (кроме ОС Windows 2000), установите флаг **Добавить** в исключения брандмауэра порты и интерфейсы сервера.





Если сервер устанавливается впервые, то в окне выбора ключей шифрования просто нажмите на кнопку **Далее**. Ключи шифрования будут автоматически сгенерированы в процессе установки. Если вы устанавливаете Сервер для имеющейся антивирусной сети, установите флаг **Использовать существующие ключи шифрования** и укажите файл с закрытым ключом, после чего будет создан файл с открытым ключом (содержание открытого ключа будет совпадать с содержанием предыдущего открытого ключа). Это позволит Агентам опознать устанавливаемый Сервер. В противном случае после установки

потребуется скопировать новый открытый ключ шифрования на все рабочие станции, на которых ранее были установлены ES-агенты.

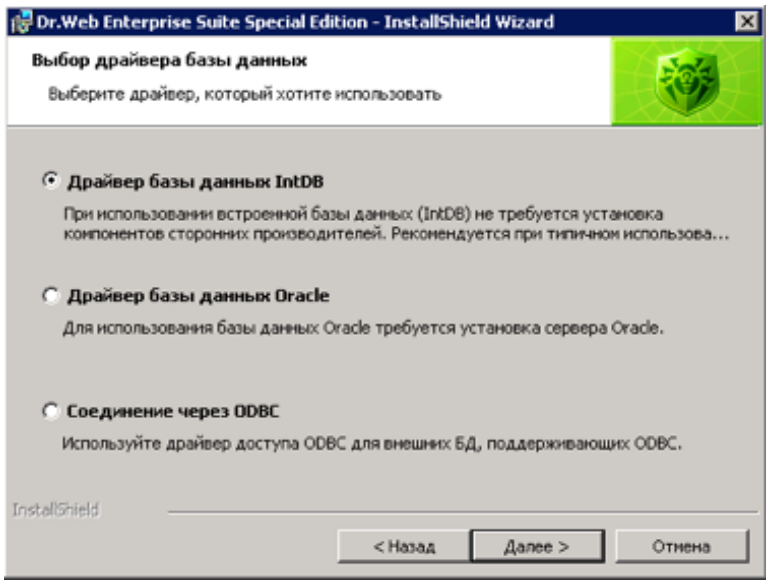


Если ранее был выбран вариант установки с существующей базой данных, то появится диалоговое окно, в котором можно указать заранее подготовленный конфигурационный файл Сервера.

В серии следующих диалоговых окон задаются основные настройки, хранящиеся в конфигурационном файле Сервера.

В диалоговом окне, посвященном конфигурации базы данных, настраиваются параметры используемой базы данных, которые зависят от выбранного ранее типа базы и наличия конфигурационного файла Сервера, задаваемого на этапе создания ключей шифрования.

При создании новой БД или в случае, если не был задан конфигурационный файл Сервера (для существующей БД), укажите драйвер, который следует использовать. Вариант **Драйвер базы данных IntDB** предписывает использовать встроенные средства антивирусного сервера. Остальные варианты подразумевают использование соответствующей внешней БД. Настройки параметров СУБД подробно описаны в руководстве администратора.

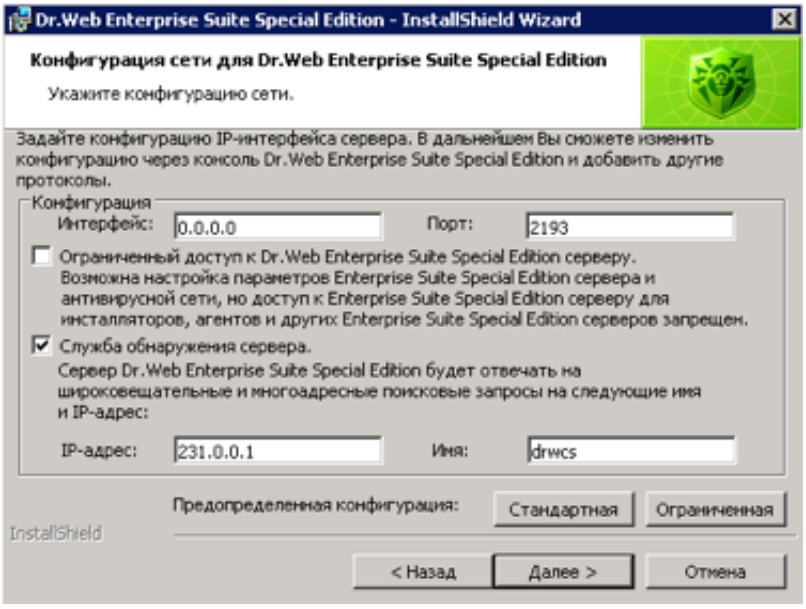


Внимание! На 64-разрядных платформах для работы антивирусного сервера с СУБД PostgreSQL версии 9.x через ODBC следует использовать 64-разрядный ODBC-драйвер версии 09.00.0310. Работа с СУБД

PostgreSQL версии 8.x через ODBC не поддерживается. Для работы на 32-разрядных платформах через ODBC с СУБД PostgreSQL, в том числе 9-й версии (x86/x64), следует использовать 32-разрядный ODBC-драйвер версии 08.04.0200. Работа с драйверами более старших версий не гарантируется.

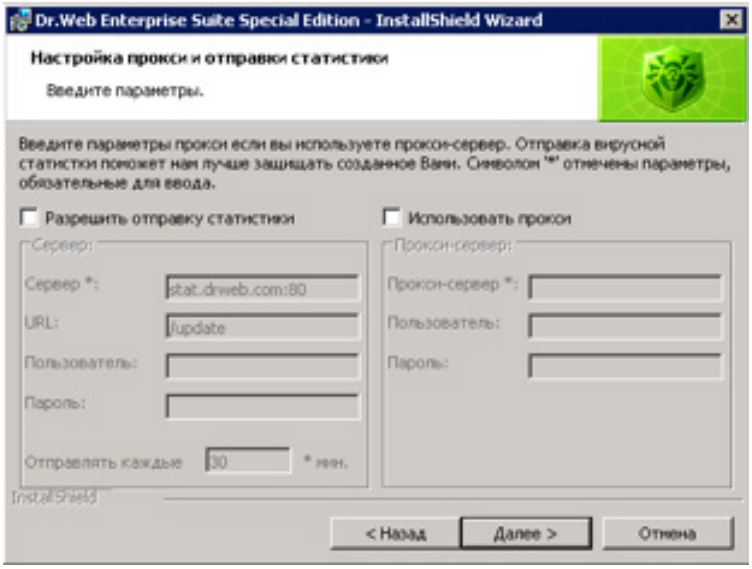
Если для создания новой БД на предыдущем шаге был выбран **Драйвер базы данных IntDB**, то в следующем окне будет выведена информация о создании новой БД. Если при использовании существующей БД вы на предыдущем шаге задали конфигурационный файл сервера или выбрали **Драйвер базы данных IntDB**, то в следующем окне необходимо будет указать файл БД, используя кнопку **Обзор** и соответствующие параметры для настройки доступа к БД.

Далее, если было задано создание новой базы или для существующей БД не был задан конфигурационный файл сервера от предыдущей установки, то будет показано диалоговое окно, посвященное конфигурации сети, в котором настраивается сетевой протокол для сервера (разрешается задать только один сетевой протокол; дополнительные протоколы можно настроить в дальнейшем). В полях **Интерфейс** и **Порт** задайте соответствующие значения для обращения к серверу. По умолчанию используется интерфейс 0.0.0.0, что означает, что к Серверу возможен доступ по всем интерфейсам. По умолчанию используется порт 2193, однако для совместимости с антивирусным ПО предыдущих версий поддерживается порт 2371. Чтобы ограничить локальный доступ к Серверу, установите флаг **Разрешить доступ только консоли Dr.Web Enterprise Suite**. Доступ инсталлятору, 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 **Администрирование**, пункт **Конфигурация сервера**, вкладка **Модули**. Установите флаг **Служба обнаружения сервера**, если хотите, чтобы сервер отвечал на широковещательные и многоадресные запросы других серверов. Чтобы задать настройки сети по умолчанию, нажмите внизу окна на кнопку **Стандартная**. Чтобы ограничить работу сервера только внутренним сетевым интерфейсом (127.0.0.1), нажмите на кнопку **Ограниченная**. При этих настройках управление возможно только из **Центра управления**, запущенного 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.



Если ранее было выбрано создание новой БД или для существующей БД не задали конфигурационный файл сервера от предыдущей установки, то в следующем окне будет выведен запрос на отправку статистики по вирусным событиям в компанию «Доктор Веб». Установите флаг **Разрешить отправку статистики** и заполните соответствующие поля. Сервер статистики — stat.drweb.com, URL — \update. Также вы можете заполнить поля **Пользователь** и **Пароль** при необходимости идентификации отправляемой статистики (получить имя пользователя и пароль можно в службе технической поддержки «Доктор Веб»). В поле **Отправлять каждые** введите интервал отправки статистики в минутах. Обязательными полями являются только адрес сервера статистики и интервал отправки статистики. Также в данном окне в случае использования прокси-сервера вы можете указать его параметры. Для этого установите флаг

Использовать прокси и введите адрес прокси-сервера (обязательный), имя пользователя и пароль для доступа к нему. Флаг **Использовать прокси** будет доступен только в том случае, если папка установки сервера не содержит конфигурационных файлов от предыдущей установки.



Если было выбрано создание новой БД, то в следующем окне задайте пароль администратора антивирусной сети.

Далее вы можете задать обновление репозитория во время установки, установив флаг **Обновить репозиторий**.

Внимание! Для проведения обновления требуется наличие доступа в сеть Интернет.

Нажмите на кнопку **Установить**. Дальнейшие действия программы установки не требуют вмешательства пользователя.

Внимание! В случае возникновения ошибок при установке антивирусного сервера на ОС Windows 2003 или Windows XP 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.

Как правило, управление установленным **Enterprise Сервером** производится при помощи **Центра управления Dr.Web**. Для удобства управления программа установки помещает в главное меню ОС Windows элементы, позволяющие осуществлять настройку и управление Сервером.

В меню **Программы** помещается папка **Dr.Web Enterprise Server**, содержащая следующие элементы:

- значок, открывающий доступ к документации администратора **Dr.Web ATM Shield**,
- папку **Server control**. Папка содержит команды запуска, перезапуска и завершения работы Сервера, а также команды настройки протоколирования и другие команды Сервера.

Каталог установки **Dr.Web Enterprise Server** имеет следующую структуру:

- var — каталог содержит подкаталоги:
  - backup — служит для хранения бэкапов БД и других критичных данных;
  - extensions — содержит пользовательские скрипты, предназначенные для автоматизации выполнения определенных заданий, все скрипты по умолчанию отключены;
  - repository — так называемый 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 на запись пользователю, от имени которого запускается Сервер (в ОС Windows — **LocalSystem**);

- templates — шаблоны отчетов;
- update–db — скрипты, необходимые для обновления структуры баз данных Сервера;
- bin — исполняемые файлы **Enterprise Сервера**;
- webmin — каталог содержит элементы **Центра управления Dr.Web**: документацию, значки, модули;
- etc — каталог содержит файлы основных настроек компонентов антивирусной сети;
- Installer — содержит программу, инициирующую процесс установки антивируса на защищаемый компьютер.

Содержимое каталога обновлений \var\repository загружается с сервера обновлений по протоколу HTTP автоматически, по установленному для Сервера расписанию, также администратор антивирусной сети может вручную помещать обновления в эти каталоги.

2.2.2. Установка внешней БД

Часто в ходе работы антивирусной сети возникает ситуация, когда возможностей внутренней базы данных, встроенной в антивирусный сервер, становится недостаточно для обеспечения стабильной и бесперебойной работы АВ-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 Dr.Web Enterprise Server**.
3) Перейдите на вкладку **База данных** и выберите в выпадающем списке **База данных** тип базы данных:
   - IntDB — встроенная БД (компонент **Enterprise Сервера**). Для встроенной БД при необходимости введите в поле **Файл** полный путь к файлу с базой данных и задайте размер кеш-памяти и режим записи данных.
   - MS SQL CE — внешняя БД для Серверов, работающих под ОС Windows.
   - Внешняя БД MS SQL CE обладает низкой производительностью и уступает по данному показателю внутренней БД. При нагрузке более 30 клиентских станций не рекомендуется использование данной БД. Однако БД MS SQL CE может успешно использоваться для создания отчетов через API ADO.NET. Если данная возможность не требуется, то рекомендуется использовать внутреннюю БД или одну из других возможных внешних БД.
   - ODBC (для Серверов, работающих под ОС Windows) — внешняя БД.
   - Oracle — внешняя БД.
     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 СУБД. Выбор этого режима создает значительную вычислительную нагрузку на Сервер. При значительном размере антивирусной сети рекомендуется использовать внешнюю СУБД.

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 1 000 станций. В противном случае необходимо использовать внешнюю БД.

Предусмотрена возможность осуществления операций, связанных с очисткой базы данных, используемой **Enterprise Сервером**, а именно: удаление записей о событиях, а также информации о станциях, не посещавших Сервер в течение определенного периода. Для очистки базы данных в меню **Администрирование** выберите пункт **База данных** и выполните соответствующую команду.

2.2.2.1. Установка Microsoft SQL Server 2008 R2 Express и настройка параметров ODBC-драйвера

Microsoft SQL Server 2008 R2 Express является наиболее доступной на сегодняшний момент СУБД для использования совместно с ES-сервером.

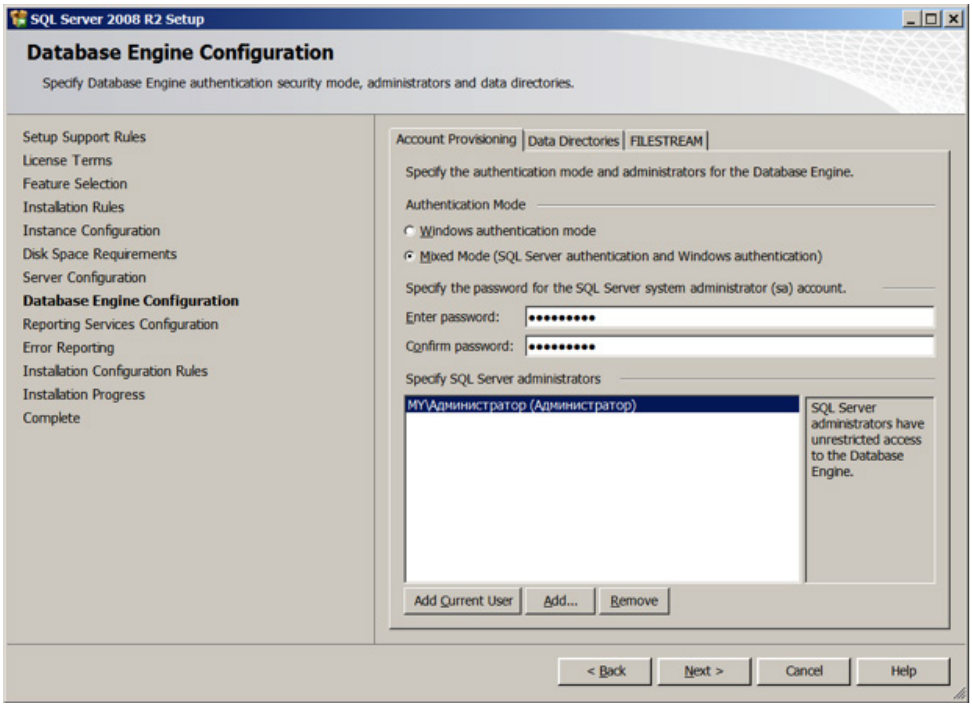
Загрузить актуальный дистрибутив Microsoft SQL Server R2 2008 Express, а также компоненты, необходимые для использования данной СУБД, можно по ссылке:

http://www.microsoft.com/sqlserver/2008/ru/ru/express.aspx. Данная СУБД совместима с Microsoft Windows XP SP2/Vista/2003 SP2/2008.

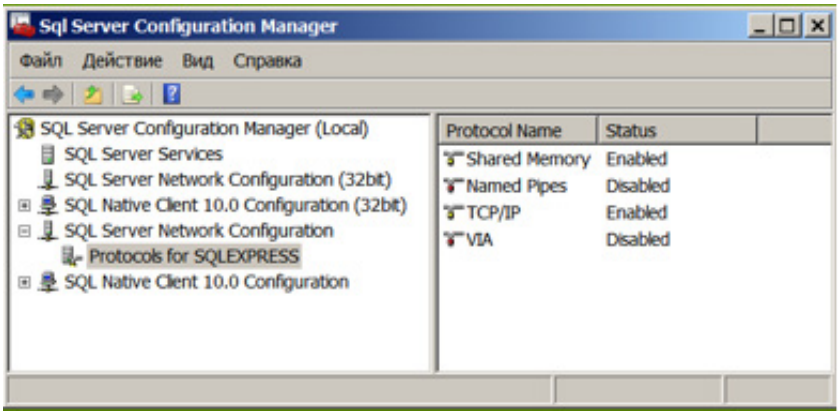
Ниже предполагается, что SQL Server и ES-сервер находятся на разных компьютерах локальной сети и между ними есть связь по протоколу TCP/IP.

При установке Microsoft SQL Server 2008 R2 Express обратите внимание на следующие моменты.

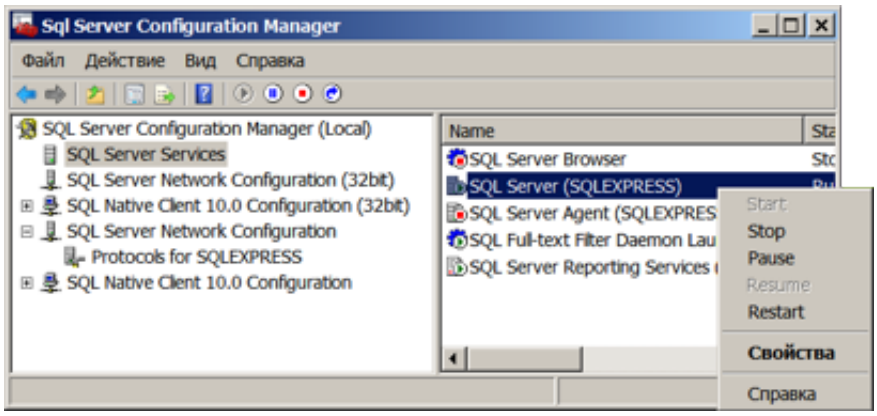
1) На этапе установки **Database Engine Configuration** выберите пункт **Mixed Mode (SQL Server authentication and Windows authentication — Смешанный режим проверки подлинности)**. Введите также любой пароль для встроенной учетной записи системного администратора SQL Server. Этот пароль необходимо запомнить.



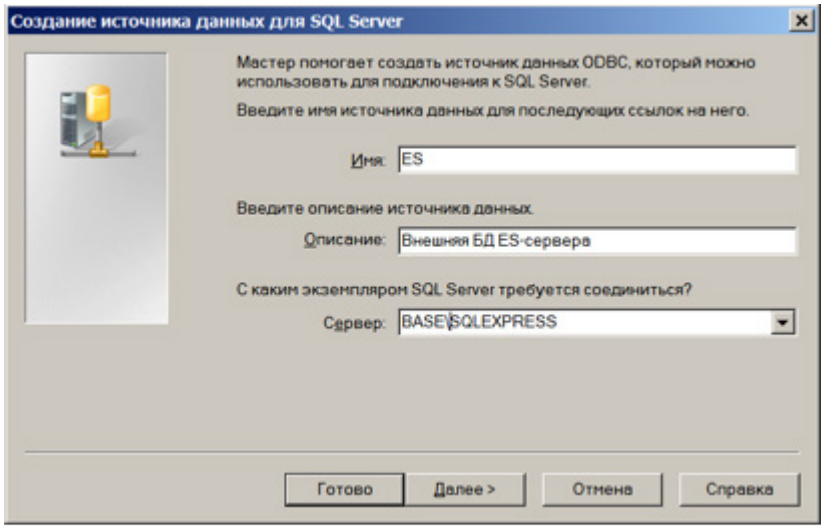
2) После установки Microsoft SQL Server R2 2008 Express необходимо открыть на компьютере с СУБД SQL Server Configuration Manager и включить протокол TCP/IP.



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

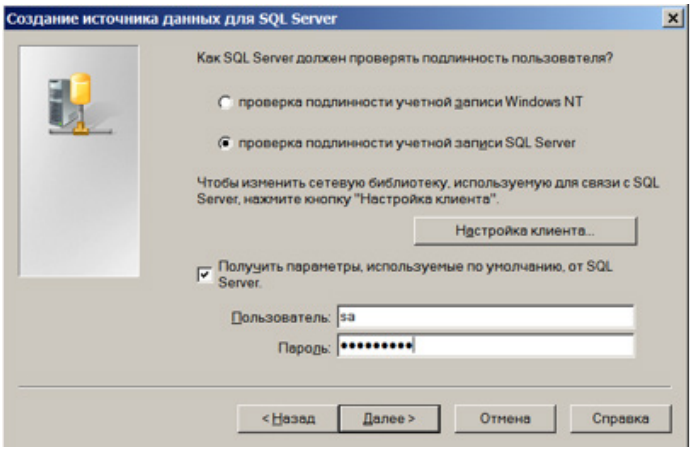


3) Для настройки ODBC-драйвера необходимо на компьютере с установленным ES-сервером произвести следующие действия (в примере рассматривается Windows Server 2008 R2, русская редакция):
   1) В **Панели управления Windows** выберите пункт **Администрирование**, в открывшемся окне дважды щелкните по значку **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.
   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 на кнопку **Настройка клиента**. Откроется окно выбора и настройки сетевого протокола.
   6) Выберите сетевую библиотеку для протокола **TCP/IP**. Нажмите на кнопку **OK**. Окно закроется. Вы вернетесь в окно настройки драйвера.
   7) 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**.



8) На последнем экране мастера выберите пункт **Изменить язык системных сообщений SQL-сервера** на и выберите **English**. Нажмите на кнопку **Готово**, а затем **OK**.

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

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

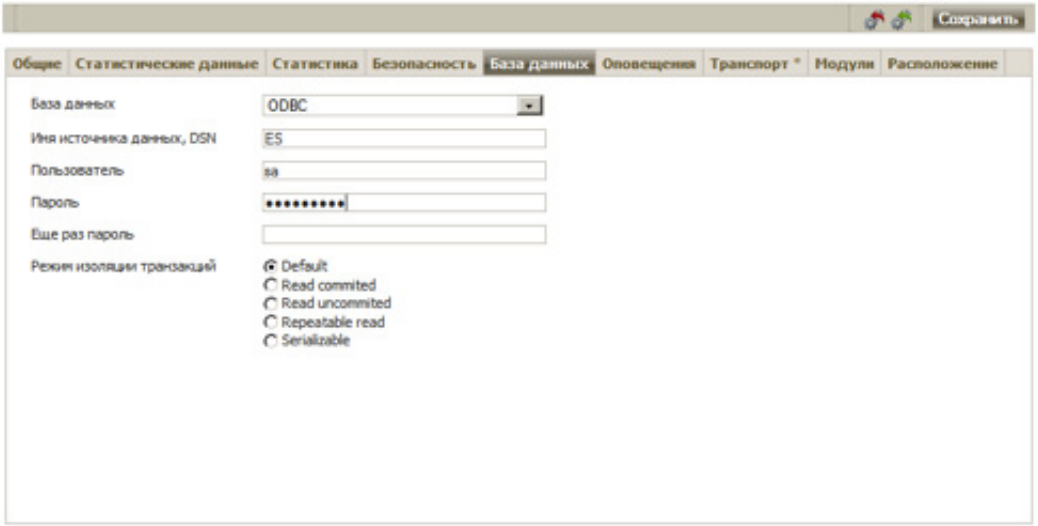
1) Остановите службу ES-сервера с помощью веб-интерфейса администратора – **Администрирование → Dr.Web Enterprise Server**, нажмите на кнопку **Остановить Dr.Web Enterprise Server**.

2) Выполните экспорт имеющейся внутренней базы данных. Для этого на компьютере с ES-сервером выполните следующую команду:

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise 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 Enterprise Server** с помощью средств управления службами Windows (**Панель управления → Администрирование → Службы**). Подключитесь к ES-серверу через Центр управления и настройте сервер на использование внешней базы данных: **Администрирование → Конфигурация Dr.Web Enterprise Server → База данных**, после чего нажмите на кнопку **Сохранить**. Откажитесь от предложения перезапустить сервер.



4) Остановите службу ES-сервера с помощью веб-интерфейса администратора – **Администрирование → Dr.Web Enterprise Server**, нажмите на кнопку **Остановить Dr.Web Enterprise Server**.

5) Проинициализируйте новую базу данных ES-сервера. Для этого на компьютере с ES-сервером перепишите в корневую папку диска C:\ ключ agent.key, относящийся к ES-серверу, и выполните следующую команду:

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

6) Импортируйте базу данных, которую вы экспортировали на предыдущих этапах, в новую базу данных. Для этого на компьютере с ES-сервером выполните следующую команду:

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

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

2.2.2.3. Установка PostgreSQL

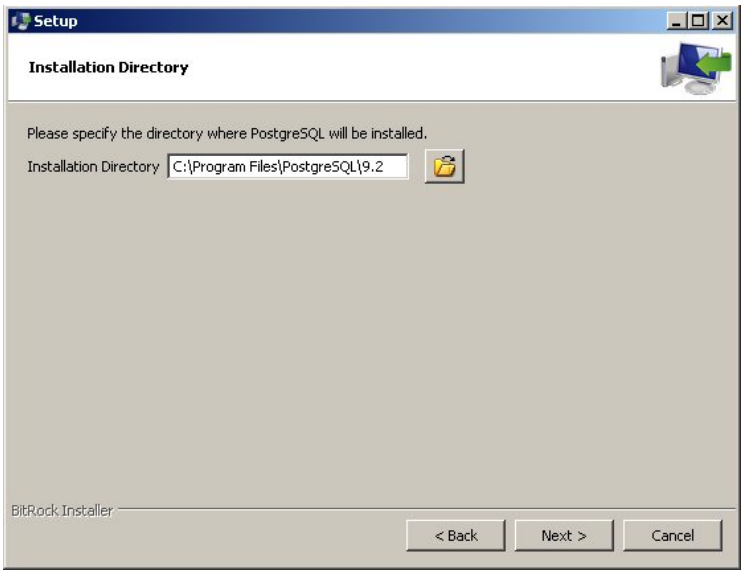
для Windows:

Установка антивирусного комплекса для ОС Windows начинается с установки внешней БД. Наиболее предпочтительным является использование PostgreSQL в качестве внешней БД наряду с MS SQL. Также возможно использование БД Oracle.

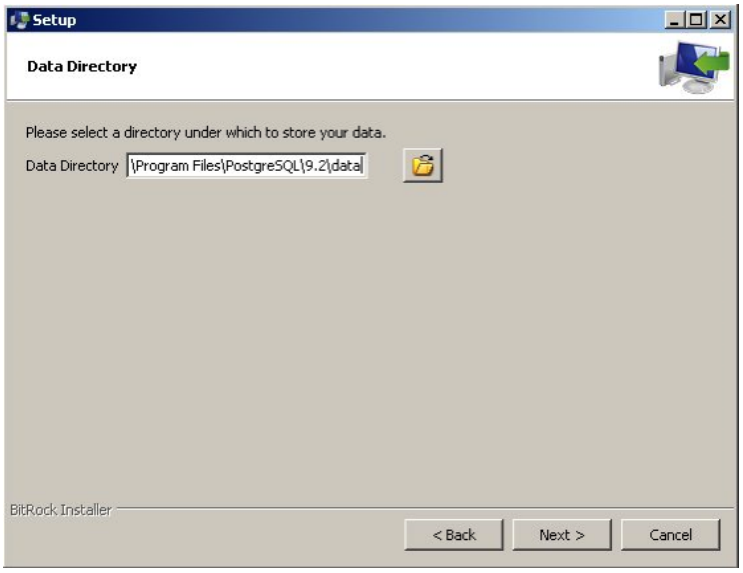
Актуальная версия PostgreSQL доступна по ссылке http://www.postgresql.org/download/windows.

Для установки базы данных PostgreSQL следует запустить файл SETUP.BAT из установочного пакета.

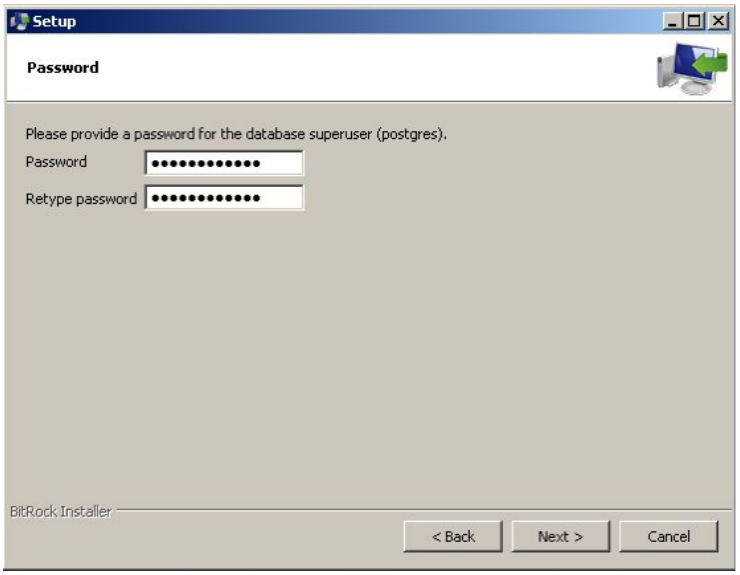
Установка PostgreSQL начинается с запуска файла дистрибутива. В появившемся окне нажмите кнопку **Next**, затем выберите папку назначения исполняемых файлов, если это требуется, и нажмите **Next** еще раз.



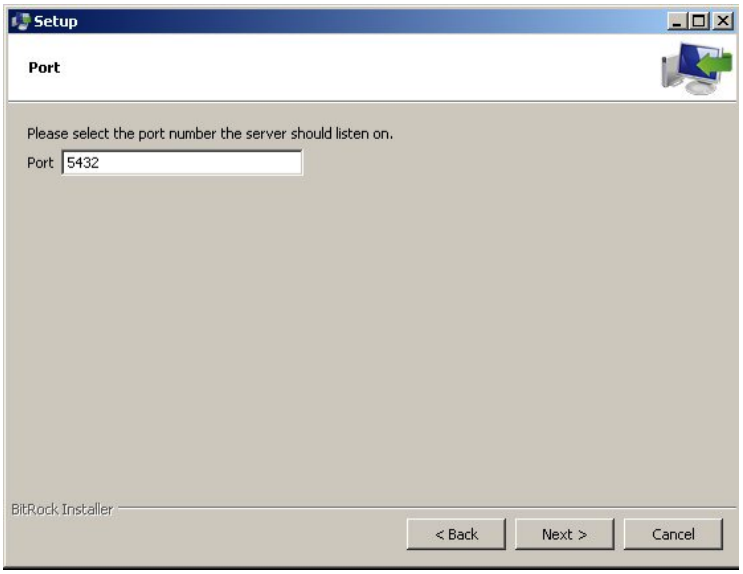
В следующем окне будет предложено выбрать папку расположения файлов БД, после чего потребуется нажать кнопку **Next**.



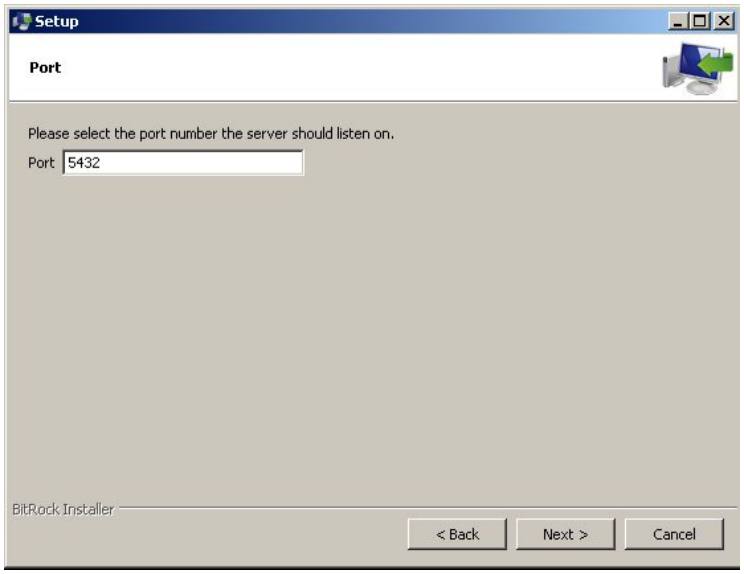
В следующем окне потребуется ввести пароль суперпользователя БД PostgreSQL (администратора), используйте только криптостойкий пароль длинной не менее 12 символов, после чего нажмите **Next** для продолжения установки.



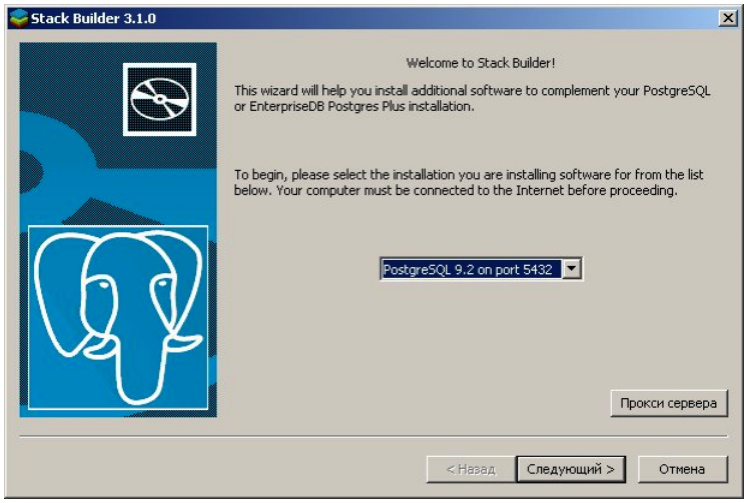
В появившемся затем окне будет предложено ввести порт, к которому будут подключатся клиенты, оставьте значение по умолчанию и нажмите **Next**.



Далее потребуется указать локаль, которую будет использовать сервер. Рекомендуется использовать **[Default locale]**, а кодировка таблиц БД будет задана затем при инициализации БД. Нажмите кнопку **Next** и дождитесь окончания установки.

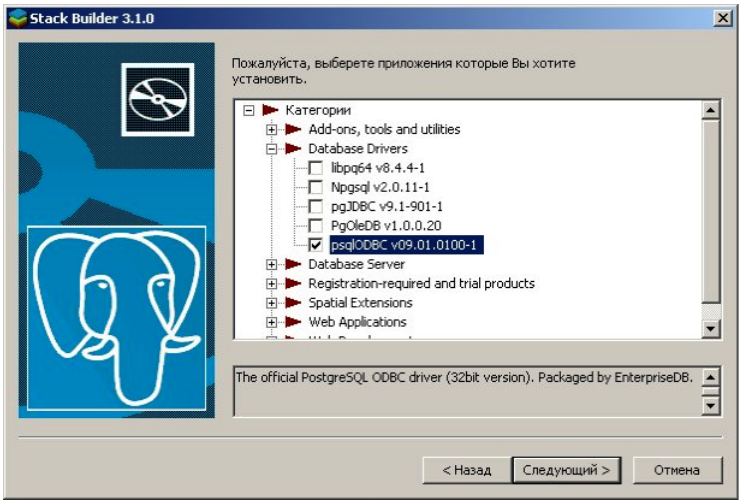


После завершения установки будет предложено запустить **Stack Builder**. Согласитесь с запуском и нажмите кнопку **Finish**. В появившемся окне Stack Builder выберите текущую установку PostgreSQL и нажмите кнопку **Next**:

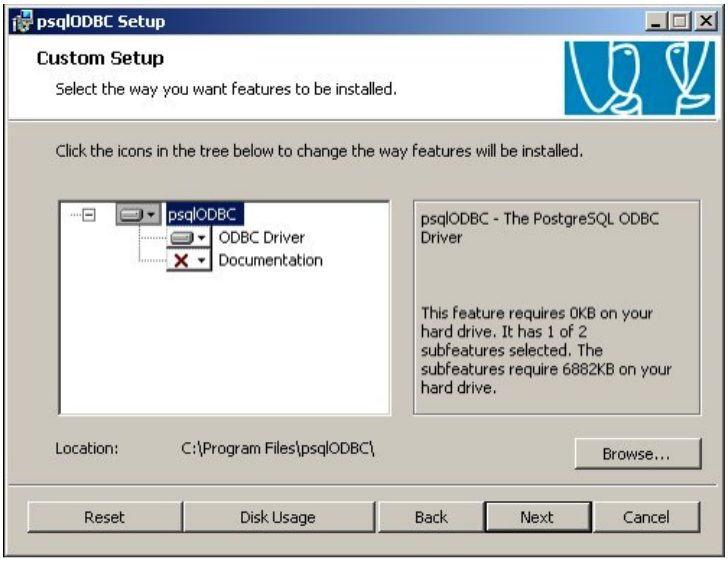


Для обеспечения работы антивирусного сервера с БД PostgreSQL необходим драйвер ODBC.

Выберите установку pgsqlODBC драйвера, как показано на рисунке ниже, или загрузите отдельно с http://www.postgresql.org/ftp/odbc/versions/msi.



В случае если установка производится с использованием архива, распакуйте его содержимое в отдельную папку и запустите инсталлятор psqlodbc.msi двойным кликом. Дальнейшая установка идентична, как и в случае использования Stack Builder. В появившемся окне нажмите **Next**, примите лицензионное соглашение и повторно нажмите **Next**. Будет предложен выбор компонентов и пути установки драйвера:



Внесите изменения в предлагаемые настройки, если это требуется, и нажмите кнопку **Next**, а в последующем окне кнопку **Install**. На этом установка PostgreSQL для Windows завершена.

После завершения установки необходимо проверить, что сервис PostgreSQL стартовал.

После успешной установки БД PostgreSQL необходимо создать пользователя и базу для антивирусного сервера. Для этого зайдите в меню **Пуск → Все программы → PostgreSQL 9.2 → SQL Shell**. 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:

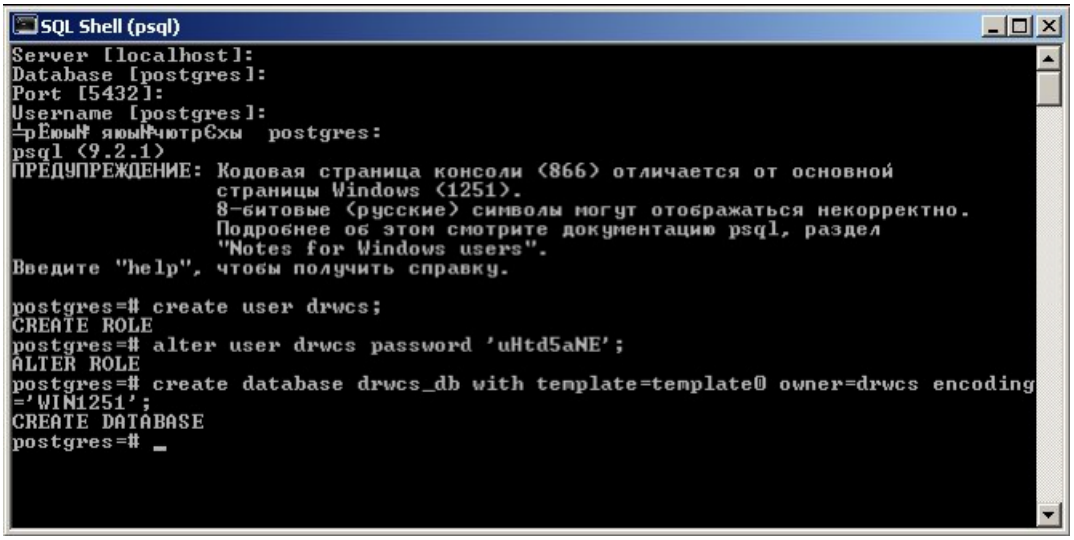
```
create user drwcs;
```

Внимание! Для задания пароля не используйте предложенный пароль:

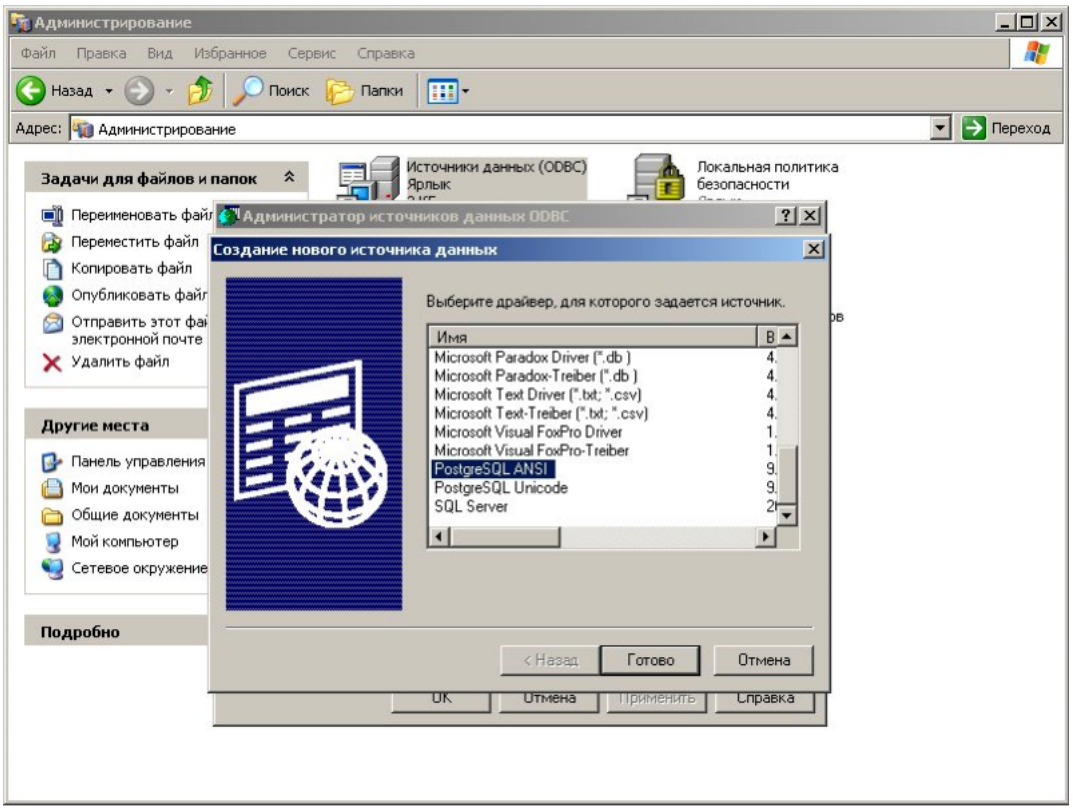
alter user drwcs password 'uHtd5aNE';

для создания БД:

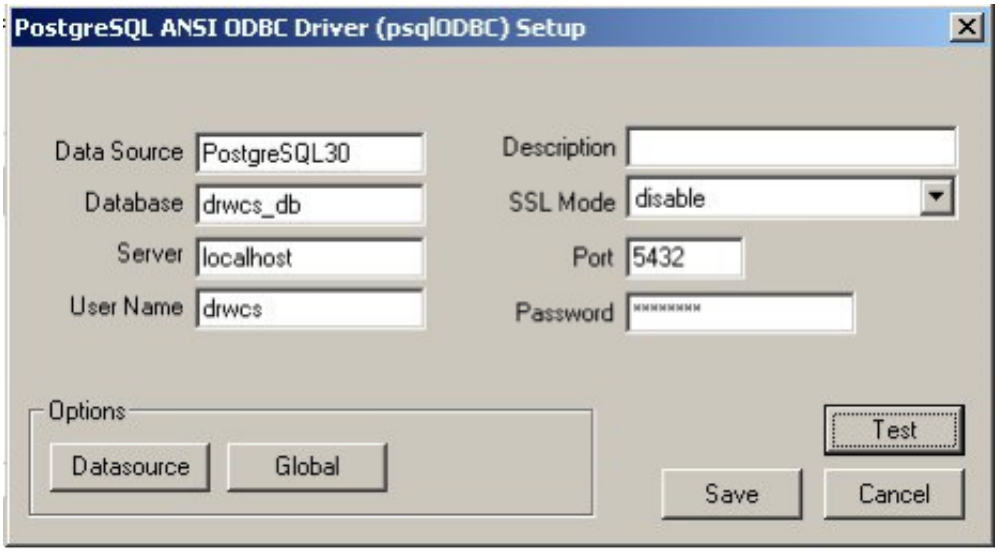
```
create database drwcs_db with template=template0 owner=drwcs encoding='WIN1251';
```



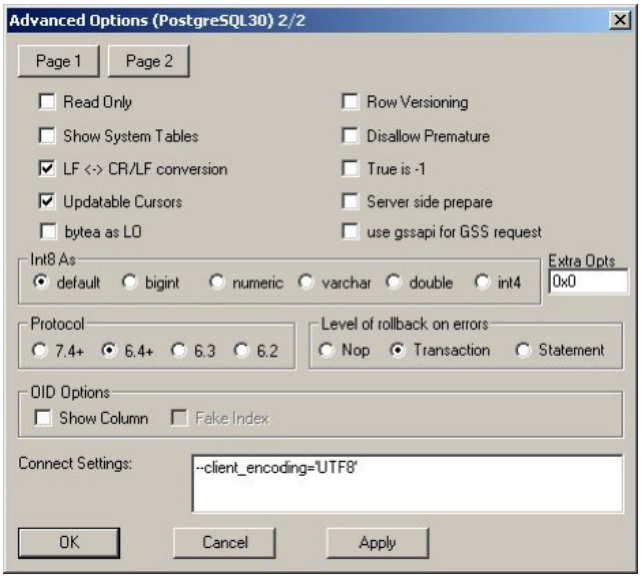
Далее следует настроить ODBC драйвер, для чего перейдите в **Панель управления** → **Администрирование** → **Источники данных (ODBC)** → **Системный DSN**, нажмите кнопку **Добавить** и в появившемся списке выберите **PostgreSQL ANSI** и нажмите **Готово**.



В появившемся окне вводятся данные, которые были использованы при создании пользователя и базы данных ранее, а именно Database drwcs_db, Server localhost, User Name drwcs, Password uHtd5aNE.



Затем нажмите кнопку **Datasource** → **Page 2** и выберите протокол 6.4+, а в поле редактирования **Connect Settings** введите `–client_encoding='UTF8` и нажмите **OK**.



Для проверки верности настроек нажмите кнопку **Test** и, в случае успеха, кнопку **Save** и **OK**. На этом установка и настройка внешней БД PostgreSQL и драйвера ODBC закончена, и можно переходить к установке антивирусного сервера для ОС Windows.

После успешной инсталляции необходимо создать и сконфигурировать внешнюю базу данных для 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.

В некоторых более новых версиях PostgreSQL инициализация БД происходит автоматически.

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:

запустить консоль управления PostgreSQL командой **Пуск → Программы → PostgreSQL 8.3 → Командная строка** и выполнить команду `psql -U postgres`.

Для создания пользователя необходимо выполнить команды:

```
create user drwcs;
```

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

В появившемся запросе вводим пароль для нового пользователя. Для простоты в примере используется uHtd5aNE, однако в целях безопасности для коммерческого использования рекомендуется создать более криптостойкий пароль длинной 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:

нужно запустить консоль управления PostgreSQL командой **Пуск → Программы → PostgreSQL 8.3 → Командная строка** и выполнить команду `psql -U postgres`.

2.3. Развертывание антивирусной сети

Установка **Enterprise Агента** должна выполняться пользователем с правами администратора данного компьютера.

Развертывание может производиться как непосредственно по локальной сети (с помощью Центра управления или настроек Active Directory) – в случае видимости банкоматов и терминалов с сервера защиты, так и локально – с помощью специально подготовленных дистрибутивов (инсталляционного пакета esinst) или сетевого инсталлятора drwinst.

Время развертывания зависит от ограничений по трафику использующейся локальной сети и может занимать до 20-30 минут при малой пропускной способности. В случае низкой пропускной способности рекомендуется использовать специально подготовленные для каждого защищаемого терминала или банкомата дистрибутивы.

Внимание! Перед установкой **Enterprise Агентов** необходимо обязательно обновить репозиторий антивирусного сервера (см. п. «Проведение обновлений автоматически и вручную», а также соответствующие разделы документации) с целью распространения актуальной версии системы защиты и снижения количества перезагрузок в связи с проведением обновлений на стороне защищаемых систем.

Если на рабочей станции уже установлен Агент, то перед началом новой инсталляции необходимо удалить установленный Агент. Для этого запустите команду drwinst 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 основных режимах:

1) В графическом режиме.
2) В фоновом режиме.

Внимание! При установке **Enterprise Агентов** на серверы ЛВС и компьютеры кластера необходимо учесть:

- В случае установки на терминальные серверы Windows (в ОС Windows установлены службы Terminal Services), для обеспечения работы Агентов в терминальных сессиях пользователей установка Агентов должна осуществляться только локально с помощью мастера установки и удаления программ на Панели управления ОС Windows.
- На серверы, выполняющие важные сетевые функции (домен-контроллеры, серверы раздачи лицензий и т. д.), а также на узлы кластера не рекомендуется устанавливать компоненты **SplDer Gate** во избежание возможных конфликтов сетевых сервисов и внутренних компонентов антивируса Dr.Web.
- Установка Агента на кластер должна выполняться отдельно на каждый узел кластера.
- Если доступ к кворум-ресурсу кластера строго ограничен, рекомендуется исключить его из проверки сторожем **SplDer Guard** и ограничиться регулярными проверками ресурса при помощи Сканера, запускаемого по расписанию или вручную.

Внимание! С помощью сетевого инсталлятора можно проводить установку **Enterprise Агентов** на операционные системы Windows XP Home Edition, Vista Starter, Home Basic, Home Premium; Windows 7 Начальная, Домашняя, Домашняя расширенная.

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

2.3.1. Установка с использованием Веб–интерфейса Центра управления Dr.Web ATM Shield

Центр управления предоставляет возможность выявлять компьютеры, на которые еще не установлена антивирусная защита **Dr.Web ATM Shield**, и удаленно устанавливать такую защиту. Удаленная установка **Enterprise Агентов** возможна только на рабочие станции, работающие под управлением ОС семейства Windows XP и выше, за исключением редакций Starter и Home.

Для того чтобы удаленно установить **Enterprise Агент** на рабочие станции, вы должны иметь права администратора соответствующих рабочих станций. Удаленная 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 Server 2003 дополнительная настройка не требуется.
- Для Windows XP:
  - рекомендуется настроить режим доступа к общим файлам: **Панель управления → Свойства папки →** Вкладка **Вид →** снять флаг **Использовать простой общий доступ к файлам**;
  - необходимо установить в локальных политиках режим сетевой модели аутентификации: **Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности → Локальные политики → Параметры безопасности → Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей → Обычная → локальные пользователи удостоверяются как они сами**.
- 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 флаг **Заблокировать учетную запись → ОК**. Щелчок правой кнопкой по записи **→ Задать пароль →** задайте пароль.

В случае если учетная запись на удаленной машине имеет пустой пароль, 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 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.

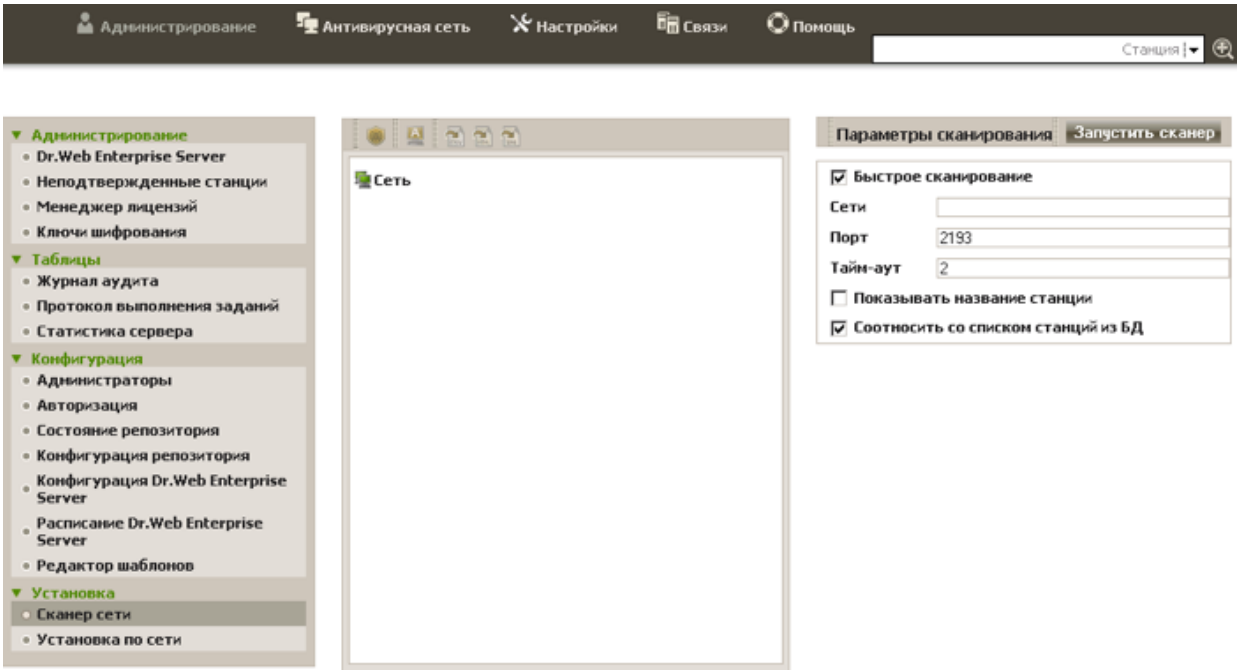
Внимание! В случае установки антивирусного сервера не на серверную операционную систему, общая папка может быть не видна по сети. В этом случае можно скопировать папку в какое-нибудь другое место и вручную сделать ее сетевой.

Для того чтобы соединиться с помощью **Веб-интерфейса** с антивирусным сервером, необходимо в адресной строке браузера ввести имя или адрес антивирусного сервера и указать порт 9080.

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

Внимание! Веб-интерфейс, входящий в состав Центра управления **Dr.Web Enterprise Security Suite**, поддерживает браузеры Windows® Internet Explorer® 7 и выше, Mozilla® Firefox® 3.0 и выше. Также возможно использование веб-браузеров Opera® 10 и выше, Safari® 4 и выше, Chrome® 7 и выше. Однако возможность работы под данными веб-браузерами не гарантируется.

Прейдите в меню **Администрирование** и выберите пункт **Сканер сети**.



Сканер сети выполняет следующие действия:

- Сканирование (обзор) сети с целью обнаружения рабочих станций.
- Определение наличия **Enterprise 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 осуществляет обработку соответствующих запросов Сканера сети, поступающих на определенный порт. По умолчанию используется порт udp/2193, однако для совместимости с ПО предыдущих версий также поддерживается порт udp/2372. 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.

Внимание! Если на станции установлен запрет (например, посредством файервола) 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.

Работа Сканера сети гарантируется под ОС Windows XP 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, из-за настроек файервола). Например, если в ОС Windows Vista и старше в настройках сети была задана **Общедоступная сеть**, то ОС будет блокировать все ping-запросы.

В случае блокирования ping-запросов в связи с используемыми сетевыми политиками можно использовать альтернативный метод последовательного опроса всех станций на наличие агента. Этот метод может использоваться как дополнение к быстрому сканированию, в случае если в сети есть станции, блокирующие ping-запросы (так, например, Windows Vista при установках сети типа «Домашняя сеть» или «Кафе» блокирует ping'и).

При обычном сканировании не рассылаются ping-запросы, а последовательно опрашиваются все станции на наличие Агента. Этот метод может использоваться как дополнение к быстрому сканированию в случае, если в сети есть станции, на которых заблокированы ping-запросы. Сканирование в случае быстрого сканирования идет параллельно, в случае медленного — последовательно, что влияет на скорость работы.

Скорость работы Сканера сети значительно отличается. 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 измените порт и значение тайм-аута.

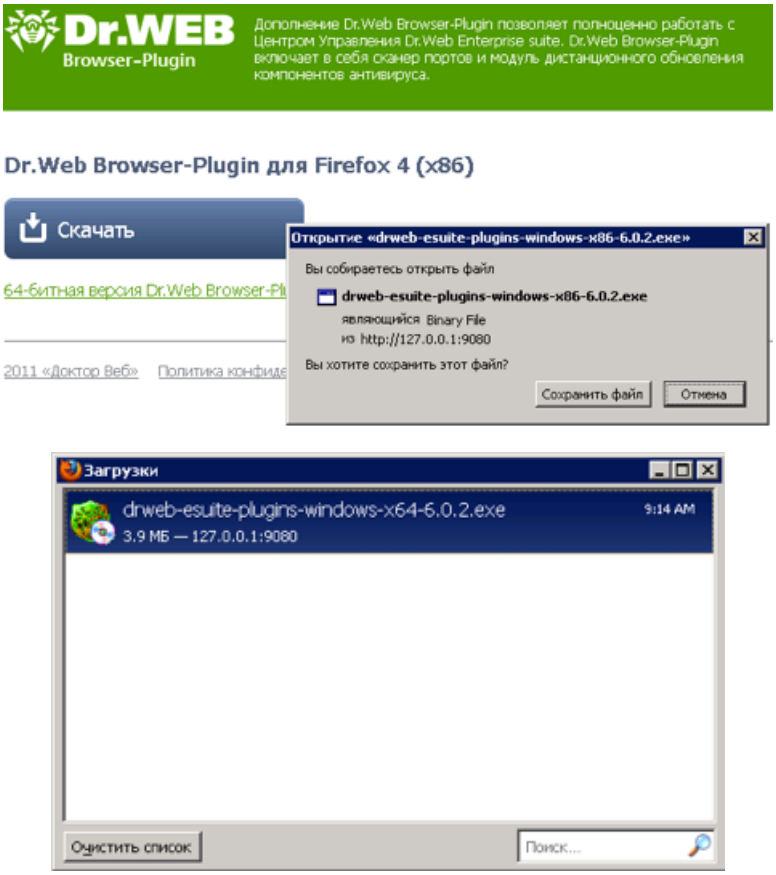
Нажмите **Запустить сканер**.

Внимание! Для отображения работы станции необходимо установить дополнительный плагин (Dr.Web Browser-plugin) к используемому браузеру. Сообщение о необходимости установки появится автоматически. Подключаемый модуль Dr.Web Browser-Plugin необходим для полноценной работы с **Центром управления**. Модуль поставляется вместе с дистрибутивом Сервера и может быть установлен:

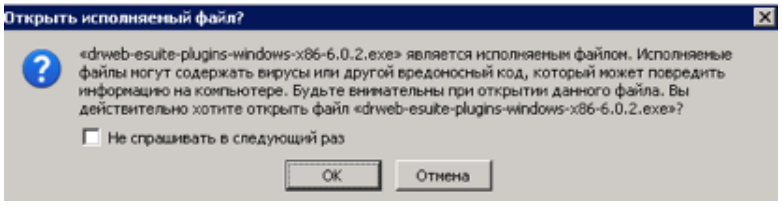
1) При помощи инсталлятора модуля **Dr.Web Browser-Plugin**. Для установки Dr.Web Browser-Plugin при помощи инсталлятора:
   1) Запустите файл дистрибутива. Откроется окно **InstallShield Wizard**, извещающее вас об устанавливаемом продукте. Нажмите на кнопку **Далее**.
   2) Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора в группе кнопок выбора укажите **Я принимаю условия лицензионного соглашения** и нажмите на кнопку **Далее**.
   3) Откроется окно выбора каталога установки. Если необходимо изменить каталог установки, заданный по умолчанию, нажмите на кнопку **Change** и выберите каталог установки. Нажмите на кнопку **Далее**.
   4) В следующем окне нажмите на кнопку **Установить** для начала процесса инсталляции. Дальнейшие действия программы установки не требуют вмешательства пользователя.
   5) После завершения установки нажмите на кнопку **Готово**.
2) По запросу браузера в процессе работы с элементами **Центра управления**, требующими подгрузку модуля (для Сканера сети, при удаленной установке антивирусных компонентов), — особенности использования данного метода будут описаны ниже.

При использовании веб-браузеров Mozilla Firefox, Opera и Chrome подключаемый модуль Dr.Web Browser-Plugin доступен только для версий, работающих под ОС Windows. При использовании веб-браузера Safari подключаемый модуль Dr.Web Browser-Plugin доступен только для версий, работающих под ОС Windows.

На появившейся странице предлагается начать скачивание плагина или (в случае, если тип плагина определен неверно) выбрать для скачивания необходимый тип плагина.

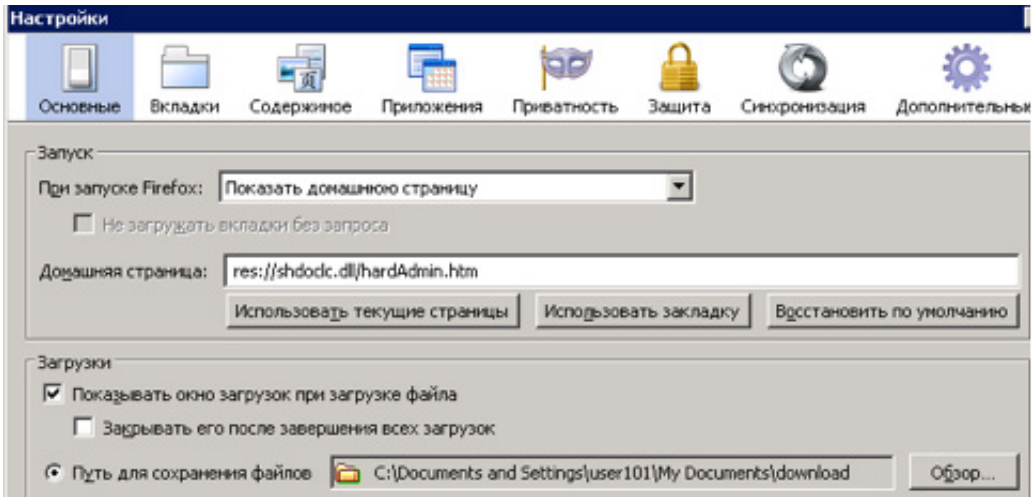


Запустить процесс установки можно сразу после окончания загрузки — кликнув по загруженному файлу в окне загрузки и подтвердив свое согласие.



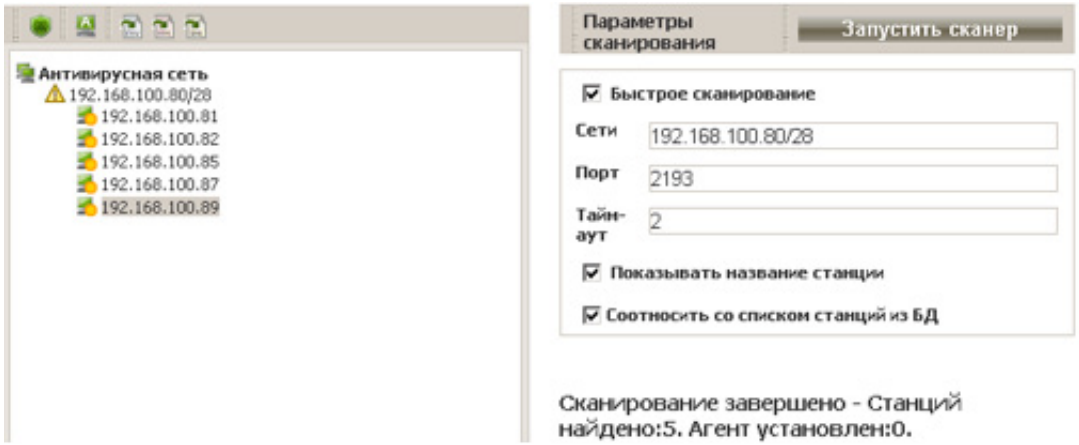
После завершения установки рекомендуется обновить страницу браузера.

Внимание! При использовании неанглоязычного браузера типа Firefox на англоязычной операционной системе Windows необходимо убедиться, что в названии папки загрузки по умолчанию не используются неанглийские символы (должна быть только латиница). Настройка папки скачивания производится на странице **Основные** меню **Настройки** браузера Mozilla Firefox.



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.

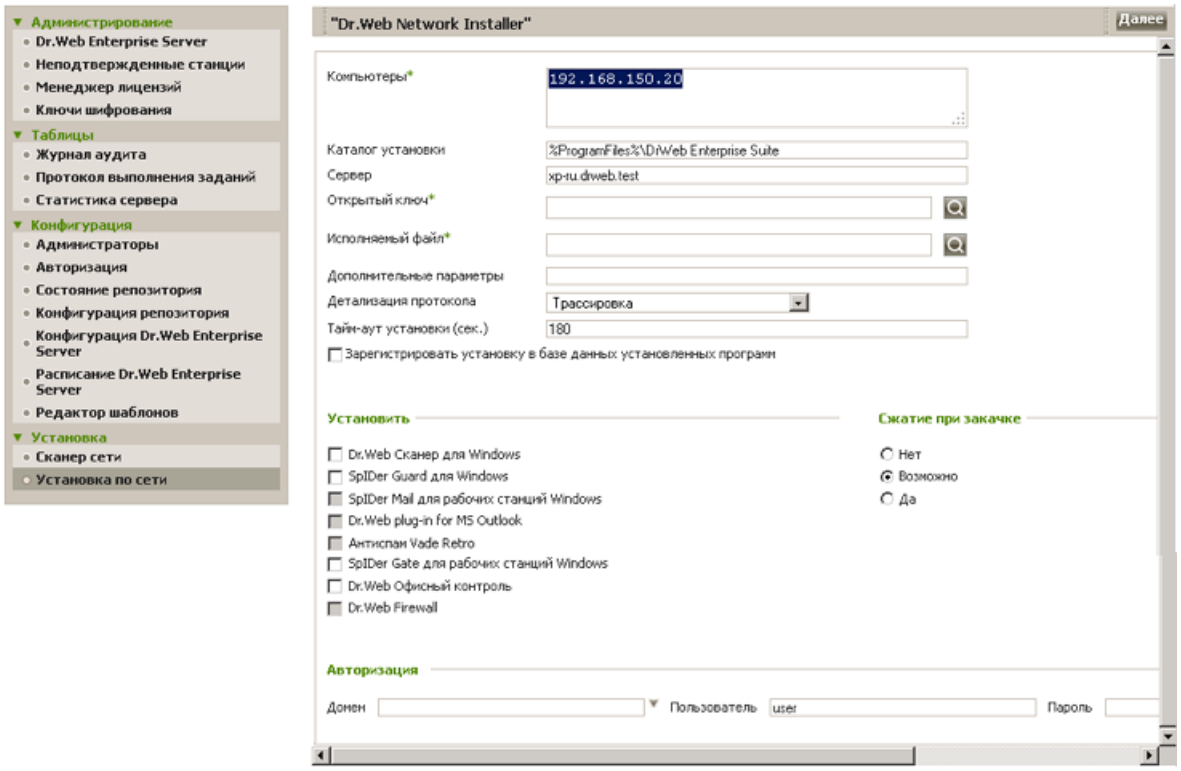
При необходимости разверните элементы каталога, соответствующие рабочим группам (доменам).



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 **Компьютеры** 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**.

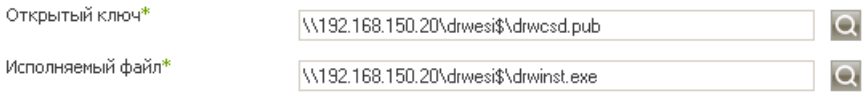
По умолчанию в поле **Сервер** отображается IP-адрес или DNS-имя **Enterprise Сервера**, к которому подключен **Центр управления**. При необходимости укажите в данном поле адрес Сервера, с которого будет устанавливаться антивирусное ПО.

При необходимости введите в поле **Дополнительные параметры** параметры командной строки сетевого инсталлятора.

Внимание! Начиная с версии 5.0 в состав **Dr.Web ATM Shield** входят компоненты **SpIDer Gate** и **Офисный контроль**. Если компоненты **SpIDer Gate** и **Офисный контроль**, входящие в состав **Dr.Web ATM Shield**, не указаны в лицензии, рекомендуется настроить список устанавливаемых компонентов на рабочих станциях, установив значение **Не может** для компонентов **SpIDer Gate** и **Офисный контроль**.

Нажмите значок напротив поля **Открытый ключ** и, введя путь к расшаренной в процессе установки сервера папке, выберите drwcsd.pub. Используемый сервер указывается в поле **Сервер**.

Нажмите значок напротив поля **Исполняемый файл** и, введя путь к расшаренной в процессе установки сервера папке, выберите файл drwinst.exe.



Внизу окна введите имя домена (по умолчанию drweb.test), имя и пароль доступа к компьютеру, на котором производится установка. Если необходимо выбрать домен из списка известных, то нажмите на кнопку . Вы можете также ввести пароли доступа для различных пользователей, используя кнопку .

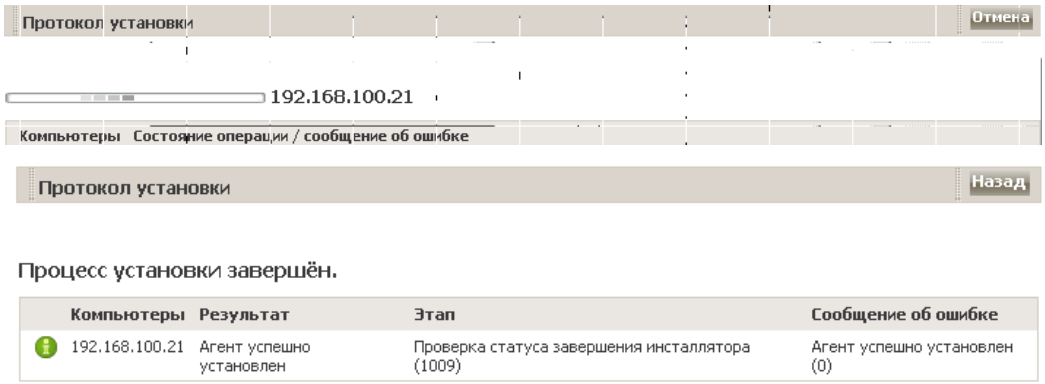
В открывшемся окне выберите параметры установки.

В разделе **Авторизация** вы можете указать параметры авторизации Агента на Сервере. Если флаг **Установить параметры** не установлен и 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.

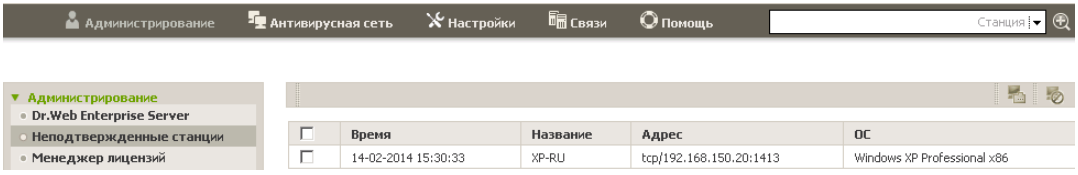
В дальнейшем эти параметры можно изменить в настройках **Enterprise Агента** и свойствах станции.

Нажмите **Установить**.

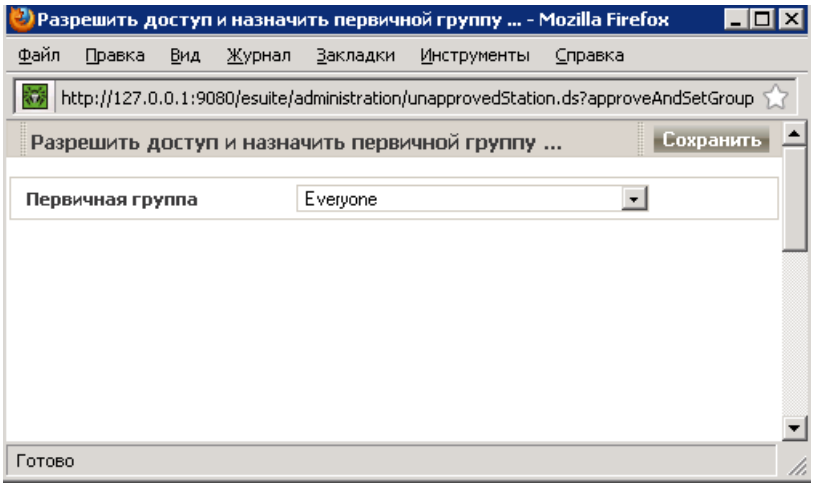


При настройках **Enterprise Сервера** по умолчанию администратору необходимо вручную подтвердить новые рабочие станции для их регистрации на Сервере (подробнее о политике подключения новых станций см. п. «Политика подключения новых станций»). При этом новые рабочие станции не подключаются автоматически, а помещаются Сервером в список неподтвержденных станций.

Выберите пункт **Неподтвержденные станции** меню **Администрирование**, отметьте станции, на которых была произведена установка, и нажмите на значок  или  . Выберите пункт **Разрешить доступ и назначить группу Everyone первичной**, чтобы задать группу **Everyone** в качестве первичной для подтвержденной станции, или пункт **Разрешить доступ и назначить первичную группу**, чтобы задать другую первичную группу для данной рабочей станции. После подтверждения станции (если этого требуют настройки **Enterprise Сервера**), автоматически будут установлены антивирусные компоненты.



При нажатии на значок  появится окно с выбором первичной группы.



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.

Для завершения установки некоторых компонентов антивирусной рабочей станции может потребоваться перезагрузка компьютера. В этом случае на фоне значка **Enterprise 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 ходе установки автоматически удаляются обнаруженные антивирусные продукты. Список антивирусных продуктов, удаление которых возможно в автоматическом режиме, приведен в документации.

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

2.3.2. Установка с использованием дистрибутивов компонентов Dr.Web ATM Shield

Установка с использованием дистрибутивов может производиться как администратором, так и пользователем. При этом для установки может использоваться инсталляционный пакет esinst.exe или Сетевой инсталлятор drwinst.

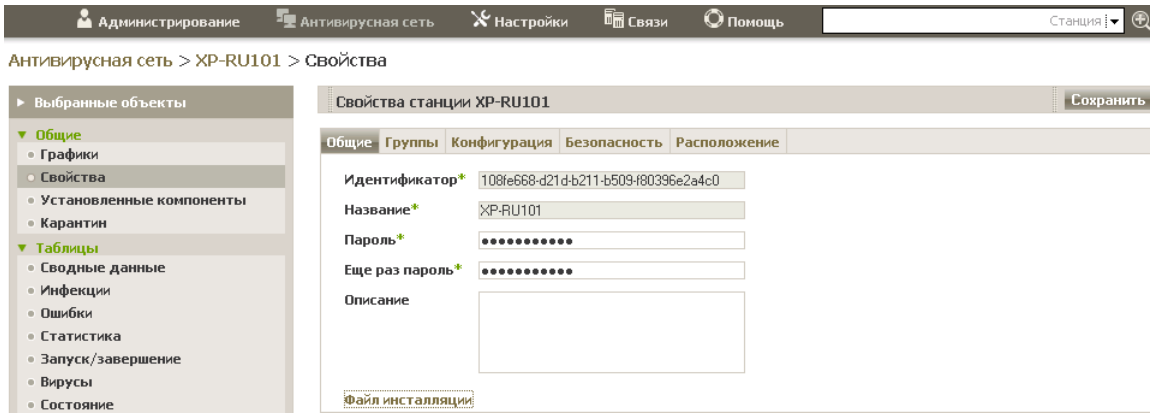
Внимание! Установка **Enterprise Агента** должна выполняться с правами администратора данного компьютера.

Для того чтобы задать список устанавливаемых компонентов, используйте пункт **Устанавливаемые компоненты** меню **Администрирование**.

2.3.2.1. Установка Dr.Web Enterprise Agent при помощи инсталляционного пакета esinst

Инсталляционный пакет esinst генерируется при создании новой учетной записи пользователя. Ссылка для скачивания esinst.exe 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.



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

Внимание! Для антивирусного сервера требуется 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 – в ОС Windows он, как правило, расположен в папке C:\Program Files\DrWeb ES Server\etc\

В связи с этим для получения файлов без указания порта необходимо в файле webmin.conf раскомментировать параметр ServerName и указать имя (актуальный адрес) сервера, сохранив указание порта. Например: ServerName avdesk.isp-name.ru: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 ОС Windows:

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

Для установки **Dr.Web Enterprise Agent** через инсталляционный пакет esinst 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.

2.3.2.1.1. Создание записи для создаваемой станции

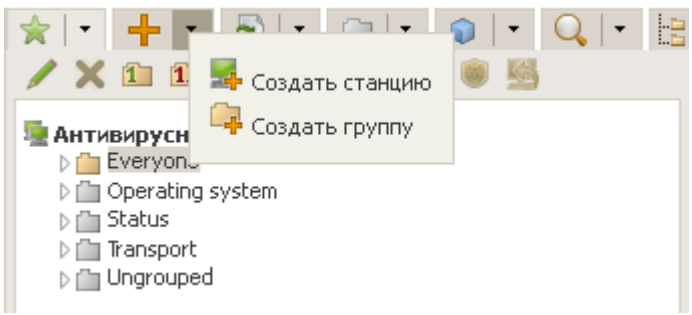
Убедитесь, что для параметра **ServerName** в конфигурационном файле webmin.conf задано значение *<Адрес_Сервера>:9080, где <Адрес_Сервера>* – IP-адрес или DNS-имя компьютера, на котором установлен **Enterprise Сервер**.

При создании учетной записи пользователя необходимо, чтобы подключение **Центра управления** к Серверу осуществлялось по IP-адресу для домена, в котором создается учетная запись. В противном случае при установке пакета будет невозможно подключиться к Серверу, поскольку при создании установочного пакета **Enterprise Агента** в нем прописывается адрес Сервера, по которому подключен **Центр управления**.

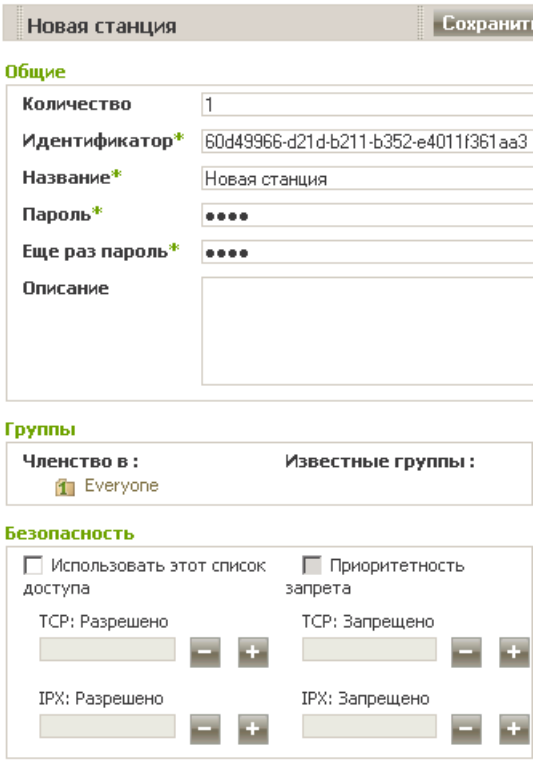
При подключении **Центра управления** к Серверу с локальной машины адрес Сервера не должен быть задан как loopback (127.0.0.1).

Для создания нового пользователя:

1) Выберите пункт **Антивирусная сеть** и нажмите на кнопку  (**Добавить станцию или группу**).



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.

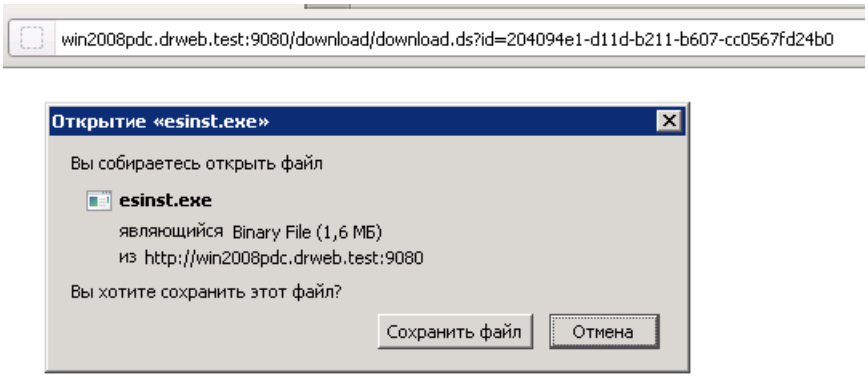
9) При необходимости заполните раздел **Безопасность**. Описание настроек данного раздела приведено в разделе документации **Настройка конфигурации рабочей станции**.

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 ссылка для загрузки дистрибутива **Агента**.

2.3.2.1.2. Локальная установка при помощи инсталляционного пакета

1) Перейдя по ссылке, полученной при создании станции в **Центре управления** (ссылка **Файл инсталляции** доступна в окне свойств станции), скачайте установочный файл esinst.exe и запустите его. Откроется окно мастера установки антивируса Dr.Web.



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 установите флаг **У меня на компьютере нет других антивирусов** и нажмите **Далее**.

3) Выберите вариант установки:

   Быстрая (рекомендуется) — наиболее простой вариант установки. Все параметры задаются автоматически. Далее перейдите к шагу **9**.

   Выборочная — вариант установки, при котором пользователь может выбрать компоненты антивирусного ПО, устанавливаемого на компьютер.

   Административная — наиболее полный вариант установки. Позволяет задать/изменить все параметры инсталляции и устанавливаемого антивирусного ПО.

   Для вариантов установки **Выборочная** и **Административная**: в следующем окне вам будет предоставлен выбор компонентов антивирусного пакета Dr.Web. Установите флаги напротив тех компонентов, которые вы хотите установить на ваш компьютер.

4) В разделе **Путь каталога установки** вы можете задать каталог, в который будет установлено антивирусное ПО. По умолчанию это каталог **Dr.Web Enterprise Suite**, расположенный в каталоге **Program files** на системном диске. Для задания/изменения пути по умолчанию нажмите на кнопку **Обзор** и укажите требуемый путь.

   Нажмите на кнопку **Далее**.

5) Далее для варианта установки **Выборочная** перейдите к шагу **9**.

6) Для варианта установки **Административная**: в следующем окне задайте настройки Сетевого инсталлятора:

   В поле **Dr.Web Enterprise Server** задается сетевой адрес **Enterprise 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 **Enterprise Агента** при помощи инсталлятора, созданного в **Центре управления**, автоматически заполняется поле **Dr.Web Enterprise Server**.

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

В поле **Dr.Web Enterprise Server публичный ключ** 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 разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** – использовать сжатие, **Нет** – не использовать, **Возможно** – использование сжатия трафика зависит от настроек на Сервере.

Флаг **Добавить Dr.Web Агент в список исключений Windows Firewall** предписывает добавление портов и интерфейсов, используемых Агентом, в список исключений сетевого экрана операционной системы. Рекомендуется установить данный флаг. Это поможет избежать ошибок, например, при автоматическом обновлении компонентов антивируса и вирусных баз.

При необходимости установите флаг **Зарегистрировать агент в списке установленных программ**.

7) Для варианта установки **Административная**: в следующем окне задайте настройки Агента:

   В разделе **Авторизация** задаются параметры авторизации Агента на Сервере. При выборе варианта **Автоматически (по умолчанию)** параметры авторизации (идентификатор и пароль) будут автоматически сгенерированы на Сервере, при этом режим доступа станции будет определяться на Сервере (см. п. «Политика подключения новых станций»). При выборе варианта **Ручная** необходимо задать параметры авторизации станции: ее **Идентификатор** на Сервере и **Пароль** доступа к нему. При этом станция получит доступ без ручного подтверждения администратором на Сервере.

   При установке **Enterprise Агента** при помощи инсталлятора, созданного в **Центре управления**, автоматически заполняются поля **Идентификатор** и **Пароль** для варианта авторизации **Ручная**.

   В разделах **Сжатие** и **Шифрование** задаются соответствующие режимы для трафика между Сервером и Агентом (подробнее см. п. «Использование шифрования и сжатия трафика»).

   Нажмите **Далее**.

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

9) После завершения инсталляции мастер установки сообщит о необходимости перезагрузить компьютер. Нажмите кнопку **Готово** 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.

2.3.2.1.3. 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.

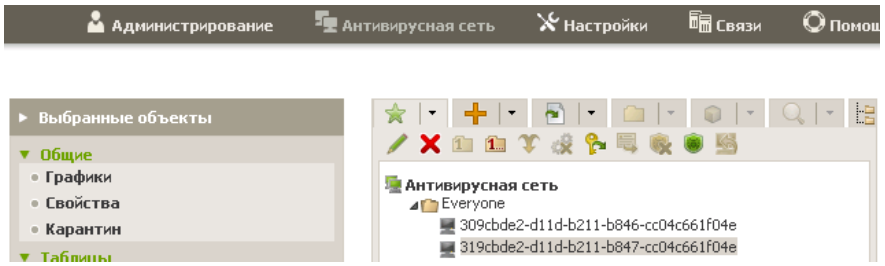
2) Произвести установку Агента на рабочую станцию.

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

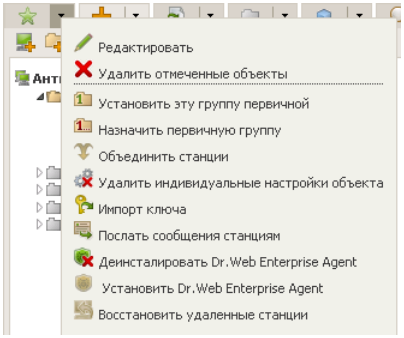
2.3.2.1.4. Удаленная установка с использованием инсталляционного пакета с заданным ID на станцию с указанием IP-адреса средствами Центра управления

Для установки Агента при помощи инсталляционного пакета:

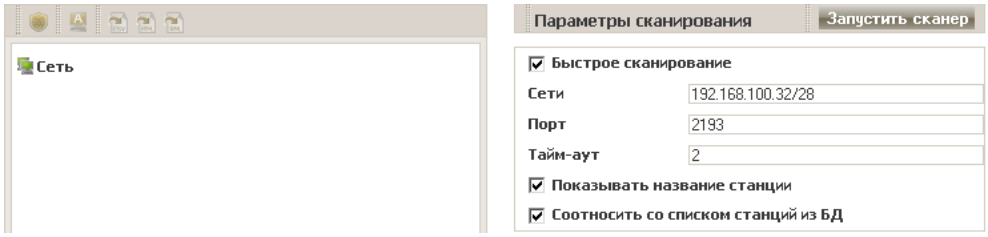
1) При помощи **Центра управления** создаем учетную запись нового пользователя на сервере и получаем ссылку для загрузки инсталляционного пакета – в иерархическом списке **Антивирусная сеть** выбираем иконку **Добавить станцию или группу**, затем **Создать станцию.**



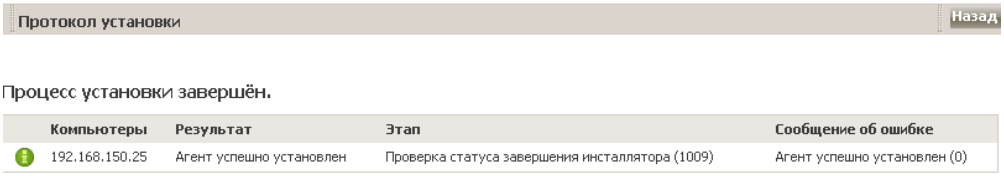
2) В появившейся панели инструментов выбираем иконку **Установить Dr.Web Enterprise Agent**.



3) Проводим сканирование сети для подтверждения существования станции и выбираем ее.



4) После нажатия на **Установить** запускается удаленная установка на выбранной станции.



2.3.2.2. Установка Dr.Web Enterprise Agent при помощи Сетевого инсталлятора

Установка при помощи Сетевого инсталлятора возможна в двух основных режимах:

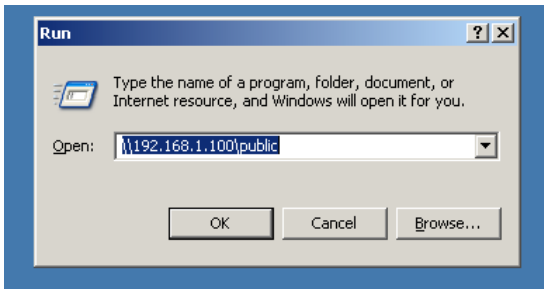
1) В фоновом режиме.
2) В графическом режиме.

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.

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.

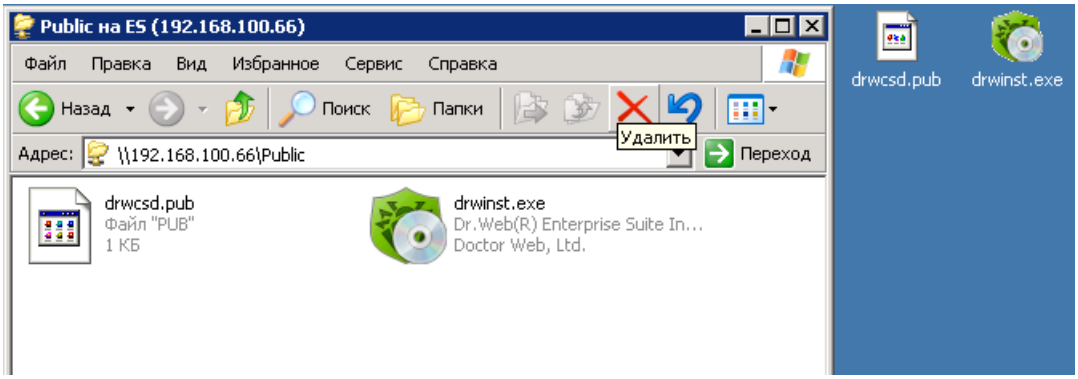
Необходимые для установки файлы можно получить двумя путями:

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://<server_address>:9080/install. Например, http:// 192.168.100.66:9080/install.

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

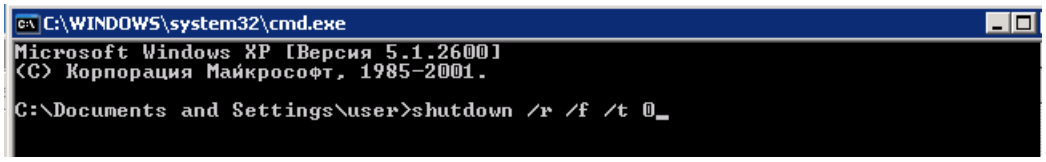


   Внимание! После завершения работы инсталлятора на компьютер будет установлено только ПО Агента (но не компоненты антивирусной защиты). После подтверждения станции на Сервере (если этого требуют настройки Сервера) антивирусный пакет будет автоматически установлен.

   Для завершения установки компонентов **Dr.Web Enterprise Security Suite** необходимо внести станцию, на которой была проведена установка, в число разрешенных. Сделать это можно, нажав **Неподтвержденные станции** в меню **Администрирование**, отметив станции, на которых была произведена установка, и нажав на значок или .

3) 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 (предварительно зарегистрированное в службе DNS):

  `drwinst <DNS_имя_Сервера>`

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

  Вы также можете использовать явное указание адреса Сервера, например

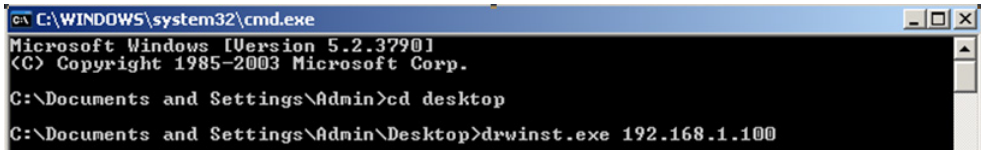
  `drwinst 192.168.1.3`
- Использование ключа -regagent позволяет при установке зарегистрировать Агент в списке добавления и удаления программ.
- Для запуска инсталлятора в графическом режиме используйте параметр -interactive.

  Полный список параметров **Сетевого инсталлятора** приведен в Приложении к «Руководству администратора».

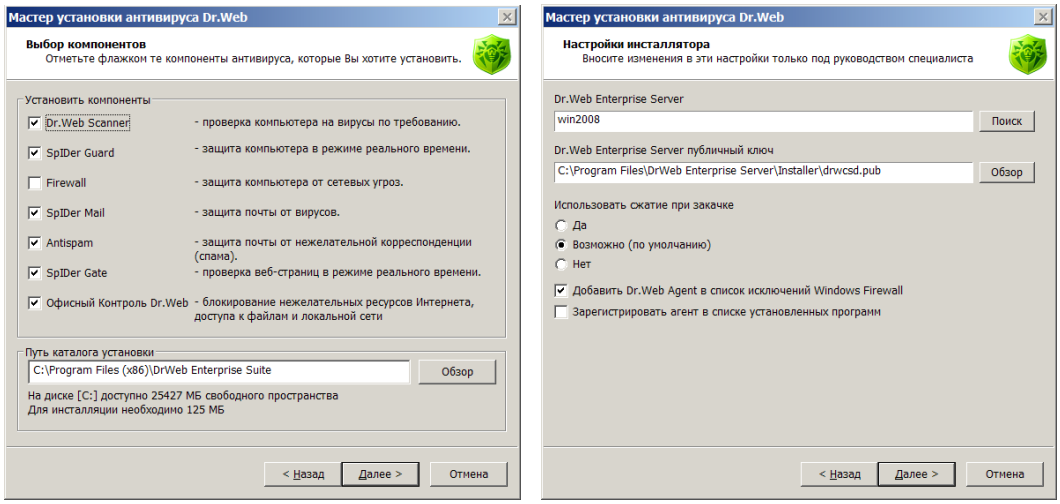
2.3.2.2.1. Установка Dr.Web Enterprise Agent при помощи Сетевого инсталлятора в фоновом режиме инсталлятора

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

1) Для установки компонентов Dr.Web ATM Shield на рабочую станцию или файловый сервер Windows необходимо либо просто запустить файл drwinst.exe (например, 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 кликните на него), либо запустить в командной строке с указанием адреса ESS-сервера.



При использовании режима **Multicast** для поиска активных **Серверов** установка **Агента** будет производиться с первого найденного **Сервера**. При этом, если имеющийся pub ключ не соответствует ключу **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.

2.3.2.2.2. Установка Dr.Web Enterprise Agent в графическом режиме инсталлятора

Чтобы установить **Dr.Web Enterprise 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 с параметром -interactive. Откроется окно мастера установки антивируса Dr.Web.

2) 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), после чего установите флаг **У меня на компьютере нет других антивирусов**. Нажмите на кнопку **Далее**.

3) В следующем окне будет предложен выбор варианта установки:
   - **Быстрая (рекомендуется)** — наиболее простой вариант установки. Все параметры задаются автоматически. Далее перейдите к шагу **7**.
   - **Выборочная** — вариант установки, при котором пользователь может выбрать компоненты антивирусного ПО, устанавливаемого на компьютер.
   - **Административная** — наиболее полный вариант установки. Позволяет задать/изменить все параметры инсталляции и устанавливаемого антивирусного ПО.

4) Для вариантов установки **Выборочная** и **Административная**: в следующем окне вам будет предоставлен выбор компонентов антивирусного пакета Dr.Web. Установите флаги напротив тех компонентов, которые вы хотите установить на ваш компьютер.

   В разделе **Путь каталога установки** вы можете задать каталог, в который будет установлено антивирусное ПО. По умолчанию это каталог **Dr.Web Enterprise Suite**, расположенный в каталоге **Program files** на системном диске. Для задания/изменения пути по умолчанию, нажмите на кнопку **Обзор** и укажите требуемый путь.

   Нажмите на кнопку **Далее**.

   Далее для варианта установки **Выборочная** перейдите к шагу **7**.

5) Для варианта установки **Административная**: в следующем окне задайте настройки **Сетевого инсталлятора**:

   В поле **Dr.Web Enterprise Server** задается сетевой адрес **Enterprise 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. Если вы заведомо не знаете адрес Сервера, нажмите на кнопку **Поиск**. Будет выведено окно для поиска активных **Enterprise Серверов** сети.

   Задайте необходимые параметры (в формате *<имя_сервера>@<IP-адрес>/<префикс_сети>:<порт>*) и нажмите кнопку **Поиск**. В списке найденных Серверов выберите тот, с которого будет устанавливаться антивирусное ПО, и нажмите на кнопку **OK**.

   В поле **Dr.Web Enterprise Server публичный ключ** 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 разделе **Использовать сжатие при закачке** выберите нужный для вас вариант компрессии трафика: **Да** — использовать сжатие, **Нет** — не использовать, **Возможно** — использование сжатия трафика зависит от настроек на Сервере.

   Флаг **Добавить Dr.Web Агент в список исключений Windows Firewall** предписывает добавление портов и интерфейсов, используемых **Агентом**, в список исключений сетевого экрана операционной системы. Рекомендуется установить данный флаг. Это поможет избежать ошибок, например, при автоматическом обновлении компонентов антивируса и вирусных баз.

   При необходимости установите флаг **Зарегистрировать агент в списке установленных программ**.

6) Для варианта установки **Административная**: в следующем окне задайте настройки Агента:

   В разделе Авторизация задаются параметры авторизации Агента на Сервере. При выборе варианта **Автоматически (по умолчанию)** параметры авторизации (идентификатор и пароль) будут автоматически сгенерированы на Сервере, при этом режим доступа станции будет определяться на Сервере (см. п. «Политика подключения новых станций»). При выборе варианта **Ручная** необходимо задать параметры авторизации станции: ее **Идентификатор** на Сервере и **Пароль** доступа к нему. При этом станция получит доступ без ручного подтверждения администратором на Сервере.

   В разделах **Сжатие** и **Шифрование** задаются соответствующие режимы для трафика между Сервером и Агентом (подробная информация доступна в «Руководстве администратора», п. «Использование шифрования и сжатия трафика»).

   Нажмите **Далее**.

7) Начнется установка **Enterprise Агента**. После установки Агента нажмите кнопку **Готово** для завершения работы мастера установки.

8) После подтверждения станции на Сервере (если этого требуют настройки Сервера, см. п. «Политика подключения новых станций», и если на шаге **6** при **Административной** установке не был выбран вариант авторизации **Ручная**) антивирусный пакет будет автоматически установлен.

9) Перезагрузите компьютер по требованию Агента.

2.3.3. Поиск станций в сети

Для поиска станций или группы станций:

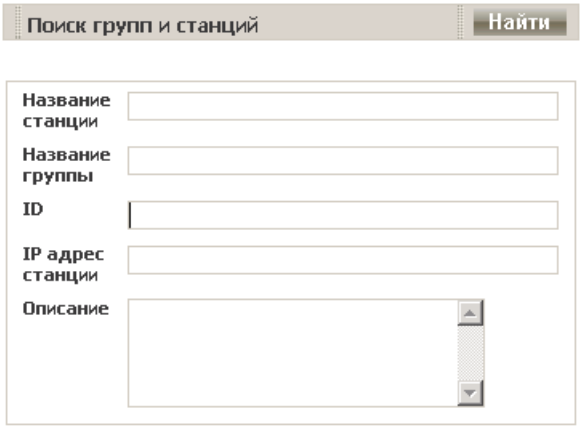
1) В выпадающем списке панели поиска выберите критерий поиска:
   - Станция — для поиска станций по названию,
   - Группа — для поиска групп по названию,

- ID — для поиска групп и станций по уникальным идентификаторам,
- Описание — для поиска групп и станций по их описанию,
- IP-адрес — для поиска станций по IP-адресу.

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».

Также вы можете воспользоваться опцией **Расширенный поиск**.

Для расширенного поиска станции необходимо нажать на кнопку **Расширенный поиск** ( ) и в появившемся окне **Поиск групп и станций** справа ввести название станции или его часть, а затем нажать **Найти**.



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

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

В иерархическом списке будут отображены все найденные элементы или сообщение «Поиск не дал результатов».

2.3.4. Установка антивирусного прокси-сервера

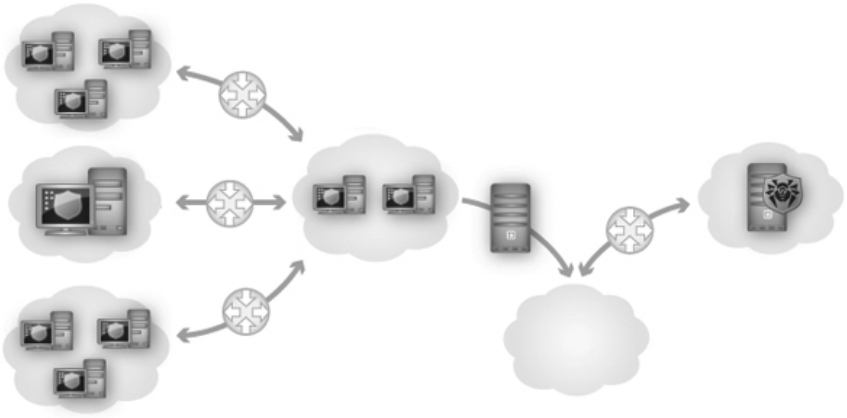
Основная задача Прокси-сервера — обеспечение связи **Enterprise Сервера** и **Enterprise Агентов** в случае невозможности организации прямого доступа (например, если **Enterprise Сервер** и **Enterprise Агенты** расположены в различных сетях, между которыми отсутствует маршрутизация пакетов).

В состав антивирусной сети может входить один или несколько Прокси-серверов, обеспечивающих получение обновлений.

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, IPv6, IPX и NetBIOS);
3) пересылка данных между **Enterprise Сервером** и **Enterprise Агентами** в соответствии с настройками прокси-сервера;
4) кеширование обновлений Агента и антивирусного пакета, передаваемых Сервером. В случае выдачи обновлений из кеша Прокси-сервера обеспечивается:
   - уменьшение сетевого трафика,
   - уменьшение времени получения обновлений Агентами.

Общая схема антивирусной сети при использовании Прокси-сервера



	Dr.Web Enterprise Server		Сервер NAP + Dr.Web NAP Validator
	Защищенный компьютер, исправный		Локальная сеть, Интернет
	Защищенный компьютер		

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 **Enterprise Сервера**. 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 **Enterprise Сервером**.

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

Прокси-сервер не имеет графического интерфейса. Задание настроек осуществляется при помощи конфигурационного файла.

Управление настройками (редактирование конфигурационного файла) Прокси-сервера может выполняться только пользователем с правами администратора данного компьютера.

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

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.

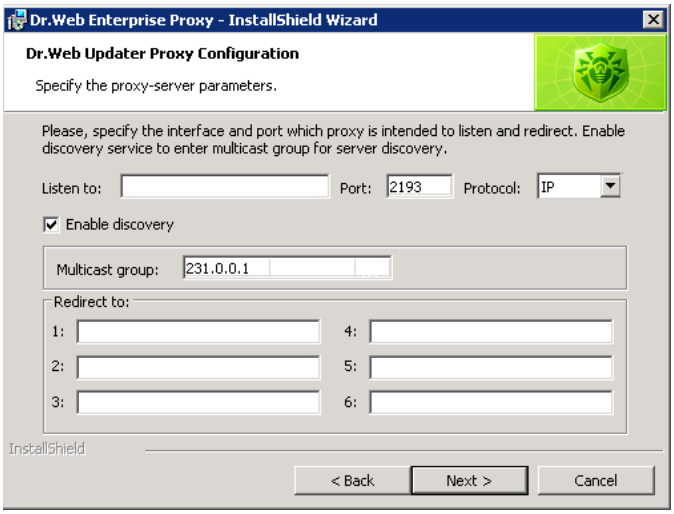
Внимание! Установка Прокси-сервера должна выполняться пользователем с правами администратора данного компьютера.

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

1) Запустите файл drweb-esuite-proxy-604-201111300-windows-nt-x86. Откроется окно InstallShield Wizard, извещающее вас об устанавливаемом продукте. Нажмите на кнопку **Далее (Next)**.

2) Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора выберите в нижней части окна пункт **I accept the terms of the license agreement** и нажмите на кнопку **Далее (Next)**.

3) Откроется окно для настройки параметров Прокси-сервера:



В поле **Listen to** задайте IP-адрес, прослушиваемый Прокси-сервером. По умолчанию — any (0.0.0.0) — прослушивать все интерфейсы.

В поле **Port** задайте номер порта, который будет слушать Прокси-сервер. По умолчанию это порт **2193** или порт **23** для протокола NetBIOS.

В выпадающем списке **Protocol** выберите тип протокола для приема входящих соединений Прокси-сервером.

Установите флаг **Enable discovery** для включения режима имитации Сервера. Данный режим позволяет Сканеру сети обнаруживать Прокси-сервер в качестве **Enterprise Сервера**.

В поле **Multicast group** задайте IP-адрес многоадресной группы, в которую будет входить Прокси-сервер. Указанный интерфейс будет прослушиваться Прокси-сервером для взаимодействия с **Сетевыми инсталляторами** при поиске активных **Enterprise Серверов** сети. Если поле оставить пустым, Прокси-сервер не будет входить ни в одну из многоадресных групп.

В разделе **Redirect to** задайте адрес или список адресов **Enterprise Серверов**, на один из которых будут перенаправляться соединения, устанавливаемые Прокси-сервером.

После задания настроек Прокси-сервера нажмите **Далее** (**Next**).

4) Откроется окно выбора каталога установки. Если необходимо изменить каталог установки, заданный по умолчанию, нажмите на кнопку **Change** и выберите каталог установки. Нажмите на кнопку **Далее** (**Next**).
5) Откроется окно, извещающее о готовности к установке Прокси-сервера. Нажмите на кнопку **Установить** (**Install**).
6) После завершения процесса установки нажмите на кнопку **Готово** (**Finish**).

По окончании установки вы можете изменить параметры работы Прокси-сервера. Для этого служит конфигурационный файл drwcsd-proxy.xml, расположенный в каталоге установки Прокси-сервера. Настройки конфигурационного файла приведены в Приложении G3 «Руководства администратора».

2.4. 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 ATM Shield** в сочетании с технологией **Microsoft Network Access Protection** (далее — NAP).

Dr.Web ATM Shield 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.

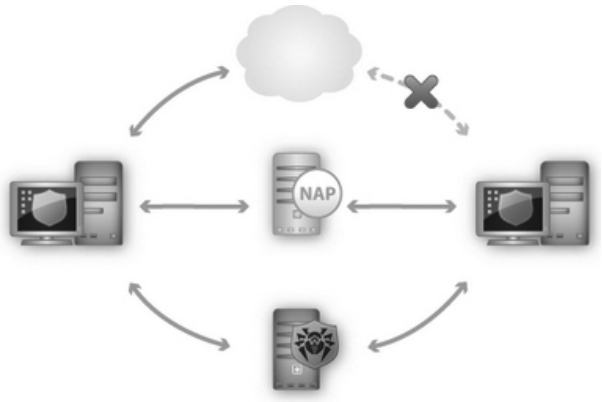
Подробное описание технологии NAP можно найти по ссылке http://www.microsoft.com/windowsserver2008/en/us/nap-product-home.aspx.

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 XP SP3 и более поздних версий Windows.

Dr.Web ATM Shield 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** – 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 **Enterprise Агента** на рабочую станцию.
- **Enterprise Сервер** служит в качестве сервера исправлений, обеспечивающего работоспособность антивирусного ПО рабочих станций.



	Dr.Web Enterprise Server	NAP	Сервер NAP + Dr.Web NAP Validator
	Защищенный компьютер, исправный		Локальная сеть, Интернет
	Защищенный компьютер, неисправный		

Процедура проверки осуществляется следующим образом:

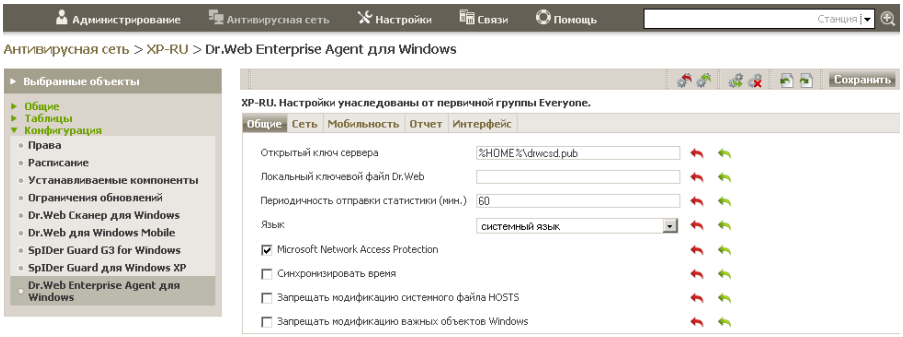
1) Активация процесса проверки производится при установке соответствующих настроек Агента раздела **Dr.Web® Enterprise Agent для Windows**.
2) SHA на рабочей станции связывается с компонентом Dr.Web NAP Validator, установленном на сервере NAP.
3) Dr.Web NAP Validator осуществляет проверку политик работоспособности (см. ниже). 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 **Enterprise Серверу**, от остальной сети они изолируются. Работоспособность станции восстанавливается при помощи Сервера, после чего станция проходит повторную процедуру проверки.

Требования к работоспособности:

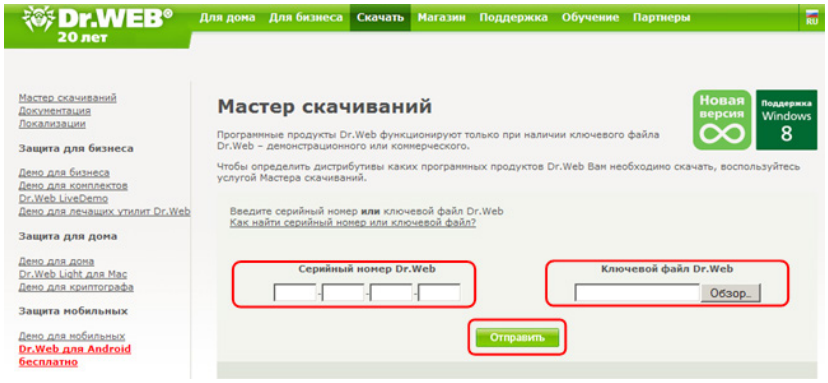
1) Рабочее состояние агента (запущен и функционирует).
2) Актуальность вирусных баз (базы совпадают с базами на сервере).

Для установки NAP Validator выполните следующие действия:

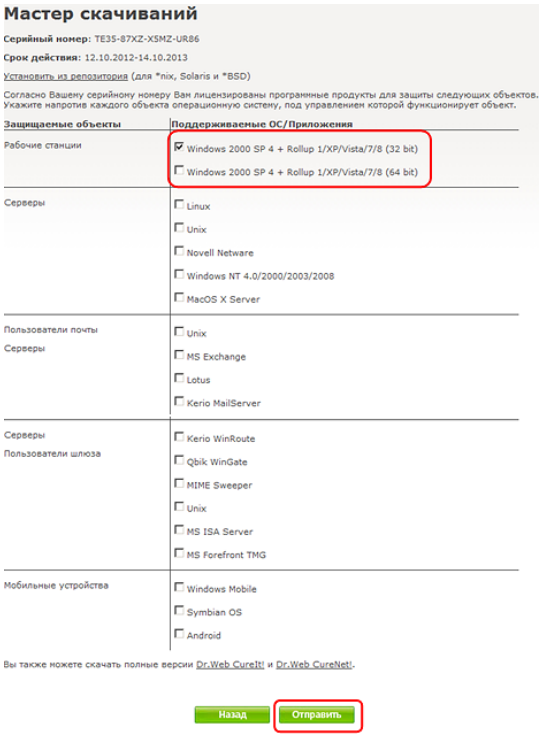
1) Выбрав для интересующих станций или групп пункт **Dr.Web® Enterprise Agent для Windows**, в меню **Антивирусная сеть** необходимо отметить пункт **Microsoft Network Access Protection** для включения поддержки технологии Microsoft® Network Access Protection, использующейся для мониторинга состояния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



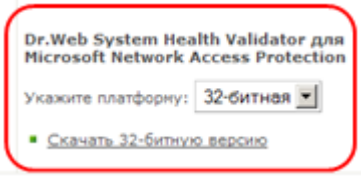
2) Перейдите в раздел **Мастер скачиваний** сайта http://www.drweb.com. Введите серийный номер или с помощью кнопки **Обзор** укажите путь к лицензионному ключевому файлу (файл agent.key или enterprise.key). Нажмите **Отправить**.



3) На следующей странице выберете любую опцию из группы **Рабочие станции** и нажмите **Отправить**.



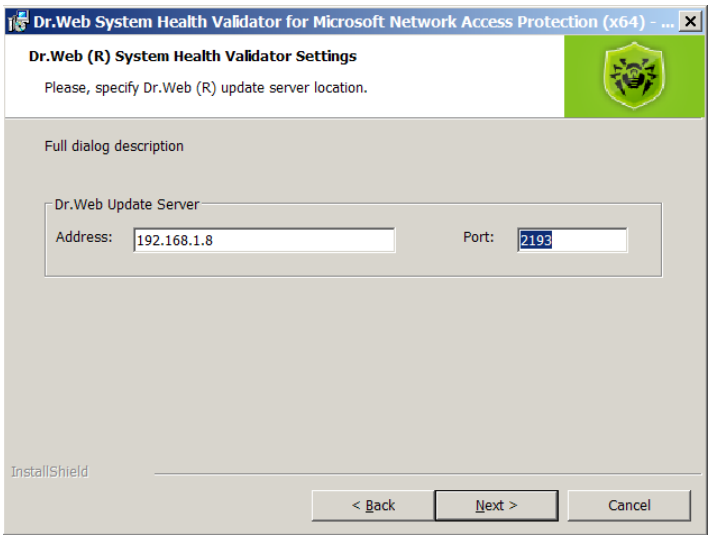
4) В зависимости от разрядности ОС Windows, в среде которой предполагается использование Dr.Web System Health Validator для Microsoft Network Access Protection, выберите подходящую платформу. Загрузите дистрибутив (в данном случае – по ссылке «Скачать 32-битную версию) Dr.Web NAP Validator. Название файла дистрибутива имеет формат drweb-esuite-napshv-6xx-xxxxxxxxx-windows-nt-yyy.msi, где yyy принимает значения x86 и x64.



5) Запустите дистрибутив. Откроется окно **InstallShield Wizard**, извещающее вас об устанавливаемом продукте. Нажмите на кнопку **Далее** (**Next**).

6) Откроется окно с текстом лицензионного договора. После ознакомления с условиями лицензионного договора в группе кнопок выбора укажите **I accept the terms in the license agreement** и нажмите на кнопку **Далее** (**Next**).

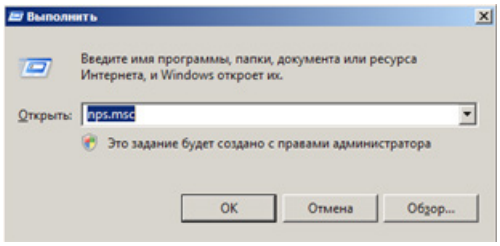
7) В открывшемся окне в полях **Адрес** (**Address**) и **Порт** (**Port**) задайте, соответственно, IP-адрес и порт ES-сервера. Обычно используется порт **2193**, если вы не изменяли стандартные настройки **Enterprise-сервера**. Нажмите на кнопку **Далее** (**Next**).



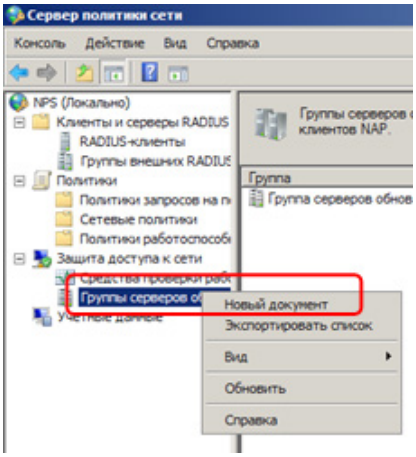
8) Нажмите на кнопку **Install**. Дальнейшие действия программы установки не требуют вмешательства пользователя. По окончании установки нажмите на кнопку **Finish**.

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

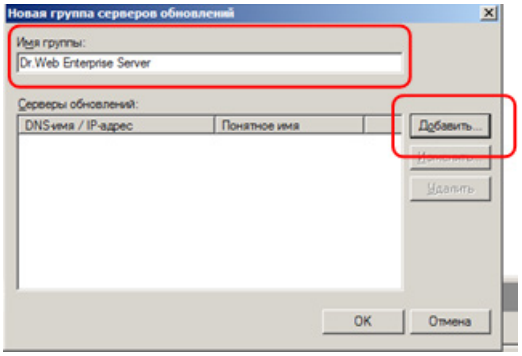
- Введите команду nps.msc.



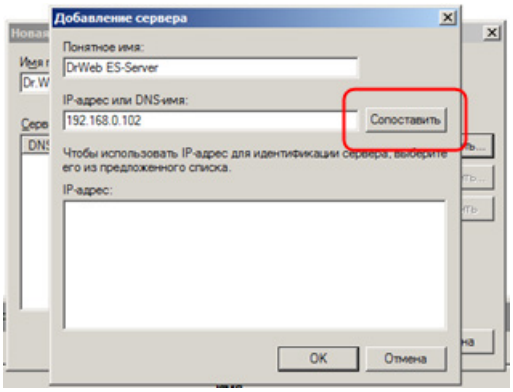
- Наведите курсор мыши на **Группы серверов обновлений**, нажмите правую клавишу мыши и выберете пункт меню **Новый документ.**



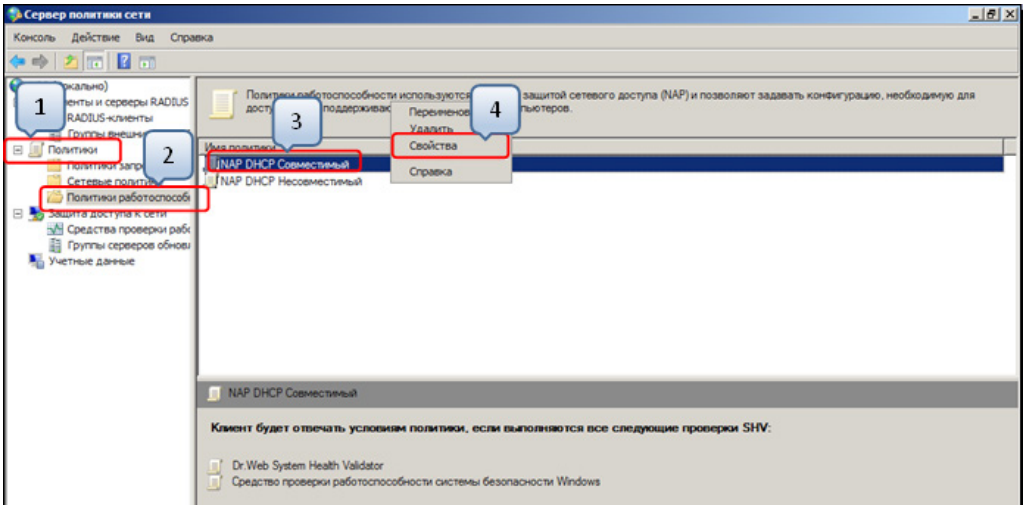
- Введите имя группы, например, Dr.Web Enterprise Server. Нажмите кнопку **Добавить**.

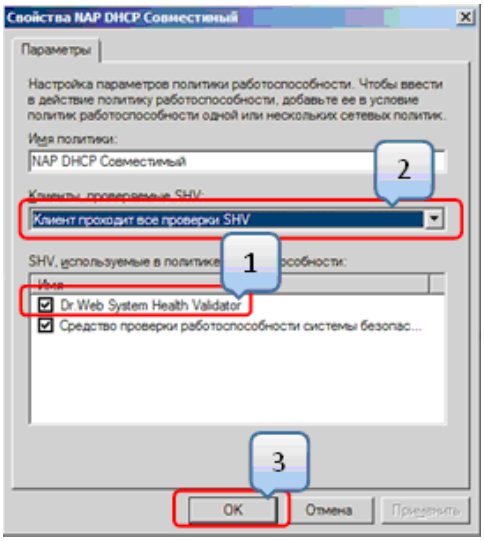


- Введите понятное имя сервера, например DrWeb ES-Server. В поле IP-адрес или DNS-имя введите IP-адрес или доменное имя **Dr.Web Enterprise Server**. Нажмите **Сопоставить**.

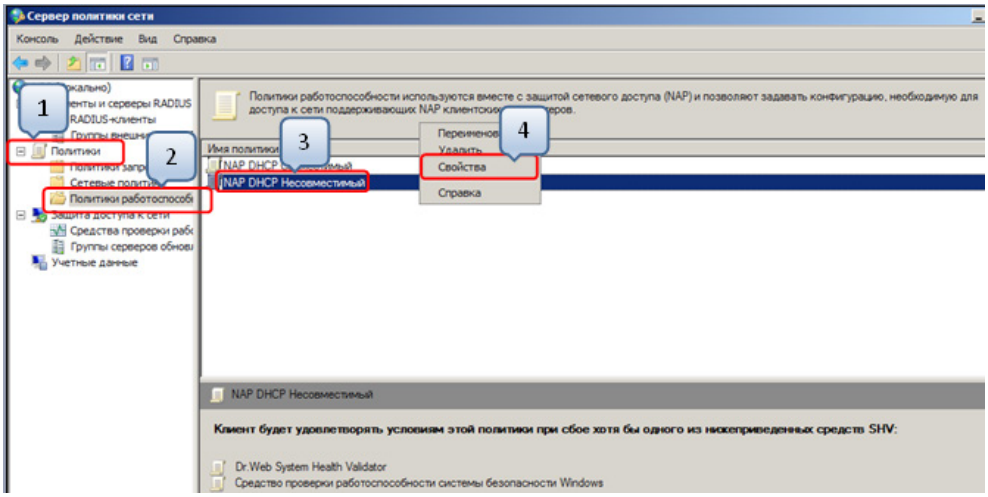


- Нажмите **OK**.
- Закройте окно **Новая группа серверов обновлений**, нажмите **OK**. **Enterprise Сервер** добавлен в группу доверенных серверов NAP.
- В разделе **Политики** (**Policies**) выберите подпункт **Политики работоспособности** (**Health Policies**) и в открывшемся окне свойств элементов: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

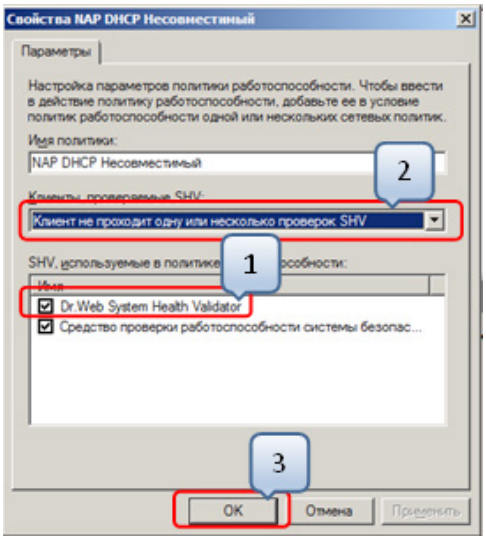




- Наведите курсор мыши на элемент **NAP DHCP Несовместимый** (**NAP DHCP Noncompliant**), нажмите правую клавишу мыши и выберете пункт **Свойства**.



- В окне настроек установите флаг 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 **OK**.

3. Управление системой антивирусной защиты локальной сети

При организации защиты встроенных устройств (в том числе банкоматов) нужно учитывать следующие особенности:

- Малое количество оперативной памяти на защищаемых устройствах.
- Возможность проведения обновлений операционной системы и установленных приложений исключительно в ходе регламентных работ (но не по мере их появления на стороне производителя) и, как правило, в присутствии обслуживающего персонала — в связи с тем, что данные обновления могут потребовать перезагрузки устройства, в том числе в момент выполнения устройством той или иной работы.

  Внимание! В связи с невозможностью проведения обновлений, потенциально требующих перезагрузки, по мере их получения клиентом для Dr.Web ATM Shield реализованы два типа обновлений: обновления антивирусных баз (не требующие перезагрузок ОС) и обновления базовых компонентов Dr.Web ATM Shield, в том числе драйверов. Порядок проведения обновлений для обоих случаев может быть настроен отдельно.
- Возможность использования встроенных устройств сотрудниками (обслуживающим персоналом) в собственных целях.

  Внимание! В связи с тем, что обновления, потенциально требующие перезагрузки, могут проводиться только в период регламентных работ, необходимо обеспечение антивирусной защитой домашних и рабочих компьютеров обслуживающего персонала с целью недопущения на сменные носители, используемые для проведения регламентных работ, новейших вредоносных программ, не обнаруживаемых до проведения обновлений системой защиты встраиваемого устройства.

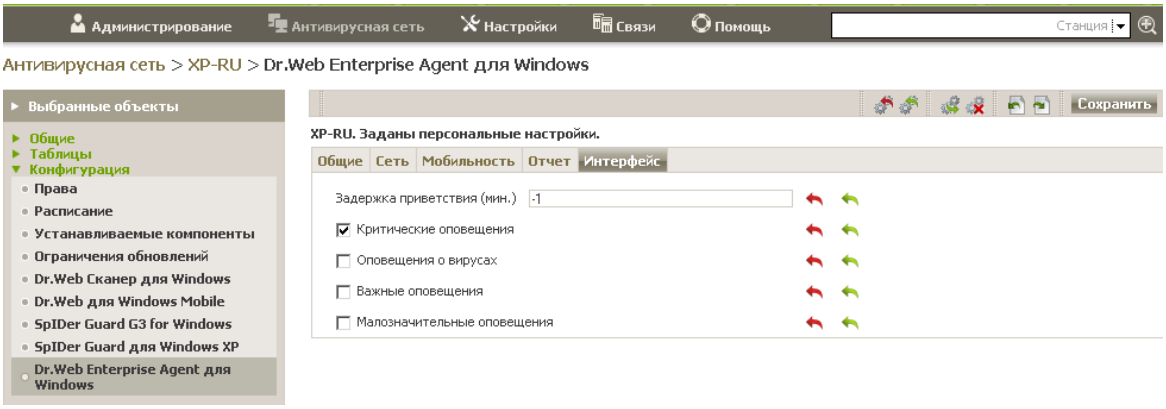
Также нужно учитывать характерные для встраиваемых устройств пути заражения. Наиболее часто заражения происходят:

- путем проникновения из зараженной внутренней сети компании — в случае наличия из нее доступа к встраиваемым системам;
- путем проникновения через уязвимости — в связи с отсутствием необходимых обновлений безопасности;
- путем заражения со сменных носителей обслуживающего персонала (в том числе в связи с использованием этих сменных носителей для иных целей, кроме обслуживания встраиваемых устройств);
- путем заражения с сайтов сети Интернет, посещаемых обслуживающим персоналом в период проведения регламентных работ.

В связи с этим необходимым условием нормального функционирования встраиваемого устройства (в том числе на слабых и устаревших конфигурациях встраиваемых систем) является антивирусная защита, имеющая в своем составе модули контроля трафика, ограничения доступа к сменным носителям и ресурсам сети Интернет.

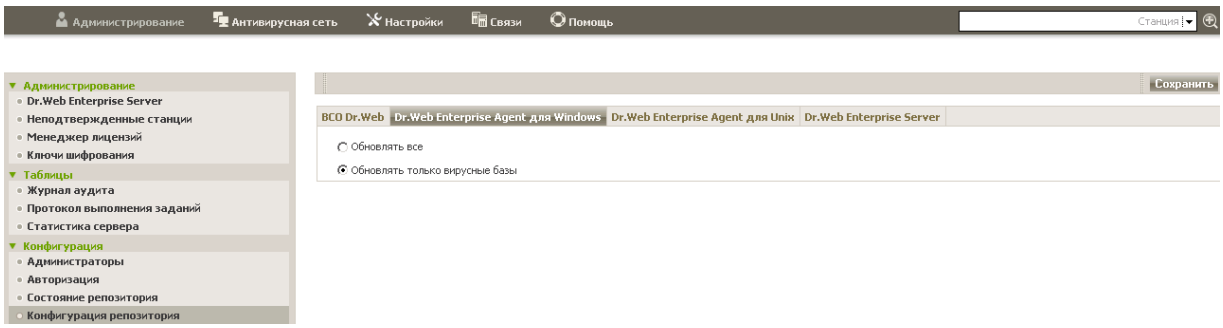
В связи с вышеперечисленными особенностями функционирования системы антивирусной защиты на защищаемых устройствах для Dr.Web ATM Shield необходимо выполнять ряд требований:

- Должна быть отключена возможность показа уведомлений во время работы приложений в полноэкранном режиме. Выберите в разделе **Антивирусная сеть** группу **Everyone** или первичную группу, в которой будут находиться устанавливаемые агенты. Затем в левом меню выберите пункт **Dr.Web Enterprise Agent для Windows**, перейдите на закладку **Интерфейс** и снимите галочки напротив всех типов оповещений. Также на этой закладке в поле **Задержка приветствия** установите значение «**–1**». Нажмите кнопку **Сохранить**.



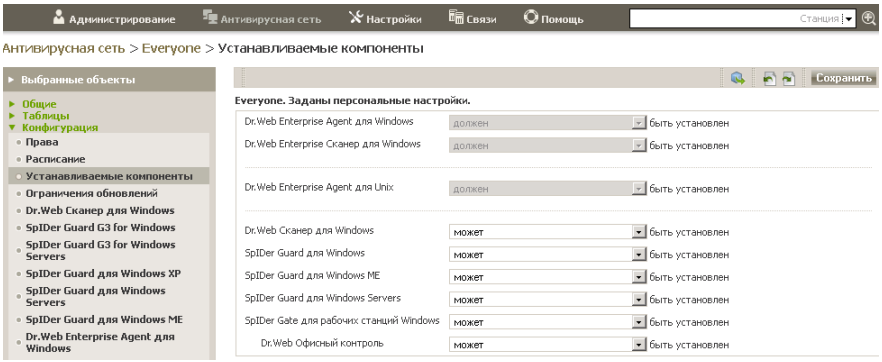
Более подробно данные параметры настройки рассмотрены в разделе **Настройка параметров защиты рабочих станций и серверов Windows**.

- В связи с тем, что защищаемые устройства должны перегружаться только в период регламентного обслуживания, необходимо отключить обновление агентов антивирусной защиты, оставив только обновление вирусных баз. В разделе **Администрирование** выберите пункт **Конфигурация репозитория** и перейдите на закладку **Dr.Web Enterprise Agent для Windows**. На данной закладке выберите чекбокс **Обновлять только вирусные базы**. Нажмите кнопку **Сохранить**.

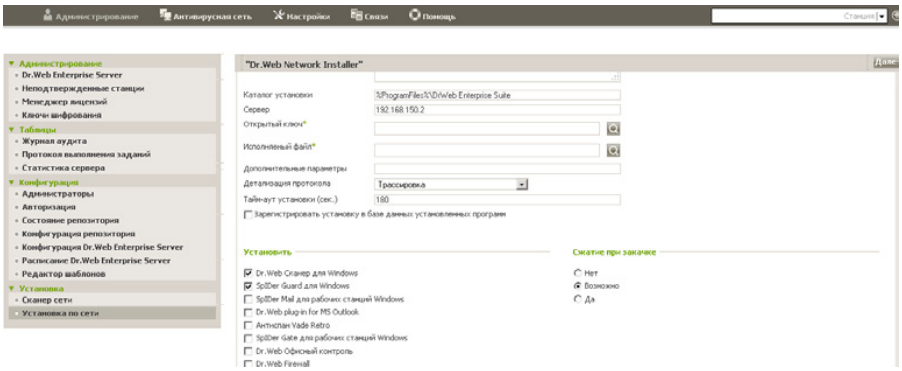


Внимание! В случае отсутствия в списке запускаемых компонентов на защищаемом устройстве UI по умолчанию автоматическая загрузка обновлений отключена. В противном случае — включена.

- Определите список компонентов, которые будут устанавливаться на защищаемые устройства. Выберите в разделе Антивирусная сеть группу Everyone или ту первичную группу, в которой будут находиться устанавливаемые агенты. Затем в левом меню выберите пункт **Устанавливаемые компоненты** и определите список устанавливаемых компонентов. Нажмите кнопку **Сохранить**.

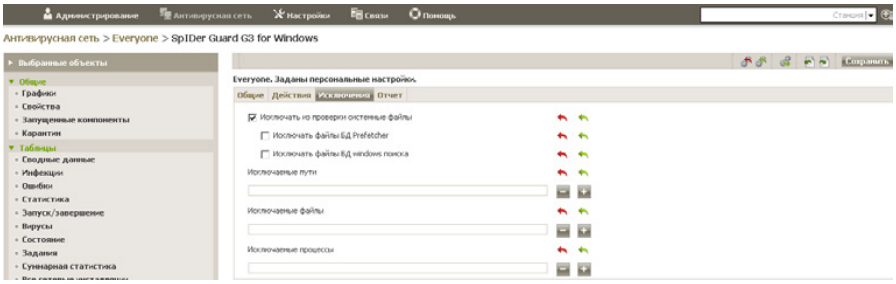


При развертывании по сети вы можете задать список компонентов непосредственно в момент развертывания, выставив галочки напротив необходимых компонентов.



Более подробно процедура установки рассмотрена в разделе **Установка с использованием Веб-интерфейса Центра управления Dr.Web ATM Shield**.

- Определите действие по умолчанию, которое должно выполняться при обнаружении вредоносной программы. Для устройства должна быть исключена ситуация появления на экране запроса на лечение. Настройка параметров проверки рассматривается в разделе **Настройка параметров защиты рабочих станций и серверов Windows**. В этом же разделе рассмотрены вопросы выбора параметров защиты, снижающих нагрузку на защищаемую рабочую станцию.
- **Внимание!** Чтобы снизить нагрузку на защищаемое устройство, можно исключить из проверки, например, отчеты программного обеспечения. Для этого в разделе Антивирусная сеть выберите первичную группу, в которой будут находиться устанавливаемые агенты, затем в левом меню выберите настройки необходимых компонентов и перейдите на закладку **Исключения** (**Исключаемые пути**, **Исключаемые файлы** – в зависимости от установленного компонента).



- Настройте систему записи действий администраторов. Данная процедура рассмотрена в разделе **Аудит действий администраторов**. Журнал действий администраторов можно отобразить в Веб-интерфейсе, перейдя в раздел **Администрирование** и выбрав пункт **Журнал аудита**.
- Проверьте, что на стороне антивирусного сервера по умолчанию включено уведомление о прекращении действия ключа.

3.1. Центр управления Dr.Web

Управление **Dr.Web Enterprise Security Suite** проводится с использованием Веб-интерфейса Центра управления. Администратор может с любой машины управлять работой сервиса, внедрять необходимые параметры, готовить отчеты и анализировать статистику.

Для того чтобы соединиться с помощью Веб-интерфейса с антивирусным сервером и производить описываемые ниже действия, необходимо на любом компьютере, имеющем сетевой доступ к **Enterprise Серверу**, 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 антивирусный сервер. 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.

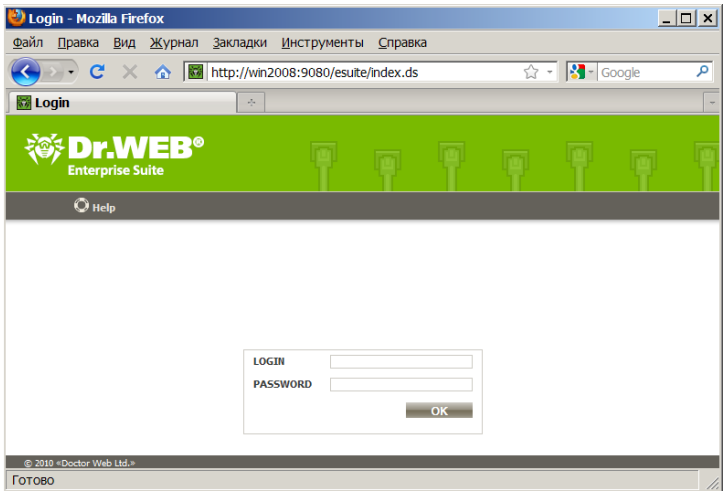
В браузере Microsoft Internet Explorer для этого необходимо выполнить следующие действия: **Tools** (Сервис) → **Internet Options** (Свойства обозревателя) → **Security** (Безопасность) → **Internet** (Интернет) → **Custom Level** (Другой) → **Scripting** (Сценарии) → установить флаг **Enable** (Активные сценарии).

Для корректной работы **Центра управления** под веб-браузером Microsoft Internet Explorer необходимо в настройках веб-браузера добавить адрес **Центра управления** в доверенную зону: **Tools** (Сервис) → **Internet Options** (Свойства обозревателя) → **Security** (Безопасность) → **Trusted Sites** (Надежные узлы).

При загрузке по https (защищенное соединение с использованием SSL) браузер запросит подтверждение сертификата, используемого Сервером. 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. Иначе загрузка будет невозможна.

В некоторых версиях браузеров, например **Mozilla Firefox 3**, 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**.

Внимание! Веб-интерфейс, входящий в состав **Центра управления Dr.Web Enterprise Security Suite**, поддерживает браузеры Internet Explorer и Mozilla Firefox.



Аутентификация администратора для подключения к **Enterprise Серверу** 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 Веб-интерфейсу и в дальнейшем может управлять защитой с помощью функций, размещенных в разделах **Администрирование** и **Антивирусная сеть**, **Настройки** и **Связи**.

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

Заголовок содержит:

- логотип продукта **Dr.Web ATM Shield**, при нажатии на который открывается начальное окно **Центра управления** (соответствует выбору пункта **Антивирусная сеть** главного меню),
- главное меню,
- имя учетной записи администратора, под которой был осуществлен вход в **Центр управления**,
- кнопку **Выход** для завершения текущего сеанса работы с **Центром управления**.

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. «Смена языка отображения Центра управления»).

В главном меню **Центра управления** доступны следующие разделы:

- Администрирование,
- Антивирусная сеть,
- Настройки,
- Связи,
- Помощь,
- Панель поиска.

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

- **Dr.Web® Enterprise Server** – 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.
- **Неподтвержденные станции** – открывает панель со списком неподтвержденных станций (см. п. «Политика подключения новых станций»).
- **Менеджер лицензий** – позволяет управлять лицензионными ключевыми файлами Сервера и Агентов (см. п. «Менеджер лицензий»).

2) Таблицы

- **Журнал аудита** – просмотр журнала событий и изменений, осуществленных при помощи **Центра управления**.
- **Протокол выполнения заданий** – содержит список назначенных заданий на Сервере с пометкой о выполнении и комментариями.

3) Конфигурация

- **Администраторы** – открывает панель управления учетными записями администраторов антивирусной сети (подробная информация доступна в «Руководстве администратора», п. «Управление учетными записями администраторов»).
- **Состояние репозитория** – проверить состояние репозитория: дату последнего обновления компонентов репозитория и их состояние.
- **Конфигурация репозитория** – открывает окно редактора репозитория (подробная информация доступна в «Руководстве администратора», п. «Редактор конфигурации репозитория»).
- **Конфигурация Dr.Web Enterprise Server** – открывает панель основных настроек Сервера (см. п. «Настройка конфигурации Dr.Web Enterprise Server»);
- **Расписание Dr.Web Enterprise Server** – открывает панель настройки расписания заданий Сервера (см. п. «Настройка расписания ES-сервера»).
- **Редактор шаблонов** – открывает окно редактора шаблонов оповещений (см. п. «Редактирование шаблонов предопределенных оповещений»).

4) Установка

- **Сканер сети** – позволяет задавать список сетей и проводить как сканирование сетей на наличие установленного антивирусного программного обеспечения, определяя состояние защиты компьютеров, так и установку последнего (см. п. «Установка с использованием Веб-интерфейса Центра управления Dr.Web Enterprise Security Suite»).
- **Установка по сети** – позволяет упростить установку ПО Агента на конкретные рабочие станции (см. п. «Установка с использованием Веб-интерфейса Центра управления Dr.Web Enterprise Security Suite»).

Меню Антивирусная сеть

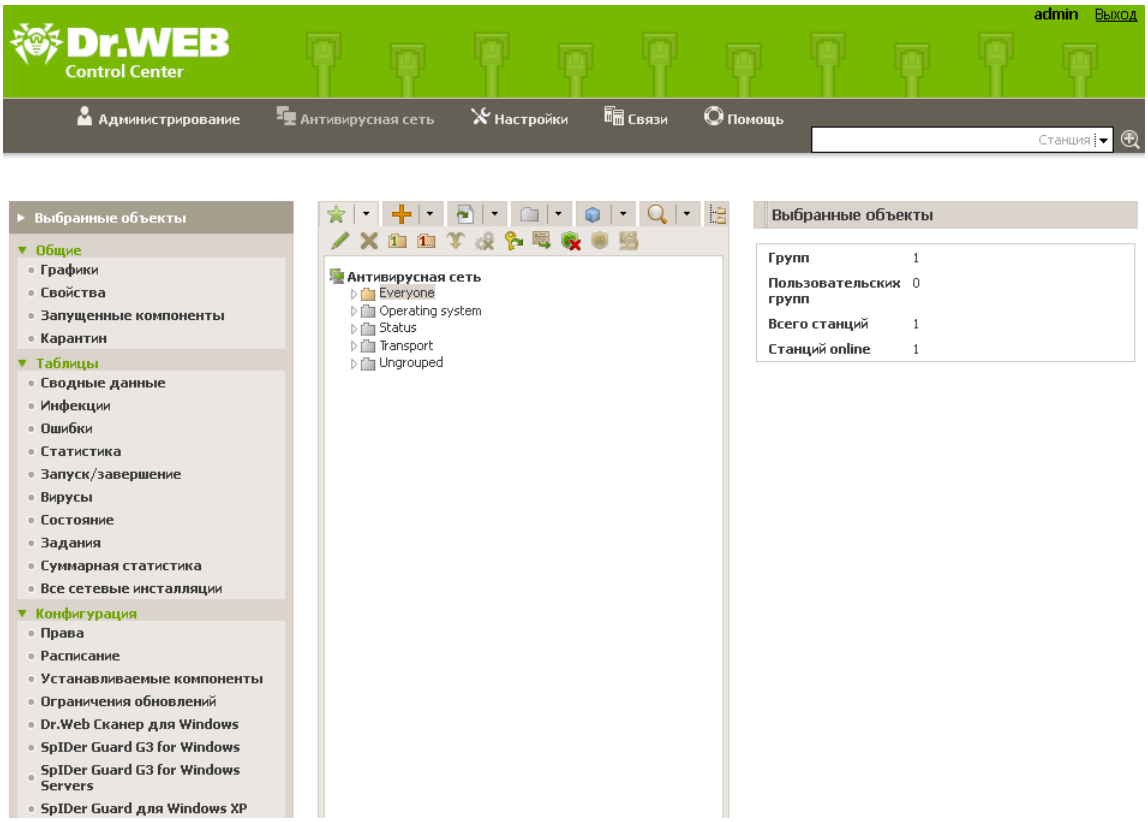
Для просмотра и редактирования информации в открывшемся окне служит управляющее меню, расположенное в левой части окна.

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 отображения управляющего меню (в левой части окна) соответствующего элемента;
- нажмите левой кнопкой мыши на значок группы для отображения содержимого группы.

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.

Знак	Описание	Значение
		Группы
	желтая папка	Группы, всегда отображаемые в иерархическом списке.
	белая папка	Отображение групп в иерархическом списке может быть отключено, если эти группы пустые.
		Рабочие станции
	зеленый значок	Доступная рабочая станции с установленным антивирусным ПО.
	серый значок	Станция недоступна.
	перечеркнутый значок	Антивирусное ПО на станции деинсталлировано.

Управление элементами каталога антивирусной сети осуществляется при помощи панели инструментов иерархического списка. Панель инструментов содержит следующие элементы.

Общие. Позволяет управлять общими параметрами иерархического списка. Выберите соответствующий пункт в выпадающем списке:

Удалить отмеченные объекты. Позволяет удалить объекты иерархического списка. Для этого выберите в списке элемент или несколько элементов и нажмите **Удалить отмеченные объекты**.

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

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

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

Объединить станции. Позволяет 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.

Убрать индивидуальные настройки объекта. Позволяет 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 удалены у всех входящих в нее станций.

Импорт ключа. Позволяет задать ключ для станции или группы.

Послать сообщение станциям. Позволяет отправить пользователям сообщение произвольного содержания (см. п. «Отправка сообщений пользователю»).

Деинсталлировать Dr.Web Агента. Удаляет Агента и антивирусное ПО с выбранной станции или группы станций.

Добавить станцию или группу. Позволяет создать новую станцию или новую группу. Для этого выберите соответствующий пункт в выпадающем списке.

Экспортировать данные. Позволяет записать общие данные о станциях антивирусной сети в файл формата CSV, HTML или XML. Требуемый формат экспорта выбирается в выпадающем списке.

Настроить отображение 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):

- Скрывать группу — 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.

Обновить все компоненты. Предписывает обновить все установленные компоненты антивируса (например, в ситуации, когда Агент долгое время не подключался к Серверу, и т. д.).

Обновить сбойные компоненты. Предписывает принудительно синхронизировать компоненты, обновление которых прошло с ошибкой.

Прервать запущенные. Предписывает остановить запущенные на станции сканирования. Подробное описание процедуры прерывания сканирований по типам приведено в п. «Запуск и останов антивирусного сканера на рабочей станции».

Сканировать. Позволяет провести сканирование станции в одном из режимов, выбираемых в выпадающем списке:

Dr.Web Сканер для Windows. Быстрое сканирование

Dr.Web Сканер для Windows. Полное сканирование

Dr.Web Сканер для Windows. Выборочное сканирование

Dr.Web Enterprise Сканер для Windows

Настройки вида дерева позволяют изменять внешний вид списка:

- для групп:
  - **Членство во всех группах**. Задает дублирование станции в списке, при вхождении ее в несколько групп одновременно (только для групп, идущих под значком белой папки – см. таблицу). Если флаг поставлен – будут показаны все вхождения станции. Если снят – станция будет отображена в списке единожды.
  - **Показывать скрытые группы**. Отобразить все группы, входящие в антивирусную сеть. При снятии данного флага пустые группы (не содержащие станции) будут скрыты. Это может быть удобно для исключения излишней информации, например, при наличии большого количества пустых групп.
  - **Сортировать группы по ролям**. Сортировать группы по типам (иначе – по алфавиту) и отобразить разделительную черту между группами различных типов (см. п. «Группы станций и их использование»).
- для станций:
  - Показывать идентификатор станции. Задает отображение станций в иерархическом списке по уникальным идентификаторам.
  - Показывать название станции. Задает отображение имен (названий) станций, если таковые заданы.
  - Показывать адрес станции. Задает отображение станций в иерархическом списке по IP-адресам.
  - Показывать сервер станции. Задает отображение имен или адресов антивирусных Серверов, к которым подключены станции.
- для всех элементов:
  - Отображать персональные настройки. Включает/выключает маркер на значках станций и групп, обозначающий наличие персональных настроек.
  - Показывать описания. Включает/выключает отображение описаний групп и станций (описания задаются в свойствах элемента).
  - Показывать число станций. Включает/выключает отображение количества станций для всех групп антивирусной сети.

Панель свойств

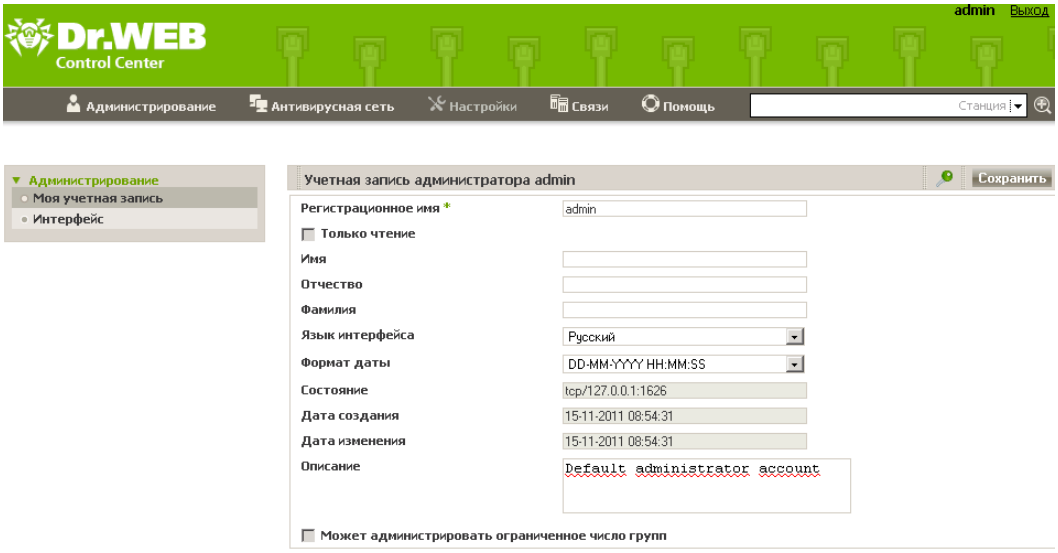
Панель свойств служит для отображения свойств и настроек рабочих станций и групп.

Для отображения панели свойств:

1) В иерархическом списке выделите станцию или группу и нажмите **Общие — Редактировать** на панели инструментов.
2) В правой части окна **Центра управления** откроется панель со свойствами рабочей станции. Данная панель содержит следующие группы настроек: **Общие, Конфигурация, Группы, Расположение**. Подробное описание данных настроек приведено в п. «Установка или ограничение прав пользователей».

Меню Настройки

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.

  Значения полей, отмеченных знаком *, должны быть обязательно заданы. При необходимости отредактируйте следующие параметры:
- **Регистрационное имя** администратора — логин для доступа к **Центру управления**.
- Установите флаг **Только чтение** для ограничения прав доступа.
- Ф. И. О. администратора.
- Язык интерфейса, использующийся данным администратором.
- Описание учетной записи.
- Для учетной записи администратора групп установите флаг **Может администрировать ограниченное число групп** для задания доступных групп.

Следующие параметры доступны только для чтения:

- Даты создания учетной записи и последнего изменения ее параметров.
- Состояние — отображает сетевой адрес последнего подключения под данной учетной записью.

После изменения параметров нажмите на 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 в разделе главного меню **Антивирусная сеть.**

Сканер сети. Параметры данного подраздела позволяют задать настройки Сканера сети по умолчанию.

Задайте следующие параметры Сканера сети:

1) В поле ввода **Сети** задайте 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 использование префикса сети (например, 10.4.0.0/24).

2) При необходимости измените **Порт** и значение параметра **Тайм-аут**.

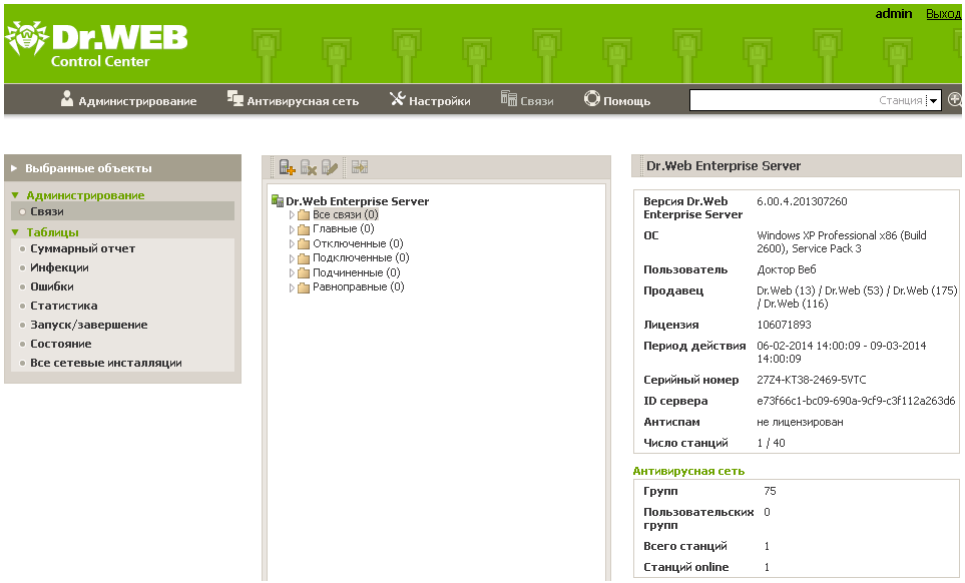
3) Для сохранения значений по умолчанию нажмите на кнопку **Сохранить**. В дальнейшем при использовании Сканера сети данные параметры будут заданы автоматически.

   Для запуска самого Сканера сети выберите в главном меню **Центра управления** пункт **Администрирование**, в управляющем меню (панель слева) выберите пункт **Сканер сети**.

Меню Связи

Для выбора просматриваемой информации служит управляющее меню, расположенное в левой части окна.

Раздел **Администрирование** управляющего меню содержит пункт **Связи**, который служит для управления связями между Серверами в многосерверной антивирусной сети (см. п. «Иерархия серверов»).



В иерархическом списке приведены все **Enterprise Серверы**, связанные с данным Сервером.

В разделе **Таблицы** управляющего меню приведена информация о работе антивирусной сети, полученная от других Серверов (см. п. «Иерархия серверов»).

Для просмотра сводных таблиц с данными по другим Серверам нажмите на соответствующий пункт раздела **Таблицы**.

Меню Помощь

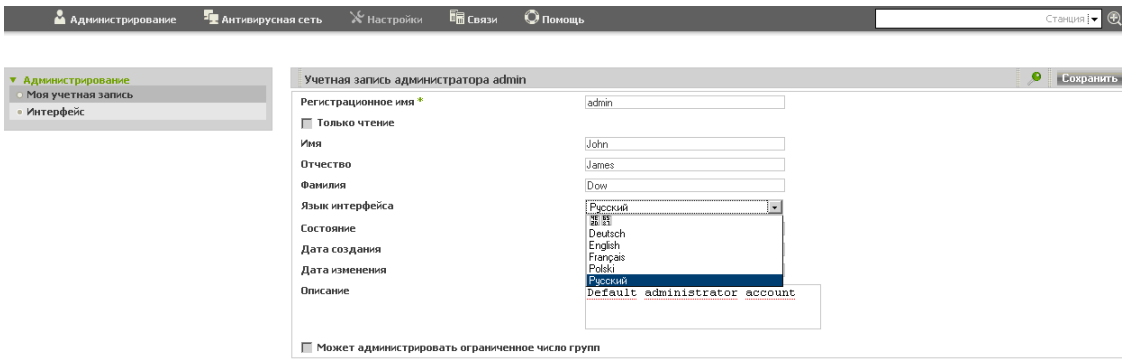
Управляющее меню, расположенное в левой части окна, содержит следующие элементы:

- Документация — открыть онлайн-документацию в формате HTML.
- Форум — перейти на форум компании «Доктор Веб».
- Задать вопрос — перейти на страницу технической поддержки «Доктор Веб».
- Прислать вирус — открыть форму для отправки вируса в лабораторию «Доктор Веб».

3.2. Смена языка отображения Центра управления

В связи с тем что **Dr.Web ATM Shield** 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 его редактирования надо перейти в раздел **Администрирование** (Administration) и выбрать пункт **Администраторы** (Administrator accounts) группы **Конфигурация** (Configuration). В списке администраторов необходимо выделить имя администратора и нажать на значок  . После выбора языка в списке **Язык интерфейса** (Interface language) нужно нажать на кнопку **Сохранить** (Save) и обновить страницу браузера.

Аналогичные параметры также доступны в разделе **Настройки** главного меню Веб-интерфейса, в секции **Моя учетная запись**.



3.3. Настройка языка интерфейса антивирусных компонентов на рабочей станции 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 **Dr.Web® Enterprise Agent для Windows,** вкладка **Общие**.
4) В поле **Язык** выберите из выпадающего списка необходимый язык.
5) Нажмите на кнопку **Сохранить**.

3.4. Группы станций и их использование. Предустановленные группы

Для удобства управления администратор может удобным для себя образом группировать защищаемые компьютеры по группам.

Объединение станций в группы позволяет задавать одной командой настройки для всех рабочих станций группы, а также инициировать выполнение определенных заданий также на всех станциях. Группы могут использоваться также для организации (структурирования) списка рабочих станций.

При установке программного комплекса создаются так называемые предустановленные группы.

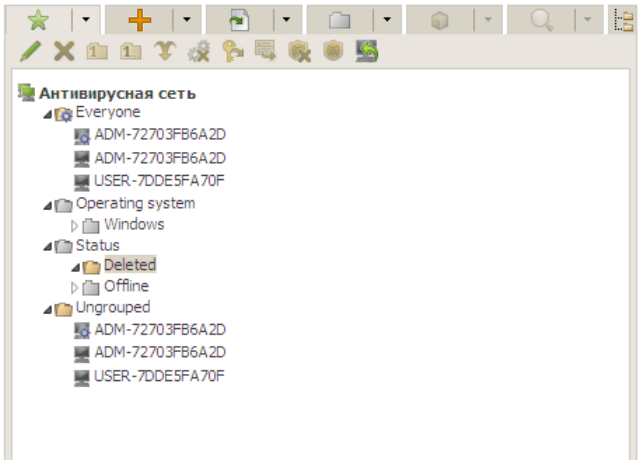
Изначально **Dr.Web ATM Shield** уже содержит набор системных групп. Эти группы создаются в момент инсталляции **Enterprise Сервера** и не могут быть удалены. Однако администратор при необходимости может скрыть их отображение.

В предустановленную группу **Everyone** входят все рабочие станции. Для группы **Everyone** отображается список всех компонентов всех активных ключей.

Состав групп **Online** и **Offline** изменяется автоматически в ходе работы сервера; первая из них включает все подключенные рабочие станции (реагирующие на запросы сервера), вторая — все неподключенные. Данные группы полностью виртуальны и не могут содержать никаких настроек, также они не могут являться первичными группами.

Кроме этого, в список групп входят группы, содержащие удаленные станции (системная группа **Deleted**) и группировка станций, не входящих в пользовательские группы (системная группа **Ungrouped**).

Остальные предустановленные группы содержат рабочие станции, работающие под управлением определенных ОС или семейств ОС, использующих определенные операционные системы. Состав предустановленных групп не может быть изменен вручную.



Пользовательские группы — группы, определяемые администратором антивирусной сети для его собственных нужд. Администратор может создавать собственные группы, а также вложенные группы и включать в них рабочие станции. Ни на состав, ни на название данных групп **Dr.Web ATM Shield** не накладывает никаких ограничений.

Для удобства в таблице ниже сведены возможные группы и типы групп, а также характерные параметры, которые поддерживаются (+) или не поддерживаются (–) данными группами.

При этом рассматриваются следующие параметры:

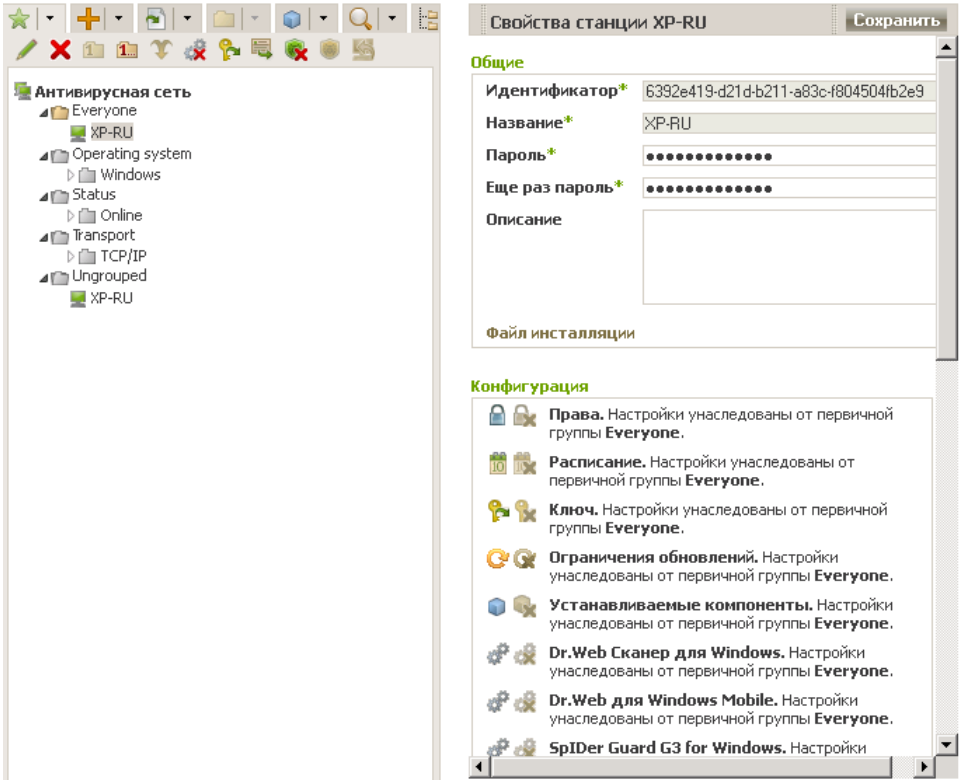
- **Автоматическое членство**. Параметр определяет возможность автоматического включения станций в группу (поддержка автоматического членства), а также автоматического изменения состава группы в процессе работы Сервера.
- **Управление членством**. Параметр определяет возможность управления администратором 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 (для возможности наследования их станциями).

Группа / тип групп	Параметр			
	Автоматическое членство	Управление	Первичная группа	Содержание настроек
Everyone	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Operating System	+	–	+	+
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.

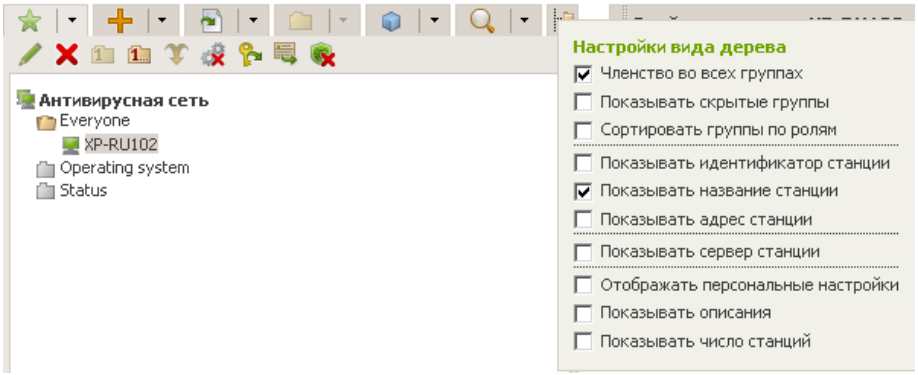
3.4.1. Просмотр параметров групп

Администратор может просматривать свойства групп и станций, используя значок  .

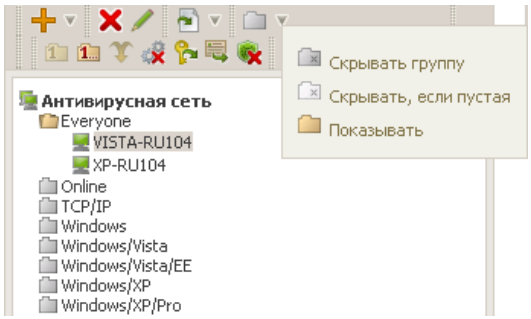


3.4.2. Настройка отображения групп

Используя значок  , администратор может настроить представление дерева групп в удобном для себя виде.



Дополнительно, используя значок , администратор имеет возможность определить режим показа группы.

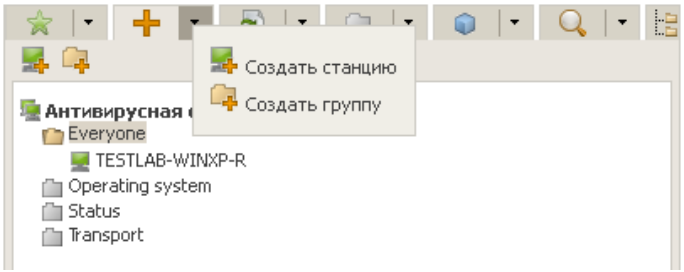


3.4.3. Создание и удаление группы

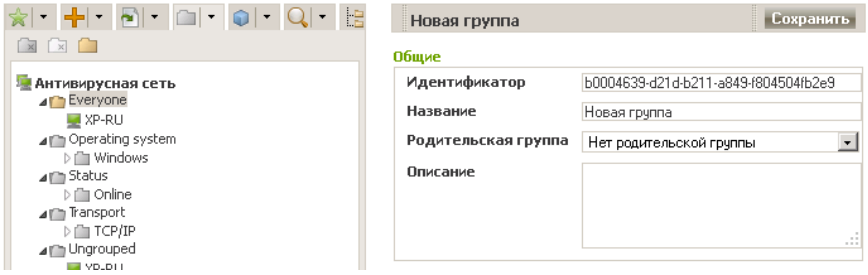
В случае необходимости администратор может создавать новые группы и станции.

Для создания группы и включения в нее рабочих станций сделайте следующее.

1) В разделе **Антивирусная сеть** Веб-интерфейса нажмите кнопку (**Добавить станцию или группу**) 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. При необходимости его можно отредактировать. Идентификатор не должен включать пробелы. Рекомендуется использовать уникальные идентификаторы, как-либо связанные со структурой сети.

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**.

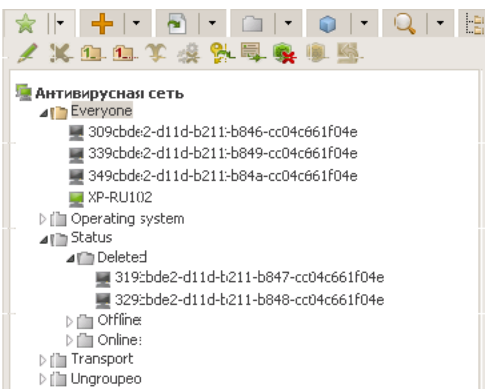
5) Введите произвольный комментарий в поле **Описание**.

6) Нажмите на кнопку **Сохранить**.

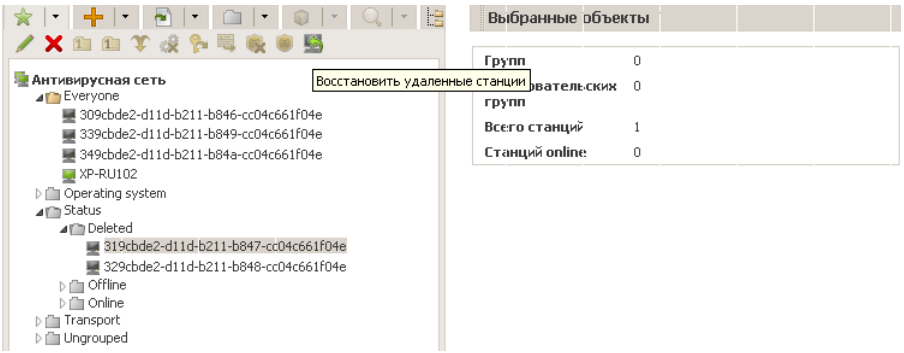
Созданные группы первоначально пусты. Процедура включения рабочих станций в группы описана ниже.

При создании станции администратор дополнительно указывает членство в группах, а также месторасположение станции, что может быть полезно для ее обслуживания в крупных компаниях.

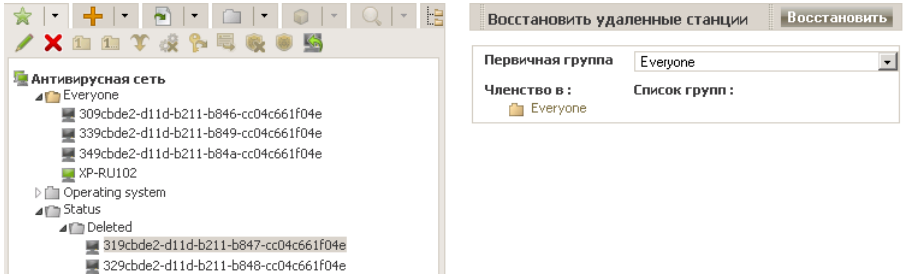
Вы также можете удалять созданные вами станции или группы (предустановленные группы удалять невозможно). Для этого выберите станцию или группу, после чего нажмите кнопку **Удалить отмеченные объекты**.



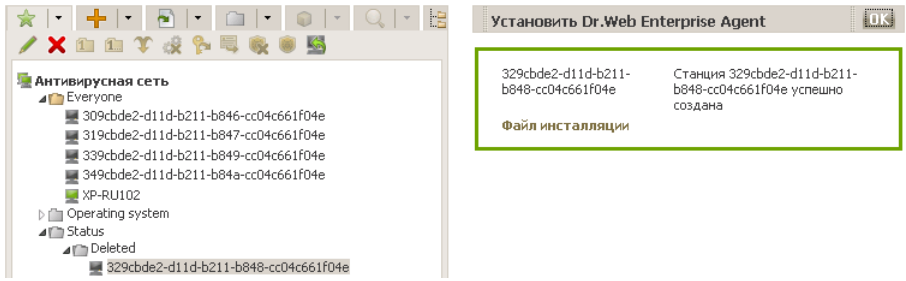
Удаленные станции помещаются в группу **Deleted**, находящуюся в группе **Status**. При этом с удаленными станциями можно работать непосредственно в дереве антивирусной сети — так же, как и с обычными станциями. В число доступных операций включается возможность восстановления удаленных при помощи элемента панели инструментов  (**Восстановить удаленные станции**).



При восстановлении станции можно указать для нее членство в группах.



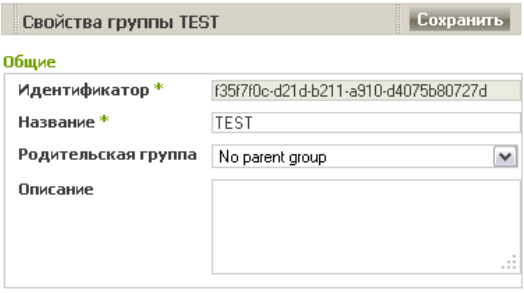
Для подтверждения восстановления нажмите кнопку **OK**.



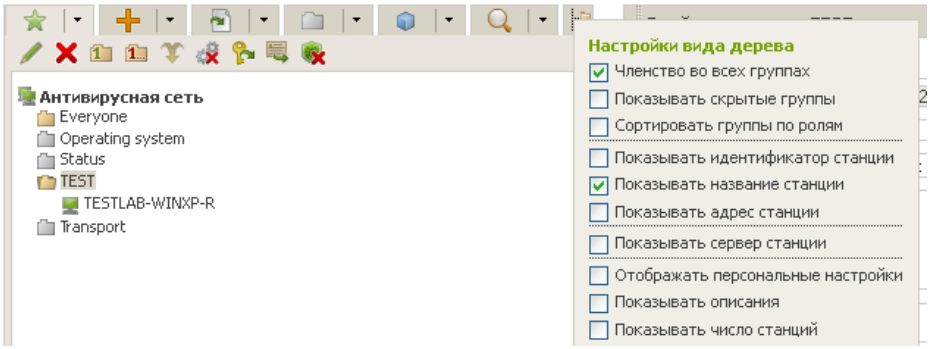
3.4.4. Настройки группы. Использование групп для настройки рабочих станций. Настройки полномочий пользователей

Сразу после установки все группы и рабочие станции имеют единые настройки, заданные по умолчанию (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.

Для того чтобы задать настройки группы (настройки по умолчанию рабочих станций группы), в разделе **Антивирусная сеть** Веб-интерфейса нужно выделить группу, которую необходимо настроить, и нажать кнопку **Редактировать**. В правой части окна откроется форма **Свойства группы <имя группы>**.

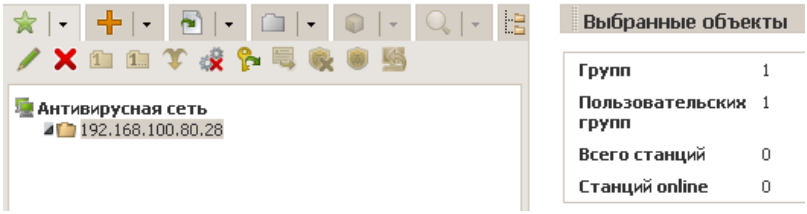


По умолчанию структура сети представлена таким образом, чтобы продемонстрировать вхождения станций только в первичных группах. Если вы хотите отображать в каталоге сети членство станций во всех группах, куда входит станция, нажмите кнопку **Настройки вида дерева** и установите флажок **Членство во всех группах**.



Настройки группы включают конфигурацию антивирусных средств, расписание и настройку прав пользователей. Настройки агента не входят в конфигурацию группы и не могут быть заданы через механизм групп.

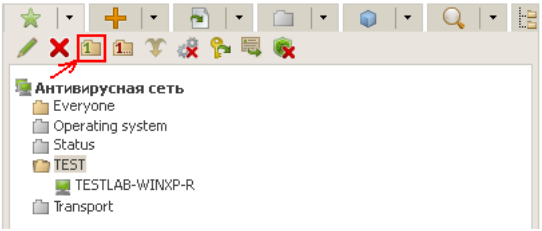
Используя пункты меню справа, вы можете запускать, просматривать и прекращать задания на сканирование как для отдельной группы, так и для нескольких выбранных групп. Точно так же вы можете просматривать статистику (в т. ч. инфекции, вирусы, запуск/завершение, ошибки сканирования и установки) и суммарную статистику для всех рабочих станций группы или нескольких групп.



3.4.5. 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 такой группы эти изменения 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**, необходимо выделить соответствующую группу и нажать кнопку **Установить эту группу первичной**.



Вы можете сделать группу первичной для всех входящих в нее рабочих станций. Для этого выделите нужную группу, после чего нажмите кнопку **Установить эту группу первичной**.

3.4.6. Добавление рабочих станций в группу. Удаление рабочих станций из группы. Восстановление станции

Созданные вами группы первоначально пусты. Все группы считаются находящимися на одном уровне иерархии каталога. Создавать вложенные группы невозможно.

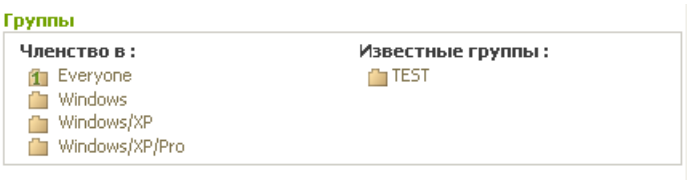
Существует несколько способов добавления рабочих станций в новые (созданные вами) группы.

Чтобы добавить станцию в группу, необходимо в разделе **Антивирусная сеть** найти и выделить перемещаемую станцию, после чего нажать кнопку **Редактировать**. Справа откроется форма **Свойства станции <имя станции>**.

Найдите в этой форме группу настроек **Группы**. В левой части вкладки в списке **Членство в** перечислены группы, в которые рабочая станция уже включена. В правой части в списке **Известные группы** расположен список всех остальных групп.

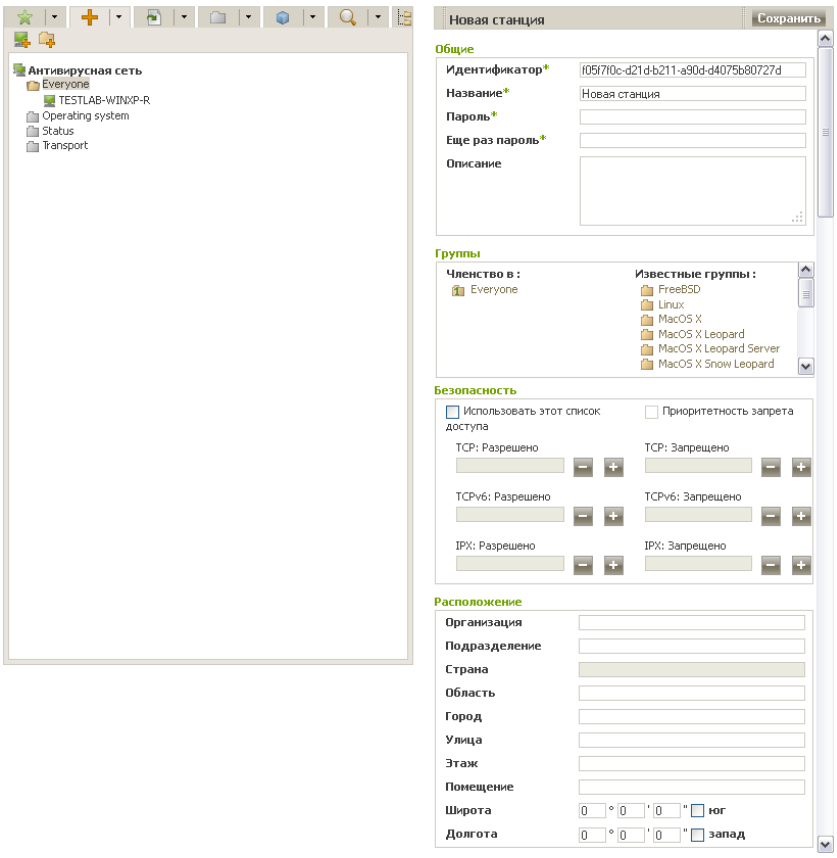
Для добавления станции в группу нажмите на ее название в списке **Известные группы**. Станция будет добавлена в данную группу, а группа — перемещена в список **Членство в**.

Для сохранения внесенных изменений нажмите на кнопку **Сохранить**.



Вы также можете включить рабочую станцию в группу, устанавливая новую группу первичной (подробнее см. «Наследование элементов конфигурации рабочей станции. Первичные группы»).

Для создания записи о новой станции при помощи **Центра управления**: выберите пункт главного меню **Антивирусная сеть**, в открывшемся окне нажмите на панели инструментов кнопку **Добавить станцию или группу**. В выпадающем меню выберите соответствующий пункт. Откроется окно создания новой рабочей станции.



Поле **Идентификатор** заполняется автоматически. При необходимости идентификатор можно отредактировать (идентификатор не должен содержать пробелов и должен быть уникальным).

Введите название станции в поле **Название**, пароль и подтверждение пароля в соответствующие поля.

При необходимости введите произвольный комментарий в поле **Описание**. Также вы можете задать параметры в группах настроек **Центра управления Группы** и **Расположение**.

Нажмите на кнопку **Сохранить**.

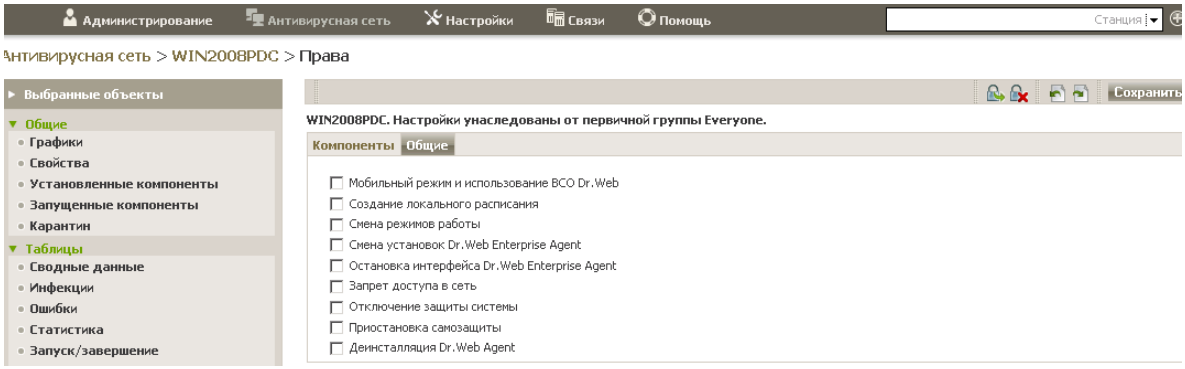
Внимание! В результате операций с базой данных или при переустановке ПО антивирусных станций в иерархическом списке антивирусной сети может появиться несколько станций с одинаковым названием (только одно из них будет соотнесено с соответствующей антивирусной станцией). Для того чтобы убрать повторяющие имена станции, выделите все имена такой станции и на панели инструментов Центра управления 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, нажмите на название группы в списке **Членство в**, и станция будет исключена из этой группы, а группа — перемещена в список **Известные группы**. Для применения настроек следует также нажать кнопку **Сохранить**.

Удаление из предопределенных групп невозможно.

Чтобы удалить запись о рабочей станции, выберите в меню **Антивирусная сеть** пункт **Общие** и, выбрав группу, нажмите на значок  (**Удалить отмеченные объекты**). Сам значок должен быть красным (активным). Для подтверждения нажмите **ОК**.

Внимание! Перед удалением убедитесь в том, что у выбранной вами станции присутствуют права на ее удаление. Для этого выберите закладку **Общие** в пункте **Права** меню **Антивирусная сеть**, отметьте пункт **Деинсталляция Dr.Web Agent** и нажмите **Сохранить**.



После удаления станций из иерархического списка они помещаются в таблицу удаленных станций, из которой возможно восстановление объектов при помощи **Центра управления**.

Чтобы восстановить запись о рабочей станции, необходимо в меню **Антивирусная сеть** выбрать пункт управляющего меню (панель слева) **Восстановление станций** и в открывшейся таблице удаленных станций, объединенных по группам, из которых они были удалены, отметить те станции, которые необходимо восстановить. Для каждой станции указывается ее название, адрес и дата удаления. Удаленные станции объединены в таблицы по группам, из которых они были удалены.

Если необходимо восстановить станцию в той группе, из которой она была удалена, то после выделения станции надо нажать кнопку **Восстановить** на панели инструментов. Если необходимо восстановить станцию в другой группе, надо нажать кнопку **Восстановить в группу** и в открывшемся окне выбрать группу, в которой будет восстановлена станция. Для сохранения необходимо нажать на **Сохранить** и далее на **Восстановить**.

3.4.7. Политика подключения новых станций

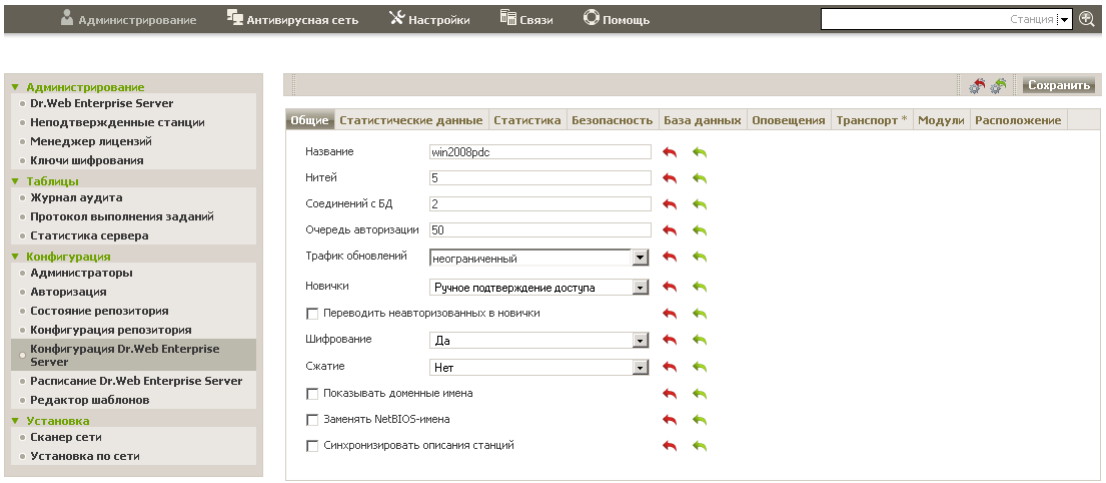
В зависимости от выбранной политики новые станции могут подключаться автоматически или вручную. Во втором случае администратор должен подтверждать подключение каждой новой станции к антивирусной сети. При этом:

- 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. «Установка Dr.Web Enterprise Agent при помощи инсталляционного пакета esinst»).

Задание типа авторизации **Агента** при его установке описано в разделе «Установка с использованием дистрибутивов компонентов Dr.Web Enterprise Security Suite».

Вы можете менять политику подключения, изменив режим доступа станций к **Enterprise Серверу**. Чтобы изменить режим доступа станций к **Dr.Web Enterprise Server**:

1) Откройте настройки конфигурации Сервера. Для этого выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.



2) На вкладке Общие в выпадающем списке **Новички** выберите одно из трех значений:

- **Ручное подтверждение доступа** (по умолчанию). В данном режиме новые станции помещаются в список неподтвержденных станций до их непосредственного рассмотрения администратором.

  Для доступа к списку неподтвержденных станций:

  1) Выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Неподтвержденные станции**. В открывшемся окне приведена таблица станций с установленными **Агентами**, запрашивающими доступ к **Серверу**, и общая информация о станциях: время получения запроса, сетевое название станции, IP-адрес станции и установленная на станции ОС.
  2) Для задания доступа к **Серверу** установите флаги для нужных станций или установите флаг в заголовке таблицы, чтобы отметить все станции. На панели инструментов выберите действие, которое будет применено для выбранных станций — разрешить доступ выбранным станциям и назначить первичную группу из предложенного списка или отказать в доступе выбранным станциям.
- **Автоматически разрешать доступ**. В данном режиме все станции, которые запрашивают доступ к **Серверу**, подключаются автоматически без дальнейших запросов администратору. При этом в качестве первичной группы назначается группа **Everyone**.

- **Всегда отказывать в доступе**. В данном режиме отказывается в доступе при получении запросов от новых станций. Администратор должен вручную создавать записи о станциях и присваивать им пароли доступа.

Для доступа к списку неподтвержденных станций через **Центр управления** выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Неподтвержденные станции**.

Список неподтвержденных станций позволяет:

- разрешить доступ выбранной станции (или всем станциям) и назначить в качестве первичной группы группу Everyone,
- разрешить доступ выбранной станции (или всем станциям) и назначить первичную группу,
- отказать в доступе выбранной станции (или всем станциям).

3.4.8. Перемещение в новую группу

Для перемещения станции в новую группу необходимо выбрать пункт меню **Assign Primary Group**, в появившемся окне **Назначить первичную группу** выбрать необходимую группу и подтвердить изменения.

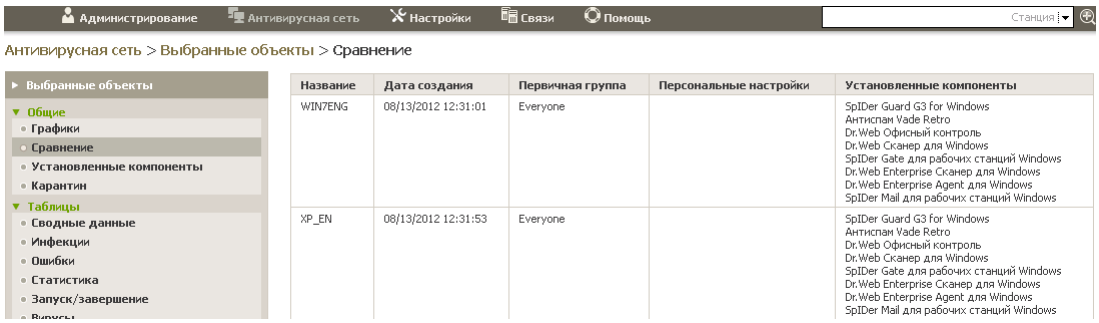
3.4.9. Сравнение станций и групп

Для сравнения станций и групп по основным параметрам:

1) Выберите пункт **Антивирусная сеть** главного меню и в открывшемся окне в иерархическом списке выберите объекты, которые вы ходите 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.
  - Персональные настройки — список компонентов, для которых назначены персональные настройки — не унаследованные от родительской группы.
- Параметры сравнения для станций:
  - Дата создания станции.
  - Первичная группа для станции.
  - Персональные настройки — список компонентов, для которых назначены персональные настройки, не унаследованные от первичной группы.
  - Установленные компоненты — список антивирусных компонентов, установленных на данной станции.

3.4.10. Управление группами. Назначение администраторов групп

Учетные записи администраторов антивирусной сети делятся на три группы:

- учетные записи с полными правами,
- учетные записи с правами «только для чтения»,
- учетные записи с правами администрирования групп.

Администраторы с полными правами имеют исключительные права на управление **Enterprise Сервером** и 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 рабочей станции. При этом он может ограничить, вплоть до полного запрета, вмешательство пользователя рабочей станции в управление антивирусным ПО (см. п. «Установка или ограничение прав пользователей»).

Администратор с полными правами может просматривать и редактировать список имеющихся административных учетных записей.

Администраторы с правами «только для чтения» могут только просматривать настройки сети в целом и отдельных ее элементов, но не менять их. Они также могут просматривать список имеющихся административных учетных записей.

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). Возможно создание данных учетных записей только для пользовательских групп (см. п. «Группы станций и их использование. Предустановленные группы»). 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**.

После установки системы в ней имеется одна учетная запись с полными правами.

Администратору антивирусной сети для текущего управления антивирусной сетью не требуются административные полномочия на компьютерах, включенных в эту антивирусную сеть. Однако удаленная установка и деинсталляция ПО Агента возможна только в локальной сети и требует полномочий администратора в этой сети, а отладка **Enterprise Сервера** — 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 **Enterprise Сервера**. В зависимости от политики безопасности в организации и кадровой ситуации администратор антивирусной сети либо должен получать полномочия администратора локальной сети, либо работать в тесном контакте с таким лицом.

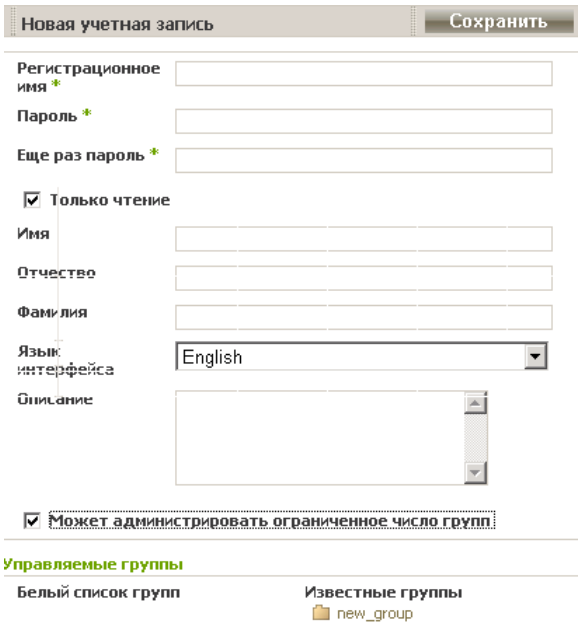
Dr.Web ATM Shield позволяет любому администратору с полными правами редактировать настройки (в том числе имя и пароль администратора), создавать новые и удалять имеющиеся учетные записи.

По умолчанию, если при установке не было задано другое, Сервер устанавливается с учетной записью администратора с полными правами (с именем **admin** и паролем, который задавался 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** выбрать **Администраторы** и нажать на кнопку .

Для администраторов групп панель настроек учетной записи открывается сразу при нажатии на пункт **Администраторы**.

В открывшейся слева панели необходимо указать данные администратора. Если необходимо создать администратора с полным доступом ко всем настройкам групп, но с правом доступа к ним только на чтение, то необходимо отметить пункт **Только чтение**; если же создается администратор с правом управления определенными группами, то необходимо отметить **Может администрировать ограниченное число групп** и перенести из открывшегося списка **Известные группы** нужные, щелкнув по названию.

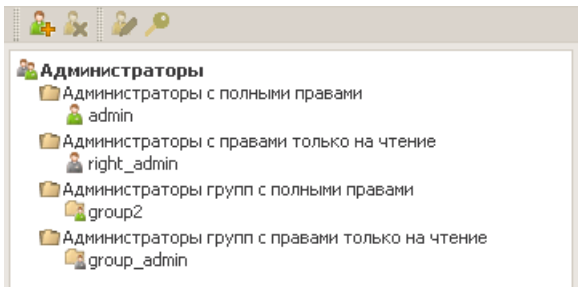


Значения полей, отмеченных знаком *, должны быть обязательно заданы.

Следующие параметры доступны только для чтения:

- Даты создания учетной записи и последнего изменения ее параметров.
- Состояние — отображает сетевой адрес последнего подключения под данной учетной записью.

После заполнения формы нужно щелкнуть по кнопке **Сохранить** и обновить экран.

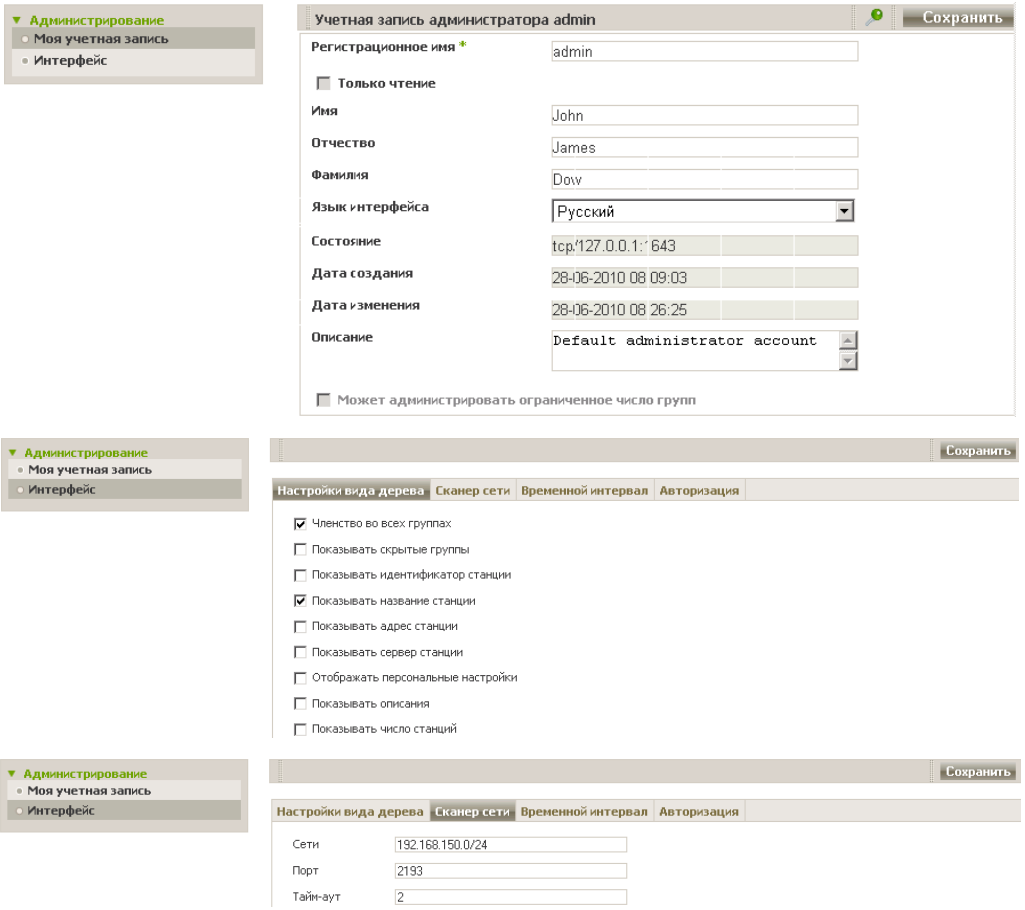


Для того чтобы добавить учетную запись, выберите в центральной панели инструментов значок **Создать учетную запись**. Откроется аналогичное окно настроек учетной записи.

Для того чтобы удалить учетную запись, выберите ее в списке, после чего на панели инструментов нажмите значок **Удалить учетную запись**.

Для изменения пароля для доступа к учетной записи нажмите на значок **Новый пароль**.

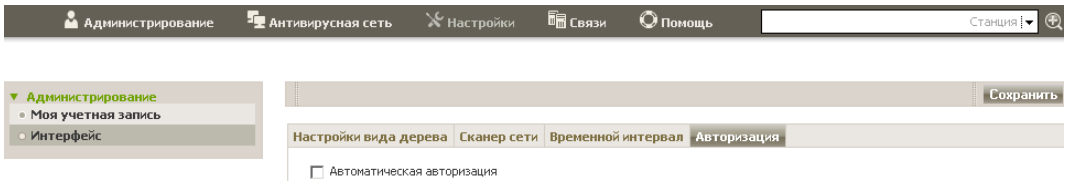
Дополнительные настройки могут быть заданы в меню **Настройки**.



3.4.10.1. Автоматическая авторизация администраторов

Автоматическая авторизация администраторов позволяет сохранить текущие имя и пароль администратора, и при следующем открытии **Центра управления** на этом ПК в этом браузере авторизация осуществляется автоматически, без запроса имени пользователя и пароля.

Для включения этой возможности необходимо выбрать пункт **Интерфейс** меню **Настройки** и зайти на закладку **Авторизация**.



3.4.10.2. Изменение порядка аутентификации администраторов

Аутентификация администратора возможна:

1) с хранением данных об администраторах в БД антивирусного сервера;
2) с хранением данных об администраторах в Active Directory (при установке сервера на ОС Windows);
3) с хранением данных об администраторах в LDAP.

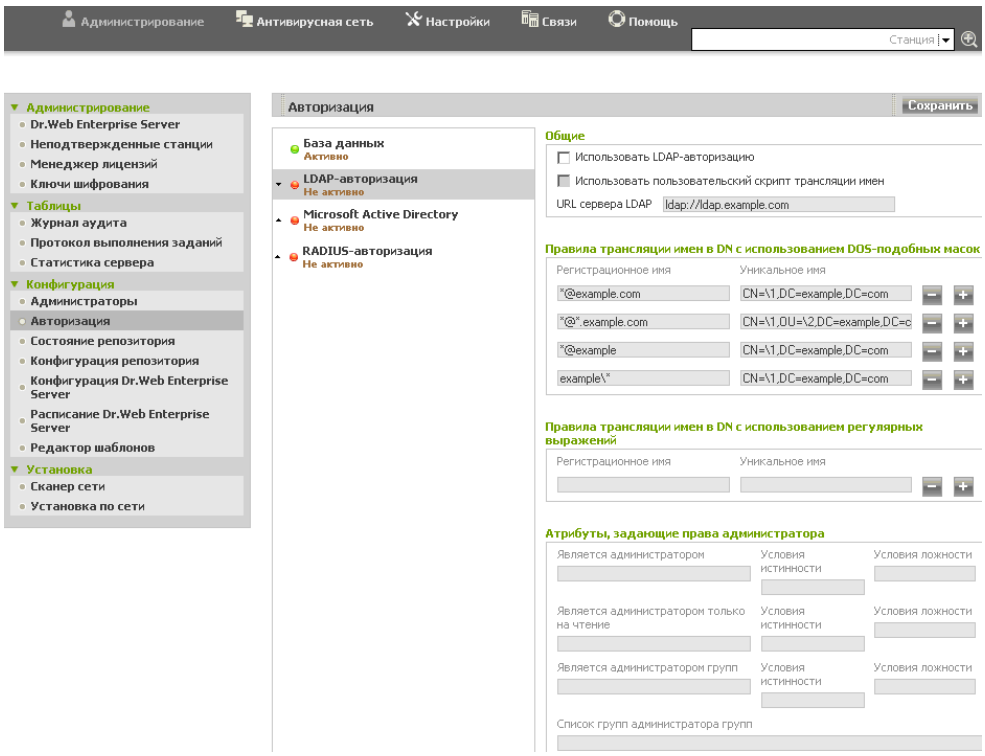
Порядок аутентификации:

1) первой всегда осуществляется попытка аутентификации администратора из БД Сервера;
2) второй по умолчанию используется аутентификация через LDAP;
3) третьей по умолчанию — через Active Directory;
4) четвертой — через RADIUS.

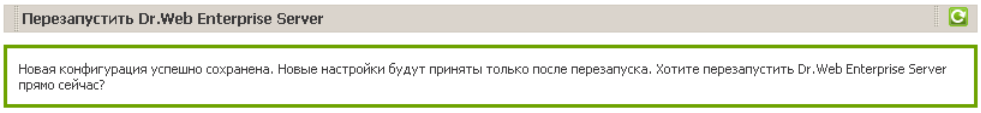
Внимание! Методы аутентификации через LDAP, Active Directory и RADIUS по умолчанию отключены.

В настройках сервера методы аутентификации через LDAP, Active Directory и RADIUS можно поменять местами, но первой всегда осуществляется попытка аутентификации администратора из БД. Для изменения порядка использования LDAP и Active Directory авторизации сделайте следующее.

1) В управляющем меню **Администрирование** выберите раздел **Авторизация**.



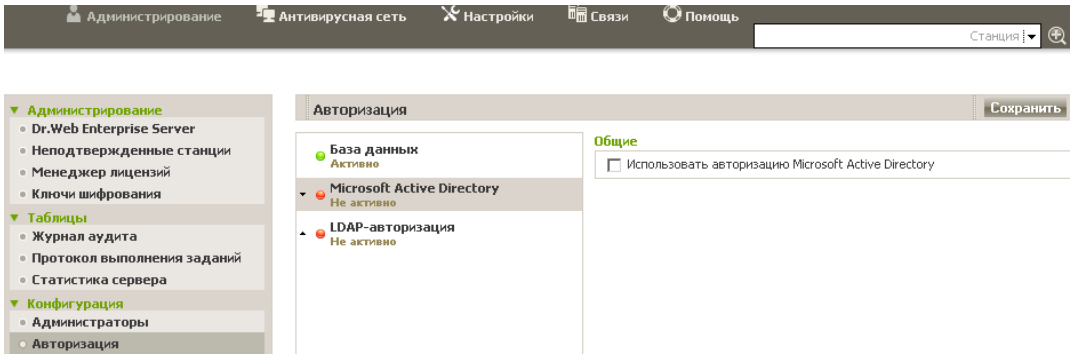
2) В открывшемся окне представлен список типов авторизации в том порядке, в котором они используются. Для изменения порядка следования нажмите на стрелку слева от названия типа авторизации. Пункты **Microsoft Active Directory** и **LDAP-авторизация** поменяются местами.



3) Нажмите  и подтвердите выбор.

Для включения аутентификации с использованием Active Directory:

1) В меню **Администрирование** выберите раздел **Авторизация**.
2) В открывшемся окне зайдите в раздел **Microsoft Active Directory** и установите флаг **Использовать авторизацию Microsoft Active Directory**.



3) Нажмите **Сохранить**.

Для управления списком администраторов, данные о которых сохранены в БД Сервера, в меню **Администрирование** выберите раздел **Администраторы**. Откроется список всех зарегистрированных в БД администраторов. Подробная информация о порядке управления правами администраторов описана в разделе «Управление учетными записями администраторов» «Руководства администратора».

3.4.10.3. 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. «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. Точно так же вы можете просматривать статистику (в т. ч. инфекции, вирусы, запуск/завершение, ошибки 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 нажмите на кнопку **Удалить эти настройки** на панели инструментов **Центра управления**.

3.4.11. 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 эти изменения наследуются входящими в группу станциями, за исключением случаев, когда станциям были заданы персональные настройки. 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**.

Возможно создание вложенных групп.

В условиях вложенных групп, если для станции не заданы персональные настройки, наследование элементов конфигурации осуществляется в соответствии со структурой вложенных групп. Поиск осуществляется вверх по иерархическому дереву, начиная с первичной группы станции, ее родительской группы и далее до корневого элемента дерева. Если при этом не были обнаружены персональные настройки, то наследуются элементы конфигурации группы **Everyone**.

Например:

Структура иерархического списка представляет собой следующее дерево:

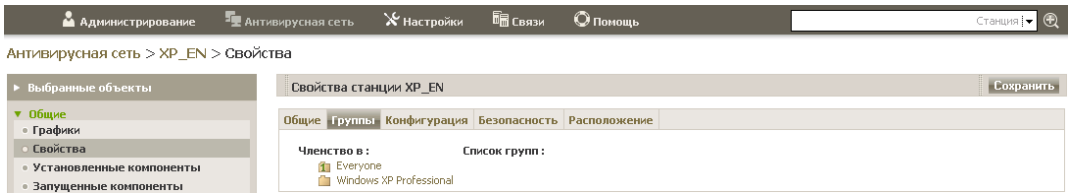
Группа **Group4** является первичной для станции **Station1**. При этом при наследовании настроек станцией **Station1** будет осуществляться поиск настроек в следующем порядке: **Station1** → **Group4** → **Group3** → **Group2** → **Group1** → **Everyone**.

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 **Свойства**. В открывшемся окне перейдите на вкладку **Группы**.



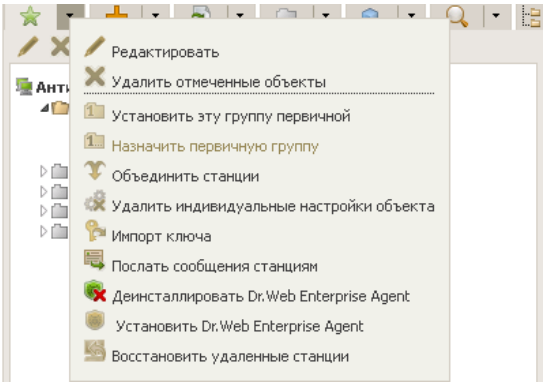
2) При необходимости назначить другую первичную группу нажмите на значок группы из списка **Членство в**.

3) Нажмите на кнопку **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**.

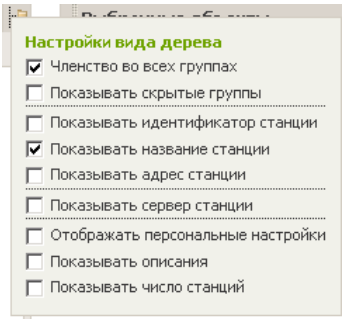
2) На панели инструментов нажмите **Общие** — **Назначить первичную группу**. Откроется окно со списком групп, которые могут быть назначены первичными для этих станций.



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 флаг **Членство во всех группах**.



3.4.11.1. Установка или ограничение прав пользователей

Внимание! Для того чтобы пользователь имел возможность изменить настройки агента, он должен быть администратором данной группы с правами на запись.

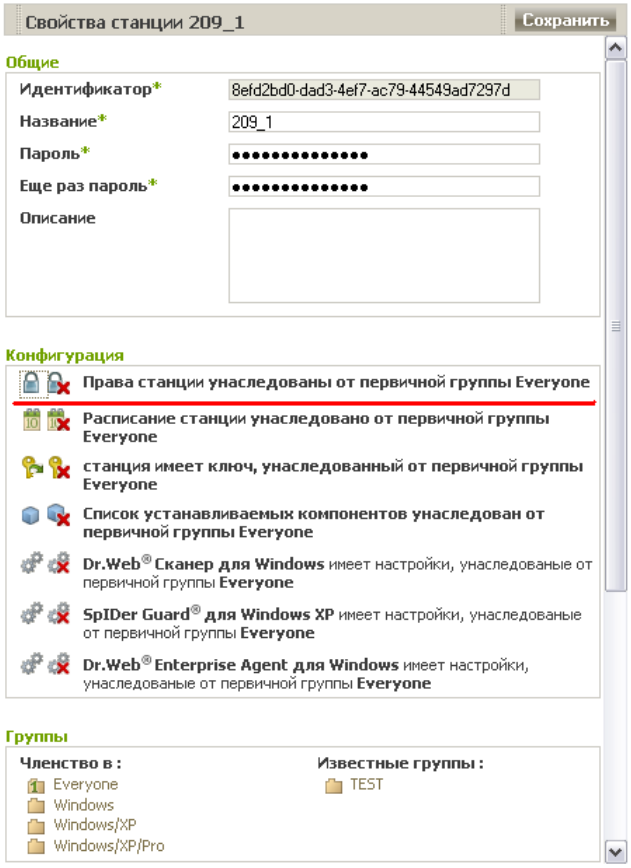
Для облегчения управления групповыми политиками в комплексе присутствует возможность управлять пользовательскими правами на запуск, конфигурирование и останов различных компонентов антивируса.

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**). После чего в появившейся форме **Свойства станции <имя станции>** нажмите кнопку (Редактировать) слева от строки **Права станции унаследованы от первичной группы <имя первичной группы>**.

Данное окно содержит следующие группы настроек: **Общие, Конфигурация, Группы, Безопасность, Расположение**. 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 **Конфигурация** вы можете изменить конфигурацию данной станции, включающую:

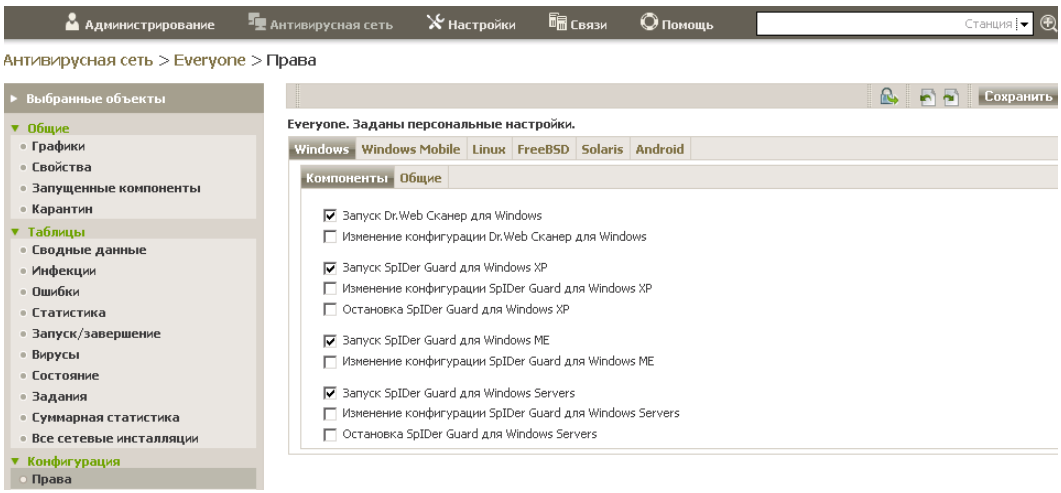
- изменение прав пользователя рабочей станции;
- настройку централизованного расписания запуска заданий на рабочей станции (описание настройки расписания приведено в п. «Расписание»);
- задание лицензионного ключа для станции;
- настройку ограничений при обновлении антивирусного ПО (описание настройки обновлений приведено в п. «Ограничение обновлений»);
- задание списка устанавливаемых компонентов;
- настройки компонентов антивирусного пакета — Dr.Web Сканер для Windows, SpIDer Guard G3 for для Windows и др. Для изменения настроек нажмите на кнопку напротив соответствующего компонента.

Из **Центра управления** также доступны кнопки для удаления персональных настроек. Они расположены справа от соответствующих кнопок настройки конфигурации. При удалении персональной конфигурации рабочей станции вновь будет установлена конфигурация, унаследованная от первичной группы.

Состав параметров компонентов и рекомендации по их заданию содержатся в руководстве «Антивирус Dr.Web® для Windows. Руководство пользователя».

Определить состав компонентов защиты и права по управлению их настройками можно, используя в пункте меню **Права** вкладку **Компоненты**.

В появившемся окне системный администратор может задать, какие действия над компонентами антивируса будут разрешены или запрещены для данной группы.

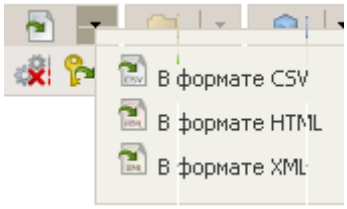


При отключении какого-либо из пунктов, отвечающих за изменение настроек Агента, будет использоваться значение, которое было задано для данной настройки в последний раз перед отключением.

Для того чтобы отказаться от данной конфигурации прав и вернуться к конфигурации по умолчанию, унаследованной от предустановленных групп, нажмите в разделе **Конфигурация** на кнопку **Удалить эти настройки**.

Распространить настройки на другой объект можно, нажав на кнопку .

Чтобы экспортировать настройки в файл, нажмите .



Чтобы импортировать эти настройки из файла, нажмите .

Для того чтобы принять сделанные изменения прав, нажмите на кнопку **Сохранить**.

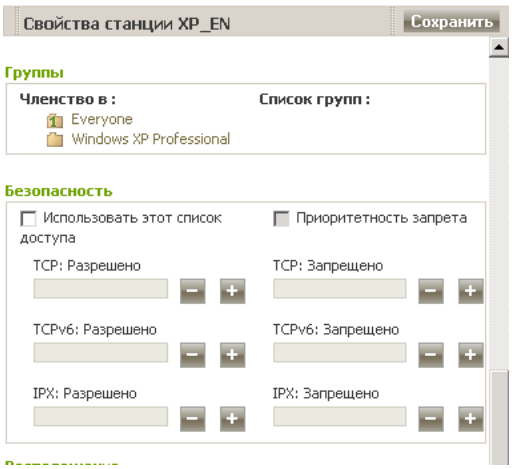
Управление настройками через **Центр управления** имеет некоторые отличия от управления настройками непосредственно через соответствующие компоненты антивируса:

- для того 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 кнопки  на панели инструментов (верхняя часть большинства окон настроек, например, **Расписание, Права, Dr.Web® Сканер для Windows, SpIDer Guard® для Windows**:
  - 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 специального формата,
  - импортировать параметры из файла специального формата,
  - для Веб-интерфейса — удалить специфическую конфигурацию для данной рабочей станции (при этом вновь будет установлена унаследованная от групп конфигурация, см. п. «Настройки группы. Использование групп для настройки рабочих станций»).
- Нажмите на кнопку **Сохранить**, чтобы согласиться с внесенными изменениями.

В разделе **Группы** вы можете изменить первичную группу для данной станции. Данная процедура описана в п. «Наследование элементов конфигурации рабочей станции. Первичные группы».

В разделе **Безопасность** задаются ограничения на сетевые адреса, с которых разрешен доступ к данной станции.



Чтобы разрешить все соединения, снимите флаг **Использовать этот список доступа**. Для того чтобы задать списки разрешенных или запрещенных адресов, установите этот флаг.

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.

Аналогично настраиваются ограничения для IPX-адресов.

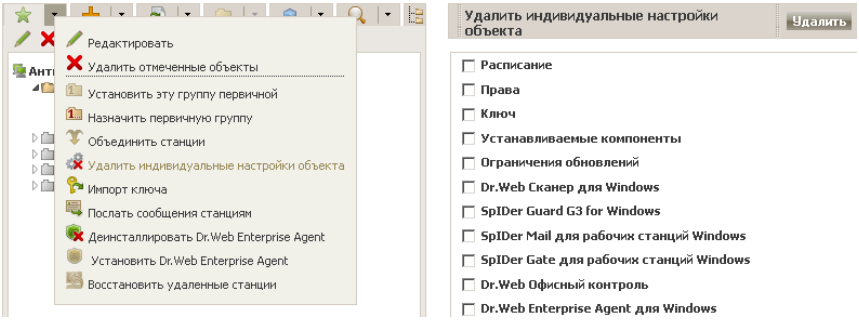
Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флаг **Приоритетность запрета**: при установленном флаге адреса, не включенные ни в один из списков (или включенные в оба), запрещаются. В противном случае такие адреса разрешаются.

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 — Убрать индивидуальные настройки объекта.** Откроется список настроек данной станции, персональные будут отмечены флагами.



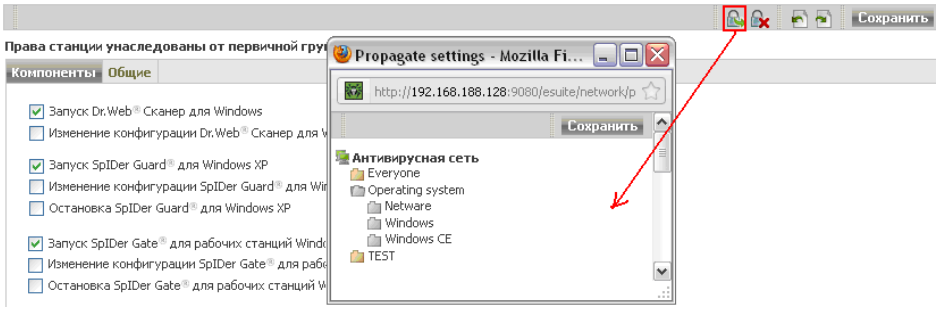
2) Для настроек, которые необходимо удалить, снимите нужные флаги и нажмите **Сохранить**. Настройки станции, унаследованные от первичной группы, будут восстановлены.

При редактировании конфигурации рабочей станции для компонентов SpIDer Guard для Windows, а также Dr.Web Сканер для Windows ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows Server 2003, ОС Windows 2000 и ОС Windows XP. Статья, содержащая необходимую информацию, находится по адресу http://support.microsoft.com/kb/822158/ru. Материал данной статьи призван помочь оптимизировать производительность системы.

3.4.11.2. Распространение настроек, в том числе на станции, которые недоступны в момент настройки. Копирование настроек в другие группы/станции

Настройки конфигурации антивирусных средств, расписаний и прав пользователей группы или рабочей станции могут быть скопированы (распространены) в группу или несколько групп и рабочих станций.

Для этого в форме редактирования конфигурации антивирусного компонента, расписания или прав станции нажмите на кнопку (**Распространить эти настройки на другой объект**). Откроется окно каталога сети, в котором необходимо выбрать группы и станции, на которые необходимо распространить настройки. Для принятия произведенных изменений нажмите кнопку **Сохранить**.



Ту же самую операцию вы можете проделать:

- в окне редактирования конфигурации антивирусного компонента,
- в окне редактирования расписания,
- в окне настройки ограничений обновления,
- в окне устанавливаемых компонентов.

3.4.11.3. 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 чекбокс **Показывать скрытые группы**, после чего нажмите кнопку **Сохранить**.

3.5. Управление параметрами защиты рабочих станций и серверов Windows

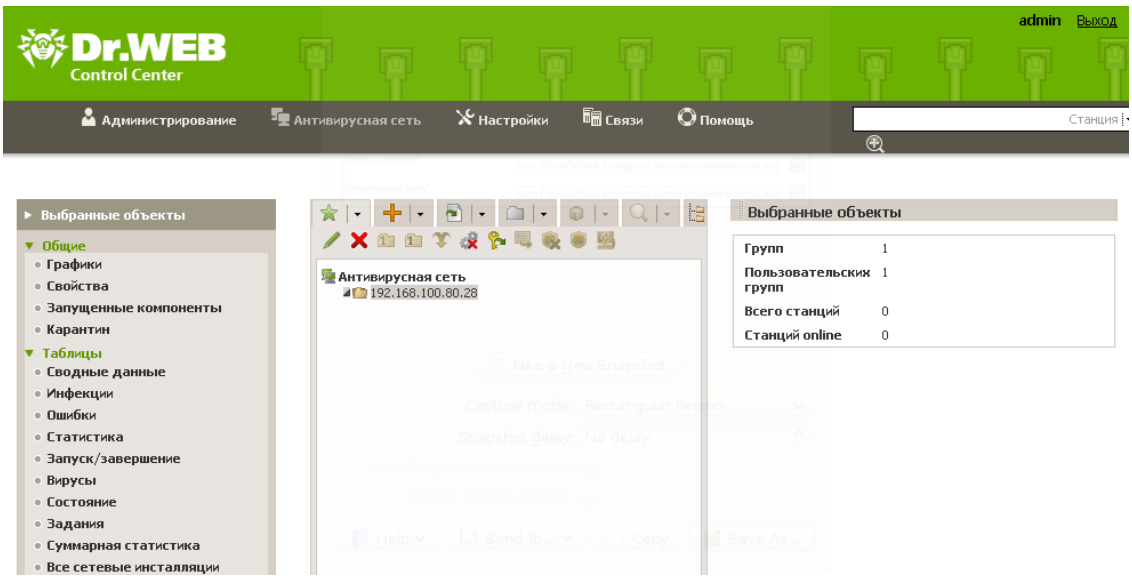
Антивирусная сеть, работающая под управлением **Dr.Web ATM Shield**, позволяет централизованно:

- настраивать конфигурационные параметры антивирусных средств,
- настраивать расписание запуска заданий на сканирование,
- запускать отдельные задания на рабочих станциях, независимо от настроек расписания,
- запускать процесс обновления рабочих станций, 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.

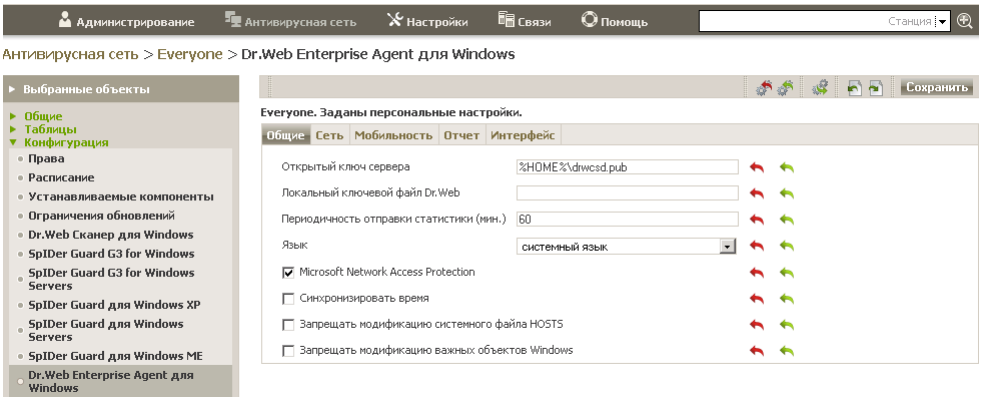


3.5.1. Настройка параметров защиты рабочих станций и серверов Windows

Администратор может определять настройки как по отношению к группам в целом, так и по отношению к отдельным членам групп.

Чтобы просмотреть или изменить настройки **Dr.Web Enterprise Agent** 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 **Dr.Web® Enterprise Agent для Windows** – откроется окно настроек Агента.



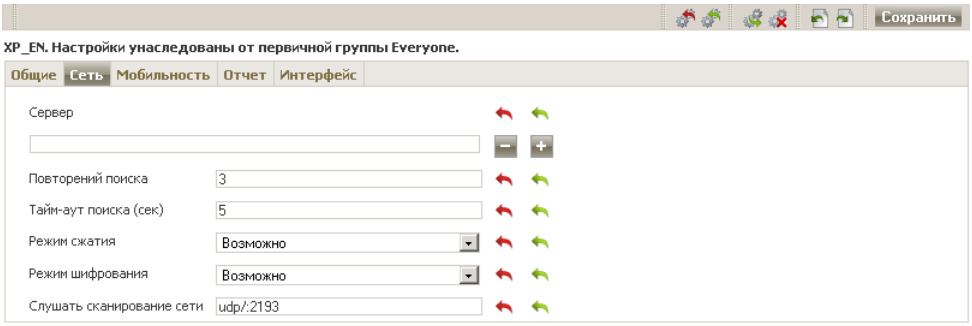
Чтобы принять сделанные изменения, нажмите на кнопку **Сохранить**.

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** указываются общие параметры Агента.

- В поле **Открытый ключ сервера** укажите путь к открытому ключу шифрования **Enterprise Сервера** на компьютере пользователя.
- В поле **Локальный ключевой файл Dr.Web®** укажите путь к локальному лицензионному ключевому файлу продукта Dr.Web, если хотите, чтобы лицензионный ключевой файл хранился в том числе на станции. В противном случае ключевой файл будет находиться только на Сервере.
- В поле **Периодичность отправки статистики (мин.)** введите значение временного интервала отправки Агентом статистики в минутах.
- В выпадающем списке **Язык** задайте язык интерфейса Агента.
- Установите флаг **Microsoft Network Access Protection** для включения поддержки технологии Microsoft® Network Access Protection, использующейся для мониторинга состояния станций (подробнее см. п. «Установка NAP Validator»).
- Установите флаг **Синхронизировать время** для включения синхронизации системного времени на машине Агента со временем на машине Dr.Web ES Server.
- Флаг **Запрещать модификацию системного файла HOSTS** устанавливает запрет на внесение изменения в файл HOSTS, который используется операционной системой для упрощения доступа к сети Интернет (преобразования текстовых имен некоторых сайтов в соответствующие им IP-адреса). Изменение файла HOSTS может свидетельствовать о действии вредоносных программ.
- Флаг **Запрещать модификацию важных объектов Windows** устанавливает запрет на изменение критически важных объектов операционной системы (реестр и т. п.).

На вкладке **Сеть** находятся параметры, определяющие настройки взаимодействия с Сервером:

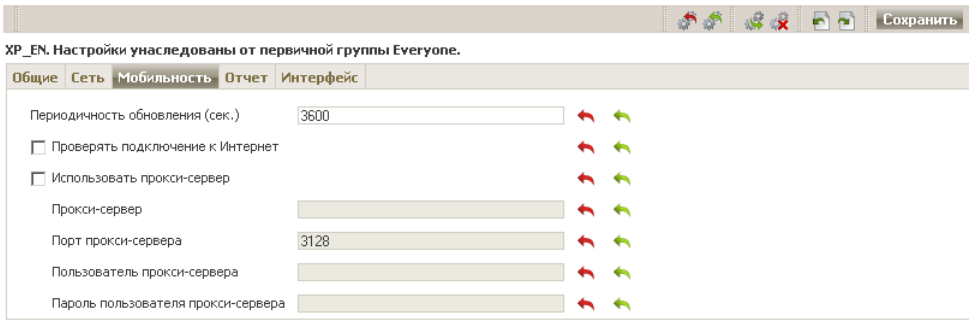


- В поле **Сервер** задается адрес **Enterprise Сервера**. Данное поле может оставаться пустым. В этом случае Агент будет использовать в качестве адреса **Enterprise Сервера** значение параметра, указанного в настройках на локальной машине пользователя (адрес Сервера, с которого производилась установка).
- Если задать некорректное/неверное значение параметра **Сервер**, то Агенты отключатся от Сервера и больше не смогут к нему подключиться. В этом случае задание адреса Сервера необходимо производить непосредственно на станции.
- В поле **Повторений поиска** задайте параметр, определяющий количество попыток поиска **Dr.Web Enterprise Server** при подключении с использованием режима Multicasting.
- В поле **Таймаут поиска (сек)** задайте промежуток между попытками поиска **Enterprise Сервера** в секундах при подключении с использованием режима Multicasting.
- Поля **Режим сжатия** и **Режим шифрования** определяют соответствующие настройки сжатия и шифрования сетевого трафика (также см. п. «Использование шифрования и сжатия трафика»).
- В поле **Слушать сканирование сети** укажите UDP-порт, используемый **Центром управления** для поиска в сети работающих **Enterprise Агентов**. Чтобы запретить прослушивание портов, введите значение **NONE**.

  Параметр задается в формате сетевого адреса.

  По умолчанию используется udp/:2193, что означает «все интерфейсы, порт 2193».

На вкладке **Мобильность** задаются параметры Мобильного режима Агента:

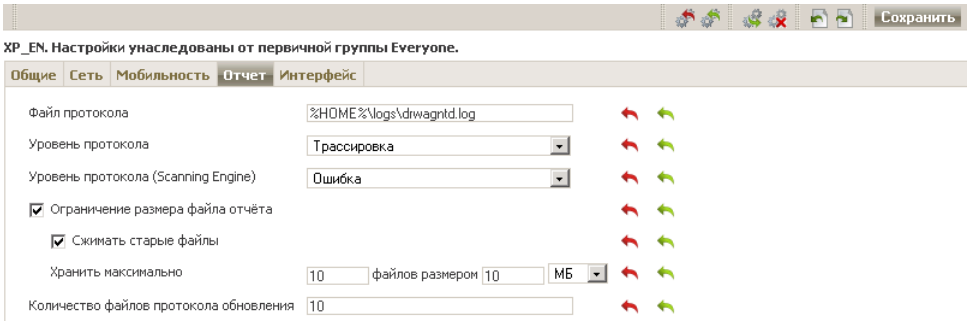


В поле **Периодичность обновлений (сек.)** укажите временной промежуток между обновлениями антивирусного ПО в секундах.

Установите флаг **Проверять подключение к Интернет** для включения проверки наличия подключения к сети Интернет перед началом процесса обновления.

Установите флаг **Использовать прокси-сервер** для использования HTTP прокси-сервера при получении обновлений из сети Интернет. При этом станут активными поля настроек используемого прокси-сервера.

На вкладке **Отчет** задаются параметры ведения протокола Агента.



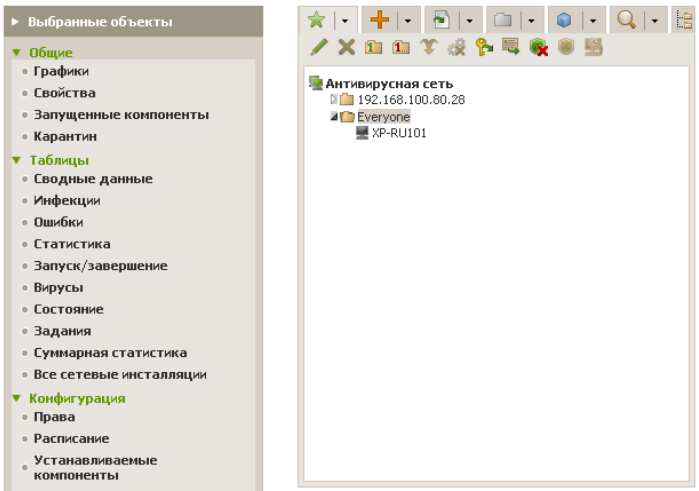
- В поле **Файл протокола** задается путь к файлу протокола и его название на компьютере пользователя.
- Параметр **Уровень протокола** определяет уровень подробности ведения протокола (подробная информация доступна в «Руководстве администратора», п. «Ведение серверного протокола»).
- Флаги: **Ограничение размера файла отчета, Сжимать старые файлы и поля: Хранить максимально <...> файлов размером <...>** определяют такие параметры логирования, как количество и размер файлов протокола, а также необходимость сжатия старых файлов.
- Параметр **Количество файлов протокола обновления** определяет максимальное количество файлов протокола обновления.

На вкладке **Интерфейс** задаются параметры интерфейса **Enterprise Агента**.

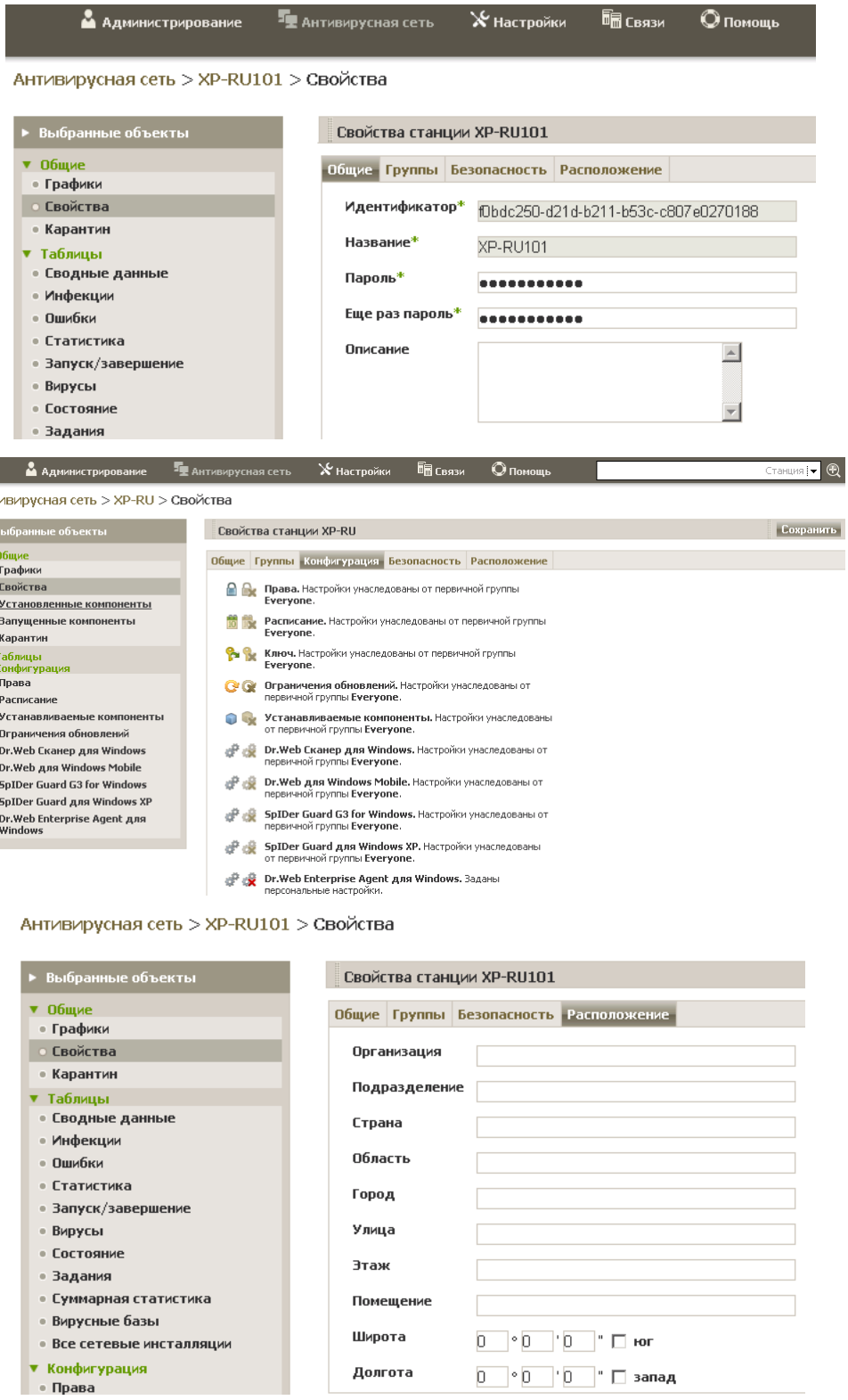
В поле **Задержка приветствия** укажите время задержки показа приветственного сообщения после запуска интерфейса Агента в минутах. Установите значение этого параметра в “–1” для запрета показа приветственного сообщения. Приветственное сообщение выводится в виде всплывающего окна, содержащего название продукта Dr.Web, его версию и информацию об авторских правах.

На вкладке **Интерфейс** вы можете отметить тип сообщений о событиях, которые будет получать пользователь. Для этого установите соответствующий флаг:

Параметры антивирусной защиты для отдельных станций и групп можно указать, выбрав соответствующую группу или станцию в разделе **Антивирусная сеть**.

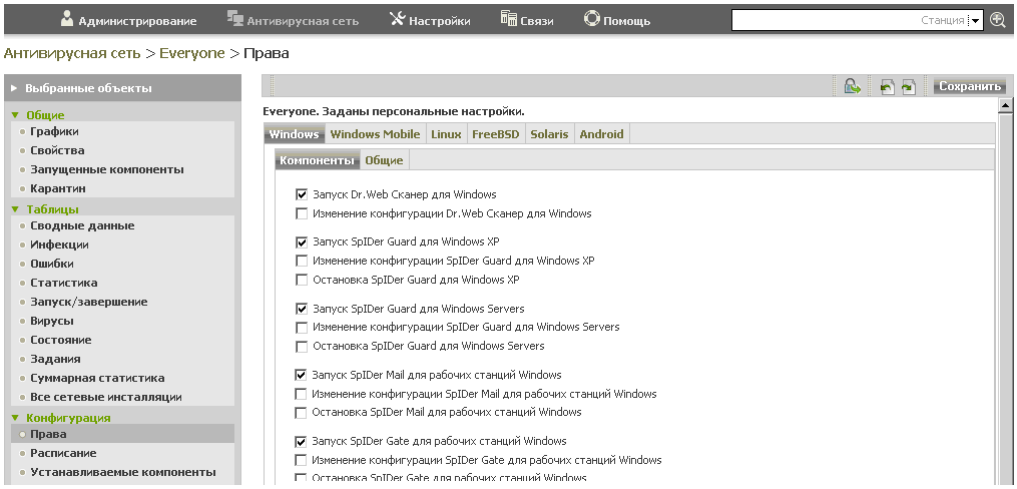


После выбора пользователя администратор может узнать текущие параметры, связанные с пользователем, выбрав пункт **Свойства** в группе **Общие**.

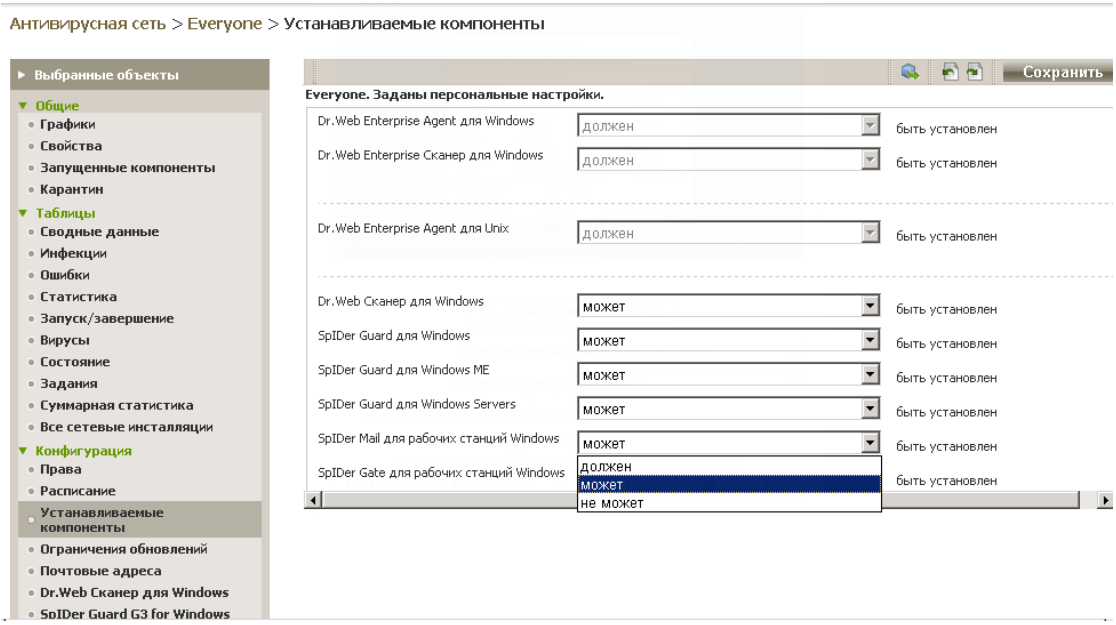


Выбрав пункт **Права** в группе **Конфигурация**, на странице **Компоненты** администратор может задать индивидуальные параметры защиты для каждого пользователя или группы, что позволяет формировать необходимые настройки в зависимости от структуры организации и функций сотрудников. В частности, на этой закладке определяется использование мобильного режима, состав запускаемых компонентов и права на изменение настроек этих компонентов самими пользователями.

Внимание! Параметры защиты различаются для сервисов защиты рабочих станций Windows (закладка Windows).



Администратор может просмотреть и определить список устанавливаемых на машине компонентов, используя пункт **Устанавливаемые компоненты** той же группы:



На этой же странице администратор может видеть список тех компонентов, установка которых разрешена или запрещена по умолчанию, а также тех, которые не установлены у пользователя.

В выпадающем списке вариант:

- **должен** — 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** — определяет возможность установки антивирусного компонента; решение об установке принимает пользователь;
- **не может** — 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.

Доступ к компонентам защиты осуществляется также в разделе **Антивирусная сеть** после выбора станции в группе **Конфигурация**.

Нажмите кнопку **Сохранить** для сохранения настроек и соответствующего изменения состава антивирусного пакета на станции.

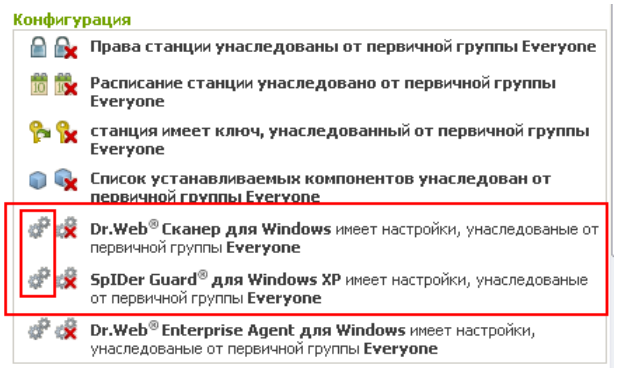
Чтобы узнать, какие вирусные базы установлены на рабочей станции:

1) Выберите пункт **Антивирусная сеть** главного меню **Центра управления**, в открывшемся окне в иерархическом списке нажмите на название станции. В открывшемся управляющем меню (панель слева) выберите из подраздела **Таблицы** пункт **Вирусные базы**.
2) Откроется информационное окно с информацией об установленных вирусных базах: название файла, содержащего конкретную вирусную базу; версия вирусной базы; количество записей в вирусной базе; дата создания вирусной базы.

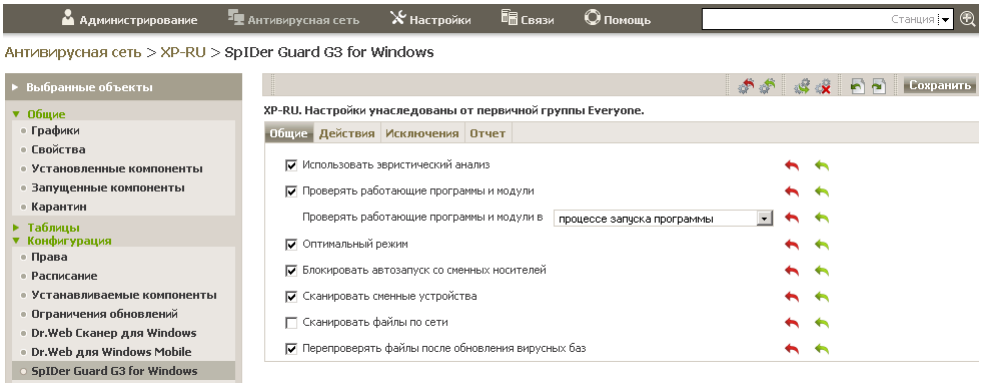
Если отображение пункта **Вирусные базы** отключено, для его включения выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**. На вкладке **Общие** установите флаг **Мониторинг вирусных баз** и **Мониторинг состояния станции**, после чего перезагрузите Сервер.

3.5.2. 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

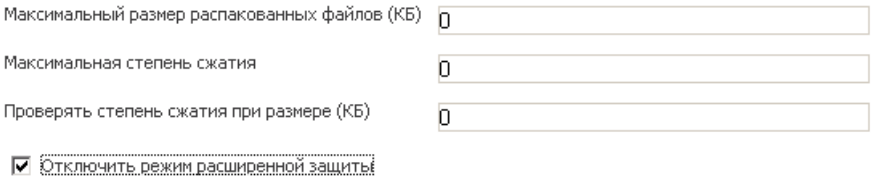
Настроить параметры защиты рабочих станций и серверов, а также групп станций можно, выделив соответствующий объект в дереве антивирусной сети и выбрав соответствующий пункт в группе настроек **Конфигурация**.



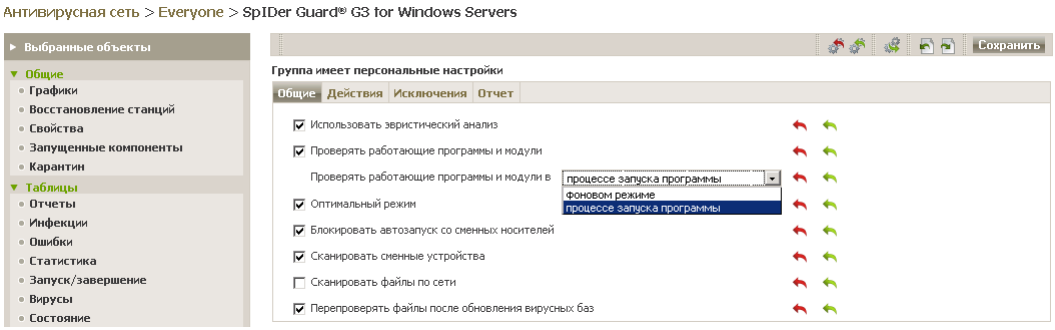
Так, для компонента **SpIDer Guard** администратор может задать параметры проверки отдельных типов файлов.



На странице **SpIDer Guard®** для Windows XP можно задать параметры, снижающие нагрузку на процессор, — например, разрешение проводить проверку только тогда, когда процессор занят фоновыми операциями.

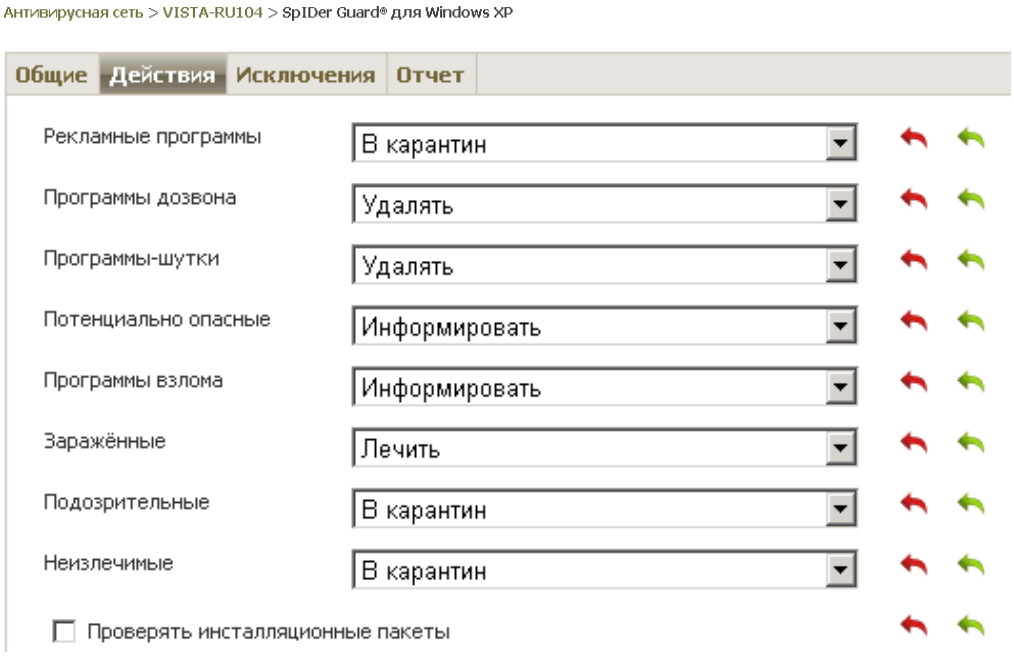


Аналогично на странице **SpIDer Guard® G3** можно выбрать режим проверки файлов.

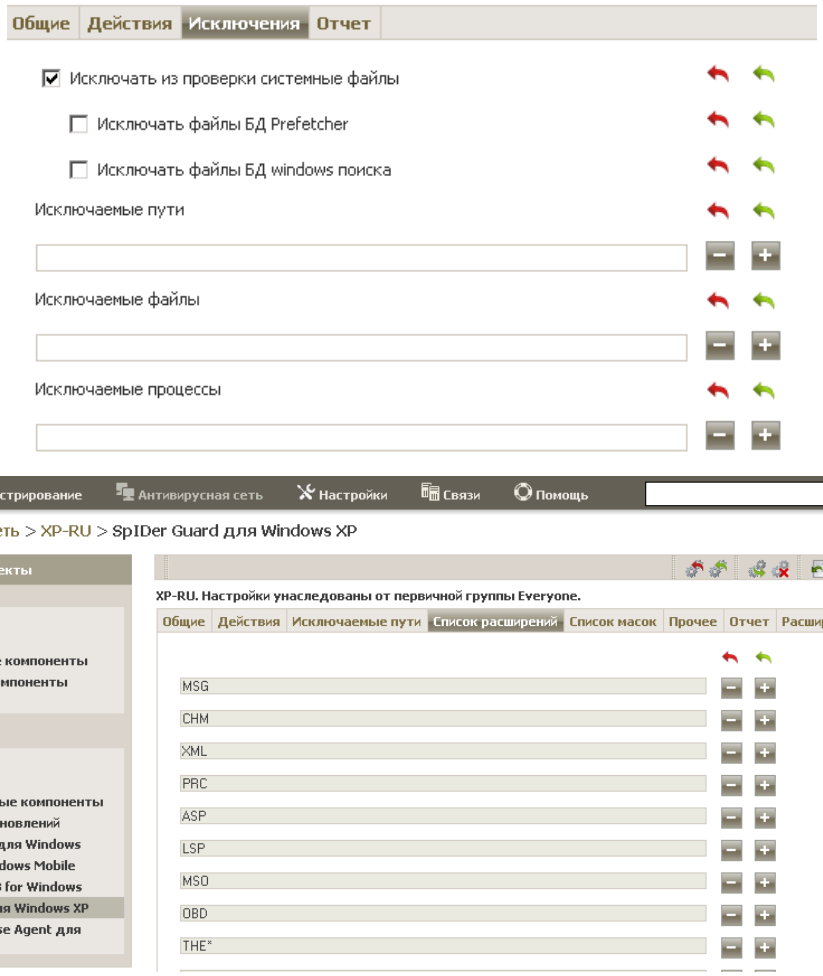


Использование значков  справа от параметров позволяет вернуть редактируемые значения либо в начальное на момент редактирования значение, либо в значение по умолчанию.

Действия программы для различных типов вредоносных объектов:



Исключаемые из проверки пути и маски файлов (что может быть полезно для ускорения проверки):



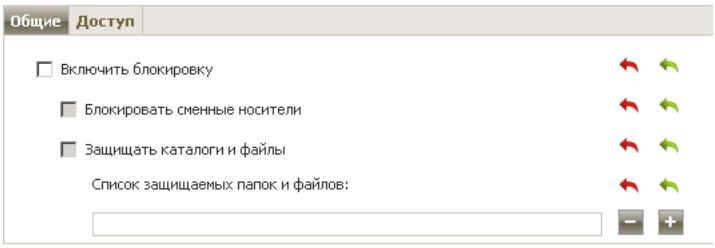
Использование значков  позволяет добавлять и удалять расширения.

В том случае, если администратор меняет настройки для конкретной станции, надпись **Станция имеет настройки, унаследованные от первичной группы <Название группы>** заменяется на **Станция имеет настройки, заданные персонально для станции**.

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.

3.5.3. Настройка доступа к защищаемым каталогам и сменным носителям

Используя возможности **Веб-интерфейса**, администратор может настроить права доступа к каталогам и сменным носителям на рабочих станциях, в том числе и для отдельных пользователей, что позволит снизить риски распространения вирусов и защитить используемые документы от повреждения вирусами. 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 **Dr.Web Офисный контроль** и, отметив **Включить блокировку**, указать тип защиты — например, вручную, добавив защищаемые каталоги.



На вкладке Общие выберите настройки блокирования и задайте ресурсы (локальные папки и файлы), к которым вы хотите запретить доступ:

- Для активизации блокировки локальных ресурсов и сменных устройств установите флаг **Включить блокировку**.
- Установите флаг **Блокировать сменные носители** для запрета доступа пользователя к сменным носителям.
- Установите флаг **Защищать каталоги и файлы** для запрета доступа к указанным ресурсам. Пути к блокируемым каталогам и файлам задаются в поле **Список защищаемых папок и файлов**. Для добавления нового пути к ресурсу нажмите на кнопку , после чего отредактируйте добавленную строку.

Если файл, доступ к которому требуется запретить, указан без пути, то он считается расположенным в папке %system32%, и в настройках **Офисного контроля** на стороне пользователя будет отображаться с префиксом c:\windows\system32.

На вкладке **Доступ** установите флаг **Фильтрация WWW**, для того чтобы настроить доступ к доменам сети Интернет. Установите флаг **Блокировать все сайты**, чтобы полностью запретить доступ к Интернету. Внесите в соответствующие списки домены, к которым необходимо разрешить/запретить доступ. Для создания новой записи нажмите на кнопку и введите значения в открывшееся поле.

В разделе **Блокировать содержимое** установите флаги напротив категорий сайтов, которые вы хотите заблокировать. Эти флаги активируют встроенный фильтр и заблокируют веб-сайты, соответствующие данным категориям.

По окончании настройки нажмите на кнопку **Сохранить**. Настройки вступят в силу после подтверждения новой конфигурации станции.

В настройках **Офисного контроля** запрещается ставить под защиту следующие папки, включая их корневые каталоги:

- `%SYSTEMROOT%,`
- `%USERPROFILE%,`
- `%PROGRAMFILES%.`

При этом допускается блокировка их подкаталогов.

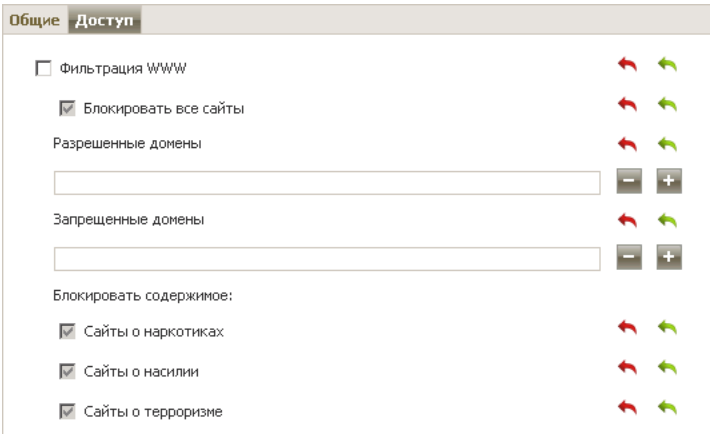
Офисный контроль не позволяет блокировать сетевые файлы и папки.

Если для станции включено разрешение редактирования конфигурации **Офисного контроля** (раздел **Права** меню **Антивирусная сеть**), пользователь будет иметь возможность самостоятельного ограничения доступа к ресурсам. При этом сохраняется возможность задания настроек на Сервере. Настройки, указанные на Сервере, будут автоматически обновляться на стороне пользователя.

В случае ошибки администратора при задании настроек **Офисного контроля** на Сервере (ошибка в пути к блокируемому ресурсу или задание запрещенной для блокировки папки) настройки обновятся на стороне пользователя, однако запрет не будет действовать. При этом об ошибке администрирования сообщено не будет.

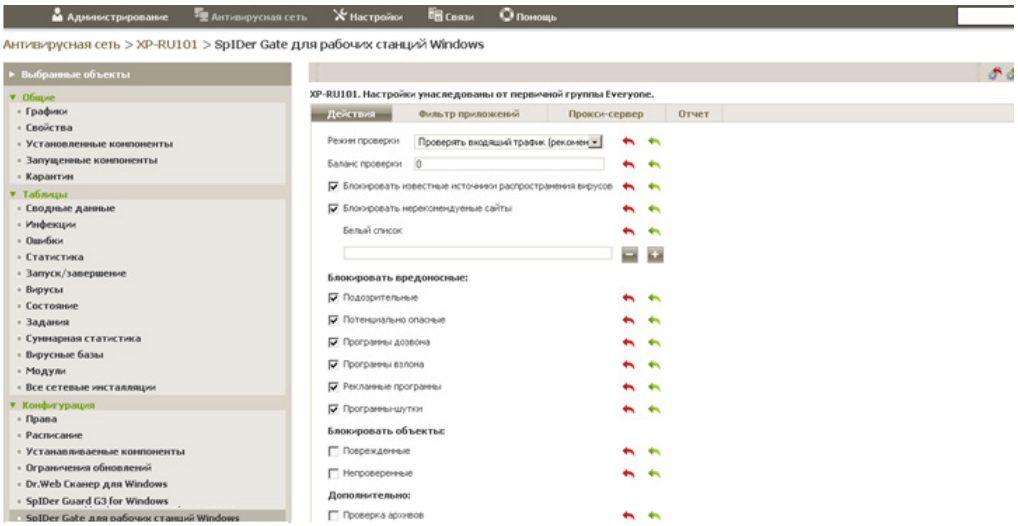
3.5.4. Настройка доступа к ресурсам и узлам сети Интернет

Ограничение доступа к ресурсам сети Интернет позволит не только уменьшить риск заражения компьютеров, но и во многих случаях поднять производительность труда сотрудников, снизить риски простоя. Для настройки параметров доступа необходимо выбрать пункт **Офисный контроль** и, отметив **Фильтрация WWW**, определить режим блокировки (**разрешать все, кроме** или **запрещать все, кроме**) отметкой **Блокировать все сайты**.

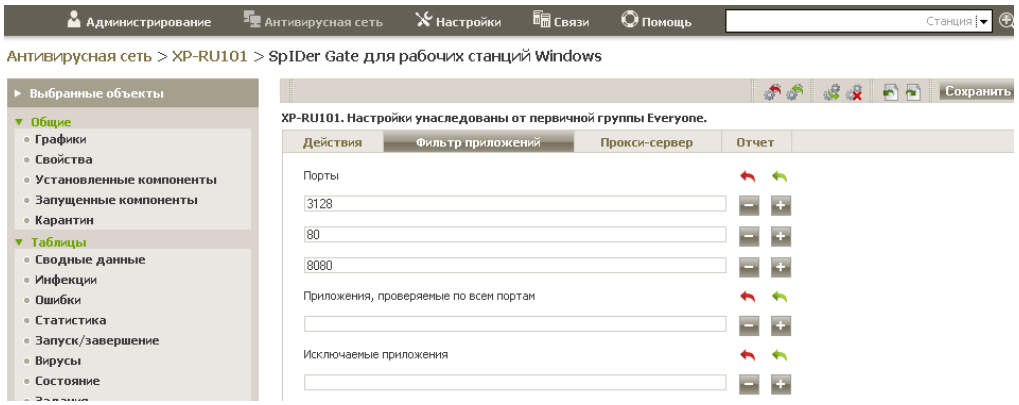


3.5.5. Настройка проверки HTTP–трафика. Выбор приложений для проверки / исключения из проверки их трафика, выбор контролируемых портов

Используя возможности компонента **Dr.Web SpIDer Gate**, администратор может гибко управлять защитой HTTP-трафика, настраивая уровень контроля различного типа программ, определяя проверяемые порты и приложения, действия при обнаружении вредоносных объектов.



На вкладке **Действия** задайте автоматическую блокировку потенциально опасных ресурсов.



В поле **Порты** вкладки **Фильтр** приложений укажите порты, обращения программ через которые необходимо проверять.

В поле **Исключаемые приложения** укажите имена исполняемых файлов программ, трафик которых не требуется проверять, например, opera.exe, firefox.exe и т. д. Для создания новой записи нажмите на кнопку и введите значения в открывшееся поле.

В поле **Приложения, проверяемые по всем портам** укажите имена исполняемых файлов веб-браузеров (например, opera.exe, firefox.exe и т. д.) и других приложений, HTTP-трафик которых будет проверяться, независимо от портов, используемых данными приложениями. Для создания новой записи нажмите на кнопку и введите значение в открывшееся поле.

Под веб-браузером сторож **SpIDer Gate** понимает любую программу, осуществляющую доступ к ресурсам по протоколу HTTP.

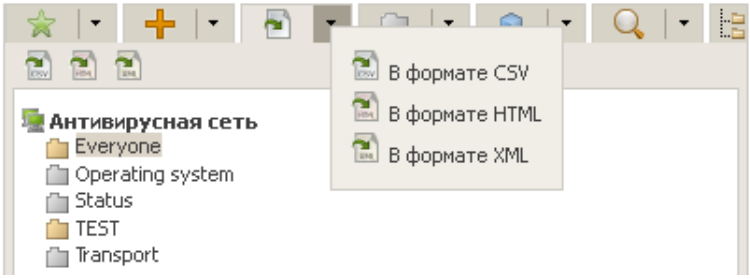
При обновлениях антивирусного ПО Dr.Web вместе с вирусными базами производится автоматическая загрузка обновленных списков адресов веб-сайтов по всем тематическим категориям.

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**.

3.5.6. Экспорт данных о станциях антивирусной сети

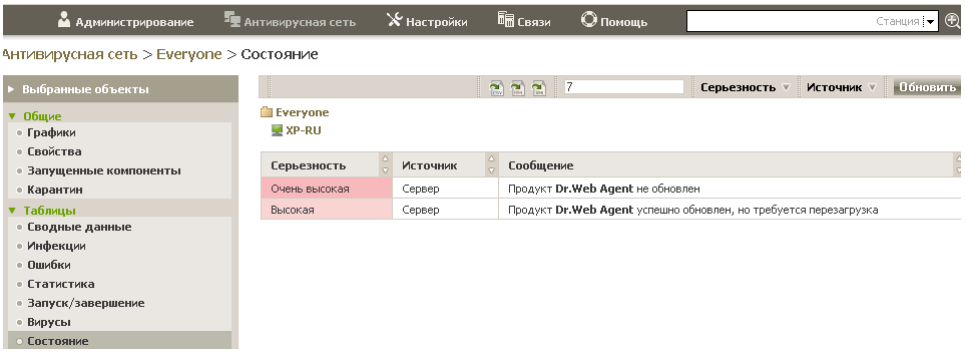
В случае необходимости администратор может сохранить все конфигурации антивирусной сети в отдельный файл, переключившись в режим показа дерева антивирусной сети и выбрав значок .



3.6. Контроль состояния защиты сети

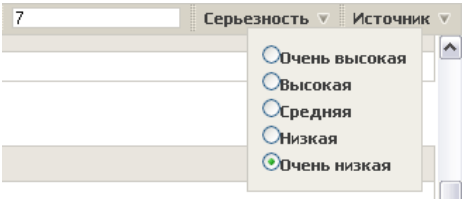
Следить за состоянием антивирусной сети, построенной на базе **Dr.Web ATM Shield**, можно с помощью таблицы состояния станций, доступной в меню **Антивирусная сеть**, а также с помощью отчетов и оповещений, формируемых антивирусным сервером.

Таблицу **Состояние**, которая показывает состояние станций, можно посмотреть, выделив в Веб-интерфейсе в дереве групп и станций группу станций или конкретную станцию, состояние которой необходимо отобразить, и выбрать в меню слева в группе настроек **Таблицы** пункт **Состояние**.

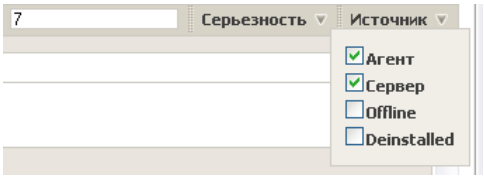


В таблице **Состояние** можно выбирать уровень минимальной серьезности отображаемых проблем. Так, если выбрать уровень **Очень низкая**, то будут отображены все сообщения о проблемах — как с очень высокой серьезностью, так и с очень низкой (информативной). Наоборот, если выбрать уровень

сообщений **Очень высокая**, 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.



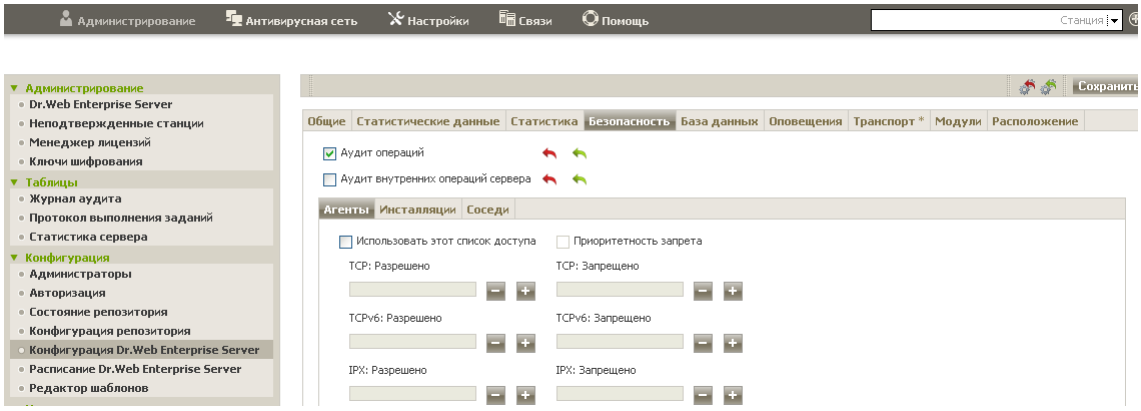
3.7. Отчеты

Dr.Web Enterprise Server ведет несколько журналов о событиях, происходящих в антивирусной сети. Среди них **Журнал аудита** и **Протокол выполнения заданий**.

Настройка параметров аудита производится на странице **Конфигурация Dr.Web® Enterprise Server** раздела **Администрирование**.

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых Агенты, сетевые инсталляторы и другие серверы смогут получать доступ к данному Серверу. Управление журналом аудита сервера осуществляется при помощи следующих флагов.

- **Аудит операций** 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 и запись журнала в БД.



На вкладке **Общие** вы также можете изменять состояние следующих флагов.

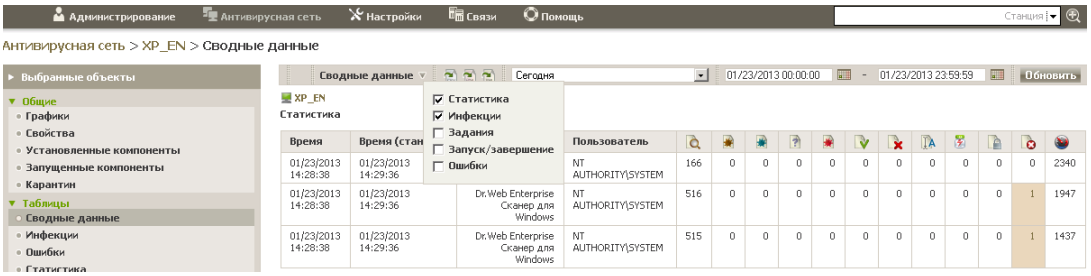
- **Показывать доменные имена** предписывает программе заносить в файл протокола не IP-адреса рабочих станций, а их доменные имена.
- **Заменять NetBios-имена** предписывает отображать в каталоге антивирусной сети **Центра управления** не наименования рабочих станций, а их доменные имена (при невозможности определения доменных имен отображаются IP-адреса).

Внимание!

- Флаги **Показывать доменные имена** и **Заменять NetBios-имена** по умолчанию сняты. При неправильной настройке службы DNS их включение может значительно замедлить работу Сервера. При включении любого из этих режимов рекомендуется разрешить кеширование имен на DNS-сервере.
- Если флаг **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:

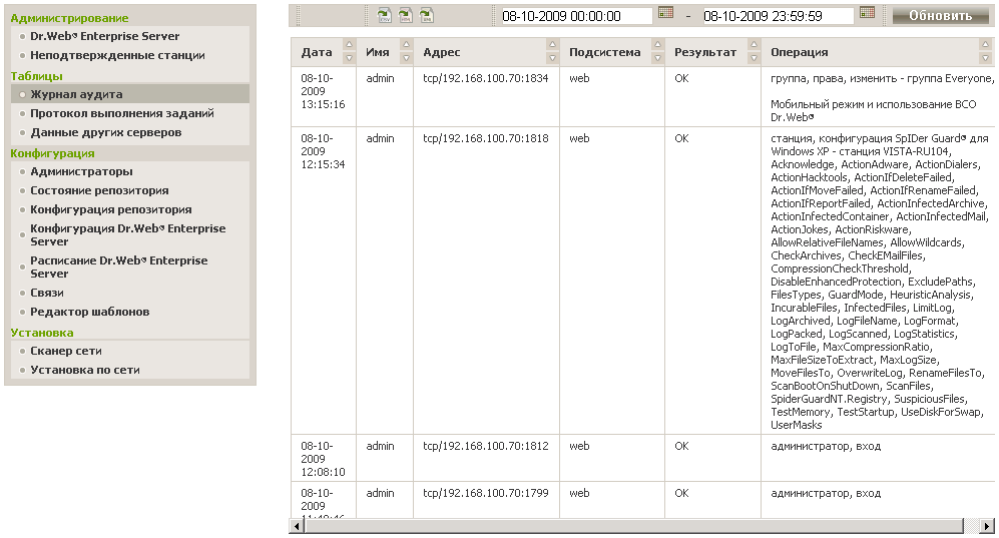
1) Выберите пункт **Антивирусная сеть** главного меню **Центра управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите в разделе **Таблицы** пункт **Сводные данные**.
2) Откроется окно, содержащее табличные данные отчета. Для того чтобы включить в отчет определенные статистические данные, нажмите на кнопку **Сводные данные** 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 **Таблицы**. 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 **Записать данные в файл в формате CSV**, **Записать данные в файл в формате HTML** или **Записать данные в файл в формате XML**.

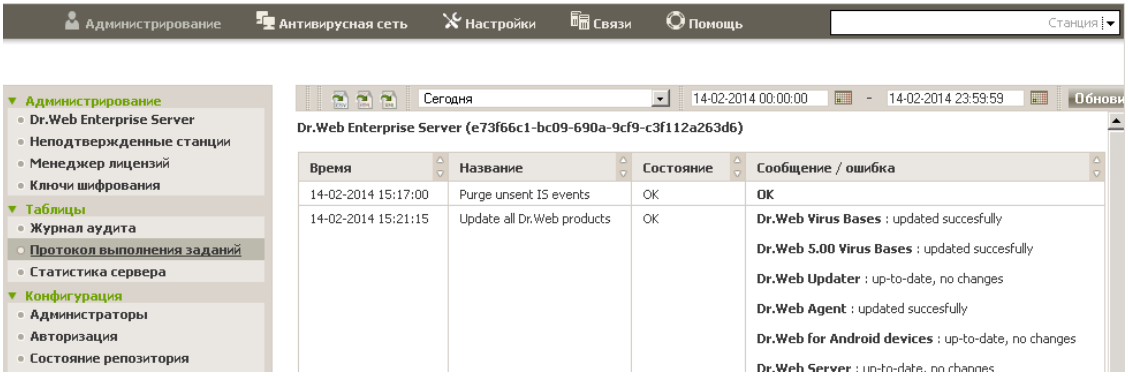
3.7.1. Аудит действий администраторов

Журнал аудита содержит информацию о действиях администраторов локальной сети. Таким образом, в случае необходимости возможности Веб-интерфейса позволяют проверить все проведенные администраторами сети действия. Журнал можно отобразить в Веб-интерфейсе, перейдя в раздел **Администрирование** и выбрав пункт **Журнал аудита**. Диапазон дат можно задать, используя значки календаря слева от дат, расположенных непосредственно над журналом.



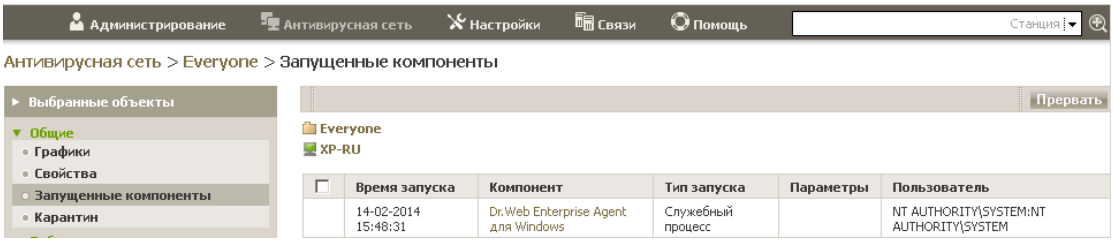
3.7.2. Анализ выполнения заданий

Протокол выполнения заданий содержит отчет об успешности или неуспешности выполнения заданий, запланированных к выполнению антивирусным сервером. Его можно отобразить в Веб-интерфейсе, если перейти в раздел **Администрирование** и выбрать пункт **Протокол выполнения заданий**. Диапазон дат можно задать, используя значки календаря слева от дат, расположенных непосредственно над журналом.



3.7.3. Контроль запущенных процессов

Администратор может контролировать все запущенные процессы. Для этого необходимо выбрать пользователя, а затем пункт **Запущенные компоненты**.



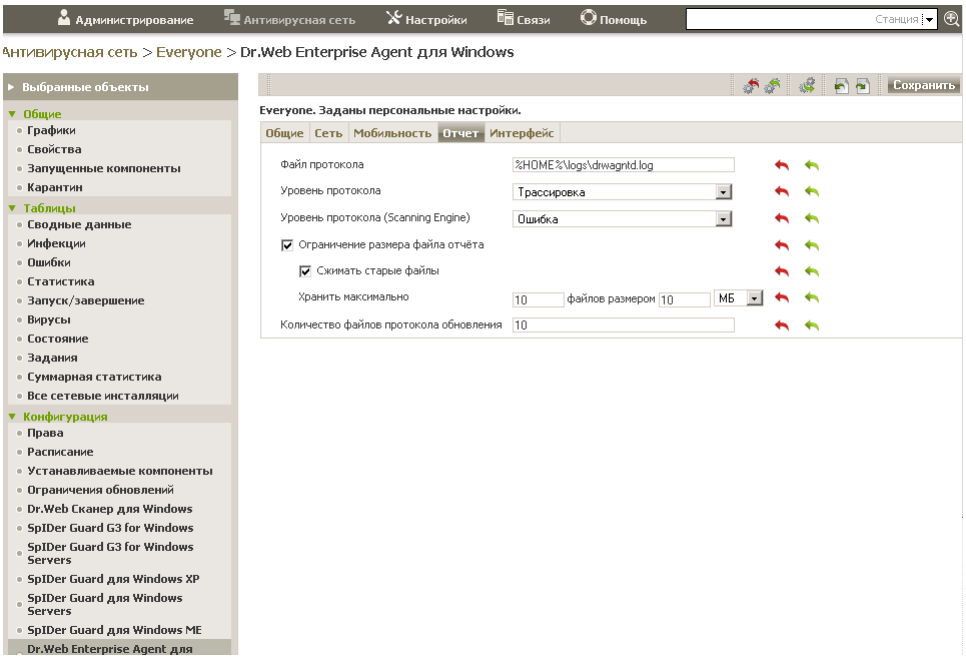
В списке отображаются в том числе и процессы, запущенные пользователем.

В случае необходимости администратор может прервать выполнение любого из них, используя кнопку Прервать.

Администратор имеет возможность, выбрав интересующий его компонент, отредактировать его настройки.

3.7.4. Создание отчетов по компонентам

В случае необходимости администратор может автоматизировать создание отчетов по каждому из компонентов антивирусной защиты, указывая при этом интересующую его степень подробности отчета. Для этого необходимо выбрать интересующий компонент защиты в группе **Конфигурация**.

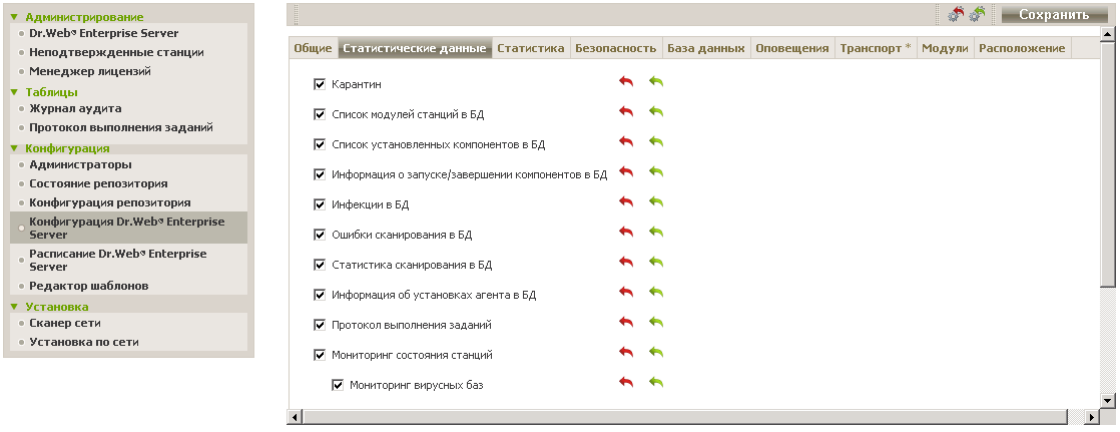


3.8. Сбор статистики. Формирование графиков активности вирусов, статистики по найденным типам вредоносных объектов, произведенным над ними действиям

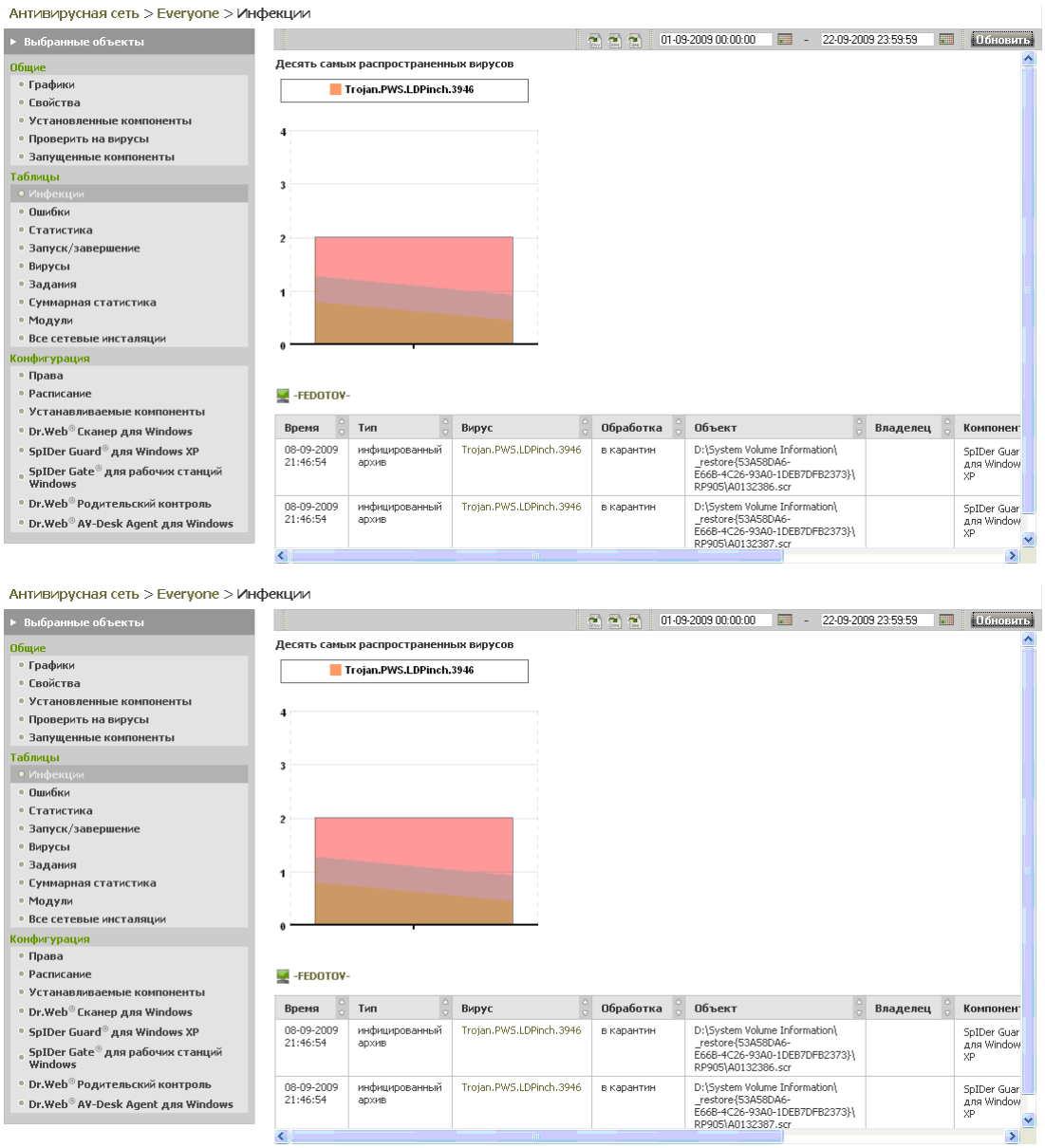
Используя возможности Веб-интерфейса, администратор может формировать отчеты о состоянии антивирусной защиты, в том числе о количестве обнаруженных вредоносных объектов, произведенных над ними действий.

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 в разделе **Конфигурация Dr.Web® Enterprise Server** меню **Администрирование**.

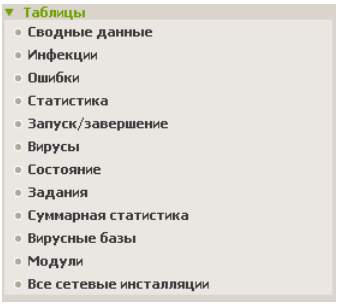


Просмотр активности вирусов производится с использованием возможностей страницы **Инфекции** группы функций **Таблицы**. На этой странице администратор может задавать интересующий его диапазон дат. Просмотр статистики возможен не только для отдельных пользователей, но и для групп и сети в целом.



Для просмотра таблиц 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 подраздела **Таблицы**.

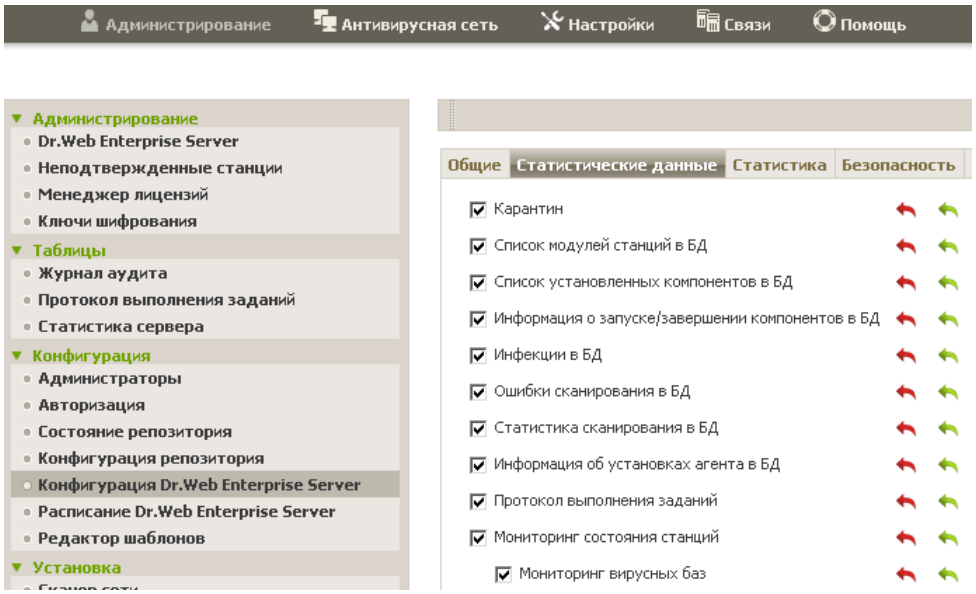
Раздел меню **Таблицы** содержит следующие пункты.



- **Сводные данные** — для просмотра и сохранения отчетов, содержащих все сводные статистические данные или выборочные сводки по заданным типам таблиц.
- **Инфекции** — для просмотра информации об обнаружении вирусов (перечень зараженных объектов, вирус, действия антивируса и т. п.).

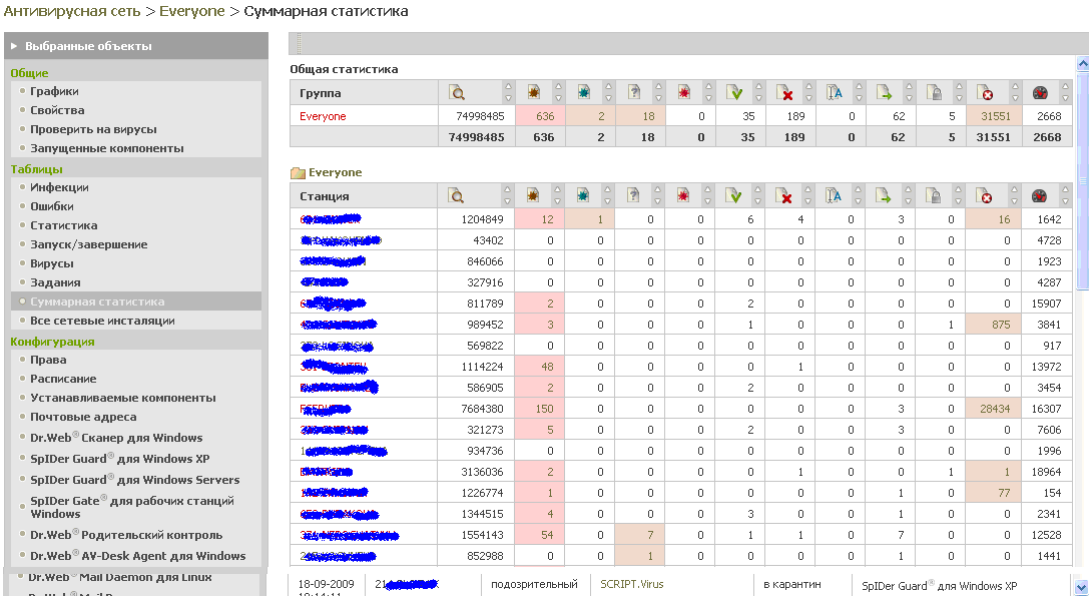
- **Ошибки** – для просмотра списка ошибок сканирования на выбранной рабочей станции за определенный период.
- **Статистика** – для получения статистики о работе антивирусных средств на рабочей станции.
- **Запуск/завершение** – для просмотра списка компонентов, запускавшихся на рабочей станции.
- **Вирусы** – для просмотра сведений об обнаружении вирусов на станции, сгруппированных по типам вирусов.
- **Состояние** – для просмотра сведения о необычном и (возможно) требующем вмешательства состоянии рабочих станций за определенный период.

  Для отключения отображения пункта **Состояние** выберите пункт **Администрирование** → **Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** снимите флаг **Мониторинг** состояния станции, после чего нажмите **Сохранить** и перезагрузите Сервер.



- **Задания** – для просмотра списка заданий, назначенных для рабочей станции в заданный период.

  Для отключения отображения/активности пункта **Задания** выберите пункт **Администрирование** → **Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** снимите флаг **Протокол выполнения заданий**, после чего нажмите **Сохранить** и перезагрузите Сервер.
- **Суммарная статистика** – для администратора доступны также суммарная статистика в виде таблицы по пользователям и группам без разбиения на сеансы.



- **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 станций.

  Для отключения отображения пункта **Вирусные базы** выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** снимите флаги **Мониторинг вирусных баз** и **Мониторинг состояния станции**, после чего нажмите **Сохранить** и перезагрузите Сервер.
- **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.
- **Все сетевые инсталляции** — для просмотра списка установок ПО на рабочую станцию.

  Для отключения отображения пункта **Все сетевые инсталляции** выберите пункт **Администрирование** главного меню, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** снимите флаг **Информация об установках агента в БД**, после чего нажмите **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 **Таблицы** при помощи **Центра управления**.

  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 с помощью клавиш **SHIFT** или **CTRL**.
2) В управляющем меню (панель слева) в разделе **Таблицы** выберите пункт **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 **Общая статистика** 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 в удобный формат, нажав на одну из кнопок  : **Записать**

данные в файл в формате CSV, Записать данные в файл в формате HTML или **Записать данные в файл в формате XML**.

10) Для того чтобы получить суммарную статистику без разбиения на сеансы, нажмите на пункт **Суммарная статистика** в управляющем меню. Откроется окно суммарной статистики.

11) Для того чтобы просмотреть статистику по вирусным событиям в форме диаграмм, в управляющем меню (панель слева) выберите пункт **Графики**. Откроется окно просмотра статистических диаграмм (подробное описание см. ниже).

Чтобы просмотреть сведения о необычном и (возможно) требующем вмешательства состоянии рабочих станций за определенный период:

1) Выберите в управляющем меню в разделе **Таблицы** пункт **Состояние**.

   Если пункт **Состояние** не отображается в управляющем меню, то выберите пункт **Администрирование → Конфигурация Dr.Web Enterprise Server**. На вкладке **Статистические данные** установите флаг **Мониторинг состояния 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 **Очень низкая**, что соответствует отображению максимального списка.

4) В список также будут включены станции, в течение определенного числа дней не имевшие связи с Сервером. Введите это число в поле ввода слева от списка **Серьезность**. При превышении данного значения ситуация считается критической, и данная информация будет отображаться в окне раздела **Состояние**.

5) Действия по детализации и форматированию информации данной таблицы аналогичны описанным выше для таблицы статистики.

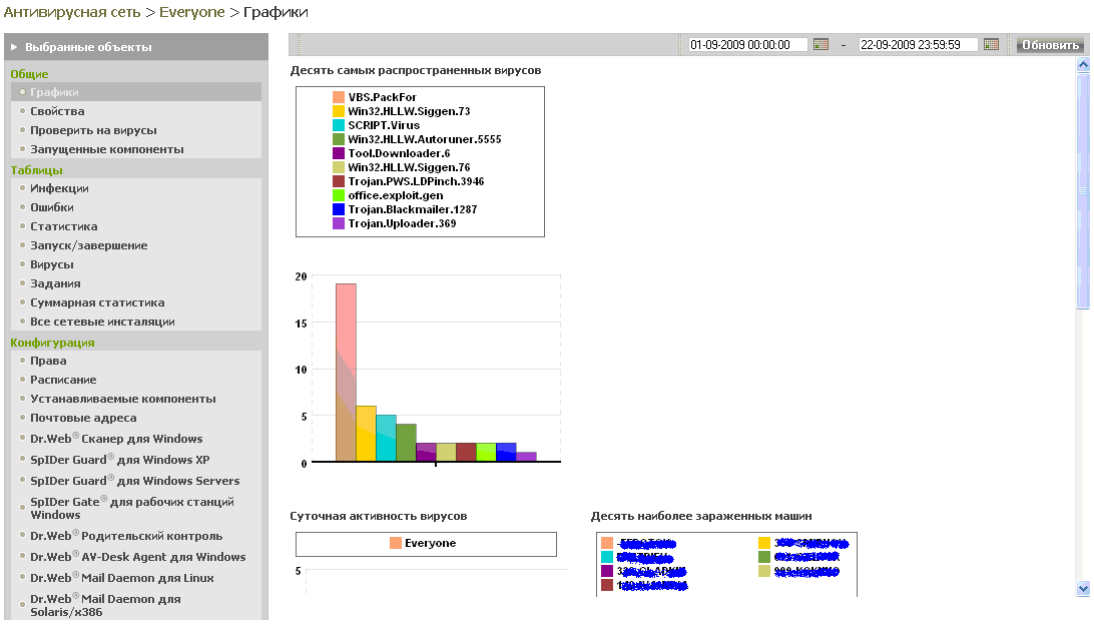
Вы также можете просмотреть результаты работы и статистику нескольких рабочих станций. Для этого необходимо отметить эти станции в каталоге сети.

Для просмотра графиков активности вирусов:

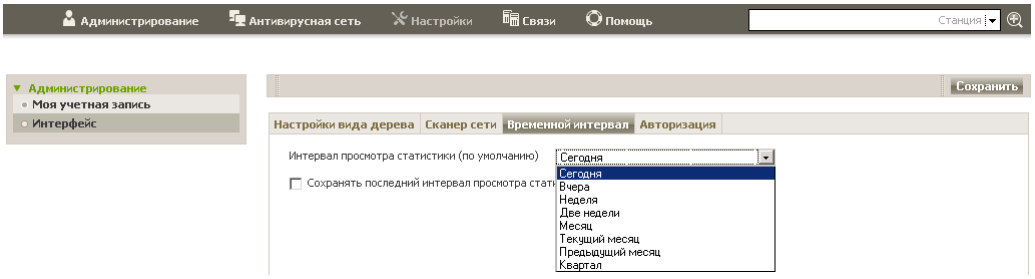
1) Выберите пункт **Антивирусная сеть** главного меню **Центра управления**, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В открывшемся управляющем меню (панель слева) выберите в разделе **Таблицы** пункт **Графики**.

2) Откроется окно, содержащее следующие графические данные:
   - **Суточная активность вирусов** — заданный временной период разбивается по суткам. На графике отображается общее количество вирусов, найденных в пределах каждых суток для всех выбранных объектов сети (станций и групп).
   - **Десять самых распространенных вирусов** — приводится список из десяти вирусов, инфицировавших наибольшее количество файлов. На графике отображаются численные данные по объектам, которые были заражены указанными вирусами.
   - **Виды инфекций** — отображаются численные данные по объектам, которые были заражены указанными видами инфекций.
   - **Произведенные действия** — отображаются численные данные по инфицированным объектам, над которыми были совершены действия, предусмотренные антивирусным ПО.

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**.



Администратор имеет возможность задания интервала просмотра статистики по умолчанию, а также сохранения интервала, который был выбран последним при просмотре статистики. Для этого необходимо выбрать в разделе **Настройки** раздел **Временной интервал** в меню **Интерфейс**. В выбранном разделе при помощи списка **Интервал** просмотра статистики (по умолчанию) можно задать интервал просмотра статистики, а при помощи опции **Сохранять последний интервал просмотра статистики** всегда сохранять тот интервал, который был выбран последним при просмотре статистики.



3.9. Управление серверным карантином

Для управления содержимым серверного карантина необходимо выбрать в меню **Антивирусная сеть** интересующую станцию или группу и затем пункт **Карантин**, находящийся в разделе **Общие**.

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 XP с SP2 и выше, Windows 2003 с SP1 и выше, Windows Vista и выше.

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 значки . После выбора интересующего периода необходимо нажать на кнопку **Обновить**.

В базу **Карантина** может быть перемещен любой зараженный или подозрительный объект. Для каждого объекта, перемещенного в Карантин, фиксируется следующая информация:

- дата и время перемещения в Карантин;
- название вируса;

- (в случае необходимости) электронный адрес отправителя письма, содержавшего зараженный объект;
- тема письма, содержавшего зараженный объект;
- электронные адреса получателей письма, содержавшего зараженный объект;
- имя зараженного файла.

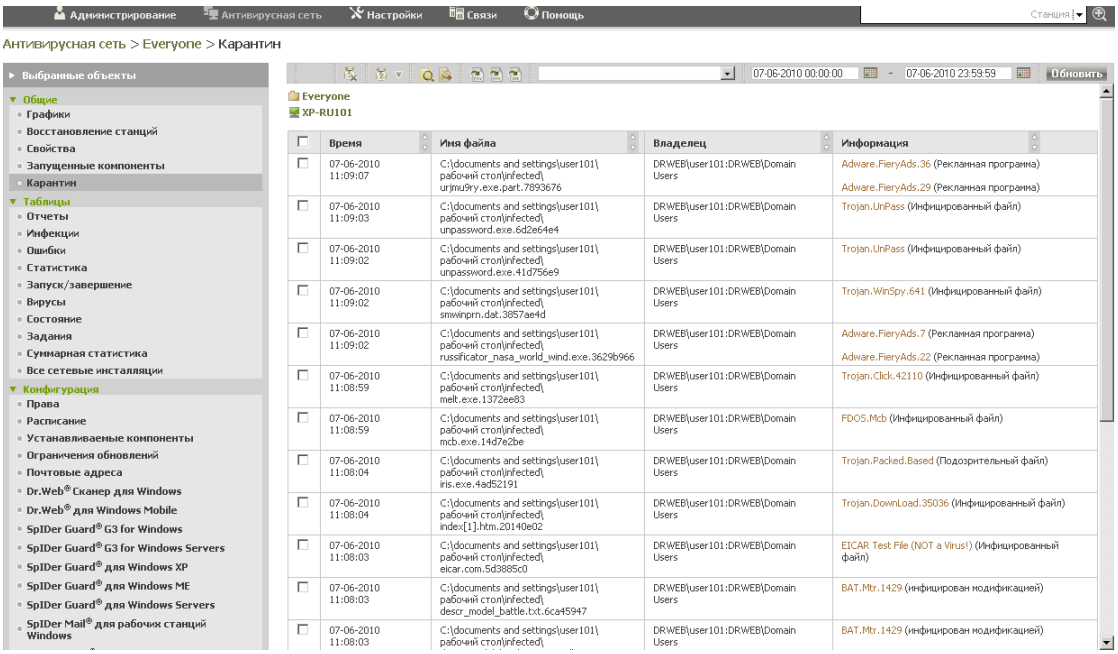
Для восстановления файлов необходимо, предварительно выбрав станцию в разделе **Антивирусная сеть** и перейдя в раздел **Карантин**, выбрать интересующий файл или группу файлов, а затем выбрать значок и в выпадающем меню указать один из вариантов:

- восстановить первоначальное местоположение файла на компьютере (восстановить файл в папку, в которой он находился до перемещения);
- переместить файл в папку, указанную администратором.

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).



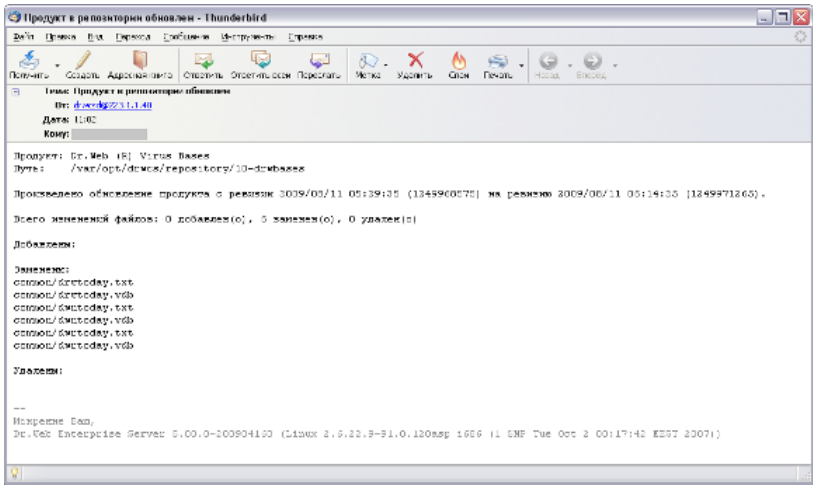
Также возможно экспортировать данные о состоянии Карантина в файл в формате: CSV, HTML, XML.

3.10. Оповещения

Сервер **Dr.Web Enterprise Security Suite** может автоматически сообщать о проблемах, обнаруживаемых в функционировании антивирусной сети 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.

Например, оповещение администратора ES-сервера о том, что заканчивается срок действия серверного ключа **Срок действия серверной лицензии истек** (Server license has expired), содержит предупреждение «Серверная лицензия закончилась, с этого момента сервер не будет позволять подключаться клиентам» (The server license was expired, it will not allow client connections since now).

В качестве примера уведомления можно привести следующее письмо:



- **Критические оповещения** — получать только критические оповещения. К ним относятся периодические напоминания:
  - об ошибке обновления антивирусного ПО или какого-либо из его компонентов;
  - о необходимости перезагрузки компьютера после обновления.

  Сообщение выводится только в том случае, если пользователь имеет права администратора.
- **Оповещения о вирусах** — получать только оповещения о вирусах. К данному типу оповещений относятся сообщения об обнаружении вируса (вирусов) одним из компонентов антивирусного ПО.
- **Важные оповещения** — получать только важные оповещения. К ним относятся сообщения:
  - об ошибках при запуске какого-либо из компонентов антивирусного ПО;
  - об ошибках обновления антивирусного ПО или какого-либо из его компонентов, отображается сразу после ошибочного завершения процедуры обновления;
  - о необходимости перезагрузки компьютера после обновления, отображается сразу после обновления;
  - о необходимости ожидания сообщения о требовании перезагрузки для окончании установки компонентов.
- Малозначительные оповещения — получать только малозначительные оповещения. К ним относятся сообщения:
  - о запуске удаленного сканирования;
  - о завершении удаленного сканирования;
  - о запуске обновления антивирусного ПО или какого-либо из его компонентов;
  - об успешном завершении обновления антивирусного ПО или какого-либо из его компонентов (без необходимости перезагрузки).

Если вы хотите, чтобы пользователь получал все группы сообщений, установите все четыре флага. В противном случае будут выводиться только сообщения указанных групп.

Пользователь может управлять получением оповещений, кроме **Критических оповещений**, получение которых настраивает только администратор.

Рекомендуется, чтобы агент сообщал пользователю как минимум о **Критических оповещениях** и **Оповещениях о вирусах**. В дальнейшем пользователь сможет самостоятельно включить/отключить те или иные оповещения на своем компьютере, кликнув правой кнопкой мыши на значке агента в трее и выбрав пункт **Настройки**.

3.10.1. Настройка предопределенных правил оповещений. Выбор способа реакции на инциденты

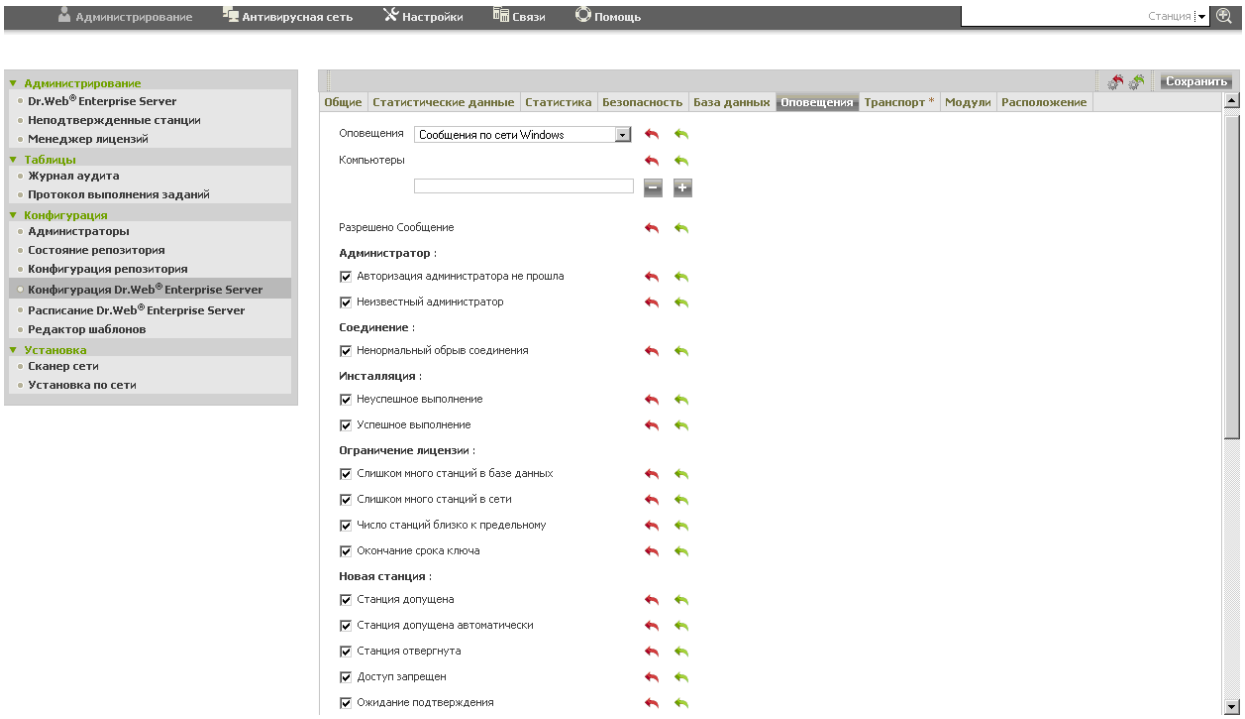
Для централизованной настройки оповещений о событиях, происходящих на компьютере клиента (обновлениях, ошибках, найденных вирусах и т. д.), администратор антивирусной сети должен выбрать группу (например, **Everyone**, если необходимо осуществить настройку для всех агентов) и в панели справа выбрать пункт **DrWeb Enterprise Agent для Windows**, перейти на вкладку **Интерфейс** и отметить те сообщения, которые будут показываться пользователю. Рекомендуется, чтобы агент сообщал пользователю как минимум о **Критических оповещениях** и **Оповещениях о вирусах**. В дальнейшем пользователь сможет самостоятельно включить/отключить те или иные оповещения на своем компьютере, кликнув правой кнопкой мыши на значке агента в трее и выбрав пункт **Настройки**.

Для того чтобы настроить автоматические оповещения, необходимо в Веб-интерфейсе перейти в раздел **Администрирование** и выбрать пункт **Конфигурация Dr.Web® Enterprise Server**, а затем перейти на вкладку **Оповещения**, где в меню **Оповещения** необходимо выбрать интересующий тип оповещений.

- **Не включать** — не посылать оповещений (режим по умолчанию),
- **Электронная почта** — посылать по электронной почте,
- **Сообщения по сети Windows** — посылать, используя Windows Messenger (только для Сервера под ОС Windows).

Внимание! Если сервер был инсталлирован на платформе Windows, администратор имеет возможность посылать уведомления средствами NetSend: в меню появляется пункт **Сообщения по сети Windows**.

Если выбран тип **Сообщения по сети Windows**, то откроется следующее окно:

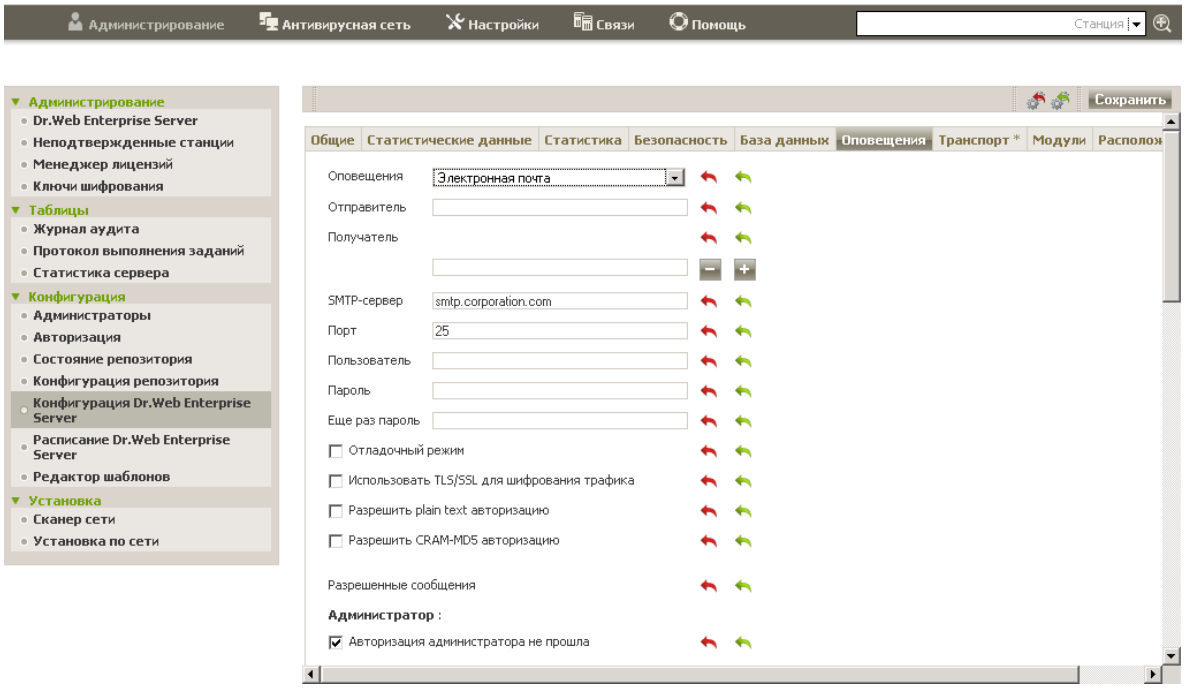


Для сообщений в сети ОС Windows задайте список имен компьютеров получателей сообщений.

Для добавления нового поля нажмите на кнопку и введите название компьютера в появившемся поле. Для удаления поля нажмите на кнопку .

В разделе **Разрешено сообщение** установите флаги для тех событий, сообщения о которых будут отсылаться.

Если администратор откроет меню **Оповещения** и выберет **Электронная почта**, то панель оповещений примет следующий вид:



В этом окне можно настроить параметры почтового ящика (используя поля **Отправитель** и **Получатель**), на который будут отправляться оповещения, а также типы событий, информация о которых будет отправляться. Задайте следующие параметры:

- адреса отправителя сообщения,
- адрес получателя сообщения,
- адрес SMTP-сервера, на который следует отправлять электронную почту,
- при необходимости имя пользователя и пароль для авторизации на SMTP-сервере.

Установите флаг **Отладочный режим** для получения детального протокола SMTP-сессии.

При необходимости установите соответствующие флаги для использования шифрования и авторизации.

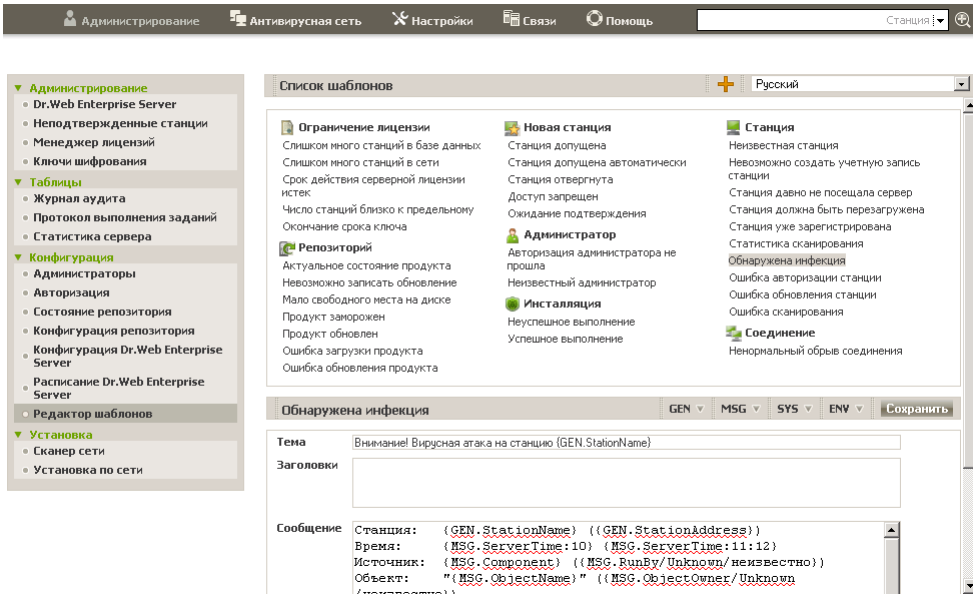
В разделе **Разрешено сообщение** установите флаги для тех событий, сообщения о которых будут отсылаться по электронной почте.

3.10.2. Редактирование шаблонов предопределенных оповещений

Текст сообщения определяется шаблоном сообщения. Шаблоны сообщений хранятся в подкаталоге var/templates каталога установки Сервера. Вы можете настроить текст сообщения, отсылаемого при определенном событии, отредактировав соответствующий шаблон.

При подготовке сообщения система оповещения заменяет переменные шаблона (в фигурных скобках) на конкретный текст, зависящий от ее текущих настроек.

Для редактирования шаблона оповещения администратор должен перейти в **Редактор шаблонов** раздела **Администрирование** и выбрать название интересующего его оповещения. Например, **Обнаружена инфекция**. Язык сообщения выбирается в выпадающем меню вверху страницы.



- В поле **Тема** можно отредактировать тему посылаемого сообщения.
- В поле **Заголовки** при необходимости задаются дополнительные заголовки электронного письма.
- В поле **Сообщение** задается шаблон текста сообщения.

Для добавления переменных можете использовать выпадающие списки в заголовке сообщения.

Для сохранения измененного шаблона нажмите на кнопку **Сохранить**.

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.

3.10.3. Отправка сообщений пользователю

В случае необходимости администратор может отправить пользователю сообщение произвольного содержания, включающее:

- текст сообщения;
- гиперссылки на интернет-ресурсы;
- логотип компании (или любое графическое изображение);
- в заголовке окна также указывается точная дата получения сообщения.

Данные сообщения выводятся на стороне пользователя в виде всплывающих окон.

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 компании в сообщении** — установите данный флаг, 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 с логотипом** и выбрать необходимый объект в открывшемся браузере по файловой системе.

Также вы можете задать заголовок сообщения или название компании в поле **Название**. Данный текст будет отображен в заголовке окна сообщения (справа от логотипа). Если данное поле останется пустым, то на его месте в окне сообщения будет выведен текст, содержащий информацию об Агенте.

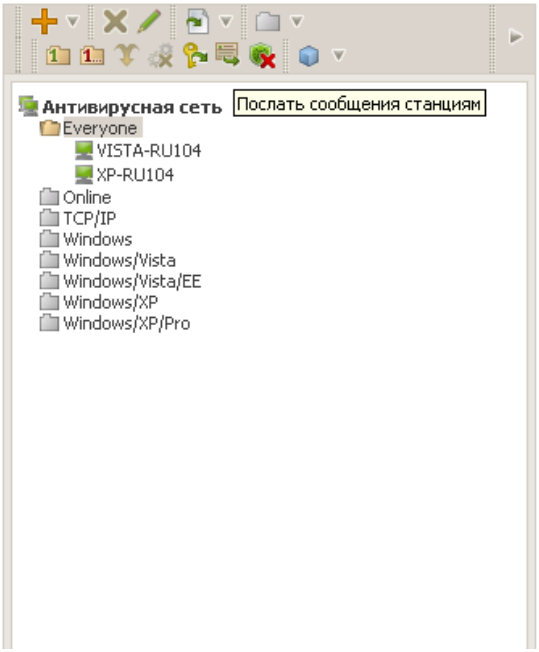
В поле **URL** можно указать ссылку на веб-страницу, которая будет открыта при нажатии на логотип (а также при нажатии на заголовок окна, если он был указан в поле **Название**).

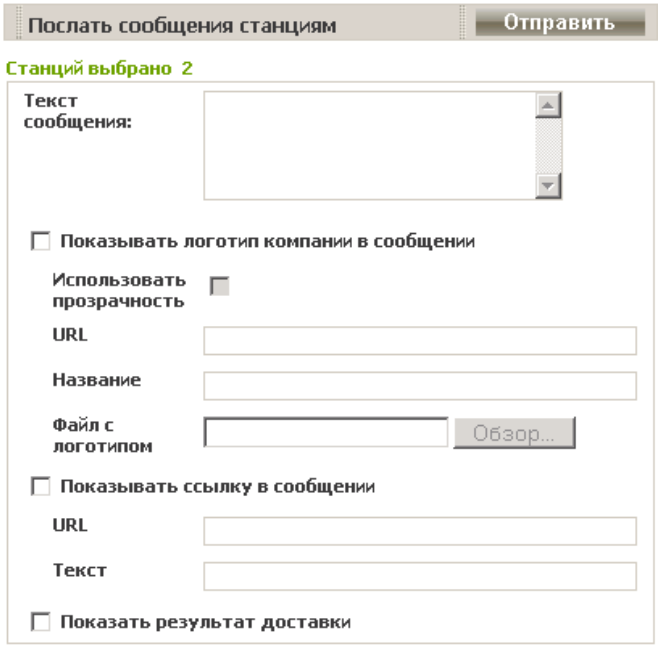
Если логотип не задан или размер логотипа превышает максимально допустимый, то на его месте в окне сообщения будет отображен значок **Enterprise Агента.**

При установленном флаге **Показывать логотип компании в сообщении** становится активным флаг **Использовать прозрачность**. Установите этот флаг для использования прозрачности в изображении логотипа.

- Показывать ссылку в сообщении — установите этот флаг, 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).

По умолчанию уведомление о доставке выключено, включить его можно, выбрав пункт **Показать результат доставки**.

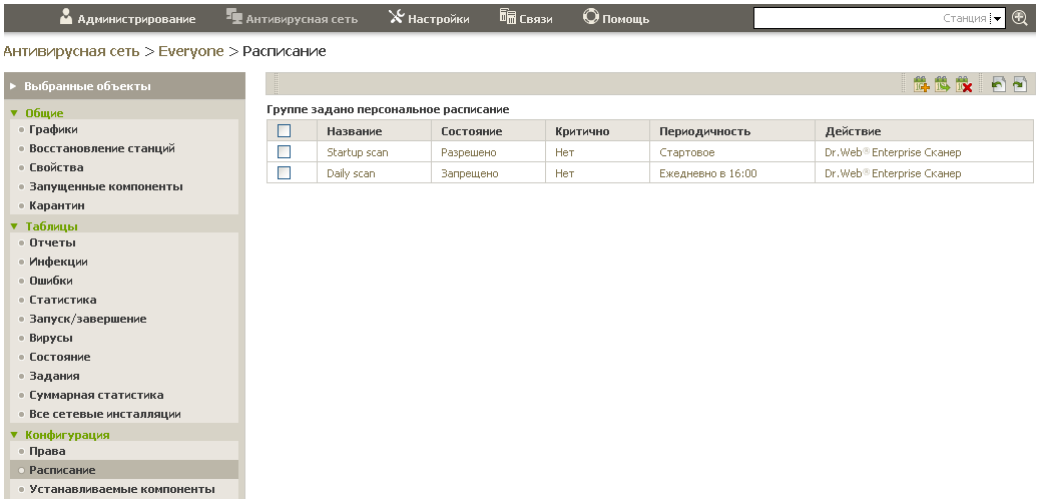




Перед отправкой пользовательского сообщения (особенно многоадресного) рекомендуется предварительно отправить его на любой компьютер с установленным Агентом, чтобы проверить корректность результата.

3.11. Расписание

Важной функцией системы управления является возможность настройки заданий. Так, например, для каждого пользователя администратор может добавлять и отменять задания, используя страницу **Расписание**. Для этого необходимо выделить пользователя или их группу в разделе **Антивирусная сеть** Веб-интерфейса, а затем выбрать пункт **Расписание** в группе **Конфигурация**.



Расписание — 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, **Enterprise Агент** позволяет выполнять некоторые другие типы действий, описанные ниже.

Расписания бывают двух типов:

- **Централизованное расписание**. Расписание, задаваемое администратором антивирусной сети и подчиняющееся всем правилам наследования конфигураций.
- **Локальное расписание станции**. Расписание, задаваемое пользователем на конкретной станции (при наличии у данной станции прав), хранящееся локально на этой станции; данное расписание не является объектом, управляемым **Enterprise Сервером**.

3.11.1. 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 Веб-интерфейса. Однако администратор может задать отдельные настройки расписания для каждой отдельной группы или пользователя. Для настройки расписания необходимо выбрать группу или пользователя в каталоге антивирусной сети в разделе **Антивирусная сеть** Веб-интерфейса, и в меню, расположенном слева, выбрать меню пункт **Расписание**. Настройка расписания станций, входящих в другие группы, а также расписание отдельных станций производится аналогично.

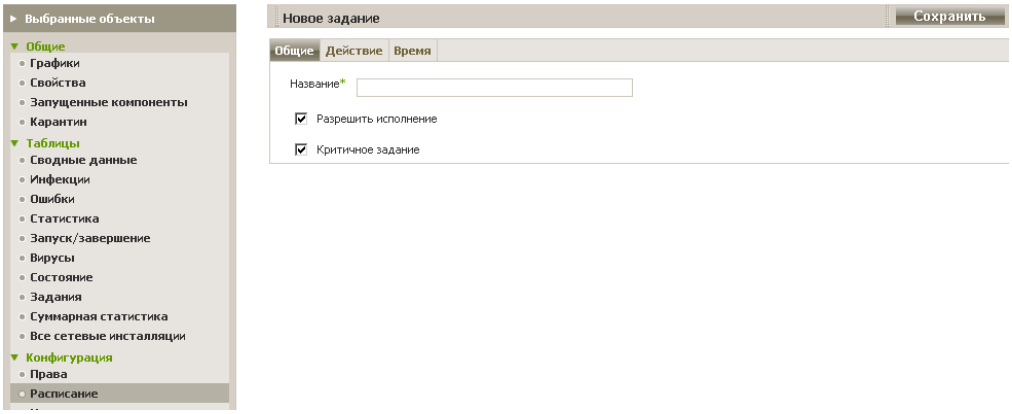
По умолчанию для станций под управлением ОС Windows и ОС Windows Mobile расписание содержит два задания:

- **Startup scan** — сканирование станции при старте (разрешено),
- **Daily scan** — ежедневное сканирование станции (запрещено).

По окончании редактирования расписания нажмите на кнопку **Сохранить**, чтобы принять изменения.

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.

Добавление заданий производится по использованию значка . Для нового задания администратор может определить используемый компонент антивируса, проверяемые объекты и каталоги.

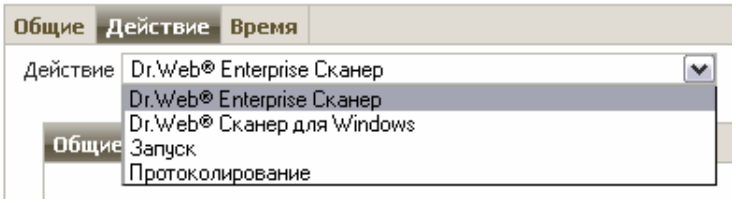


В данном окне можно отредактировать существующие задания и добавить новые по аналогии с подобными операциями для расписания ES-сервера. Вы можете запретить выполнение задания или разрешить выполнение ранее запрещенного задания. Значения полей, отмеченных знаком *, должны быть обязательно заданы.

На вкладке **Общие** задайте следующие параметры:

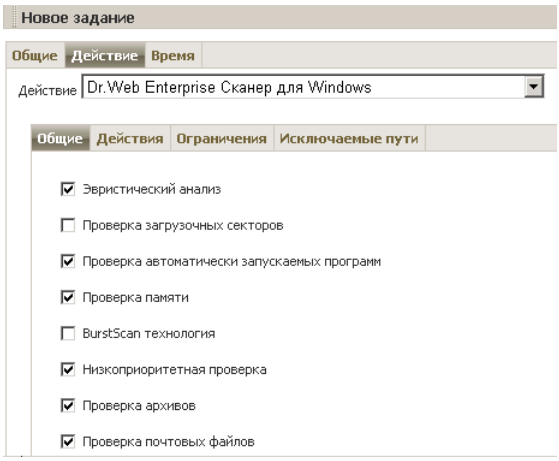
- В поле **Название** – наименование задания, под которым оно будет отображаться в расписании.
- Чтобы активировать выполнение задания, установите флаг **Разрешить исполнение**. Если флаг не установлен, задание будет присутствовать в списке, но не будет исполняться.
- Установленный флаг **Критичное задание** дает указание выполнить задание при следующем запуске **Enterprise Агента**, если выполнение данного задания будет пропущено (**Enterprise Агент** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Enterprise Агента** оно выполняется один раз.

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 для разных альтернатив.



Возможны четыре вида действий, исполняемых по расписанию:

- **Dr.Web® Enterprise Сканер** – прозрачная для пользователей проверка рабочих станций на наличие вирусов указанным продуктом с возможностью тонкого задания настроек антивирусного сканирования.



- **Dr.Web® Сканер для Windows** – проверка рабочих станций продуктом Dr.Web® Сканер для Windows.
- **Запуск** – выполнение произвольного приложения на стороне рабочей станции. Возможные параметры – путь к исполняемому файлу и аргументы командной строки для исполняемого приложения.
- **Протоколирование** – отправка на сервер заданного сообщения. Параметр – отправляемое сообщение (текстовая строка).

На вкладке **Время** настройте время запуска задания. Для этого в первую очередь выберите в выпадающем списке **Периодичность** один из режимов запуска:

- Ежедневно
- Ежемесячно
- Еженедельно
- Ежечасно
- Каждые X минут
- Стартовое

Описание параметров каждого из режимов приводится в таблице ниже.

Режим запуска	Параметры и описание
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 X минут	Необходимо ввести значение X. При X равном 60 или больше задание будет запускаться каждые X минут. При X меньше 60 задание будет запускаться в каждую минуту часа, кратную X.
Стартовое	Дополнительные параметры не требуются. Задание будет запускаться при старте работы Агента.

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**.

Чтобы удалить какое-либо задание:

1) Установите флаг напротив задания.
2) Нажмите на кнопку **Удалить эти настройки** на панели инструментов **Центра управления**.

3.11.2. 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 **Dr.Web 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 запущенных 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 **Запущенные компоненты**. Откроется список работающих компонентов.
2) При необходимости прервать какой-либо из компонентов установите флаг напротив этого компонента, после чего на панели инструментов нажмите на кнопку **Прервать**. Компонент будет остановлен и удален из списка **Прерывание сканирований** и запущенных компонентов по типам. При использовании данной опции буду прерваны текущие сканирования и запущенные мониторы, за исключением **SpIDer Guard**.

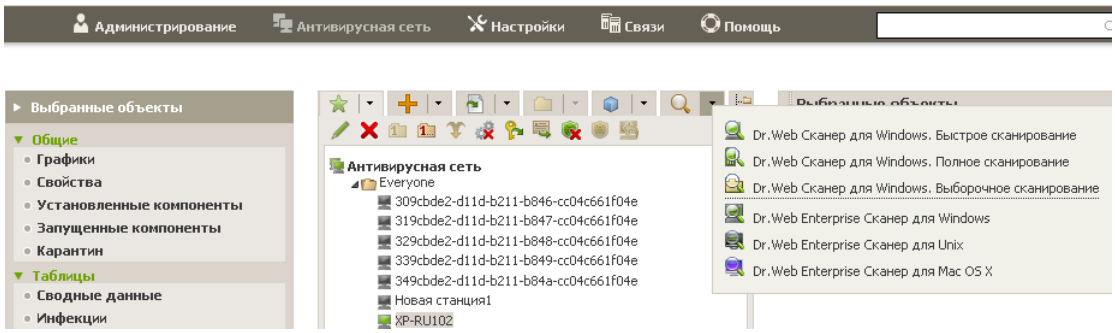
Внимание! Запуск мониторов **SpIDer Gate** из **Центра управления** невозможен.

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. Это особенно удобно, если такую команду выдают сразу многим станциям.

Чтобы прервать все исполняемые компоненты определенного типа:

1) Выберите пункт **Антивирусная сеть** 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**. Откроется окно настройки типа прерываемых компонентов.
3) Установите флаги напротив названий тех типов компонентов, которые вы хотите немедленно прервать, либо напротив заголовка области **Прерывание сканирований** — для выбора всех процессов из списка.
4) Нажмите на кнопку **Прервать**.

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. В открывшемся списке на панели инструментов выберите один из режимов сканирования:

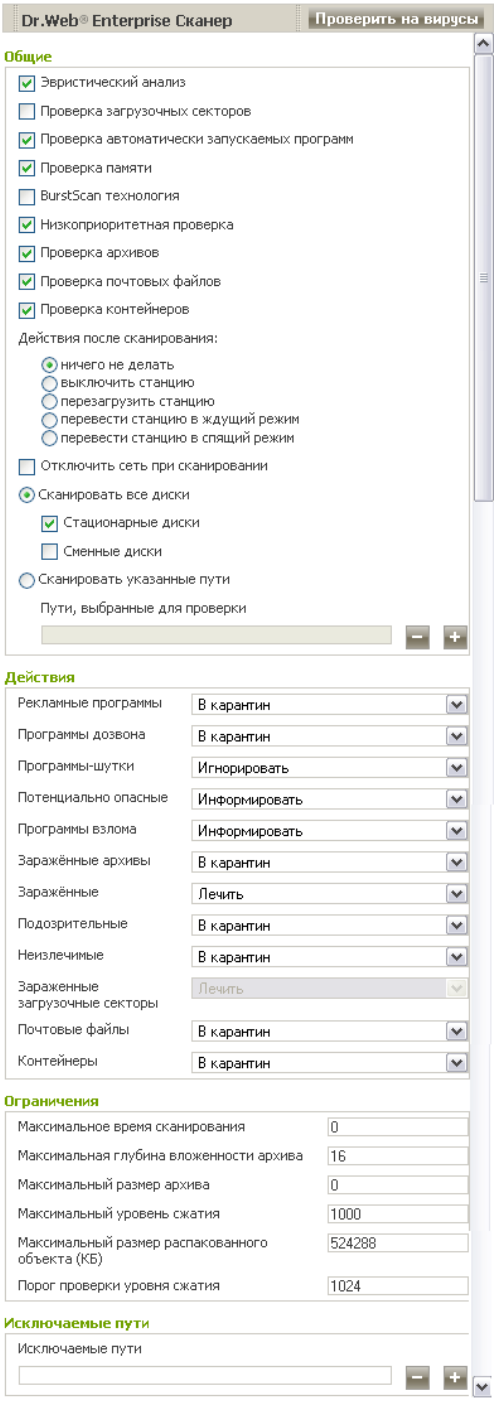


- **Dr.Web Сканер для Windows. Быстрое сканирование.** В данном режиме производится сканирование следующих объектов:
  - оперативная память,
  - загрузочные секторы всех дисков,
  - объекты автозапуска,
  - корневой каталог загрузочного диска,
  - корневой каталог диска установки ОС Windows,
  - системный каталог ОС Windows,

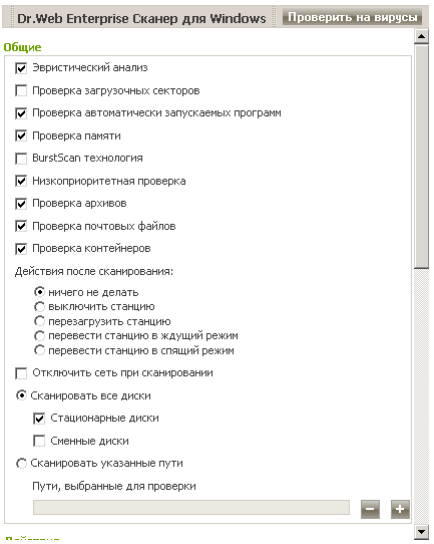
- папка **Мои документы**,
- временный каталог системы,
- временный каталог пользователя.

При выборе данного пункта начнется проверка на вирусы с параметрами Сканера, заданными по умолчанию.

- **Dr.Web Сканер для Windows. 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.
- **Dr.Web Сканер для Windows. Выборочное сканирование.** Данный режим предоставляет возможность выбрать любые папки и файлы для последующего сканирования. 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 **Проверить на вирусы**.

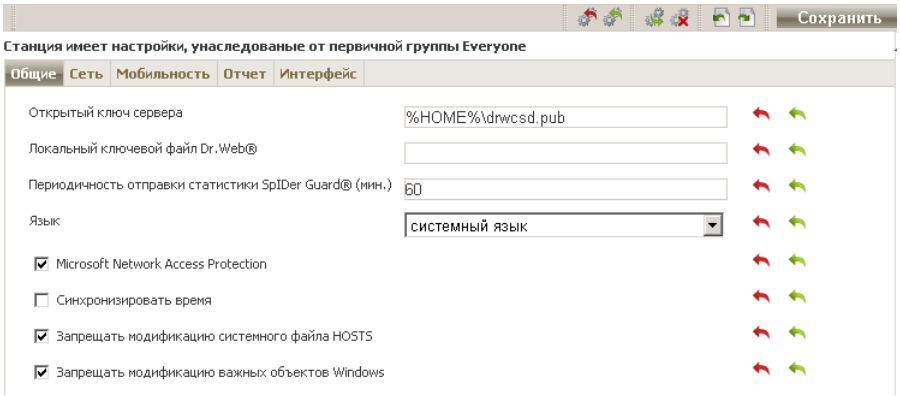


- **Dr.Web Enterprise Сканер для Windows**. В данном режиме осуществляется выборочное сканирование при помощи **Dr.Web Enterprise Сканера**. При выборе данного пункта откроется окно настройки Сканера. Задайте параметры сканирования и состав проверяемых объектов файловой системы (эти действия подробно описываются ниже) и нажмите кнопку **Проверить на вирусы**.



В том случае, если существует подозрение на заражение станции, можно выбрать пункт **Отключить сеть при сканировании**. Выбор пункта **BurstScan** позволяет существенно увеличить скорость сканирования на современных системах, а флаг **Выключить после сканирования** предписывает автоматическое выключение компьютера сразу после окончания процесса сканирования. Данные пункты доступны только для **Enterprise Сканера**.

Кроме этого, выбрав пункт **Dr.Web® Enterprise Agent для Windows** в меню **Антивирусная сеть**, можно запретить модификацию важных системных файлов:



Возможен также запуск сканирования по расписанию для этих сканеров.

3.11.2.1. 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. На панели инструментов нажмите на пункт **Сканировать**. В открывшемся списке на панели инструментов выберите пункт **Dr.Web Enterprise Сканер для Windows**. На панели справа откроется окно настроек **Сканера**. Данный список параметров позволяет задать только основные параметры для **Enterprise Сканера**, входящие в группы настроек **Общие, Действия** и **Исключаемые пути**.

2) 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 **Dr.Web® Сканер для Windows**. Откроется окно настроек **Сканера**. Данный список параметров является наиболее полным и включает все группы параметров, описанные ниже.

3) 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 **Dr.Web Сканер для Windows. Выборочное сканирование.**

   На панели справа откроется окно настроек **Сканера**. Данный список параметров является сокращенным и позволяет настроить только основные параметры, входящие в группы настроек **Общие, Действия, Отчет** и **Прочее**.

Перед запуском процесса сканирования на вирусы ознакомьтесь с рекомендациями по использованию антивирусных программ для компьютеров под управлением ОС Windows Server 2003, ОС Windows 2000 и ОС Windows XP. Статья, содержащая необходимую информацию, находится по адресу: http://support.microsoft.com/kb/822158/ru. Материал данной статьи призван помочь оптимизировать производительность системы.

- Общие
  - Флаг **Эвристический анализ** установлен по умолчанию; при этом Сканер пытается обнаруживать неизвестные вирусы при помощи эвристического анализатора. В данном режиме возможны ложные срабатывания Сканера.
  - Флаг **Проверка архиво**в установлен по умолчанию. Предписывает Сканеру искать вирусы в файлах, упакованных в файловые архивы.
  - Флаг **Проверка работающих модулей и процессов (Проверка памяти для Enterprise Сканера)** установлен по умолчанию. Предписывает проверять процессы, запущенные в оперативной памяти.
  - Флаг **Проверка автоматически запускаемых программ установлен по умолчанию**. Предписывает проверять файлы, автоматически запускаемые при старте операционной системы.
  - Флаг **Проверка загрузочных секторов установлен по умолчанию**. Предписывает Сканеру проверку загрузочных секторов. Проверяются как загрузочные секторы логических дисков, так и главные загрузочные секторы физических дисков.
  - Флаг **Проверка подкаталогов** (отсутствует для **Enterprise Сканера**) установлен по умолчанию. Используется при задании пути на сканирование и предписывает Сканеру проверять не только файлы, но и все вложенные подкаталоги по заданному пути.

  При задании настроек Сканера через пункт управляющего меню Dr.Web® Сканер для Windows доступны следующие параметры:
  - Флаг **Проверять файл HOSTS** предписывает проверку состояния системного файла HOSTS, который используется операционной системой для упрощения доступа к сети Интернет: для преобразования текстовых имен некоторых сайтов в соответствующие им IP-адреса. Изменение файла HOSTS может свидетельствовать о действии вредоносных программ.
  - Пункт **Сканировать** определяет режим проверки. В выпадающем списке выберите один из вариантов:
    - **Все файлы** – для сканирования всех файлов, независимо от их имени и расширения.
    - **По маске** – для сканирования только тех файлов, имена и расширения которых входят в список, задаваемый в разделе Список масок.
    - **Перечисленные типы** – для сканирования только тех файлов, расширения которых входят в список, задаваемый в разделе Список расширений.
  - Флаг **Подтверждение действий** предписывает получение пользователем сообщений о событиях и запросов на подтверждение действий Сканера.

- Флаг **Запрос проверки следующей дискеты** используется при проверке сменных носителей информации (накопителей на магнитных дисках (дискеты), CD/DVD-дисков, флеш-накопителей) и предписывает выдачу запроса на подключение (смену текущего) и проверку следующего носителя информации.

При задании настроек Сканера при вызове его из панели инструментов выберите один из двух альтернативных режимов.

1) **Сканировать все диски**

   Для **Enterprise Сканера** в варианте **Сканировать все диски** задайте, какие из дисков системы должны проверяться:

   - установите флаг **Стационарные диски** для проверки стационарных жестких дисков (винчестер и т. п.);
   - установите флаг **Сменные диски** для проверки всех сменных носителей информации, таких как накопители на магнитных дисках (дискеты), CD/DVD-диски, флеш-накопители и т. д.

   В данном режиме также может быть задан список **Исключаемые пути** (способ их задания описывается ниже).

2) **Сканировать указанные пути**. В варианте **Сканировать указанные пути** задайте список проверяемых путей (способ их задания описывается ниже).

Для **Enterprise Сканера** также доступны следующие флаги.

- Флаг **BurstScan технология** предписывает использовать данную технологию, значительно ускоряющую сканирование на современных системах, оснащенных многоядерными процессорами.
- Установленный по умолчанию флаг **Низкоприоритетная проверка** позволяет снизить нагрузку Сканера на имеющиеся вычислительные ресурсы системы. При этом остальные процессы могут обладать более высоким приоритетом при исполнении, чем в случае выключенной настройки. Это достигается путем динамического изменения приоритетов потоков сканирования.
- Флаг **Проверка контейнеров** предписывает Сканеру проверять файловые контейнеры различных типов.
- Список **Действия после сканирования** предписывает автоматическое выполнение заданного действия сразу после окончания процесса сканирования: выключить, перезагрузить, перевести в соответствующий режим либо не предпринимать никаких действий с компьютером пользователя.
- Флаг **Отключить сеть при сканировании** позволяет отключить компьютер от локальной сети и Интернета на время сканирования.

В разделе **Ограничения** доступны следующие настройки.

- **Максимальное время сканирования** — максимальное время в миллисекундах, в течение которого объект проверяется. По истечении указанного времени проверка объекта будет прекращена.
- **Максимальная глубина вложенности архива** — если уровень вложенности в архив превышает указанный, проверка будет производиться только до указанного уровня вложенности.
- **Максимальный размер архива** — если размер архива превышает указанный, распаковка и проверка производиться не будут.
- **Максимальный уровень сжатия** — если Сканер определяет, что коэффициент сжатия архива превышает указанный, распаковка и проверка производиться не будут.
- **Максимальный размер распакованного объекта (КБ)** — если Сканер определяет, что после распаковки архив будет больше указанного размера в (килобайтах), распаковка и проверка производиться не будут.
- **Порог проверки уровня сжатия** — минимальный размер файла внутри архива, начиная с которого будет производиться проверка коэффициента сжатия.

- **Действия**. В группе параметров **Действия** задается реакция антивируса на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов. Предусмотрены следующие действия над обнаруженными объектами.
  - **Лечить** — восстановить состояние инфицированного объекта до заражения. При невозможности лечения применяется настройка, заданная 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.
  - **В карантин** — переместить зараженные объекты в каталог Карантина.
  - **Переименовывать** — переименовать зараженные объекты в соответствии с правилом, заданным в поле **Шаблон** для переименования.
  - **Информировать** — ограничиться оповещением об обнаружении вируса (о настройке режима оповещений см. в п. «Оповещения»).
  - **Игнорировать** — пропустить объект без выполнения каких-либо действий и не выводить оповещения.

Действие	Объект				
	Рекламные программы	Зараженные контейнеры	Зараженные	Подозрительные	Неизлечимые
Лечить			+/*		
Удалять	+	+	+	+	+
В карантин	+	+/*	+	+	+/*
Переименовывать	+	+	+	+	+
Информировать	+/*	+	+	+/*	+
Игнорировать	+				

Здесь:

+ действие разрешено для данного типов объектов

+/* действие установлено как реакция по умолчанию для данного типов объектов

Для задания действий над обнаруженными вредоносными объектами служат следующие настройки.

В поле **Шаблон для переименования** указывается маска расширения, которое получают переименованные объекты, если для них было указано действие **Переименовывать при обнаружении**. По умолчанию предлагается вариант #??, т. е. первый символ расширения заменяется на символ #. Данную маску можно изменять, однако в качестве замены не следует использовать стандартные расширения (EXE, COM, BAT, DOC, PAS, BAS и пр.).

Выпадающий список **Рекламные программы** задает реакцию Сканера на обнаружение данной разновидности нежелательного ПО. При задании действия **Игнорировать для рекламных программ** не будет произведено никаких действий: пользователю не будет выдано предупреждение, как в случае включенной опции **Информировать при обнаружении вируса**.

Аналогично действиям над рекламными программами настраивается реакция Сканера при обнаружении прочего нежелательного ПО, такого как программы дозвона, программы-шутки, потенциально опасные, программы взлома.

- Выпадающий список **Перезагрузка** задает режим перезагрузки компьютера после завершения сканирования.
- Выпадающий список **Зараженные контейнеры** задает реакцию Сканера на обнаружение зараженного или подозрительного файла в составе файлового архива или контейнера. Реакция задается для всего архива в целом.

- Выпадающий список **Зараженные** 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).
- Флаг **Разрешить удаление архивов** позволяет удалять обнаруженные зараженные архивы и почтовые файлы. Если данный флаг установлен, то в разделах **Зараженные архивы** и **Зараженные почтовые файлы**, расположенных ниже, будет присутствовать вариант действий **Удалять**. При снятии данного флага допустимы только действия В карантин (по умолчанию для архивов), **Переименовывать** и **Информировать** (по умолчанию для почтовых файлов).

Список исключаемых путей содержит в явном виде пути (диски и каталоги), исключаемые из сканирования. Список исключаемых файлов содержит в явном виде файлы, исключаемые из сканирования. При редактировании списков исключаемых путей и файлов:

- Введите требуемый абсолютный путь в строку **Исключаемые пути**.
- Введите требуемый файл илди маску файла (без указания пути) в строку **Исключаемые файлы**.
- Для того чтобы добавить новую строку в список, нажмите на кнопку  и в открывшуюся строку введите требуемый путь.
- Для того чтобы удалить элемент из списка, нажмите на кнопку  напротив соответствующей строки.

Список исключаемых объектов может содержать элементы следующих видов:

- 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.
- Регулярное выражение. Пути могут задаваться регулярными выражениями. Также любой файл, полное имя которого (с путем) соответствует регулярному выражению, исключается из проверки.

  Синтаксис регулярных выражений, используемых 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 приведены ниже:

  - 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.

Ссылки на подробные описания синтаксиса регулярных выражений приведены в «Руководстве администратора».

Раздел **Список расширений** (при вызове настроек через управляющее меню) активен только в том случае, когда в разделе **Общие** в пункте **Сканировать** задан вариант **Перечисленные типы**. При этом сканированию подлежат только те файлы, расширения которых входят в данный список.

При изменении списка расширений используйте кнопку для добавления новых элементов списка, кнопку для удаления имеющихся элементов списка.

В элементах списка расширений могут использоваться специальные символы * и ?. По умолчанию хранится список расширений исполняемых и архивных файлов. Для восстановления списка по умолчанию используйте кнопку **Список масок** (при вызове настроек через управляющее меню).

Раздел **Список масок** активен только в том случае, когда в разделе **Общие** в пункте **Сканировать** задан вариант **По маске**. При этом сканированию подлежат только те файлы, имена и расширения которых входят в данный список.

При изменении списка масок используйте кнопку для добавления новых элементов списка, кнопку для удаления имеющихся элементов списка.

В элементах списка расширений могут использоваться специальные символы * и ?. По умолчанию хранится список исполняемых и архивных файлов. Для восстановления списка по умолчанию используйте кнопку .

В разделе **Прочее** (кроме **Enterprise Сканера**) указываются дополнительные параметры Сканера:

- Флаг **Использовать диск для создания файла подкачки** предписывает использование жесткого диска для создания файла подкачки во избежание нехватки оперативной памяти, используемой Сканером при проверке данных больших объемов (крупных архивов и т. п.).
- Флаг **Восстановить дату доступа** предписывает после сканирования восстанавливать дату последнего обращения к файлу (заменять на дату перед началом сканирования).
- Флаг **Сохранять настройки автоматически** предписывает автоматическое сохранение настроек конфигурации Сканера после завершения текущего сеанса работы.
- В поле **Приоритет сканирования** задается приоритет потоков процесса сканирования. Допускается задание приоритета от 1 до 50 (50 — наивысший приоритет):
- 1 ... 4 — простаивающий. Не рекомендуется устанавливать данный уровень приоритета во избежание замедления работы Сканера и, соответственно, значительного увеличения времени сканирования.
- 5 ... 11 — низший.
- 12 ... 18 — ниже обычного.
- 19 ... 25 — обычный. Рекомендуемый приоритет сканирования.
- 26 ... 32 — выше обычного.
- 33 ... 39 — высший.
- 40 ... 50 — критичный ко времени. Не рекомендуется устанавливать данный уровень приоритета во избежание сильной загрузки операционной системы Сканером во время сканирования.

В разделе **Отчет** вы можете назначить ведение файла протокола работы **Сканера**. Для этого установите флаг **Записывать отчет в файл** и задайте необходимые параметры ведения протокола.

В разделе **Звуки** (при вызове настроек через управляющее меню) вы можете задать воспроизведение звуковых файлов для событий определенных типов. Для этого установите флаг **Проигрывать звуки** и задайте имена звуковых файлов в полях, соответствующих конкретным событиям.

Вы можете просматривать результаты работы компонентов рабочей станции — обновлений ПО, антивирусных сканирований и антивирусного мониторинга. Для этого служат статистические таблицы и графики.

3.11.3. Настройка локального расписания станций

При установках рабочей станции по умолчанию, т. е. без всякого вмешательства администратора антивирусной сети, на рабочей станции работает антивирусный монитор, а также периодически запускаются задания на обновление ПО и антивирусное сканирование.

Чтобы отредактировать локальное расписание рабочей станции:

1) В контекстном меню Агента в пункте **Расписание** выберите вариант **Локальное**.
2) Откроется окно редактирования локального расписания **Enterprise Агента**.

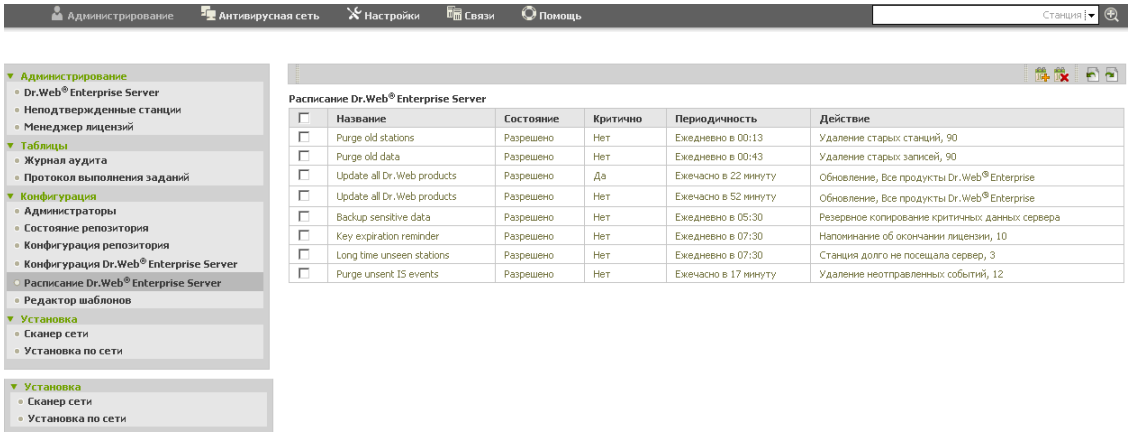
В контекстном меню вариант **Локальное** будет доступен только в том случае, если при редактировании прав антивирусной станции был установлен флаг **Создание локального расписания**.

Используя локальное расписание, пользователь может запускать сканирование с заданием параметров. Варианты задания объектов сканирования, ключи командной строки, задающие параметры программы, а также параметры командной строки для модуля автоматического обновления описаны в руководстве «Антивирус Dr.Web® для Windows. Руководство пользователя».

По окончании редактирования нажмите на кнопку **Закрыть**.

3.11.4. Настройка расписания ES-сервера

Для выполнения настройки расписания ES-сервера необходимо выбрать в разделе **Администрирование** Веб-интерфейса пункт **Расписание Dr.Web® Enterprise Server**. Будет отображен перечень текущих заданий ES-сервера.



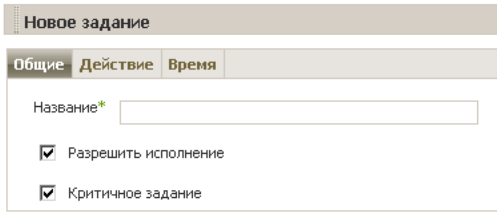
Для того чтобы удалить задание из списка, выделите его с помощью флажка, после чего нажмите на панели инструментов кнопку (**Удалить эти настройки**).

Для того чтобы отредактировать параметры задания, нажмите на название соответствующего задания (оно выполнено в виде ссылки). При этом откроется **Редактор заданий**, описываемый ниже. Укажите необходимые параметры (см. ниже) и нажмите на кнопку **Сохранить**.

Для того чтобы добавить задание в список, нажмите на панели инструментов кнопку (**Новое задание**). При этом также откроется группа настроек **Новое задание**.

Вы также можете запретить выполнение задания или разрешить выполнение ранее запрещенного задания.

При создании нового задания или редактировании имеющегося открывается окно ввода параметров задания.

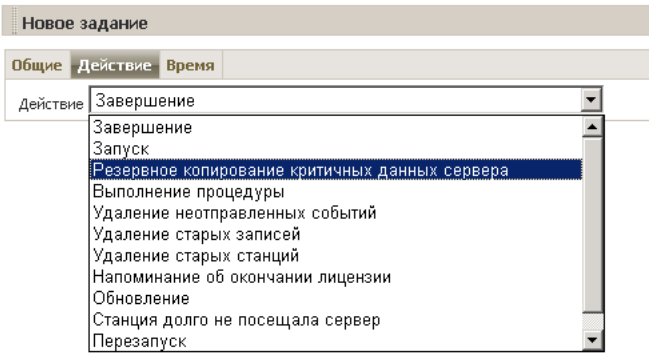


Для того чтобы отредактировать параметры задания:

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 флаг не установлен, задание будет присутствовать в списке, но не будет исполняться.
3) С помощью флажка **Критичное задание** определите, является ли данное задание критичным для выполнения. Установленный флаг **Критичное задание** дает указание выполнить задание при следующем запуске **Enterprise Сервера**, если выполнение данного задания будет пропущено (**Enterprise Сервер** отключен на момент выполнения задания). Если за определенный период задание пропущено несколько раз, то при запуске **Enterprise Сервера** оно выполняется один раз.

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 по типам).



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).

Нажмите на кнопку **Сохранить**.

Задания типов **Завершение** (завершение работы Сервера) и **Перезапуск** (перезапуск Сервера) параметров не имеют.

Для задания типа **Запуск** введите в поле **Путь** путь к исполняемому файлу сервера, в поле **Аргументы** – параметры командной строки при запуске. С помощью флажка **Выполнять синхронно** (синхронизация с Сервером – ожидание завершения выполнения данной программы перед выполнением других заданий типа **Запуск**) определите способ выполнения задания. Если флаг **Выполнять синхронно** не установлен, то Сервер запускает программу и протоколирует только ее запуск. Если флаг **Выполнять синхронно** установлен, то Сервер протоколирует ее запуск, код возврата и время завершения программы.

Для задания типа **Протоколирование** следует указать текст сообщения, которое заносится в протокол.

Для задания типа **Напоминание об окончании лицензии** следует указать период, до которого будет получено напоминание об окончании срока лицензии на продукт Dr. Web (как лицензии Сервера, так и Агента).

Для заданий типа **Удаление старых станций** и **Удаление старых записей** необходимо указать период, при превышении которого записи или станции признаются старыми. Под записями здесь понимается вся информация, хранящаяся в таблицах о рабочих станциях (кроме самих станций): статистические данные компонентов, протоколы выполнения заданий, информация о вирусных событиях и т. п.

Старые данные автоматически удаляются из базы данных с целью экономии дискового пространства. Указываемый по умолчанию период для **Удаления старых записей** и **Удаления 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.

Для заданий типа **Станция долго не посещала сервер** необходимо указать период, по истечении которого станция считается долго не посещавшей сервер.

Для заданий типа **Выполнение процедуры** необходимо указать название выполняемой процедуры в поле **Название**. Название процедуры должно соответствовать названию исполняемого пользовательского lua-скрипта (без расширения), расположенного в каталоге var/extensions каталога установки Сервера.

Для заданий типа **Удаление неотправленных событий** необходимо указать период, по истечении которого неотправленные события будут удаляться. Здесь имеются в виду события, передаваемые подчиненным Сервером главному. При неудачной передаче события оно заносится в список неотправленных. Подчиненный Сервер с заданной периодичностью осуществляет попытки передачи. При выполнении задания **Удаление неотправленных событий** осуществляется удаление всех событий, длительность хранения которых достигла и превысила заданный период.

Задания типа **Резервное копирование критичных данных сервера** предназначены для создания резервной копии критичных данных сервера (база данных, серверный лицензионный ключевой файл, закрытый ключ шифрования). Следует указать путь к каталогу, в который будут сохранены данные (пустой путь означает каталог по умолчанию), и максимальное количество резервных копий (значение 0 означает отмену этого ограничения).

Задания типа **Обновление** предназначены для автоматического обновления продукта в репозитории и имеют единственный параметр: название обновляемого продукта, выбираемое из выпадающего списка.

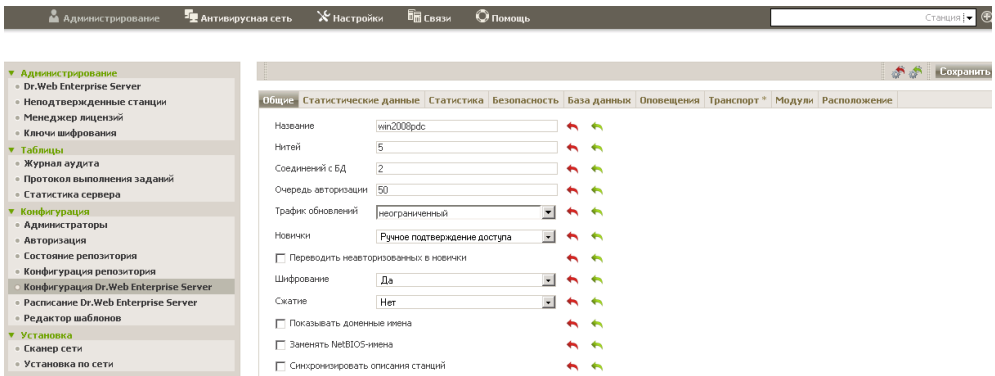
1) Для того чтобы экспортировать расписание в файл специального формата, нажмите на кнопку панели инструментов.
2) Для того чтобы импортировать параметры из такого файла, нажмите на кнопку панели инструментов.

4. Управление сервером Dr.Web Enterprise Security Suite

4.1. Настройка конфигурации Dr.Web Enterprise Server

Чтобы настроить конфигурационные параметры для **Dr.Web Enterprise Server**, выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.

Значения полей, отмеченных знаком *, должны быть обязательно заданы.



Вкладка Общие

Параметр **Название** определяет имя данного Сервера. Если оно не задано, применяется имя компьютера, на котором работает ПО **Enterprise Сервера**.

Параметр **Нитей** определяет количество потоков для обработки данных, поступающих от Агентов. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.

Параметр **Соединений с БД** задает количество соединений Сервера с БД. Значение, установленное по умолчанию, рекомендуется изменять только после согласования со службой поддержки.

В поле **Очередь авторизации** задается максимальное количество станций в очереди для авторизации на Сервере. Допускает ввод любого целого числа.

В выпадающем списке **Трафик обновлений** задается максимальная полоса пропускания сетевого трафика при передаче обновлений между Сервером и Агентами. При этом:

- Если данный параметр имеет значение **Unlimited**, то обновления для различных Агентов передаются параллельно.
- Если для данного параметра установлено значение, отличное от **Unlimited** (конкретное числовое значение), то обновления передаются последовательно.

В выпадающем списке **Новички** задается политика подключения новых рабочих станций (см. п. «Политика подключения новых станций»). Флаг **Переводить неавторизованных в новички** предписывает программе сбрасывать параметры соединения с Сервером у станций, не прошедших авторизацию. Данная опция может быть полезна при изменении настроек Сервера (таких как открытый ключ) или при смене БД. В подобных случаях станции не смогут подключиться и потребуется повторное получение новых параметров для доступа к Серверу.

В выпадающих списках **Шифрование** и **Сжатие** выбирается политика шифрования и сжатия трафика между **Enterprise Сервером**, **Агентами** и **Центром управления** (подробнее об этих параметрах см. п. «Использование шифрования и сжатия трафика»).

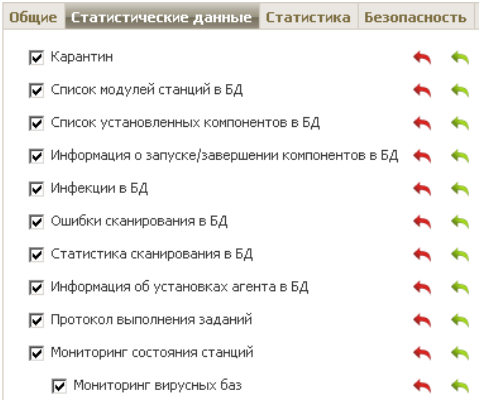
Вы также можете изменять состояние следующих флагов.

- **Показывать доменные имена** предписывает программе заносить в файл протокола не IP-адреса рабочих станций, а их доменные имена.
- **Заменять NetBios-имена** предписывает отображать в каталоге антивирусной сети не наименования рабочих станций, а их доменные имена (при невозможности определения доменных имен отображаются IP-адреса).

Оба флага – **Показывать доменные имена** 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 кеширование имен на DNS-сервере.

- **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.

На вкладке **Статистические данные** задается статистическая информация, которая записывается в журнал протокола и заносится в базу данных Сервера.



Для добавления в БД соответствующего типа информации установите следующие флаги.

- **Карантин** – разрешает запись состояния Карантина на станциях.
- **Список модулей станций в БД** – разрешает записывать состав модулей Антивируса на рабочей станции.
- **Список установленных компонентов в БД** – разрешает записывать, какие компоненты Антивируса (Сканер, Мониторы и т. п.) установлены на рабочей станции.
- **Информация о запуске/завершении компонентов в БД** – разрешает записывать информацию о запуске и завершении работы компонентов Антивируса (Сканер, Мониторы и т. п.) на рабочих станциях.
- **Инфекции в БД** – разрешает запись статистических данных об инфекциях, обнаруженных на рабочих станциях.
- **Ошибки сканирования в БД** – разрешает запись информации обо всех ошибках при сканировании на рабочих станциях.
- **Статистика сканирования в БД** – разрешает запись результатов сканирования на рабочих станциях.
- **Информация об установках агента в БД** – разрешает записывать информацию об инсталляциях Агентов на рабочих станциях.
- **Протокол выполнения заданий** разрешает записывать в БД результат выполнения заданий на станциях.
- **Мониторинг состояния станции** разрешает вести учет изменений состояния станции и запись информации в БД.

Журнал изменения состояния станции можно просмотреть, выбрав в контекстном меню станции пункт **Таблицы**, пункт **Состояние**.

- **Мониторинг вирусных баз** разрешает вести учет состояния (состава, изменения) вирусных баз на станции и запись информации в БД.

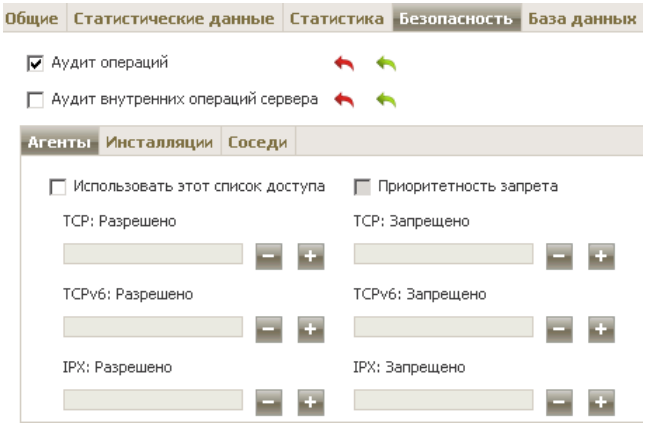
На вкладке **Статистика** настраиваются параметры отправки статистики по вирусным событиям в компанию «Доктор Веб». Для активации отправки статистики установите флаг **Статистика**. Станут доступны следующие поля:

- **Интервал** – интервал отправки статистики в минутах;
- **Адрес сервера** – IP-адрес или DNS-имя и порт сервера статистики (по умолчанию stat.drweb.com:80);
- **URL** – каталог на сервере статистики (по умолчанию /update);
- **Идентификатор клиента** – MD5 ключ Сервера (находится в ключевом файле Сервера enterprise.key);
- **Пользователь** – имя пользователя для регистрации статистики. Имя пользователя можно получить в службе технической поддержки компании «Доктор Веб»;
- **Пароль** – пароль для регистрации статистики. Пароль можно получить в службе технической поддержки компании «Доктор Веб»;
- **Прокси-сервер** – при необходимости можно указать адрес прокси-сервера для отправки статистики;
- **Пользователь прокси** – имя пользователя прокси-сервера (не указывается при анонимной авторизации прокси);
- **Пароль пользователя прокси** – пароль для доступа к прокси-серверу (не указывается при анонимной авторизации прокси).

Обязательными полями являются только **Адрес сервера статистики** и **Интервал отправки статистики**.

Для сохранения внесенных изменений нажмите на кнопку **Сохранить**.

На вкладке **Безопасность** задаются ограничения на сетевые адреса, с которых Агенты, Центр управления, сетевые инсталляторы и другие («соседние») Серверы смогут получать доступ к данному Серверу.



Управление журналом аудита Сервера осуществляется при помощи следующих флагов.

- **Аудит операций** 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 и запись журнала в БД.

Журнал аудита можно посмотреть, выбрав в главном меню **Администрирование** пункт **Журнал аудита**.

На вкладке **Безопасность** размещаются дополнительные вкладки **Агенты**, **Инсталляции** и **Соседи**, на которых настраиваются ограничения для соответствующих типов соединений.

Для того чтобы настроить ограничения доступа для какого-либо типа соединения:

1) Перейдите на соответствующую вкладку (**Агенты**, **Инсталляции** или **Соседи**).
2) Чтобы разрешить все соединения, снимите флаг **Использовать этот список доступа**.
3) Для того чтобы задать списки разрешенных или запрещенных адресов, установите флаг **Использовать этот список доступа**.
4) Для того чтобы разрешить доступ с определенного TCP-адреса, включите его в список **TCP: разрешено** или **TCPv6: разрешено**.
5) Для того чтобы запретить какой-либо TCP-адрес, включите его в список **TCP: запрещено** или **TCPv6: запрещено**.

Для редактирования списка адресов:

1) Введите сетевой адрес в соответствующее поле и нажмите на кнопку **Сохранить**.
2) Для добавления нового поля адреса нажмите на кнопку соответствующего раздела.
3) Для удаления поля нажмите на кнопку .

Сетевой адрес задается в виде: <IP-адрес>/[<префикс>].

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.*.*.*

Аналогично настраиваются ограничения для IPX-адресов.

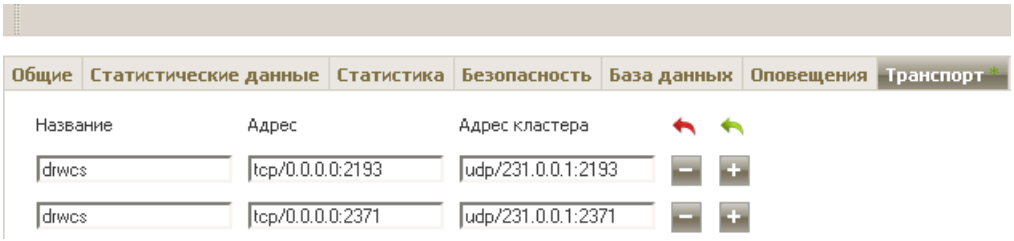
Адреса, не включенные ни в один из списков, разрешаются или запрещаются в зависимости от того, установлен ли флаг **Приоритетность запрета**: при установленном флаге адреса, не включенные ни в один из списков (или включенные в оба), запрещаются. В противном случае такие адреса разрешаются.

На вкладке **База данных** задается выбор СУБД для хранения централизованного журнала антивирусной сети и ее настройки (подробнее об этих параметрах см. «Руководство администратора», п. «Настройка режима работы с БД»).

Параметры на вкладке **Оповещения** позволяют настроить режим оповещения администраторов антивирусной сети и других лиц о вирусных атаках и других событиях, выявленных компонентами **Dr.Web ATM Shield** (подробнее об этой настройке см. в п. «Оповещения»).

На вкладке **Транспорт** настраиваются параметры используемых Сервером транспортных протоколов.

Для каждого из протоколов можно указать в поле **Название** имя **Enterprise Сервера**. Если оно не задано, используется имя, заданное на вкладке **Общие** (см. выше; в частности, если на указанной вкладке не задано никакое имя, используется имя компьютера). Если для протокола задано иное имя, чем определенное на вкладке **Общие**, используется имя из описания протокола. Данное имя используется службой обнаружения Сервера Агентами и т. д.



В поле **Адрес** необходимо указать адрес интерфейса, прослушиваемого Сервером для взаимодействия с Агентами, установленными на рабочих станциях.

В поле **Адрес кластера** необходимо указать адрес интерфейса, прослушиваемого Сервером для взаимодействия с Агентами и Сетевыми инсталляторами при поиске активных **Enterprise Серверов** сети. Более подробное описание приведено в разделе «Служба обнаружения Сервера».

Данные параметры задаются в формате сетевого адреса.

На вкладке **Модули** задается режим использования протоколов взаимодействия Сервера с другими компонентами **Dr.Web ES**. По умолчанию разрешено взаимодействие с **Enterprise Агентами**, компонентом NAP Validator и программами установки Агента, и отключено взаимодействие **Enterprise Сервера** с другими **Enterprise Серверами**.

При задании многосерверной конфигурации сети (см. п. «Иерархия серверов») включите этот протокол, установив соответствующий флаг.

Дополнение **Веб-администрирование** определяет возможность использования встроенного **Центра управления Dr.Web** для управления антивирусной сетью. Для того чтобы активировать данное дополнение, установите флаг напротив данного пункта. Для запрета запуска **Центра управления** снимите этот флаг.

На вкладке **Расположение** вы можете указать дополнительную информацию о компьютере, на котором установлено ПО **Enterprise Сервера**.

4.1.1. Настройка межсетевого 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 флаг **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.

4.1.2. Настройка сетевых соединений

К **Enterprise Серверу** подключаются следующие клиенты:

- **Enterprise Агенты**,
- Сетевые инсталляторы **Enterprise Агентов**,
- другие **Enterprise Серверы**.

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.

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/231.0.0.1:2371`
- `udp/231.0.0.1:2193`

Данный параметра задается в настройках Сервера **Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт** → поле **Адрес кластера**.

4.1.2.1. Установка прямых соединений (Direct connection)

Данный вариант подключения следует использовать, если необходима перенастройка всей системы, в частности, если требуется перенести **Enterprise Сервер** на другой компьютер или поменять IP-адрес машины, на которой установлен Сервер.

При конфигурации антивирусной сети **ES** на использование прямых соединений Служба обнаружения Сервера может быть отключена. Для этого в описании транспортов (**Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт**) поле **Адрес** кластера следует оставить пустым.

Для настройки **Dr.Web Enterprise Server** в настройках Сервера должно быть указано, какой адрес необходимо прослушивать для приема входящих TCP-соединений. Данный параметр задается в настройках Сервера **Администрирование** → **Конфигурация Dr.Web Enterprise Server** → вкладка **Транспорт** → поле **Адрес**.

По умолчанию для прослушивания Сервером устанавливаются:

- tcp/0.0.0.0:2371 – поддерживается для обратной совместимости; в частности, для устранения проблем с переходом с версий 4.XX, в которых используется порт 2371.

- tcp/0.0.0.0:2193 — при использовании порта 2193, зарегистрированного за **Dr.Web Enterprise Suite** в IANA.

Обозначение 0.0.0.0 означает «все сетевые интерфейсы» для данной машины, на которой установлен Сервер.

Для корректной работы всей системы ES достаточно, чтобы Сервер «слушал» хотя бы один TCP-порт, который должен быть известен всем клиентам.

Для того чтобы **Dr.Web Enterprise Agent** использовал прямые соединения при установке Агента, адрес Сервера (IP-адрес или сетевое имя машины, на которой запущен **Enterprise Сервер**) может быть явно указан в параметрах установки: drwinst <Адрес_Сервера> (по умолчанию команда drwinst, запущенная без параметров, будет сканировать сеть на наличие **Enterprise Серверов** и попытается установить Агент с первого найденного Сервера в сети (режим Multicasting с использованием Службы обнаружения Сервера)).

Таким образом, адрес **Enterprise Сервера** становится известен Агенту при установке.

В дальнейшем адрес Сервера может быть изменен вручную в настройках Агента. Просмотр и редактирование настроек соединения с **Enterprise Сервером** осуществляется при помощи пункта контекстного меню значка Агента **Настройки → Соединение**...

При установке Агента рекомендуется использовать имя Сервера, предварительно зарегистрированное в службе DNS. Это упростит процесс настройки антивирусной сети, связанный с процедурой переустановки **Enterprise Сервера** на другой компьютер.

Альтернативным способом является редактирование конфигурационного файла. Чтобы агент искал установленный сервер по известному адресу и не использовал широковещательные пакеты UDP, нужно отредактировать файл C:\Program Files\DrWeb Enterprise Suite\drweb32.ini. В данном файле можно указать:

```
[DwProt]
EnableLock = No
LockLAN = No
LockRemovable = No
BlockFolders = No
LngFileName = ru-drweb.dwl
```

Эти же настройки можно задать в конфигурации агента через **Веб-интерфейс**.

Если станция в силу ряда причин не видна с сервера и сервер не может распространить на нее настройки, то можно задать адрес сервера непосредственно в реестре. Для этого необходимо поправить в ветви HKLM\SOFTWARE\IDAVLab\Enterprise Suite\Dr.Web (R) Enterprise Agent\Settings значение ключа Server. В качестве значения необходимо указать адрес сервера и его порт. Например, tcp/192.168.0.5:2193.

4.1.3. Использование шифрования и сжатия трафика

Антивирусная сеть **Dr.Web ATM Shield** позволяет зашифровать трафик между Сервером и рабочими станциями (**Enterprise Агентами**), между **Enterprise Серверами** (при многосерверной конфигурации сети), а также между Сервером и Сетевыми инсталляторами. Этот режим используется, чтобы избежать возможного разглашения пользовательских ключей, а также сведений об оборудовании и пользователях антивирусной сети.

Политика использования шифрования настраивается раздельно на каждом из компонентов антивирусной сети, при этом настройки остальных компонентов должны быть согласованы с настройками Сервера.

Чтобы задать политики сжатия и шифрования для **Dr.Web Enterprise Server**:

1) Выберите пункт **Администрирование** главного меню **Центра управления**.

2) В открывшемся окне выберите пункт управляющего меню **Конфигурация Dr.Web Enterprise Server**.

3) На вкладке **Общие** выберите в выпадающих списках **Шифрование** и **Сжатие** один из вариантов:

- **Да** — шифрование (или сжатие) трафика со всеми компонентами обязательно.
- **Возможно** — шифрование (или сжатие) будет выполняться для трафика с теми из компонентов, настройки которых этого не запрещают (устанавливается по умолчанию, если параметр не был изменен при установке Сервера). По умолчанию **Enterprise Агент** устанавливается с настройками шифрования **Возможно**. Данное сочетание означает, что по умолчанию шифрование будет производиться, но может быть отменено редактированием настроек **Enterprise Сервера**.
- **Нет** — шифрование (или сжатие) не поддерживается.

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 утрате 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 (–), и о том, какие сочетания являются недопустимыми (Ошибка).

Настройки сервера/настройки компонента	Да	Возможно	Нет
Да	+	+	Ошибка
Возможно	+	+	–
Нет	Ошибка	–	–

Использование шифрования трафика создает заметную вычислительную нагрузку на компьютеры с производительностью, близкой к минимально допустимой для установленных на них компонентов. В тех случаях, когда шифрование трафика не требуется для обеспечения дополнительной безопасности, можно отказаться от этого режима. Шифрование трафика также не рекомендуется в больших сетях (от 2 000 клиентов). При этом следует последовательно переключать Сервер и компоненты сначала в режим **Возможно**, не допуская создания несовместимых пар Сетевой инсталлятор — Сервер и Агент — Сервер. Несоблюдение этого правила может привести к потере управляемости компонента и необходимости его переустановки.

Ввиду того что трафик между компонентами (особенно Серверами) может быть весьма значительным, антивирусная сеть позволяет установить сжатие (компрессию) этого трафика. 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 значительно увеличивает вычислительную нагрузку на компьютеры, в большей степени, чем шифрование.

4.1.4. Ведение серверного протокола

Enterprise Сервер 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 Windows: в подкаталоге var каталога установки Сервера.

Файл имеет простой текстовый формат.

4.1.5. Управление репозиторием Dr.Web Enterprise Server

Репозиторий **Enterprise Сервера** предназначен для хранения эталонных образцов ПО и обновления их с серверов ВСО.

Для этой цели репозиторий оперирует наборами файлов, называемыми продуктами. Каждый продукт размещается в отдельном подкаталоге каталога 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 **Enterprise Сервер** с сайта обновления продукта (по протоколу HTTP);

Для версий Сервера 5.0 и выше, вне зависимости от настроек репозитория для ПО Сервера, обновления с серверов ВСО не поставляются.

Для обновления Сервера используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах «Обновление Dr.Web ES для ОС Windows®».

b) между различными **Enterprise Серверами** в многосерверной конфигурации (в соответствии с заданной политикой обмена);

c) с **Enterprise Сервера** 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 создание новых продуктов, для которых также будет выполняться синхронизация.

В настоящее время в поставку входят следующие продукты:

- **Enterprise Сервер**,
- **Enterprise Агент** (ПО Агента, антивирусное ПО рабочей станции),
- **Центр управления Dr.Web**,
- Вирусные базы.

Чтобы проверить текущее состояние репозитория или обновить компоненты антивирусной сети, выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Состояние репозитория**.

В открывшемся окне приведен список компонентов антивирусной сети, дата их последнего обновления и их текущее состояние.

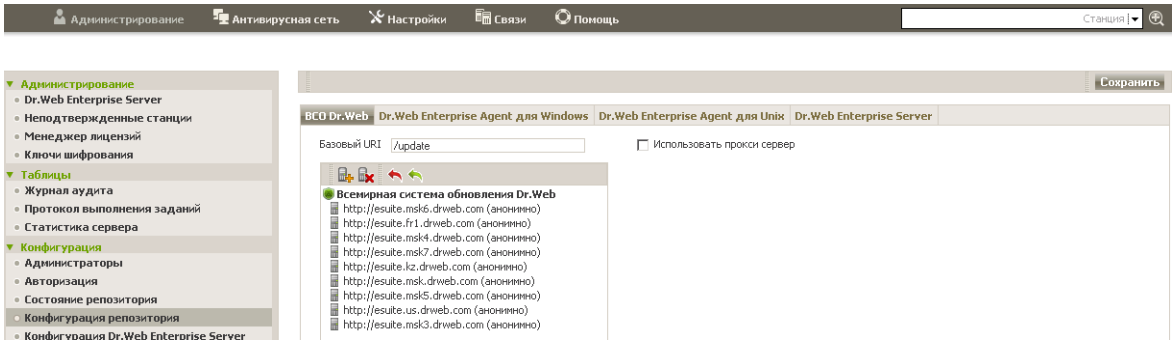
Для проверки наличия обновлений и загрузки имеющихся обновлений компонентов с серверов ВСО нажмите на кнопку **Проверить обновления**.

4.1.5.1. Редактор конфигурации репозитория

Редактор конфигурации репозитория позволяет задать общие параметры конфигурации репозитория для всех продуктов.

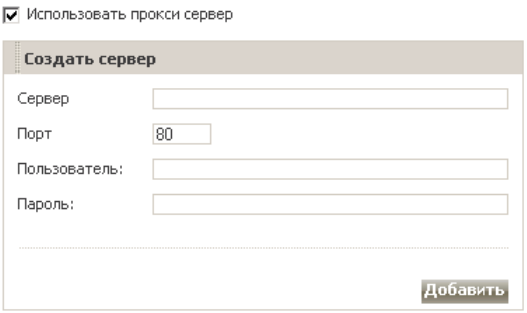
После изменения настроек репозитория необходимо произвести успешное обновление ПО компонентов антивирусной сети для изменения состояния репозитория в соответствии с выбранными вами настройками.

Чтобы отредактировать конфигурацию репозитория, выберите пункт **Администрирование** главного меню **Центра управления**, в открывшемся окне выберите пункт управляющего меню **Конфигурация репозитория**.



На вкладке **BCO Dr.Web®** осуществляется настройка параметров Всемирной системы обновлений. Вы можете:

- Удалить сервер из списка. Для этого выделите один или несколько серверов и на панели инструментов нажмите на кнопку **Удалить сервер из списка** .
- Для выбора нескольких серверов одновременно используйте кнопки **CTRL** или **SHIFT**.
- Добавить сервер в список. Для этого на панели инструментов нажмите на кнопку **Создать сервер** и задайте настройки сервера согласно процедуре, приведенной ниже.
- Задать прокси-сервер. Для этого установите флаг **Использовать прокси–сервер** (настройки прокси аналогичны настройкам серверов обновлений), в открывшемся окне настроек прокси-сервера установите параметры, аналогичные параметрам сервера обновлений, нажмите на кнопку **Добавить** и **Сохранить**.



При настройке прокси-сервера особое внимание следует обратить на тип используемой авторизации.

В текущей версии **Dr.Web ATM Shield** поддерживается только базовая HTTP-авторизация и Proxy-HTTP-авторизация.

Если необходимо отключить серверы обновлений от прокси-сервера, снимите флаг **Использовать прокси-сервер**.

- Настроить адрес сервера и параметры авторизации пользователя. Для этого нажмите на значок сервера.

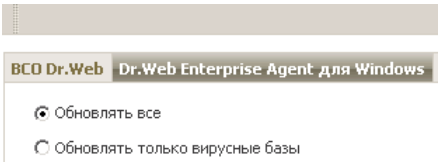
При настройке или добавлении сервера открывается окно настроек сервера.

Для задания настроек сервера обновления:

1) Нажмите на значок соответствующего сервера.
2) В полях ввода **Сервер** укажите, соответственно, адрес и порт сервера.
3) В полях **Пользователь** и **Пароль** можете задать имя пользователя и пароль на сервере обновлений. Если авторизация на сервере не требуется, **оставьте эти поля пустыми**.
4) Для сохранения измененных настроек нажмите на кнопку **Сохранить**.

Также вы можете настроить обращение ко всем серверам обновления через прокси-сервер.

На вкладке **Dr.Web® Enterprise Agent для Windows** в группе кнопок выбора указывается, требуется ли обновление всех файлов или только вирусных баз для рабочих станций под ОС Windows.



На вкладке **Dr.Web® Enterprise Server** в группе кнопок выбора указывается, для каких ОС требуется обновление файлов Сервера.

Для версий Сервера 5.0 и выше, вне зависимости от настроек данного раздела, обновления с серверов BCO не поставляются.

Для обновления Сервера используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах «Обновление Dr.Web ES для ОС Windows®».

4.2. Иерархия серверов

В случае необходимости администратор имеет возможность организации иерархии серверов **Dr.Web Enterprise Suite** и **Dr.Web ATM Shield**. Использование иерархии серверов позволяет не только экономить трафик, но и гибко распределять нагрузку между серверами.

Dr.Web Enterprise Security Suite позволяет организовать два типа связей между серверами: связь типа главный-подчиненный, при которой главный передает подчиненному обновления и получает обратно информацию о событиях, и связь между равноправными, при которой направления передачи и типы информации настраиваются индивидуально.

В антивирусной сети можно установить несколько **Enterprise Серверов**. При этом каждый **Enterprise Агент** присоединяется к одному из Серверов. Каждый Сервер вместе с присоединенными антивирусными рабочими станциями функционирует как отдельная антивирусная сеть, как описано в предыдущих разделах.

Dr.Web ATM Shield позволяет связать такие антивирусные сети, организовав передачу информации между **Enterprise Серверами**.

Dr.Web Enterprise Server может передавать другому Серверу **Dr.Web Enterprise Server**:

- обновления ПО и вирусных баз. При этом получать обновления серверов BCO Dr.Web будет только один из них.

  Мы рекомендуем вам добавить в расписание подчиненного **Enterprise Сервера** задание на обновление подчиненного **Enterprise Сервера** с серверов BCO на тот случай, если главный Сервер будет

временно недоступным. Это позволит Агентам получать обновление вирусных баз и программных модулей (подробная информация доступна в «Руководстве администратора», п. «Редактор конфигурации репозитория»).

- информацию о вирусных событиях, статистику работы и т. д.

При планировании структуры антивирусной сети следует обратить внимание на особенности лицензирования сети с несколькими Серверами.

Внимание! Каждый из входящих в сеть серверов должен использовать индивидуальные ключи enterprise.key с различными значениями ID сервера. Для того чтобы узнать значение ID, откройте ключ enterprise.key любым текстовым редактором и в секции [Enterprise] посмотрите значение параметра ID1.

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.

При помощи данного протокола:

- обновления передаются немедленно при их получении;
- отпадает необходимость в настройке расписания обновления на Сервере (кроме тех Серверов, которые получают обновления с серверов ВСО Dr.Web с использованием протокола HTTP).

Некоторые из преимуществ антивирусной сети с несколькими Серверами **Dr.Web Enterprise Server**:

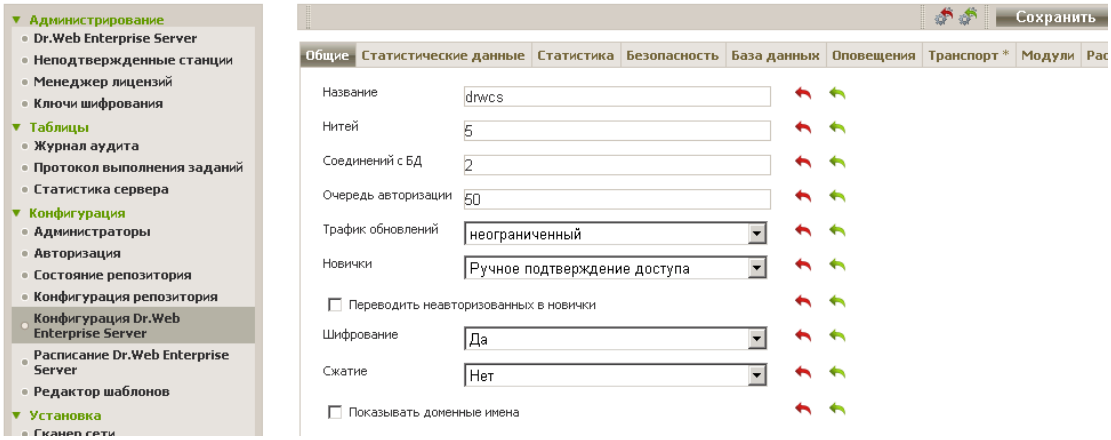
- возможность получения обновлений с серверов ВСО Dr.Web через один **Enterprise Сервер** с последующей передачей на остальные Серверы напрямую или через промежуточные звенья;
- возможность распределения рабочих станций по нескольким Серверам с уменьшением нагрузки на каждый из них;
- объединение информации от нескольких Серверов на одном; возможность получения ее в сеансе **Центра управления** на этом Сервере в консолидированном виде.

Dr.Web ATM Shield самостоятельно отслеживает и не допускает возникновения циклических путей передачи информации.

4.2.1. Соединение главного и подчиненного ES-серверов

Убедитесь, что оба **Enterprise Сервера** нормально функционируют и для каждого из **Enterprise Серверов** используются различные ключи enterprise.key, в каждом их которых прописаны индивидуальные ID сервера.

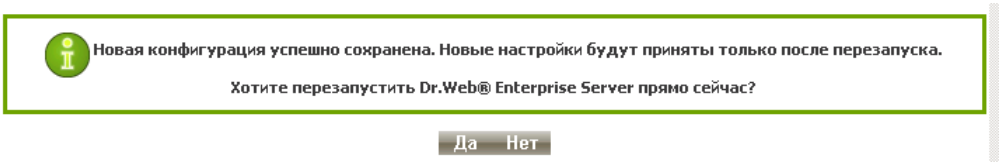
Проверьте, что все серверы имеют имена. Для того чтобы дать серверу имя, в пункте Конфигурация **Dr.Web® Enterprise Server** раздела **Администрирование** заполните поле **Название** и нажмите **Сохранить**.



Включите на обоих серверах серверный протокол. Для этого в пункте **Конфигурация Dr.Web® Enterprise Server** раздела **Администрирование** перейдите на закладку **Модули** и установите флаг **Протокол Dr.Web® Enterprise Server**.

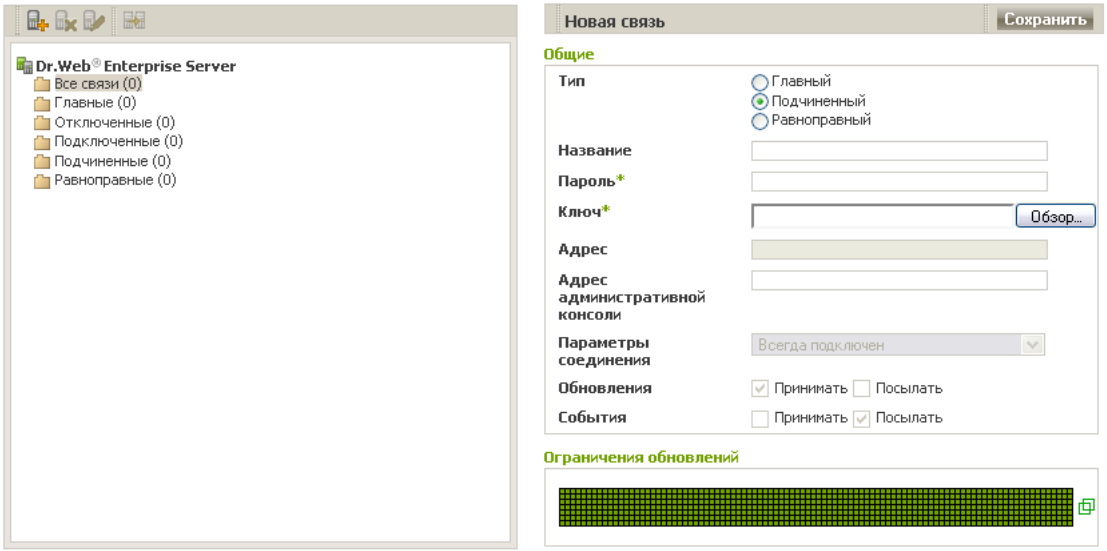
Если серверный протокол не включен, при создании новой связи в **Центре управления** будет выведено сообщение о необходимости включения данного протокола и дана ссылка на соответствующий раздел **Центра управления**.

Нажмите **Сохранить** и перезапустите оба сервера, ответив **Да** на запрос подтверждения



либо используя значок пункта **Dr.Web Enterprise Server** меню **Администрирование**.

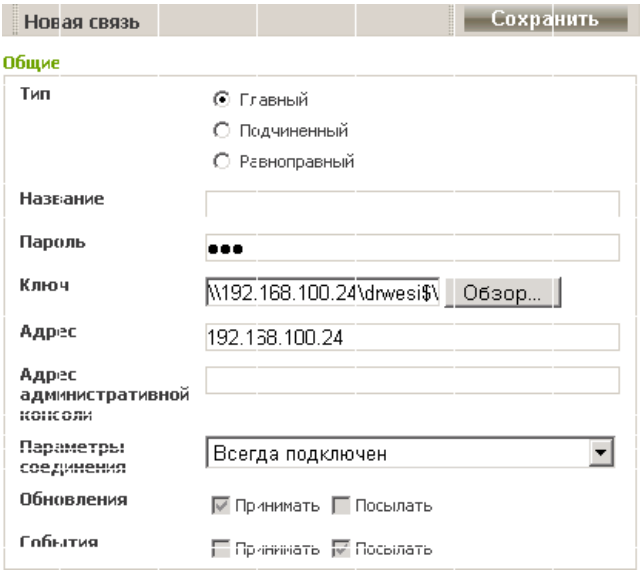
Выберите в разделе **Администрирование** пункт **Связи**. Откроется окно, содержащее иерархический список серверов антивирусной сети, «соседних» с данным. Для того чтобы добавить сервер в этот список, выберите в контекстном меню любого элемента или группы элементов пункт **Создать связь**. Откроется окно описания связей между текущим и добавляемым серверами.



Выберите тип **Главный**. В поле **Название** введите название главного для данного сервера, в поле **Пароль** введите произвольный пароль для доступа к нему. Справа от поля **Ключ** нажмите на кнопку и укажите ключ drwcsd.pub, относящийся к главному серверу, а в поле **Адрес** введите его адрес. При необходимости в поле **Адрес административной консоли** введите адрес компьютера, на котором запущена веб-консоль. В поле **Параметры соединения** выберите строку **Всегда подключен**. Нажмите на кнопку **Сохранить**.

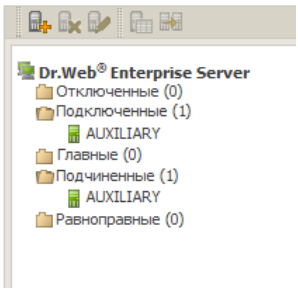
Флаги в разделах **Обновления** и **События** установлены в соответствии с принципом связи главный-подчиненный и не подлежат изменению:

- главный Сервер посылает обновления на подчиненные Серверы;
- главный Сервер принимает информацию о событиях с подчиненных Серверов.

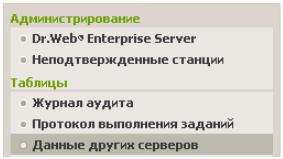


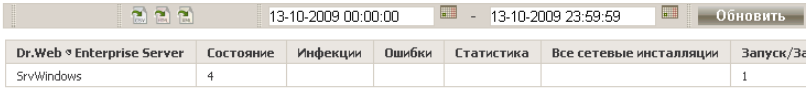
В результате главный сервер попадет в папки **Главные** и **Отключенные**. Аналогично добавьте подчиненный сервер в список соседних серверов главного сервера через его Веб-интерфейс. Поле **Адрес** заполнять не нужно. Пароль должен быть указан тот же, что и в первом случае, ключ drwcsd.pub должен относиться к подчиненному серверу. В результате подчиненный сервер будет включен в папки **Подчиненные** и **Отключенные**.

Установление связи занимает порядка минуты. Для проверки периодически обновляйте список серверов. После установления связи подчиненный сервер перейдет из папки **Отключенные** в папку **Подключенные**.



Просмотреть информацию и работе других серверов можно, используя пункт **Данные других серверов** меню **Администрирование**. Выведенная таблица содержит сведения об обнаруженных инфекциях, ошибках сканирования, статистики, сетевых инсталляциях, запуске и завершении заданий.





Невозможно связать два Сервера с одинаковым лицензионным ключом (enterprise.key) либо с различными ключами, использующими одинаковые значения ID сервера.

При создании связей между Серверами можно задать ограничение обновлений для связываемых Серверов. Для этого при создании связи на панели **Ограничение обновлений** нажмите на кнопку . Откроется окно редактирования режимов обновлений, описанное в п. «Ограничение обновлений».

Установка соединения между Серверами **Dr.Web Enterprise Server** невозможна в следующих случаях:

- Проблемы связи по сети.
- При настройке связи задан неверный адрес главного Сервера.
- Задан неверный открытый ключ шифрования drwcsd.pub на одном из Серверов.
- Задан неверный пароль доступа на одном из Серверов (заданы несовпадающие пароли на соединяемых Серверах).
- Одинаковый лицензионный ключ enterprise.key на обоих Серверах.

  Внимание! Значение ID внутри ключей enterprise.key на обоих Серверах должны различаться. При получении или продлении ключей для обоих Серверов необходимо указывать различные значения ID.
- Лицензионный ключ enterprise.key подключаемого подчиненного Сервера совпадает с лицензионным ключом подчиненного Сервера, уже подключенного к тому же к главному Серверу.

4.2.2. Использование антивирусной сети с несколькими антивирусными серверами

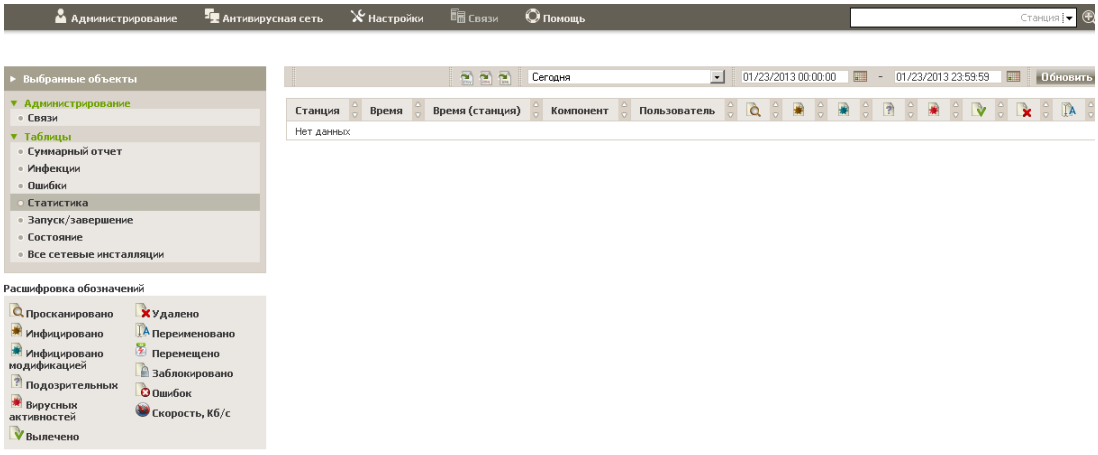
Особенностью сети с несколькими Серверами является получение обновлений с серверов ВСО Dr.Web через часть **Enterprise Серверов** (как правило, один или несколько главных Серверов). При этом только на этих Серверах следует настраивать расписание, содержащее задание на обновление (см. п. «Настройка расписания Dr.Web Enterprise Server»). 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 ATM Shield 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 Enterprise Server**, связанных с данным:

1) Выберите пункт **Связи** главного меню **Центра управления**, в открывшемся окне в разделе управляющего меню **Таблицы** выберите пункт для просмотра сведений об общем количестве имеющихся на данном Сервере записей о состоянии (пункт **Состояние**), обнаруженных инфекциях (пункт **Инфекции**), ошибках сканирования (пункт **Ошибки**), статистики (пункт **Статистика**), сетевых инсталляциях (пункт **Все сетевые инсталляции**), запуске и завершении заданий (пункт **Запуск/завершение**).



2) Задайте временной интервал выводимой статистики и нажмите на кнопку **Обновить**, чтобы загрузить в таблицу данные.

3) При необходимости сохранить таблицу для распечатки или дальнейшей обработки нажмите на панели инструментов на кнопку **Записать данные в файл в формате CSV, Записать данные в файл в формате HTML** или на кнопку **Записать данные в файл в формате XML**.

4.3. Резервное копирование критичных данных сервера

Перед началом эксплуатации антивирусного ПО рекомендуется изменить настройку каталога резервного копирования критичных данных Сервера (см. п. «Настройка расписания Dr.Web Enterprise Server»). Данный каталог желательно разместить на другом локальном диске, чтобы уменьшить вероятность одновременной потери файлов ПО Сервера и резервной копии.

Резервная копия критичных данных сервера (содержимого базы данных, лицензионного ключевого файла Сервера, закрытого ключа шифрования, конфигурационного файла и Веб-интерфейса) 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, можно импортировать в другую БД сервера при помощи ключа importdb и таким образом восстановить данные.

Сервер регулярно сохраняет резервные копии важной информации в \var\Backup рабочего каталога. Для этого в расписание включено ежедневное задание, выполняющее эту функцию. Если такое задание в расписании отсутствует, рекомендуется создать его.

Процедура восстановления сервера подробно описана в документации по продукту.

4.4. Восстановление забытого пароля

В случае если пароль администратора для доступа к ES-серверу забыт, то есть возможность его просмотра или изменения на любой желаемый с использованием прямого доступа к базе данных сервера.

Параметры учетных записей администраторов хранятся в таблице admins. В случае если используется внутренняя база, то необходимо применять утилиту drwidbsh, входящую в поставку сервера. Если используется внешняя база, то необходимо использовать sql-клиент.

Изменение пароля администратора при помощи утилиты drwidbsh

Запустите утилиту и укажите путь до файла базы:

Для Windows:

"C:\Program Files\DrWeb Enterprise Server\bin\drwidbsh" "C:\Program Files\DrWeb Enterprise Server\var\dbinternal.dbs"

Чтобы увидеть все данные, хранящиеся в таблице admins, необходимо выполнить команду:

```
select * from admins;
```

Чтобы увидеть пароли для имеющихся учетных записей администраторов, необходимо выполнить команду:

```
select login,password from admins;
```

Результат для варианта, когда существует только одна учетная запись "admin" и у нее пароль "root":

Для изменения пароля используется команда update. Пример изменения пароля от учетной записи "admin" на "qwerty":

```
update admins set password='qwerty' where login='admin';
```

Для выхода из утилиты требуется ввести команду

```
.exit
```

Описание работы утилиты drwidbsh можно найти в онлайн-документации по ссылке http://support.drweb.com/esuite/doc_ru/es_ru.html?h6.htm.

5. Обновление антивирусной сети Dr.Web Enterprise Security Suite

5.1. Обновление защищаемых узлов сети

Внимание! Рекомендации, приведенные в данном пункте, необходимо выполнить в обязательном порядке перед инсталляцией антивирусных агентов.

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.

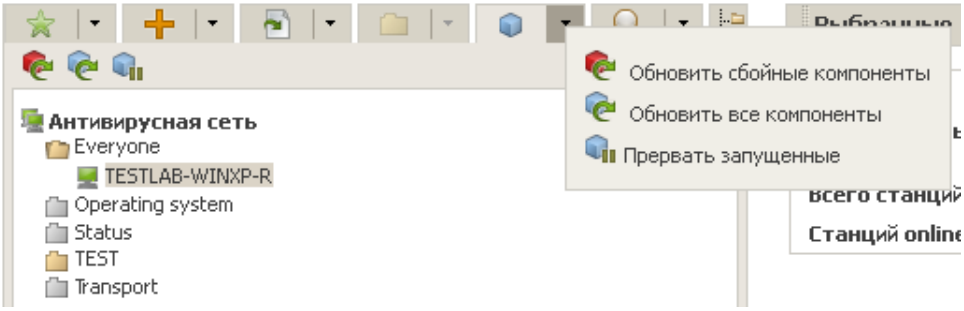
5.1.1. Проведение обновлений автоматически и вручную

Перед началом обновления **Dr.Web ES** и его отдельных компонентов настоятельно рекомендуем проверить корректность настроек протокола TCP/IP для возможности доступа в Интернет. В частности, должна быть включена и содержать корректные настройки служба DNS.

Чтобы проверить наличие обновления продуктов Dr.Web ATM Shield на сервере обновлений, выберите пункт **Состояние репозитория** меню **Администрирование**. В открывшемся окне отображается информация обо всех компонентах, а также дата их последней ревизии и ее текущее состояние. Для проверки наличия обновлений нажмите на кнопку **Проверить обновления**. Если проверяемый компонент устарел, то его обновление произойдет автоматически в процессе проверки.

Название	Последняя ревизия от	Состояние
Dr.Web Enterprise Agent для Windows Mobile	16-09-2011 16:06:55	Состояние продукта нормальное.
Dr.Web Enterprise Agent для Unix	16-09-2011 16:06:55	Состояние продукта нормальное.
Dr.Web Enterprise Agent для Windows	16-09-2011 16:06:43	Состояние продукта нормальное.
Dr.Web Enterprise Server	неизвестное время	Состояние продукта нормальное.
Dr.Web Enterprise Updater	16-09-2011 16:06:55	Состояние продукта нормальное.
Вирусные базы 5.0	16-09-2011 16:06:45	Состояние продукта нормальное.
Вирусные базы	16-09-2011 16:06:45	Состояние продукта нормальное.
Dr.Web Enterprise Agent для Android	16-09-2011 16:06:45	Состояние продукта нормальное.

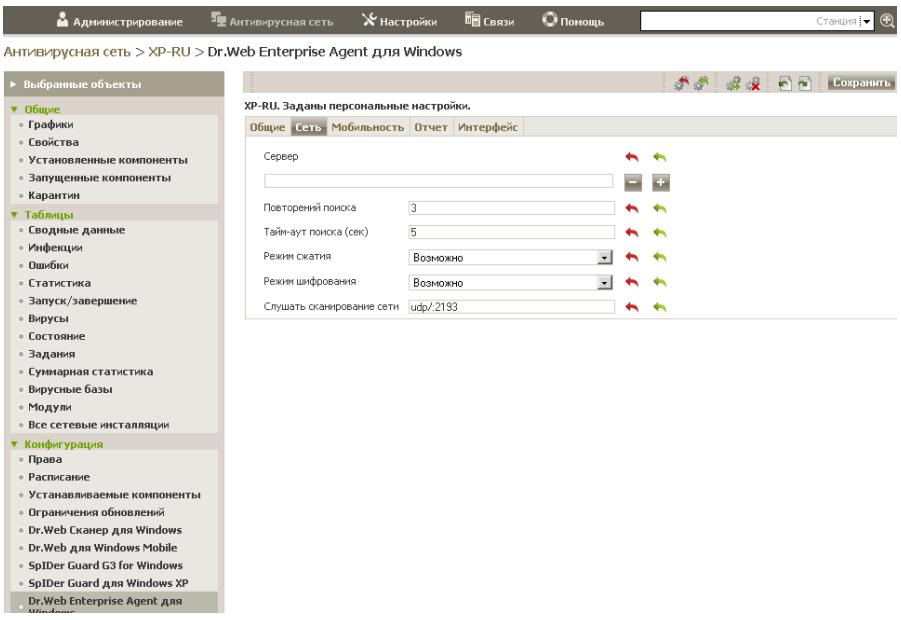
Для запуска процесса обновления выберите станцию или группу и выберите . В открывшемся подменю выберите пункт **Обновить сбойные компоненты**, если вы хотите обновить только те компоненты, предыдущее обновление которых сопровождалось ошибкой, и сбросить состояние ошибки; **Обновить все компоненты**, если вы хотите запустить принудительное обновление для всех компонентов.



Вы также можете провести эту операцию с помощью средств управления самого **Enterprise Агента**.

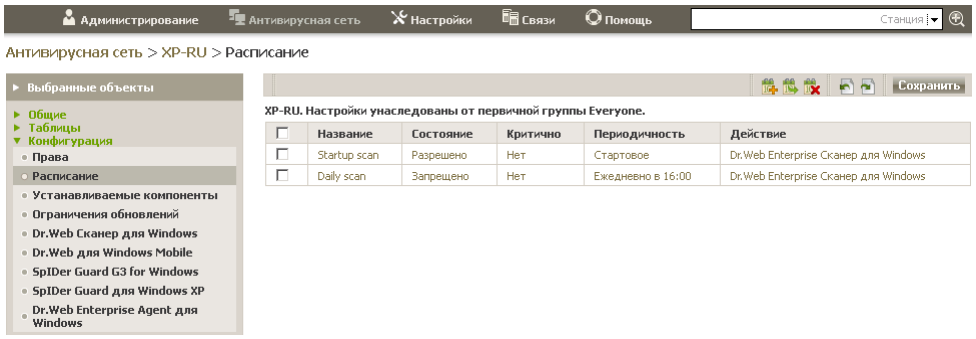
5.1.2. Настройка параметров обновлений рабочих станций и серверов

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 **Администрирование** и в закладке **Сеть** пункта **Dr.Web Enterprise Agent для Windows** задайте адрес источника обновлений.



5.1.2.1. Настройка обновления групп

Механизм групп позволяет одновременно изменять настройки для всех станций, входящих в определенную группу. Все подключенные 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 веб-интерфейса администратора. Для настройки расписания группы необходимо выбрать эту группу в каталоге антивирусной сети и в меню, расположенном слева, выбрать пункт **Расписание**.



В данном окне по можно отредактировать существующие задания и добавить новые по аналогии с подобными операциями для расписания ES-сервера.

Возможны четыре вида действий, исполняемых по расписанию.

Dr.Web® Enterprise Scanner для Windows — прозрачная для пользователей проверка рабочих станций на наличие вирусов Enterprise-сканером с возможностью тонкого задания настроек антивирусного сканирования.

Dr.Web® Сканер для Windows — проверка рабочих станций Сканером для Windows, возможные параметры — командная строка сканера.

Запуск — выполнение произвольного приложения на стороне рабочей станции. Возможные параметры — путь к исполняемому файлу и аргументы командной строки для исполняемого приложения.

Протоколирование — отправка на сервер заданного сообщения. Параметр — отправляемое сообщение (текстовая строка).

5.2. Управление ключевыми файлами

Права пользователя на использование антивируса регулируются при помощи пары ключевых файлов (ключевой файл для Сервера и ключевой файл для рабочей станции).

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® ATM Shield** зависят от количества защищаемых станций в сети (в том числе серверов, входящих в состав сети **Dr.Web® ATM Shield** как защищаемые станции).

Внимание! При покупке решения **Dr.Web ATM Shield** необходимо обязательно сообщить продавцу лицензии количество **Enterprise Серверов**, входящих в состав иерархической сети, в связи с тем что при подсчете защищаемых станций необходимо учитывать соединения между **Enterprise Серверами**, поскольку такие соединения требуют дополнительной лицензии. Для каждого **Enterprise Сервера** каждая межсерверная связь, вне зависимости от ее типа, требует отдельной лицензии, т. е. при связи двух Серверов дополнительная лицензия на межсерверную связь нужна обоим. Количество используемых независимых (не связанных друг с другом) **Enterprise Серверов** не влияет на увеличение стоимости лицензии.

Ключевые файлы поставляются пользователю в виде zip-архива, содержащего ключевой файл для **Сервера** (enterprise.key) и ключевой файл для рабочей станции (agent.key). Лицензионные ключевые файлы могут входить в комплект антивируса **Dr.Web® ATM Shield** 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 http://buy.drweb.com/register, если иной адрес не указан в регистрационной карточке, прилагаемой к продукту). Зайдите на указанный сайт, заполните форму со сведениями о покупателе и введите в указанное поле регистрационный серийный номер (находится на регистрационной карточке). Архив с ключевыми файлами будет выслан по указанному вами адресу. 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 http://download.drweb.com/demo. Ваш запрос будет рассмотрен в индивидуальном порядке. В случае положительного решения архив с ключевыми файлами будет выслан по указанному вами адресу.

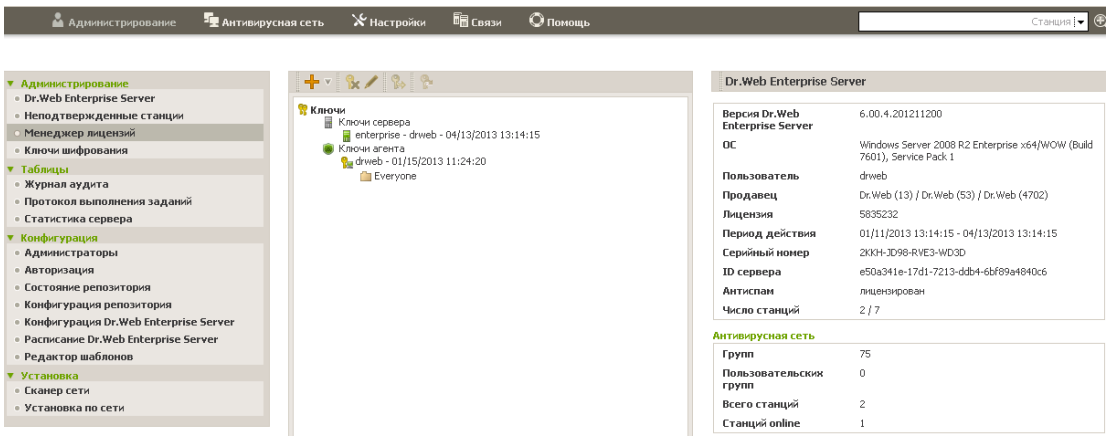
Использование полученных ключевых файлов в процессе установки программы описывается в разделах, рассказывающих о возможных вариантах установки **Dr.Web Enterprise Server**.

Использование ключевых файлов для уже развернутой антивирусной сети описано в разделе «Обновление антивирусной сети».

5.2.1. Менеджер лицензий

В состав **Enterprise Сервера** входит **Менеджер лицензий**. Данный компонент облегчает управление лицензионными ключевыми файлами Сервера и Агентов.

Для того чтобы открыть окно **Менеджера лицензий**, выберите в главном меню **Центра управления** пункт **Администрирование**, в открывшемся окне выберите пункт управляющего меню (панель слева) **Менеджер лицензий**.



Главное окно **Менеджера лицензий** содержит иерархический список, включающий:

- **Ключи сервера**. Элементами данного пункта являются учетные записи, содержащие лицензионные ключи Сервера. При этом только одна из учетных записей активна (используется Сервером в данный момент).
- **Ключи агента**. Элементами данного пункта являются учетные записи, содержащие лицензионные ключи Агента. Каждый лицензионный ключ может быть назначен для нескольких групп или станций, которые отображаются в окне **Менеджера лицензий** как вложенные элементы учетной записи ключа.

Для управления лицензионными ключами используются элементы Панели инструментов:

- **Импорт ключа** – позволяет добавить новую запись о ключевом файле. Для этого выберите соответствующий пункт выпадающего меню:
  - **Импорт серверного ключа** – для добавления нового ключевого файла Сервера.
  - **Импорт агентского ключа** – для добавления нового ключевого файла Агентов.
- **Удалить ключ** – позволяет удалить учетные записи ключевых файлов. Нельзя удалить учетную запись Агентского ключа, назначенного для группы **Everyone**, и текущую активную запись ключевого файла Сервера.
- **Редактировать** – для просмотра информации о лицензии, ее активации (только для Сервера) и, при необходимости, замены ключевого файла (только для Агента). Данный пункт активен, только если в главном окне выбрана учетная запись ключевого файла для Сервера или Агента.
- **Распространить эти настройки на другой объект** – позволяет назначить выбранный ключ на заданную группу или станцию, которые указываются в открывающемся списке. Данный пункт активен, только если в главном окне выбрана учетная запись ключевого файла для Агента.

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 лицензии, выберите в главном окне Менеджера лицензий учетную запись, информацию о которой вы хотите просмотреть, и нажмите на кнопку **Редактировать** на панели инструментов. В открывшейся панели будет выведена такая информация, как:

- пользователь лицензии,
- продавец, у которого была приобретена данная лицензия,
- идентификационный номер лицензии,
- дата истечения срока действия лицензии.

2) **Добавлять новые лицензионные ключи Сервера**. Для того чтобы добавить новый лицензионный ключ:
   1) нажмите на кнопку **Импорт ключа** на панели инструментов и в выпадающем списке выберите пункт **Импорт серверного ключа**;
   2) на открывшейся панели нажмите на кнопку **Обзор** и выберите файл с лицензионным ключом Сервера;
   3) нажмите на кнопку **Сохранить**.

Допускается задание нескольких учетных записей с ключевыми файлами. При этом только одна из лицензий Сервера будет активна.

3) **Изменять активность лицензии Сервера**:
   1) выберите учетную запись с той лицензией, которую вы хотите установить для Сервера, и нажмите на кнопку **Редактировать** на панели инструментов;
   2) в открывшейся панели нажмите на кнопку **Активировать**;
   3) после активации нового серверного ключа для продолжения работы перезагрузите Сервер.

4) **Удалять лицензионные ключи Сервера**. Для того чтобы удалить имеющийся лицензионный ключ Сервера:
   1) выберите в главном окне **Менеджера лицензий** ключ, который вы хотите удалить, и нажмите на кнопку **Удалить ключ** на панели инструментов;
   2) в диалоговом окне подтвердите удаление ключа.

Нельзя удалить текущую активную запись ключевого файла Сервера.

При помощи **Менеджера лицензий** вы можете осуществлять следующие действия над лицензионными ключами для **Dr.Web Enterprise Agent**.

1) **Просматривать информацию о лицензии**. Для того чтобы просмотреть сводную информацию о лицензии, выберите в главном окне **Менеджера лицензий** учетную запись, информацию о которой вы хотите просмотреть, и нажмите на кнопку **Редактировать** на панели инструментов. В открывшейся панели будет выведена такая информация, как:
   - пользователь лицензии,
   - продавец, у которого была приобретена данная лицензия,
   - идентификационный номер лицензии,
   - дата истечения срока действия лицензии,
   - поддержку каких антивирусных компонентов включает данная лицензия.
2) **Добавлять новые лицензионные ключи Агента.** Для того чтобы добавить новый лицензионный ключ Агента:
   1) нажмите на кнопку **Импорт ключа** на панели инструментов и в выпадающем списке выберите пункт **Импорт агентского ключа**;
   2) на открывшейся панели нажмите на кнопку **Обзор** и выберите файл с лицензионным ключом Агента;
   3) нажмите на кнопку **Сохранить**.

   Допускается задание нескольких учетных записей с ключевыми файлами Агентов.
3) **Заменять лицензионные ключи Агента на новые.** Для того чтобы заменить текущий лицензионный ключ Агента на новый:
   1) выберите в главном окне Менеджера лицензий объект (станцию или группу), для которого назначен ключ, который вы хотите заменить, и нажмите на кнопку **Редактировать** на панели инструментов;
   2) в открывшейся панели нажмите на кнопку **Обзор** и выберите файл с лицензионным ключом Агента;
   3) нажмите на кнопку **Сохранить**.

   Если список компонентов, лицензируемых для установки на станции, в новом ключе отличается от списка старого лицензионного ключа, то будет выведен запрос на задание настроек согласно списку компонентов из нового ключа.

   В предлагаемом списке объектов указаны станции и группы, у которых списки в старом и импортируемом ключах различны, а также список отличий (какие компоненты отсутствуют или добавлены в новом ключе).

   Установите флаги для тех объектов, для которых будут заданы новые настройки списков устанавливаемых компонентов. Для остальных объектов (для которых флаги не установлены) настройки останутся в том виде, в котором они были до замены ключа.
4) **Заменять лицензионные ключи Агента на ключи, уже входящие в антивирусную сеть.** Для того чтобы заменить текущий лицензионный ключ Агента на уже входящий в антивирусную сеть ключ:
   1) выберите в главном окне **Менеджера лицензий** ключ, который вы хотите назначить для объекта (станции или группы), и нажмите на кнопку **Распространить эти настройки** на другой

объект на панели инструментов;

2) в открывшемся окне выберите из списка нужную станцию или группу (эта группа должна содержать станции). Для выделения объекта или нескольких объектов достаточно нажать на них левой кнопкой мыши, аналогично для снятия выделения;

3) нажмите на кнопку **Сохранить**.

Если для станции или группы уже назначен ключ в персональных настройках, для назначения нового ключа, имеющегося в списке главного окна **Менеджера лицензий**, достаточно переместить данную группу или станцию при помощи мыши (drag and drop) на учетную запись ключа (при этом может наблюдаться небольшая задержка при обновлении списка главного окна).

Если список компонентов, лицензируемых для установки на станции, в новом ключе отличается от списка старого лицензионного ключа, то будет выведен запрос на задание настроек согласно списку компонентов из нового ключа.

В предлагаемом списке объектов указаны станции и группы, у которых списки в старом и импортируемом ключах различны, а также список отличий (какие компоненты отсутствуют или добавлены в новом ключе). Установите флаги для тех объектов, для которых будут заданы новые настройки списков устанавливаемых компонентов. Для остальных объектов (для которых флаги не установлены) настройки останутся в том виде, в котором они были до замены ключа.

5) **Удалять лицензионные ключи Агента.** Для того чтобы удалить имеющийся лицензионный ключ Агента:

1) выберите в главном окне **Менеджера лицензий** ключ, который вы хотите удалить, или объект (станцию или группу), для которой назначен этот ключ, и нажмите на кнопку **Удалить ключ** на панели инструментов;

2) в диалоговом окне подтвердите удаление ключа;

3) если для объекта, для которого удаляется ключ, были заданы персональные настройки списка устанавливаемых компонентов, то будет выведен запрос на удаление персональных настроек.

В предлагаемом списке объектов указаны станции и группы с персональными настройками. Установите флаги для тех объектов, для которых будет задано наследование настроек родительской группы. Для остальных объектов будут сохранены персональные настройки списков устанавливаемых компонентов в том виде, в котором они были до удаления ключа.

Нельзя удалить учетную запись Агентского ключа, назначенного для группы Everyone.

Если вы хотите полностью заменить (например, обновить закончившиеся лицензии) все лицензионные ключи компонентов антивирусной сети (как Сервера, так и Агента), выполните следующую последовательность действий в **Менеджере лицензий**.

1) Добавьте новый ключ Сервера.

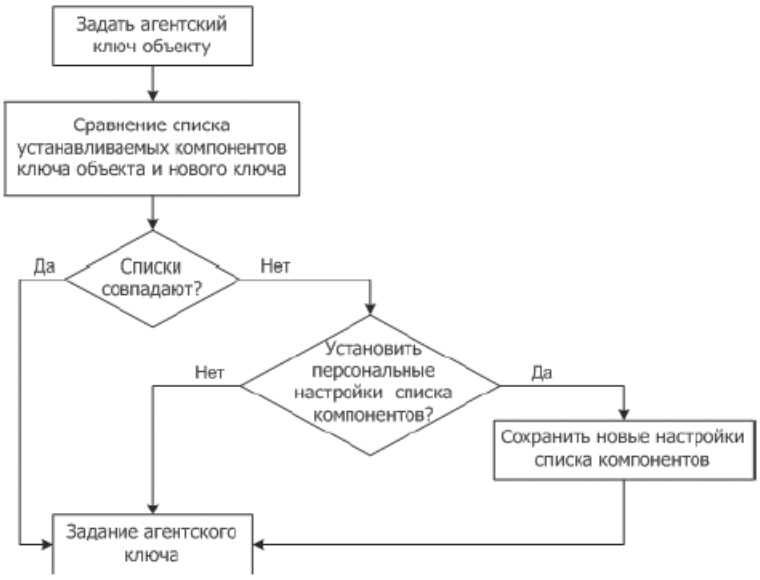
2) Активируйте новый ключ Сервера.

3) Удалите старый ключ Сервера.

4) Замените лицензионный ключ Агента для группы **Everyone** и, при необходимости, для остальных групп и станций, для которых лицензионные ключи были назначены персонально.

5.2.2. Изменение списка устанавливаемых компонентов при замене и удалении ключей

Если списки устанавливаемых компонентов в новом и старом ключах отличаются, настройки списков устанавливаемых компонентов объекта могут либо заменяться на новые, либо сохраняться (процедура замены лицензионного ключа Агента описана выше).



При задании новых настроек:

1) Если в новом ключе содержатся компоненты, которых не было в старом ключе, то для таких компонентов в списке **Устанавливаемые компоненты** будет задано значение **может**. В дальнейшем пользователь будет иметь возможность установить данные компоненты на станциях, лицензируемых новым ключом.
2) Если в новый ключ не включены компоненты, которые были включены в старый ключ, то для таких компонентов в списке **Устанавливаемые компоненты** будет выставлено значение **не может**, и они будут удалены со станций, лицензируемых новым ключом.
3) Для всех остальных компонентов, которые были включены в старый и новый ключи, настройки со страницы **Устанавливаемые компоненты** будут сохранены в том виде, в котором они были до замены ключа.

При сохранении настроек на странице **Устанавливаемые компоненты** настройки останутся в том виде, в котором они были до замены ключа.

При удалении лицензионного ключа группы настройки списков устанавливаемых компонентов могут либо наследоваться от родительской группы, либо сохраняться.

При наследовании настроек — на странице **Устанавливаемые компоненты** будут удалены персональные настройки и задано наследование настроек родительской группы.

При сохранении настроек — на странице **Устанавливаемые компоненты** настройки останутся в том виде, в котором они были до удаления ключа.

5.2.3. Импорт/обновление лицензионных ключей

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.

Если на компьютере с **Enterprise Сервером** установлен Агент с включенным компонентом самозащиты Dr.Web SelfPROtect, то перед заменой ключевых файлов необходимо отключить данный компонент через настройки Агента.

Для изменения ключевых файлов с помощью **Центра управления** вы можете использовать **Менеджер лицензий**. Кроме этого, замена ключей возможна в ручном режиме:

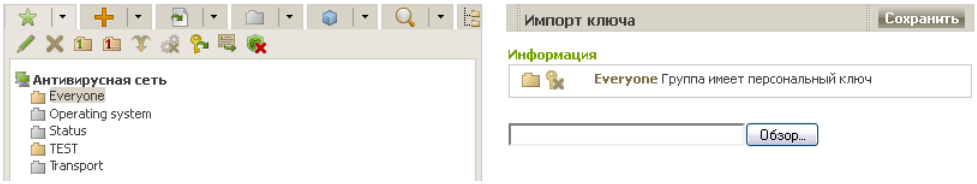
Для операционной системы Windows

Откройте старый и новый ключи enterprise.key любым текстовым редактором и в секции [Enterprise] посмотрите значение параметра ID1.

Если значения параметров ID1совпадают:

Поместите файл enterprise.key в подкаталог etc каталога установки Сервера вместо имеющегося там одноименного файла и перезапустите сервер, используя кнопку  , доступную в пункте **Dr.Web® Enterprise Server** меню **Администрирование**.

В каталоге антивирусной сети выберите группу **Everyone** и нажмите  .



Используя кнопку **Обзор**, укажите ключевой файл для рабочей станции (agent.key) и нажмите **Сохранить**.

Если значения параметров ID1 различаются:

Выберите пункт **Конфигурация Dr.Web® Enterprise Server** в меню **Администрирование** и перейдите на вкладку **Модули**. Снимите флаги **Протокол Dr.Web® Enterprise Agent** и **Протокол Dr.Web® Network Installer**. Нажмите **Сохранить**.

Откроется запрос перезапуска Сервера. Нажмите **Да**.

Выберите пункт **Расписание Dr.Web® Enterprise Server** в меню **Администрирование** и на панели инструментов нажмите .

Расписание Dr.Web Enterprise Server

	Название	Состояние	Критично	Периодичность	Действие
☐	Purge old stations	Разрешено	Нет	Ежедневно в 00:13	Удаление старых станций, 90
☐	Purge old data	Разрешено	Нет	Ежедневно в 00:43	Удаление старых записей, 90
☐	Update all Dr.Web products	Разрешено	Да	Ежечасно в 28 минуту	Обновление, Все продукты Dr.Web Enterprise
☐	Update all Dr.Web products	Разрешено	Нет	Ежечасно в 58 минуту	Обновление, Все продукты Dr.Web Enterprise
☐	Backup sensitive data	Разрешено	Нет	Ежедневно в 05:30	Резервное копирование критичных данных сервера
☐	Key expiration reminder	Разрешено	Нет	Ежедневно в 07:30	Напоминание об окончании лицензии, 10
☐	Long time unseen stations	Разрешено	Нет	Ежедневно в 07:30	Станция долго не посещала сервер, 3
☐	Purge unsent IS events	Разрешено	Нет	Ежечасно в 17 минуту	Удаление неотправленных событий, 12

Выберите пункт **Расписание Dr.Web® Enterprise Server** в меню **Администрирование** и на панели инструментов, нажав **Удалить эти настройки**, удалите расписание ESS-сервера.

В случае иерархической сети удалите все настроенные межсерверные связи меню **Администрирование**, пункт **Связи**.

Поместите файл с серверным ключом enterprise.key в подкаталог etc каталога установки сервера вместо имеющегося там одноименного файла.

Перезапустите сервер.

В каталоге антивирусной сети выберите группу **Everyone** и на панели инструментов нажмите **Импорт ключа**. Используя кнопку **Обзор**, укажите ключевой файл для рабочей станции. Нажмите **Сохранить**.

Для задания ключевых файлов вы также можете использовать **Менеджер лицензий**.

Включите отключенные ранее протоколы Агента и Сетевого инсталлятора.

Настройте расписание сервера заново или импортируйте из файла сохраненное расписание.

В случае иерархической сети настройте все ранее удаленные связи.

Перезапустите сервер.

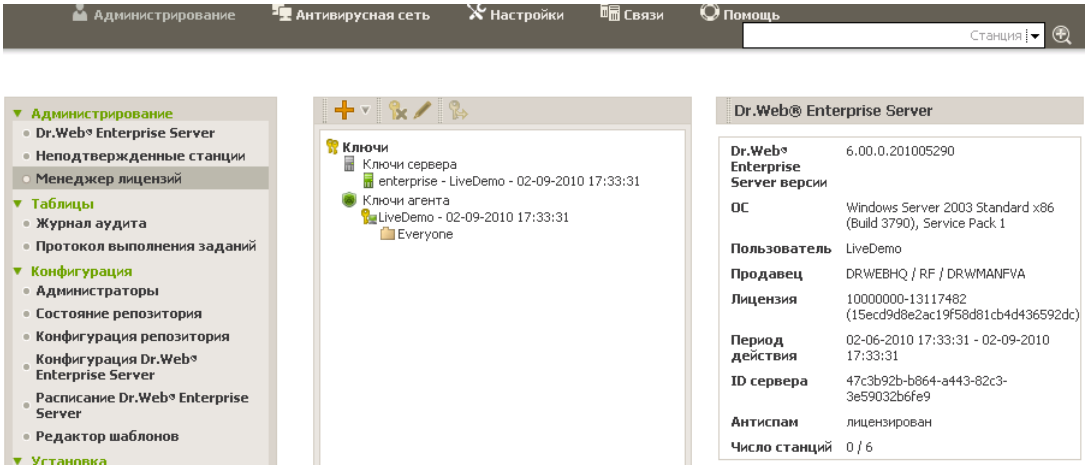
Далее следует обновить агентский лицензионный ключ. Обновление агентского лицензионного ключа выполняется импортом файла агентского ключа `agent.key` всем антивирусным станциям, для чего в веб-консоли перейдите в раздел **Антивирусная сеть**, выберите в списке группу **Everyone** и в верхнем меню нажмите кнопку **Импорт ключа** в виде ключа со стрелкой. В появившемся справа разделе нажмите кнопку **Обзор**, выберите файл `agent.key`, после чего нажмите кнопку **Сохранить**.

Если используется устаревшая версия сервера 5.xx, вместо agent.key следует использовать `agent0.key`, а лицензионный ключ `agent1.key` нужно таким же образом импортировать в группу `AV+AS+PS+SRV`.

После импорта агентского лицензионного ключа следует убедиться, что ни одна из групп не содержит просроченных агентских ключей. Для этого в веб-консоли перейдите в раздел **Администрирование**, в левой части страницы выберите **Менеджер лицензий** и в появившемся списке выберите и удалите все просроченные ключи. Для удаления просроченного ключа выберите соответствующую запись из списка и нажмите кнопку **Удалить ключ** с изображением креста на фоне ключа в меню выше. Станции и группы, ключи которых были удалены таким способом, унаследуют агентский лицензионный ключ от родительской группы (чаще всего **Everyone**).

5.2.4. Просмотр информации о лицензиях

Для просмотра информации о текущих лицензиях необходимо перейти в раздел **Администрирование** (Administration) и выбрать пункт **Менеджер лицензий (License manager)**.



Для того чтобы добавить или удалить ключ, необходимо выбрать значок или .

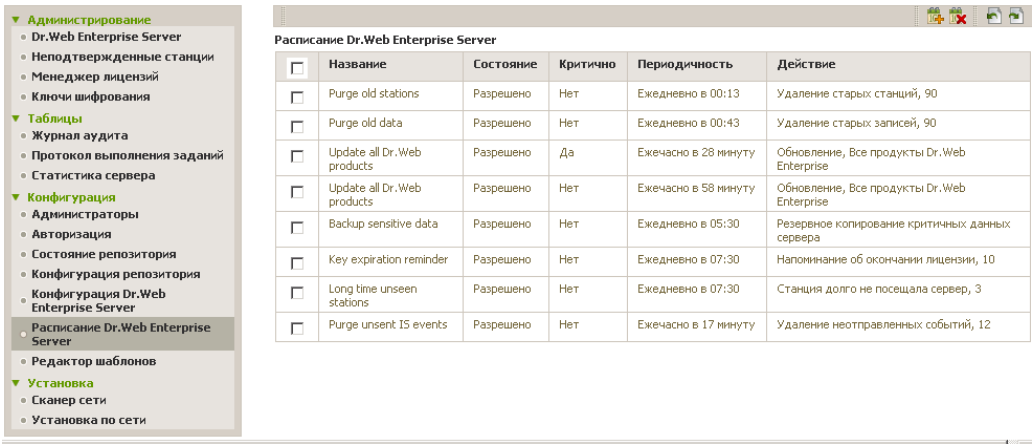
5.3. Обновление сервера Dr.Web Enterprise Security Suite

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 антивирусного сервера. Рекомендуется постепенное обновление с ограничением доступа к серверу в пределах сегментов сети. Также целесообразно уведомить специалистов технической поддержки об обновлении антивирусного ПО.

В связи с выходом новых версий возникает необходимость обновлять серверную часть комплекса. Начиная с версии 5.00 реализован механизм, позволяющий автоматически обновлять клиентов более ранних версий (в том числе 4.44) до версии, установленной на сервере. При обновлении также сохраняются настройки сервера, хранящиеся в БД и все настройки и записи, касающиеся имеющихся ID. Однако обновление с копированием файлов новой версии поверх устаревшей в ряде случаев не может быть выполнено корректно, поэтому необходимо сначала удалить устаревшую версию, после чего произвести установку новой версии с последующим восстановлением конфигурационных файлов.

5.3.1. Настройка обновления антивирусного сервера

Чтобы настроить расписание выполнения заданий, выберите в меню **Администрирование** пункт **Расписание Dr.Web® Enterprise Server**. Откроется текущий список заданий сервера. Используя данную страницу, вы можете добавлять, удалять и настраивать любые задания, в том числе задания обновления.

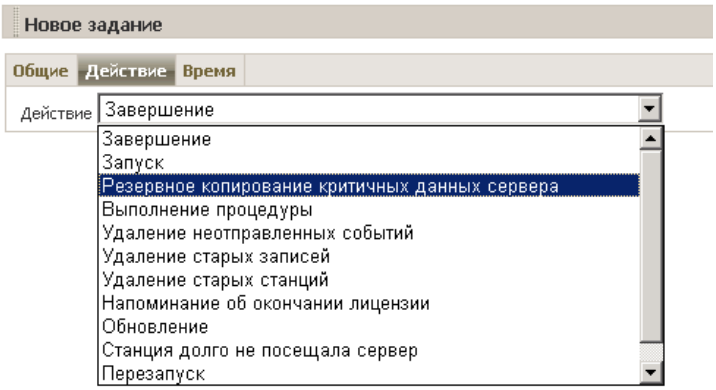


Для того чтобы добавить задание в список, выберите в контекстном меню значок . Откроется окно редактирования задания.

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.

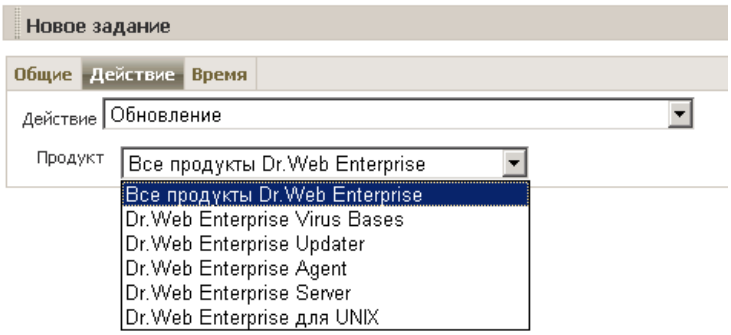
Перейдите на закладку **Действие** и в выпадающем меню выберите тип задания **Обновление**. При этом изменится вид нижней части окна, содержащей параметры данного типа задания. Введите эти параметры (ниже параметры типа задания рассмотрены отдельно по типам).



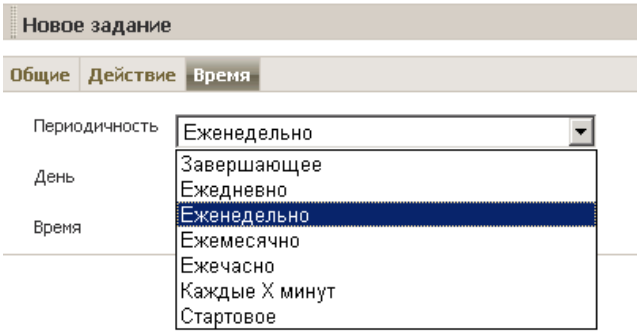
В выпадающем списке выберите вид обновляемого данным заданием продукта — **Dr.Web® Enterprise Agent, Dr.Web® Enterprise Server, Dr.Web® Enterprise Updater, Dr.Web® Virus Bases** или **Все продукты Dr.Web® Enterprise**, если вы хотите дать задание на обновление всех компонентов **Dr.Web ES**.

Для версий 5.0 и выше обновления ПО Сервера с серверов ВСО не поставляются. Для обновления Сервера используйте инсталлятор необходимой версии и проведите процедуру обновления согласно общим правилам, приведенным в разделах «Обновление Dr.Web ES для ОС Windows®».

Выберите в выпадающем списке **Продукт** вид обновляемого данным заданием продукта.



На закладке **Время** выберите в списке периодичность запуска задания и настройте время в соответствии с выбранной периодичностью.



Задания типов **Завершение** и **Перезапуск** параметров не имеют.

Для задания типа **Запуск** введите в поле **Путь** путь к исполняемому файлу сервера, в поле **Аргументы** – параметры командной строки при запуске. С помощью флажка **Выполнять синхронно** определите способ выполнения задания.

Для задания типа **Протоколирование** следует указать текст сообщения, которое заносится в протокол.

Для заданий типа **Удаление старых станций** и **Удаление старых записей** необходимо указать период, при превышении которого записи или станции признаются старыми.

Для заданий типа **Станция долго не посещала сервер** необходимо указать период, по истечении которого станция считается долго не посещавшей сервер.

Задания типа **Резервное копирование критичных данных сервера** предназначены для создания резервной копии критичных данных сервера (база данных, серверный лицензионный ключевой файл, закрытый ключ шифрования). Следует указать путь к каталогу, в который будут сохранены данные (пустой путь означает каталог по умолчанию), и максимальное количество резервных копий (значение 0 означает отмену этого ограничения).

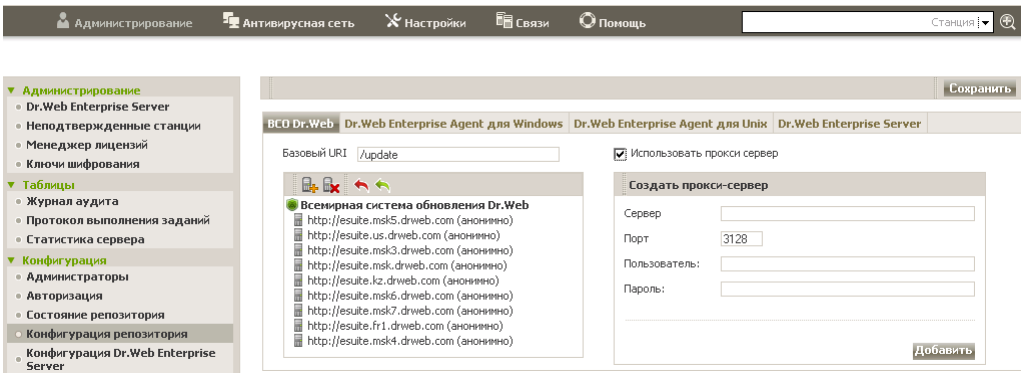
Задания типа **Обновление** предназначены для автоматического обновления продукта в репозитории и имеют единственный параметр: название обновляемого продукта, выбираемое из выпадающего списка.

Для того чтобы сохранить изменения настройки, нажмите на кнопку **Сохранить**.

Для того чтобы удалить задание из списка, выделите его с помощью флажка и нажмите кнопку **Удалить эти настройки** на панели инструментов.

Для того чтобы отредактировать параметры задания, выберите его в списке, после чего в контекстном меню выберите пункт **Редактировать**. При этом откроется **Редактор заданий**, описываемый ниже.

Включение авторизации на прокси-серверах MS ISA и IIS для обновления **Enterprise Сервера** с BCO осуществляется на странице **Конфигурация репозитория** меню **Администрирование**. Для конфигурирования параметров доступа необходимо выбрать пункт **Использовать прокси-сервер** и указать необходимые параметры.



При этом выбор способа шифрования из возможных Basic, Digest / Digest IE, NTLM (Kerberos) осуществляется автоматически.

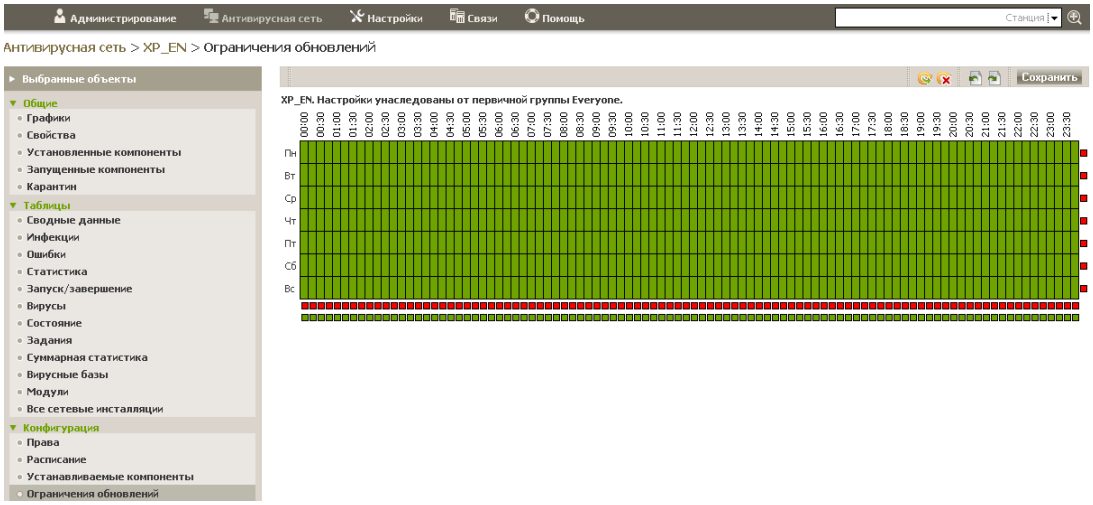
5.3.1.1. Ограничение обновлений

При помощи **Центра управления** вы можете задать режим обновлений (разрешено/запрещено) для компонентов **Dr.Web ATM Shield** в определенные промежутки времени. Для этого:

1) Выберите пункт **Антивирусная сеть** главного меню, в открывшемся окне в иерархическом списке нажмите на название станции или группы. В управляющем меню (панель слева) выберите пункт **Ограничение обновлений** — откроется таблица, в которой задается режим обновления в следующей цветовой градации:

- зеленый цвет — обновление разрешено;
- красный цвет — обновление запрещено.

При этом ограничение задается отдельно на каждые 15 минут каждого дня недели.



Для изменения режима обновлений нажмите на соответствующий блок таблицы. Для изменения режима целой строки (одного дня полностью) нажмите на маркер соответствующего цвета справа от требуемой строки таблицы. Для изменения режима целого столбца (одного 15-минутного интервала для всех дней недели) нажмите на маркер соответствующего цвета под требуемым столбцом таблицы.

После завершения редактирования нажмите на кнопку **Сохранить** для принятия внесенных изменений.

На панели инструментов доступны следующие опции.

Распространить эти настройки на другой объект — для копирования настроек обновлений данной станции или группы в настройки другой станции или группы.

Удалить эти настройки — для сброса настроек обновлений в исходное значение по умолчанию (все обновления разрешены).

Экспортировать настройки в файл — для сохранения настроек обновлений в файл специального формата.

Импортировать настройки из файла — для загрузки настроек обновлений из файла специального формата.

5.3.1.2. Обновление при отсутствии выхода в Интернет

В случае отсутствия выхода в Интернет репозиторий можно обновить вручную, скопировав репозиторий с другого сервера. Для этого необходимо выполнить следующие действия.

Остановите оба сервера — например, нажав кнопку , доступную в пункте **Dr.Web® Enterprise Server**, меню **Администрирование**.

Запустите сервер, подключенный к Интернету, с ключом syncrepository. Пример для Windows:

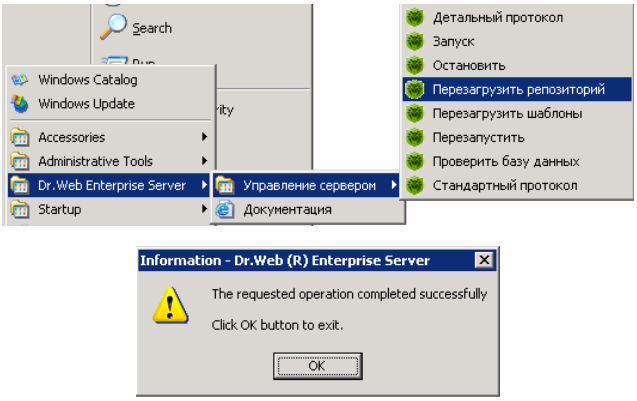
```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\
DrWeb Enterprise Server" syncrepository
```

Скопируйте содержимое каталога репозитория данного сервера в аналогичный каталог другого сервера. Обычно это var\repository под Windows.

Выполните на обновляемом сервере команду drwcsd rerepository, предварительно сменив каталог на место размещения утилиты. На сервере Windows это можно сделать, выполнив в командной строке команду

```
cd "C:\Program Files\DrWeb Enterprise Server\bin"
drwcsd.exe rerepository
```

или выполнив команду **Dr.Web Enterprise Server → Server control → Reload** из меню **Пуск**.



Запустите обновленный сервер.

5.3.2. Обновление сервера Dr.Web ATM Shield под ОС Windows

Обновление ранее установленного **Dr.Web Enterprise Security Suite** версий 4.44, 4.70 и 5.0 осуществляется автоматически средствами инсталлятора. При обновлении ранее установленного **Dr.Web Enterprise Security Suite** в пределах версии 6.0.X необходимо вручную удалить установленный **Dr.Web Enterprise Security Suite** и произвести установку заново.

При удалении текущей версии инсталлятор сохраняет следующие файлы:

- `dbinternal.dbs` – внутренняя БД,
- `drwcsd.conf` (имя может отличаться) – конфигурационный файл Сервера,
- `drwcsd.pri` и `drwcsd.pub` – закрытый и открытый ключи шифрования,
- `enterprise.key` и `agent.key` (имена могут отличаться) – лицензионные ключи Сервера и Агента,
- `certificate.pem` – сертификат для SSL,
- `private-key.pem` – закрытый ключ RSA.

При необходимости сохраните другие важные для вас файлы в другом месте, отличном от каталога установки сервера **Dr.Web Enterprise Security Suite**, например, конфигурационный файл **Центра управления** webmin.conf и шаблоны отчетов, находящиеся в каталоге \var\templates. После установки вы сможете заменить новые файлы сохраненными.

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.

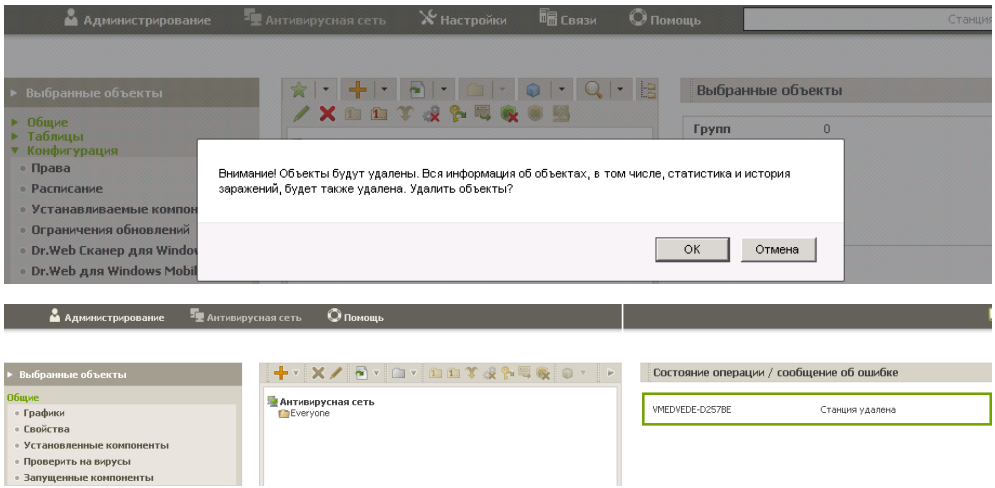
Возможны два варианта обновления ПО Сервера до версии 6.0.4.

- Автоматическое – обновление Сервера с версий 5.0 и 6.0.0 средствами инсталлятора. Автоматическое обновление возможно только для Серверов с одинаковой разрядностью. Например, если на x64 компьютере был установлен x32 Сервер, запущенный x64 инсталлятор не обнаружит установленный Сервер для запуска процесса обновления и установит новый Сервер параллельно.
- Ручное – при обновлении Сервера с версий 4.XX, 6.0.2 и выше необходимо вручную удалить предыдущий Сервер и установить новый Сервер.

6. Удаление компонентов антивирусной сети Dr.Web Enterprise Security Suite

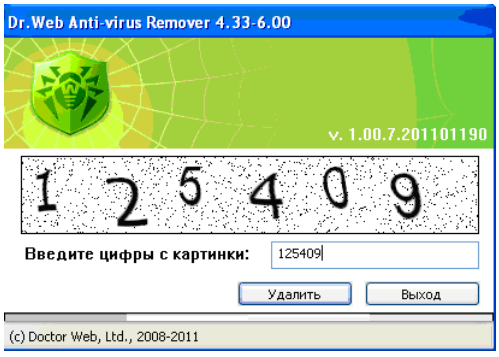
6.1. Удаление с использованием Веб-администратора Центра управления Dr.Web Enterprise Security Suite

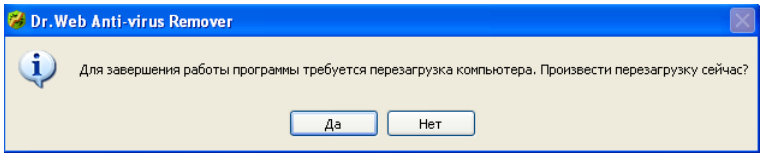
Для удаления ранее установленного агента необходимо в разделе **Антивирусная сеть** выбрать необходимую станцию, нажать на ✖ и подтвердить удаление.



6.2. Удаление с использованием утилиты Drw_remover

Для удаления ранее установленных продуктов на отдельных рабочих станциях и серверах можно использовать утилиту Drw_remover.exe. После ее запуска на машине с установленным продуктом необходимо ввести подтверждение и подтвердить перезагрузку.

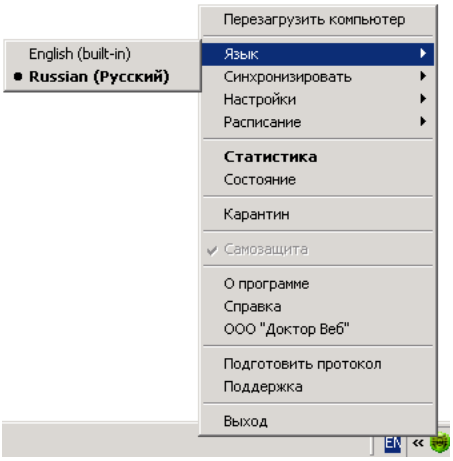




7. Настройка антивирусной защиты на стороне пользователя

7.1. Настройка языка интерфейса

Для смены языка выберите в контекстном меню значка агента пункт меню **Язык**. В выпадающем списке укажите необходимый язык интерфейса.

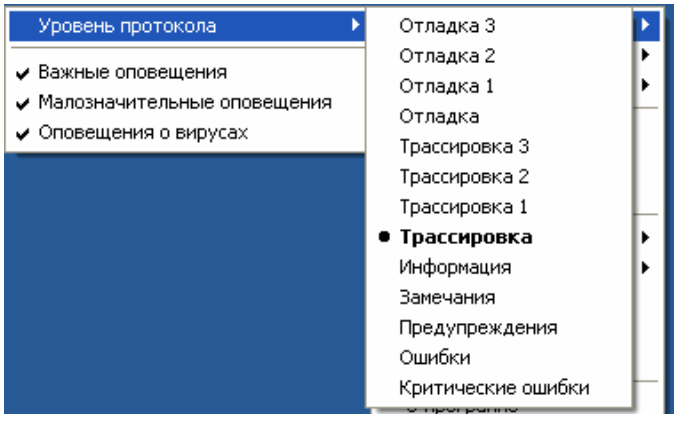


7.2. Обновления

В случае необходимости и при наличии соответствующих прав пользователь может самостоятельно обновить вирусные базы. Для запуска обновления необходимо выбрать пункт контекстного меню **Синхронизировать** и в появившемся меню указать **Только сбойные компоненты** или **Все компоненты**.

7.2.1. Изменение уровня подробности протокола событий

Изменение уровня протокола осуществляется при помощи пункта контекстного меню **Настройки** → **Уровень протокола**.

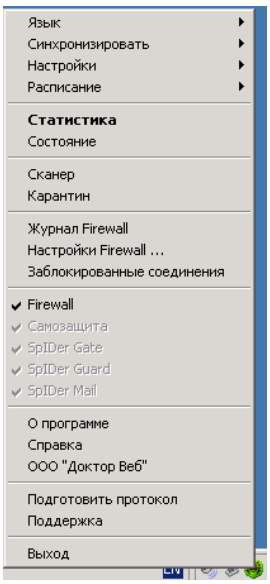


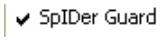
Данный пункт доступен в меню только при наличии у пользователя прав, позволяющих изменять данные настройки, и прав администратора на данном компьютере.

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. Для устранения проблемы необходимо установить соответствующий язык системы для программ, не поддерживающих Unicode.

7.3. Изменение списка разрешенных компонентов на рабочей станции

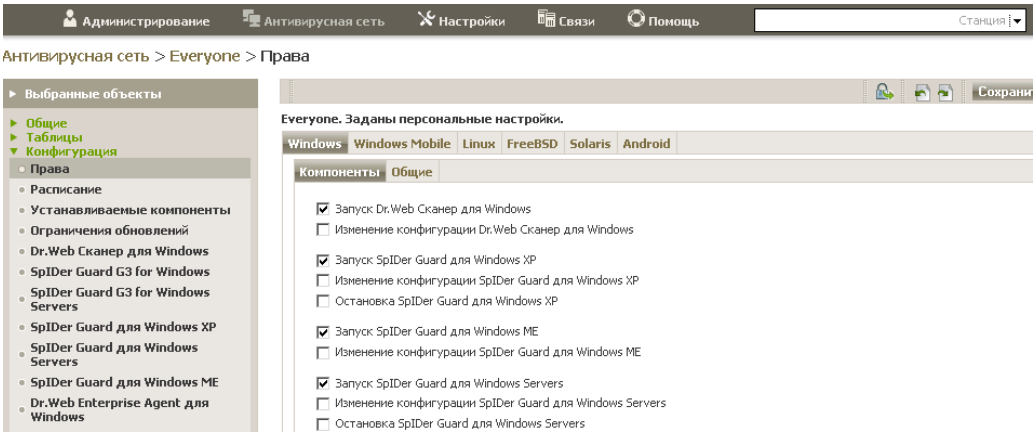
Пользователь всегда может изменить список действующих у него на компьютере компонентов защиты – остановить и запустить их. Для выполнения этих действий он должен выбрать значок в панели задач и снять флаг слева от названия компонента.



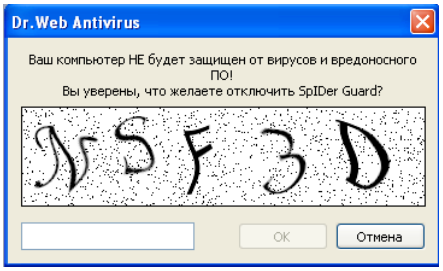


Внимание! Часть пунктов может быть недоступна для редактирования. Доступность настроек для редактирования определяется правами, определенными для группы или конкретной станции.

Для того чтобы настройки компонентов были доступны для пользователя, их надо разрешить для данной станции или группы в разделе **Права**.



Для подтверждения своих действий пользователь должен ввести код из появившегося окна.



7.4. Антивирусная проверка станции. Выбор приоритета сканирования

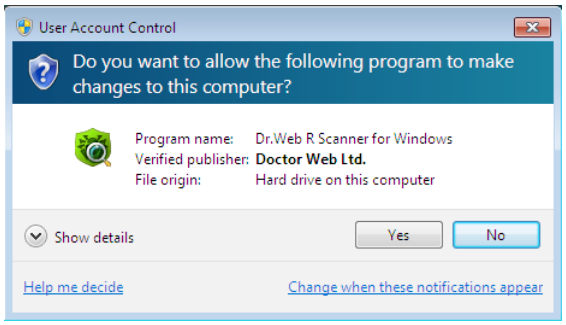
Рекомендуется сразу после инсталляции провести полную проверку системы. Рекомендуется также проводить такую проверку регулярно. В частности, это необходимо в связи с тем, что проверенные файловым монитором и записанные на диск файлы (в том числе сохраненные в архивы) могут содержать вирусы, неизвестные на момент их записи на диск, а значит, при передаче их на незащищенные компьютеры возникает риск их заражения.

Для проведения проверки необходимо щелкнуть правой кнопкой мыши на иконке Dr.Web и выбрать пункт **Сканер**, либо дважды щелкнуть по иконке 

, находящейся на рабочем столе.

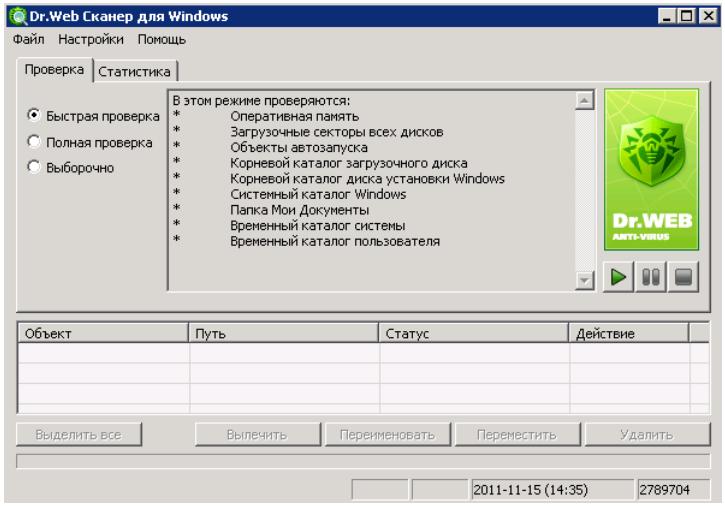
Внимание! По умолчанию для тестовой среды доступ в сеть Интернет закрыт. В связи с этим часть вирусов из тестовых коллекций может не обнаруживаться. Для проведения тестирования на качество детектирования на основе коллекций, содержащих актуальные вредоносные файлы, необходимо либо провести обновление вручную, либо при заказе тестирования указать необходимость доступа в сеть Интернет для проведения обновлений.

Внимание! Если вы используете Windows 7, то далее вам нужно будет подтвердить запуск программы, нажав на **Yes**.



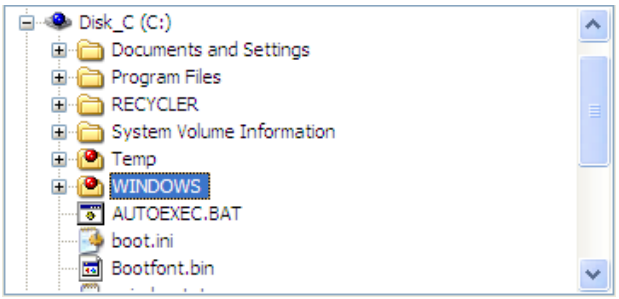
7.4.1. Антивирусная проверка Сканером NT4

После завершения загрузки сканера, в ходе которой производится быстрая проверка областей системы, наиболее подверженных заражению, в главном окне необходимо выбрать нужный тип проверки — полный или выборочный.



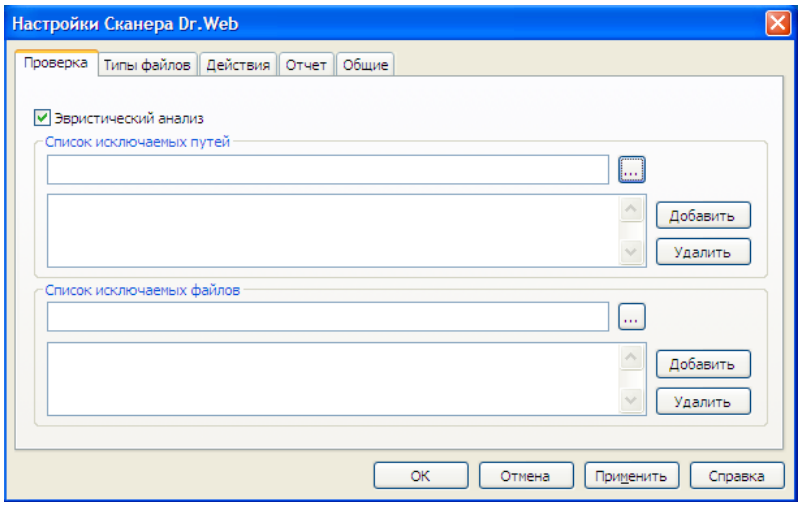
В случае выборочного типа проверки в окне сканера будут показаны все имеющиеся диски системы. Пользователь может отметить для проверки весь диск целиком или отдельные каталоги. Выбор

осуществляется щелчком левой кнопкой мыши по интересующей папке. Помеченные для проверки каталоги помечаются значком .



Пользователь может как запустить проверку с настройками по умолчанию, так и изменить предложенные настройки. В первом случае он должен просто щелкнуть по кнопке . Для изменения настроек необходимо выбрать пункт меню **Настройки** и затем подменю **Изменить настройки**, или просто нажать кнопку F9, находясь в окне сканера.

На закладке **Проверка** можно уточнить список проверяемых каталогов, задав исключаемые из проверки папки и файлы. Это можно сделать, нажав на значок … и выбрав их из появившегося дерева каталогов. Для добавления выбранной папки необходимо нажать на кнопку **Добавить**.

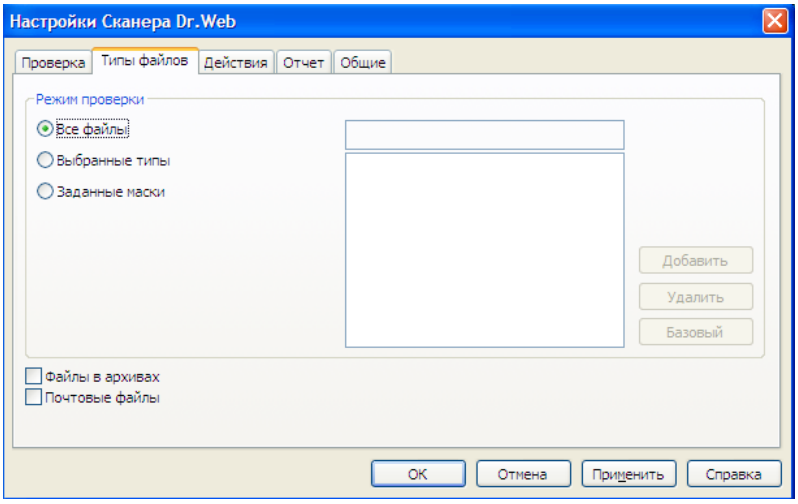


На этой же закладке пользователь может выбрать — использовать ли при проверке эвристический анализ или нет. Использование эвристического анализа позволяет находить вредоносные файлы, не занесенные в вирусные базы, однако замедляет процесс проверки.

На закладке **Типы файлов** уточняется список проверяемых файлов. Пользователь может сделать это, выбрав пункты **Выбранные типы** или **Заданные папки**. Отредактировать списки можно с помощью кнопок **Добавить** и **Удалить**. Пользователь всегда может вернуться к настройкам по умолчанию, нажав кнопку **Базовый**.

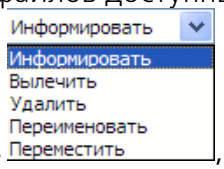
По умолчанию в ходе проверки сканер не проверяет архивы и почтовые файлы, так как их проверка занимает много времени, а вредоносные файлы из них могут быть запущены только после обработки архиваторами или почтовыми программами, в ходе чего они будут обнаружены специализированными компонентами. Однако если пользователь желает проверять эти форматы, он можете отметить их, выбрав соответствующие пункты.

Внимание! Рекомендуется всегда проверять архивы перед их отправкой кому-либо.

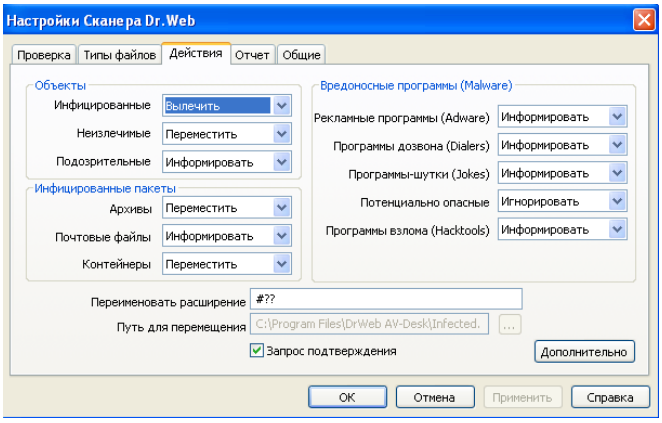


На закладке **Действия** пользователь может определить действия, применяемые к вредоносным объектам различного типа. По умолчанию для всех объектов стоит действие **Информировать**. В этом случае при обнаружении каждого вредоносного объекта пользователь должен будет принимать решение о том, что с ним нужно сделать, что может быть неудобно и требует постоянного присутствия пользователя за проверяемой машиной.

Необходимо отметить, что для различных объектов список возможных действий является различным. Так, если для инфицированных файлов доступны действия **Информировать**, **Вылечить, Удалить, Переименовать** и **Переместить**

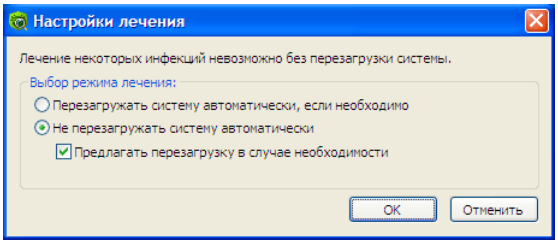


, то для неизлечимых пункт **Вылечить** недоступен.

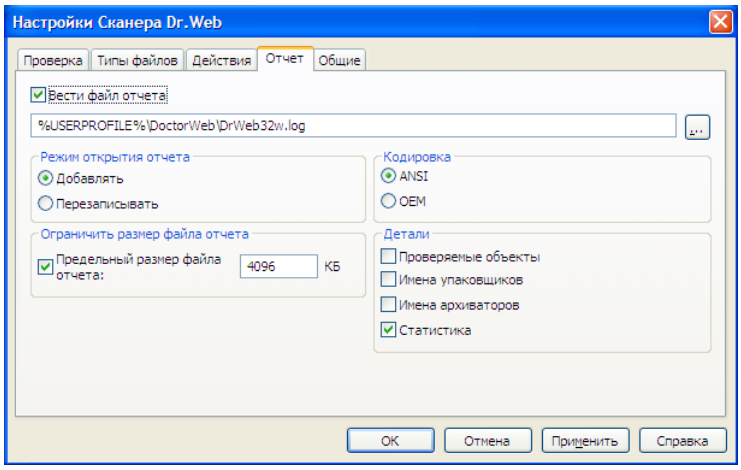


На этой же закладке задается путь к папке карантина — месту хранения вредоносных файлов. Рекомендуется использовать опцию сохранения копий зараженных файлов. Это позволит, в частности, проанализировать пути их распространения, получить иную дополнительную информацию либо восстановить утерянную информацию, в случае если файл был поврежден вирусом и не может быть восстановлен.

После нажатия кнопки **Дополнительно** пользователь должен решить, что необходимо делать при обнаружении вирусов, лечение которых требует перезагрузки.

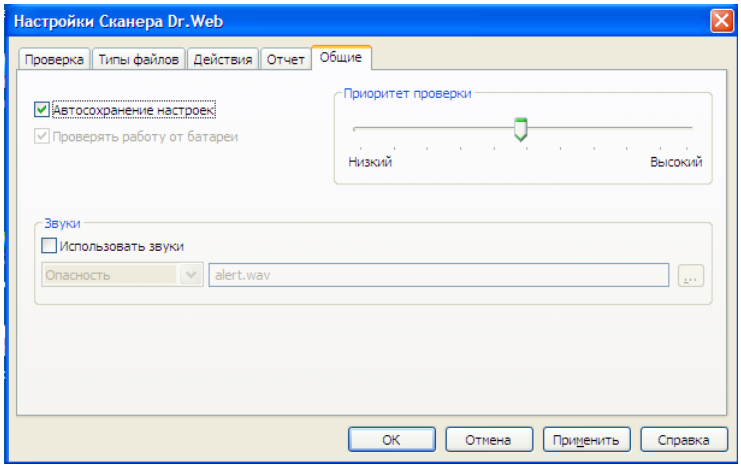


На закладке **Отчет** задается место размещения отчета, его детализация и предельный размер. Ограничение отчета позволяет предотвратить переполнение раздела, на котором создается отчет, но при слишком малом размере отчета возможна ситуация потери необходимой части информации.



Не рекомендуется отказываться от ведения отчета о проверке, хотя это и несколько ускоряет ее ход.

На вкладке **Общие** пользователь может с помощью бегунка выбрать приоритет проверки. Высокий приоритет проверки сокращает ее время, однако может создать проблемы для работы других программ в случае высокой загрузки компьютера.



Пользователь может как сохранить сделанные настройки, нажав на кнопки **OK** или **Применить**, так и отказаться от их сохранения, вернувшись к имеющимся настройкам.

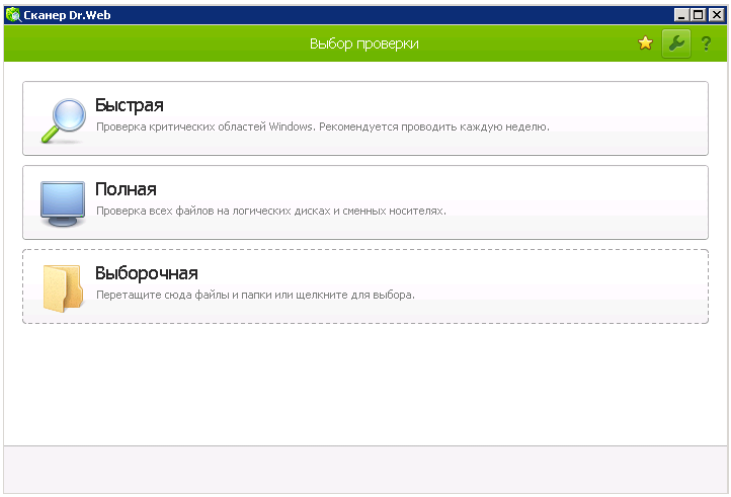
Для запуска сканирования надо нажать на кнопку  в главном окне программы.

Внимание! Дополнительные возможности по оптимизации скорости работы продукта и нагрузки на процессор доступны для настройки через интерфейс управления.

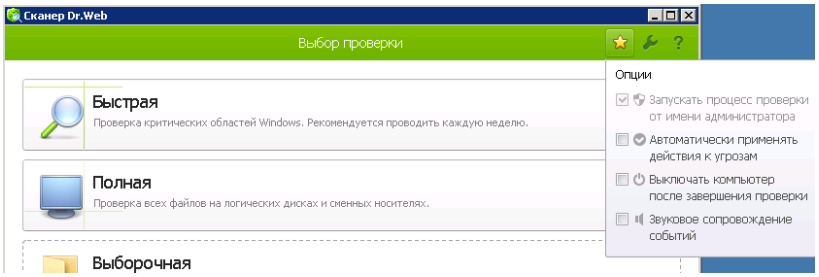
7.4.2. Антивирусная проверка Сканером SE

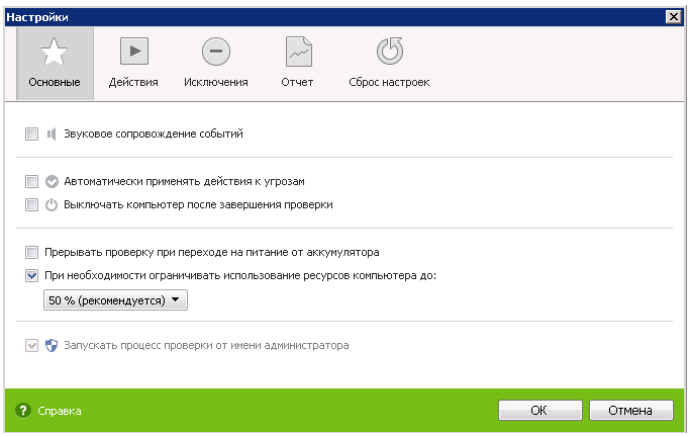
Для антивирусной проверки операционных систем Windows 2000 с SP4 и Update Rollup1, Windows XP с SP2 и выше, Windows 2003 с SP1 и выше, Windows Vista и выше доступен антивирусный сканер нового поколения. Вместе с данным сканером поставляется компонент **ArkAPI**, используемый для проверки на руткиты.

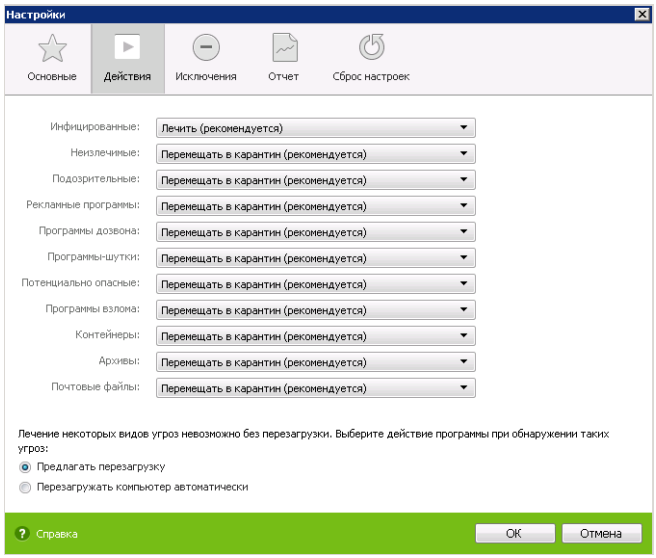
После завершения загрузки сканера в главном окне необходимо выбрать нужный тип проверки — быстрый, полный или выборочный.



Пользователь может как запустить проверку с настройками по умолчанию, так и изменить предложенные настройки – нажав на значки и , можно настроить параметры работы антивирусного сканера.







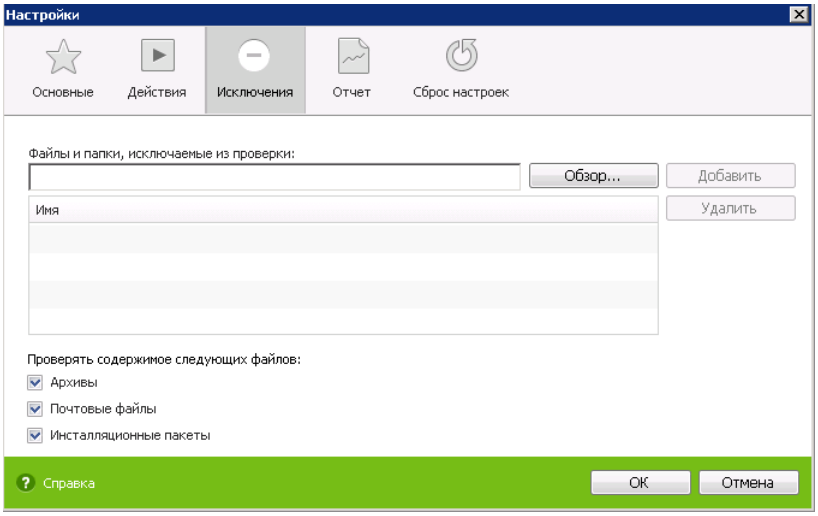
На закладке **Действия** пользователь может определить действия, применяемые к вредоносным объектам различного типа. По умолчанию для всех объектов (кроме инфицированных) стоит действие **Перемещать в карантин**.

Необходимо отметить, что для различных объектов список возможных действий является различным. Так, для неизлечимых пункт **Лечить** недоступен — в отличие от инфицированных.

Внимание! Новый сканер не поддерживает действие **Переименовать** в связи с отсутствием гарантий последующей безопасности системы при применении этого действия — возможностью отмены этого действия вручную. Однако в связи с необходимостью поддержки сканеров обоих типов данное действие сохранено в **Центре управления**. При выборе данного действия для каких-либо типов инфицированных файлов в веб-интерфейсе **Центра управления**, для этих типов инфицированных файлов будет применяться перемещение в карантин. При этом в файл отчета сканера будет заноситься строка **Ignore (invalid parameter): JOKR**, сообщающая, что действие не применилось.

Кроме этого:

- для почтовых файлов убрано действие **Удалить**. При выборе данного действия в веб-интерфейсе **Центра управления**, к найденным файлам будет применено действие перемещения в карантин;
- если в настройках антивирусного сканера для подозрительных файлов выбрано действие **Игнорировать**, на сервер передается действие **Информировать** — в связи с отсутствием в веб-интерфейсе **Центра управления** для данной категории файлов действия **Игнорировать**. При выборе в веб-интерфейсе **Центра управления** действия **Информировать** для каких-либо типов вредоносных файлов, в настройках антивирусного сканера останутся прежние настройки — сохраненные до применения этого действия — в связи с тем, что действие **Информировать** для антивирусного сканера является действием по умолчанию и отрабатывает вне зависимости от настроек, если не проставлен параметр **Автоматическое применение действий**.

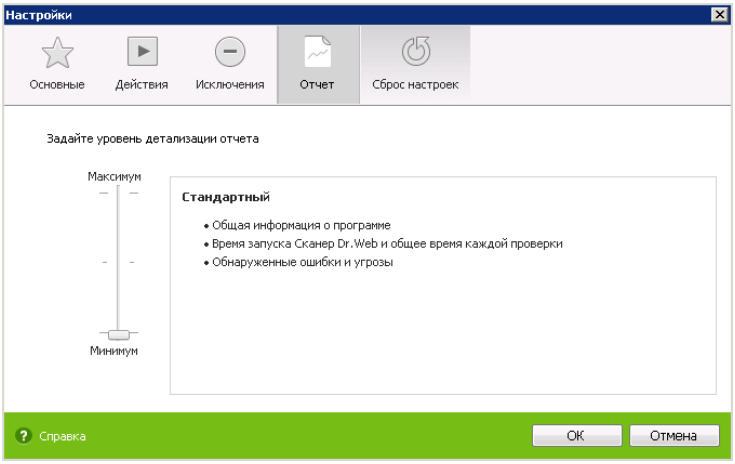


На закладке **Исключения** можно уточнить список проверяемых каталогов, задав исключаемые из проверки папки и файлы. Для добавления выбранной папки необходимо нажать на кнопку **Добавить**.

На этой же закладке уточняется список проверяемых файлов. Пользователь может сделать это, выбрав пункты **Архивы, Почтовые файлы** и **Инсталляционные пакеты**. Пользователь всегда может вернуться к настройкам по умолчанию, нажав кнопку **Сброс настроек**.

По умолчанию в ходе проверки сканер не проверяет архивы и почтовые файлы, так как их проверка занимает много времени, а вредоносные файлы из них могут быть запущены только после обработки архиваторами или почтовыми программами, в ходе чего они будут обнаружены специализированными компонентами. Однако если пользователь желает проверять эти форматы, он можете отметить их, выбрав соответствующие пункты.

Внимание! Рекомендуется всегда проверять архивы перед их отправкой кому-либо.

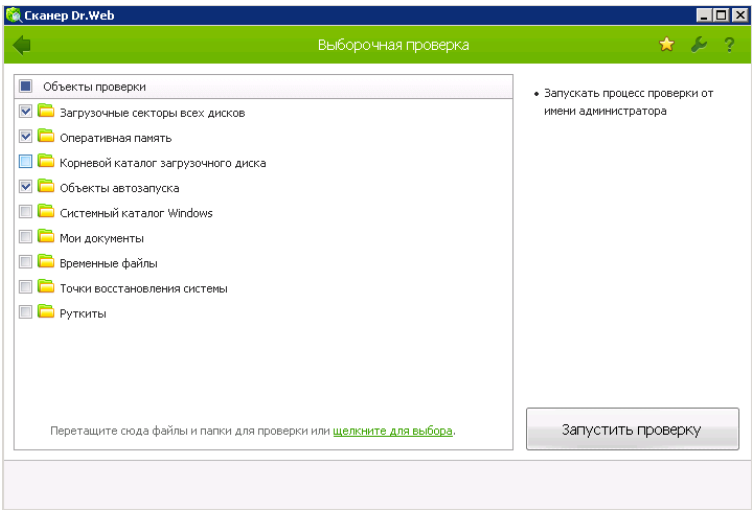


На закладке **Отчет** задается его детализация.

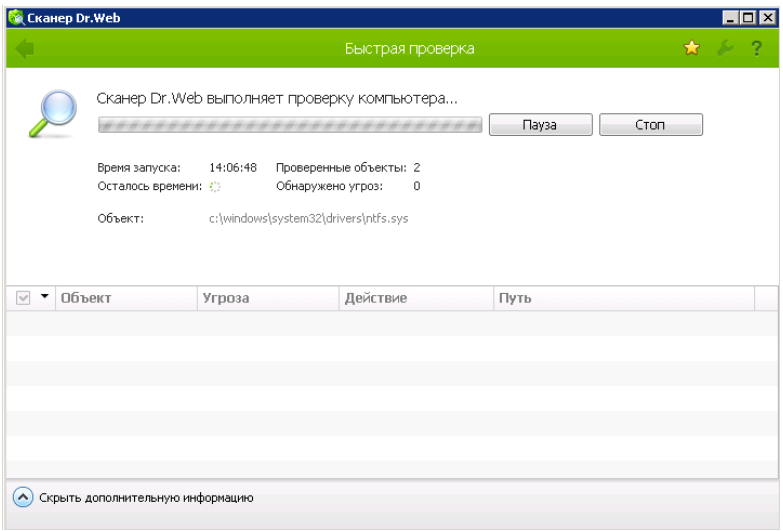
Не рекомендуется отказываться от ведения отчета о проверке, хотя это и несколько ускоряет ее ход.

Пользователь может как сохранить сделанные настройки, нажав на **ОК**, так и отказаться от их сохранения, вернувшись к имеющимся настройкам.

В случае выборочного типа проверки пользователь может указать интересующие объекты проверки. Для проверки дисков, отдельных папок и файлов пользователь должен перетащить их в окно сканера.



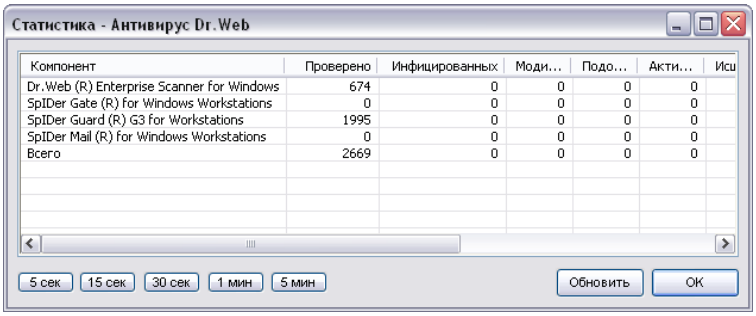
Для запуска быстрой или полной проверки нужно в главном окне сканера нажать на пункты **Быстрая** и **Полная** соответственно. Выборочная проверка запускается из окна настроек **Выборочная проверка**.



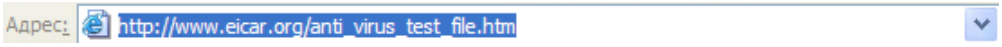
7.5. Проверка работоспособности продукта

Пользователь всегда может убедиться в работоспособности выбранного продукта. Для этого необходимы следующие действия.

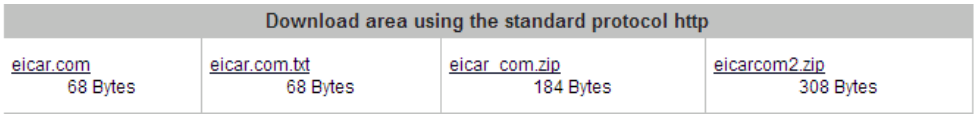
Щелкните правой кнопкой мыши значок в системном трее. Затем выберите пункт **Статистика**. В открывшемся окне статистики запомните количество обнаруженных инфицированных объектов в строке с данными по компоненту **SpIDer Gate**.



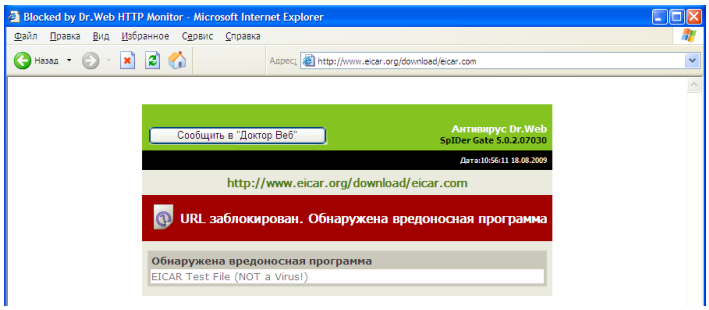
Откройте браузер и перейдите по адресу



На открывшейся странице найдите текст

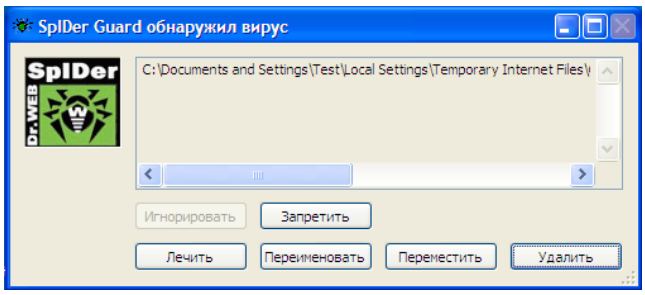


и выберите для скачивания любой из предложенных вариантов, например первый — eicar.com. В том случае, если защита работает корректно, ваш браузер должен показать следующее окно:



Щелкните правой кнопкой мыши значок в системном трее. Затем выберите пункт **Статистика**. Количество обнаруженных инфицированных объектов компонентом **SpIDer Gate** должно увеличиться на единицу.

Если вы хотите проверить работу файлового монитора, то вы должны сначала получить файл с тестовым вирусом. Для этого отключите **SpIDer Gate**: щелкните правой кнопкой мыши значок в системном трее и снимите флаг **SpIDer Gate**. Вернитесь на сайт eicar.org и снова попытайтесь закачать тестовый вирус. Итогом попытки должно стать окно типа:

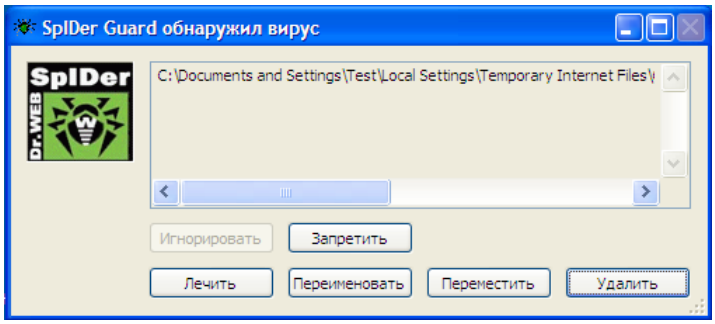


После завершения проверки включите **SpIDer Gate**: щелкните правой кнопкой мыши значок в системном трее и установите флаг **SpIDer Gate**.

7.6. Выбор действия по умолчанию

По умолчанию для всех вредоносных объектов стоит действие **Информировать**. По этому действию пользователь сам должен принимать решение о том, что делать с обнаруженными вредоносными объектами.

При обнаружении вредоносного объекта он получает уведомление типа:

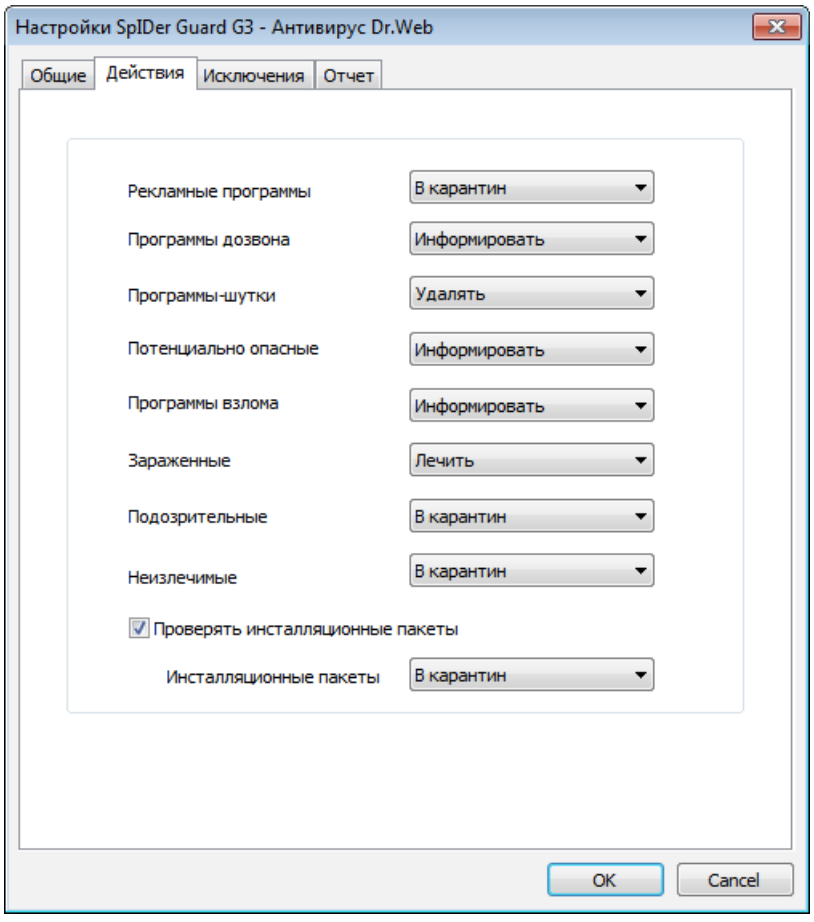


Предлагаемый в этом окне список действий различается для вредоносных программ различного типа. Так, для вирусов на выбор предлагаются действия **Лечить, Переименовать, Переместить** и **Удалить**. Для троянских программ действие **Лечить** недоступно — программы такого типа не имеют механизма размножения, и их лечение невозможно.

Уведомления отвлекают от выполнения повседневных задач. Кроме того, при их использовании есть вероятность выбора по ошибке неверного действия и попадания вируса в систему. В связи с этим рекомендуется переопределять действия по умолчанию.

Для настройки действий по отношению к вредоносным программам необходимо сделать следующее.

Щелкните правой кнопкой мыши значок в системном трее. Затем выберите пункт **Настройки SpIDer Guard**. Перейдите на закладку **Действия**.

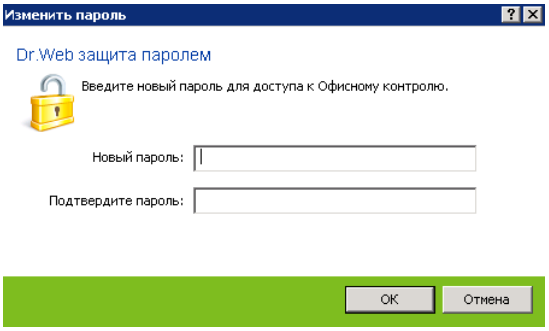


7.7. Контроль доступа к локальным ресурсам

Пользователь может ограничить доступ к сменным носителям, файлам и папкам, тем самым уменьшив риск проникновения вредоносных программ. Для этого он может воспользоваться функциями **Офисного контроля**.

Рекомендуется следующий порядок действий по настройке:

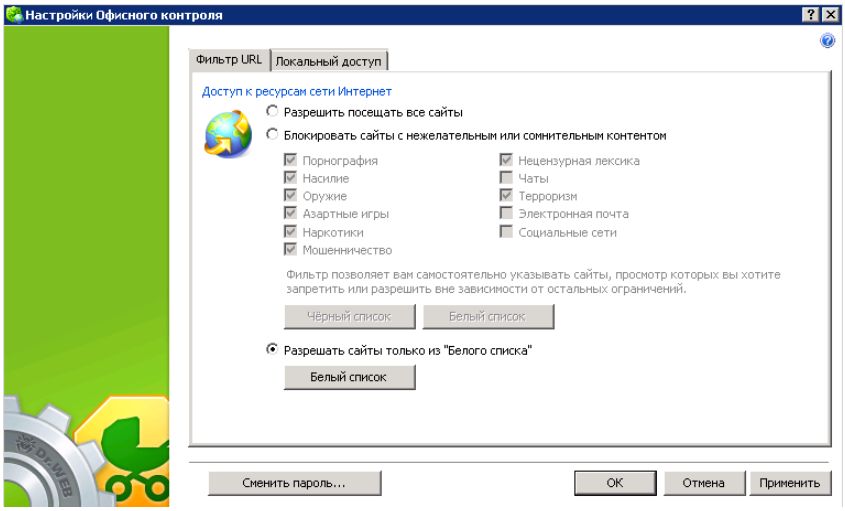
Щелкните правой кнопкой мыши значок в системном трее. Выберите пункт **Настройки Офисного контроля**. Если вы настраиваете права доступа впервые, то вам будет предложено задать пароль и логин доступа. По умолчанию пароль отсутствует. Хотя вы можете не задавать пароль и перейти к настройкам, просто закрыв окно, делать это не рекомендуется. Кроме того, не рекомендуется использовать простые, легко поддающиеся взлому пароли — использование таких паролей сводит на нет все усилия по обеспечению безопасности.



Задав пароль, нажмите на кнопку **OK**.

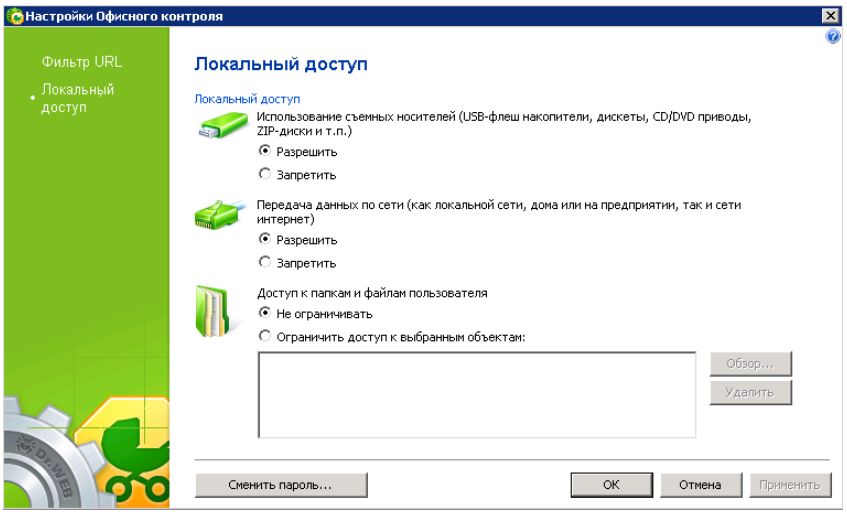
С помощью **Офисного контроля** вы можете либо запретить доступ ко всем сайтам, кроме избранных, либо разрешить доступ ко всем, кроме определенных.

Если вы хотите запретить доступ ко всем сайтам, кроме избранных, то щелкните на пункте **Включить фильтр URL** на закладке **Фильтр URL**, введите имена разрешенных ресурсов сети Интернет рядом со значком «+» под полем разрешенных адресов, нажимая при этом значок после ввода полного пути к каждому ресурсу. После формирования полного списка разрешенных ресурсов щелкните по пункту **Все, кроме разрешенных адресов** и нажмите кнопку **Применить**.

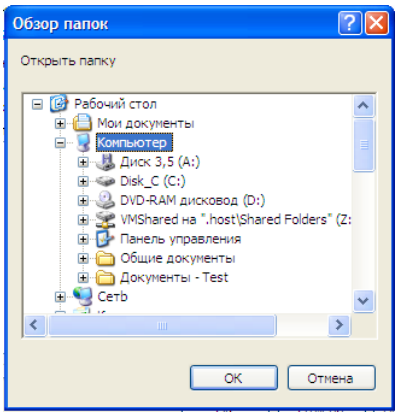


Если вы хотите разрешить доступ ко всем сайтам, кроме запрещенных, то щелкните по пункту **Включить фильтр URL** на закладке **Фильтр URL**, затем по пункту **Пользовательский список** и введите имена разрешенных ресурсов сети Интернет рядом со значком «+» под полем пользовательского списка, нажимая этот значок после ввода полного пути к каждому ресурсу. Если вы хотите воспользоваться списками уже известных адресов — используйте списки категорий. Если вы не хотите использовать эти списки, снимите галочки, стоящие против всех пунктов списка. После завершения настройки нажмите кнопку **Применить**.

Если вы хотите настроить права доступа к локальным ресурсам, то перейдите на закладку **Локальный доступ** и щелкните по пункту **Ограничить локальный доступ**. Если вы ходите запретить доступ к флеш- и смарт-картам, дисководам и CD/DVD-дискам, щелкните по пункту **Съемные диски**, если вы хотите запретить доступ к сети, выберите пункт **Доступ к сети**.



Если же вы хотите ограничить доступ к конкретным папкам и файлам, то выберите пункт **Файлы и папки**, щелкните по значку  и в появившемся списке



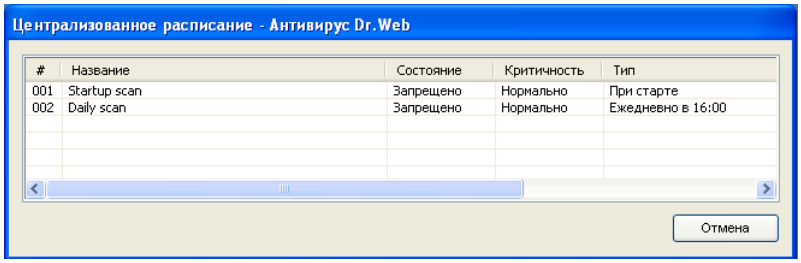
выберите тот ресурс, доступ к которому вы хотите закрыть.

После завершения настроек нажмите на пункт **Применить** или на кнопку **OK**.

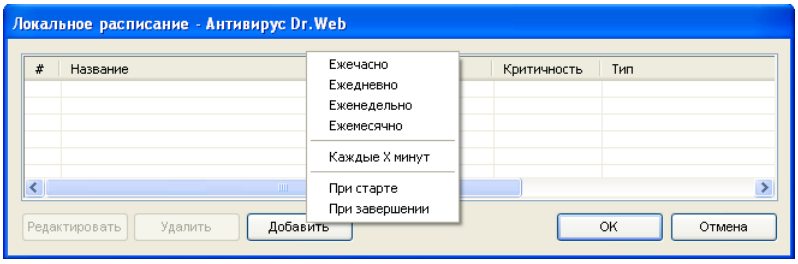
7.8. Редактирование расписания автоматического запуска заданий

В зависимости от наличия у пользователя соответствующих прав (прав, позволяющих изменять данные настройки, и прав администратора на данном компьютере) он может редактировать и просматривать расписание работы антивирусного сканера. В частности, задавать и менять локальное расписание проверок, просматривать централизованное расписание проверок.

Для настройки расписания необходимо выбрать интересующий пункт в выпадающем меню команды **Расписание** контекстного меню.

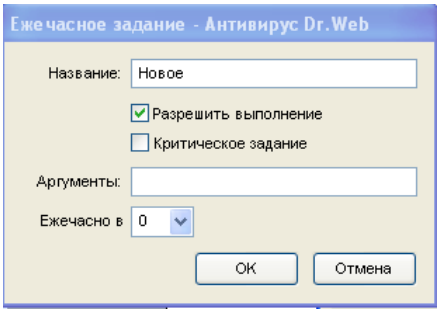


Для редактирования локального расписания щелкните правой кнопкой мыши значок в системном трее, выберите последовательно пункты **Расписания** и **Локальное**.



Внимание! Доступность для пользователя создания локального расписания должна быть разрешена в настройках группы или самого пользователя — в случае, если при редактировании прав антивирусной станции был установлен флаг **Создание локального расписания**.

Для добавления нового задания пользователь должен выбрать пункт **Локальное** и нажать кнопку **Добавить**. Далее в появившемся меню необходимо выбрать тип задания (ежечасно, ежедневно, еженедельно, ежемесячно, каждые X минут, при старте, при завершении). В появившемся окне введите название задания и его аргументы.



Если в дальнейшем нужно будет отредактировать какое-либо из назначенных заданий, необходимо выбрать интересующее задание и нажать кнопку **Редактировать**.

Для удаления задания необходимо нажать кнопку **Удалить**.

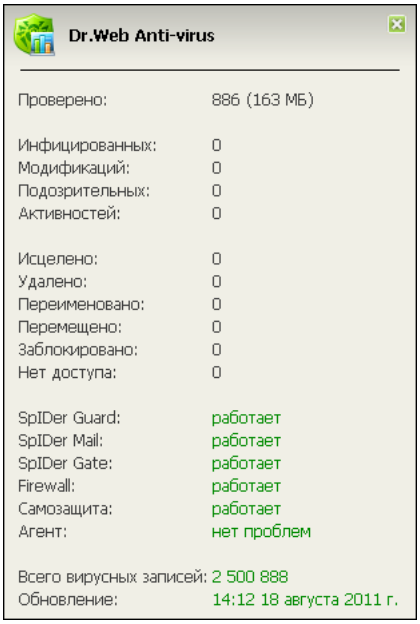
Запустить сканирование немедленно можно, выбрав команду **Сканер** в контекстном меню или в меню **Пуск**, пункт **Программы**.

Варианты задания объектов сканирования, ключи командной строки, задающие параметры программы, а также параметры командной строки для модуля автоматического обновления описаны в руководстве «Антивирус Dr.Web для Windows. Руководство пользователя».

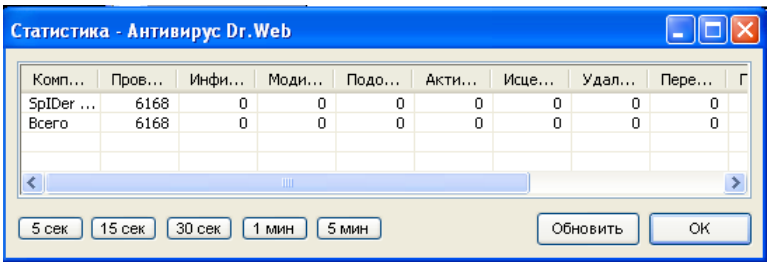
При выполнении некоторых запланированных заданий, в частности задания по запуску утилиты обновления, требуется, чтобы антивирусный Сервер был остановлен. В противном случае появляется сообщение об ошибке и задание не будет выполнено.

7.9. Просмотр статистики работы

Пользователь может в любой момент времени ознакомиться со статистикой работы системы защиты. Для этого необходимо навести указатель мыши на значок в системном трее.

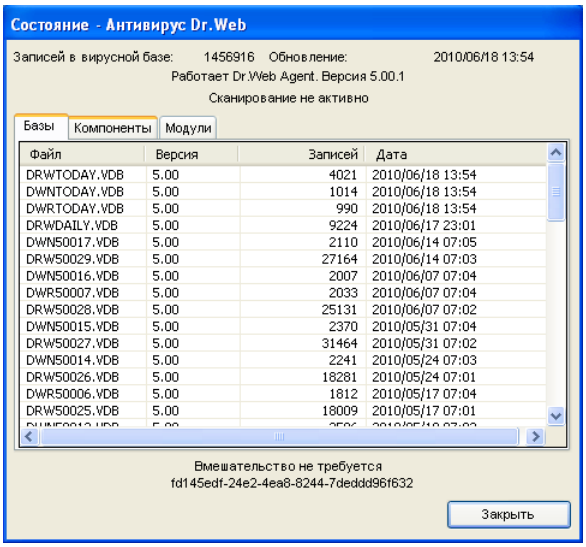


Для получения более подробной информации пользователь может щелкнуть по этому же значку правой кнопкой мыши и в появившемся меню выбрать пункт **Статистика**.



7.10. Просмотр состояния антивирусного ПО

Для просмотра состояния антивирусного ПО, установленного на рабочей станции, выберите в контекстном меню пункт **Состояние**.



В верхней части открывшегося окна выводится общая информация: общее количество записей в вирусной базе, дата последнего обновления, версия работающего на станции агента, активность сканирования (запущен ли в данный момент на станции сканер).

Окно состояния содержит следующие вкладки — **Базы** с информацией обо всех установленных вирусных базах, **Компоненты** с информацией обо всех установленных на рабочей станции компонентах антивируса Dr.Web и их состояниях (запущен (работает) или не запущен (выключен)), **Модули** с информацией о модулях.

В нижней части окна состояния выводится строка состояния, содержащая важные оповещения (при нормальной работе выводится сообщение **Вмешательство не требуется**) и уникальный идентификационный номер агента.

7.11. Карантин

Карантин антивируса Dr.Web служит для изоляции подозрительных файлов.

Папки карантина создаются отдельно на каждом логическом диске, где были обнаружены подозрительные файлы. Папка карантина под названием **Dr.Web Quarantine** создается в корне диска и является скрытой. Пользователь не имеет прав доступа к файлам папки карантина.

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.

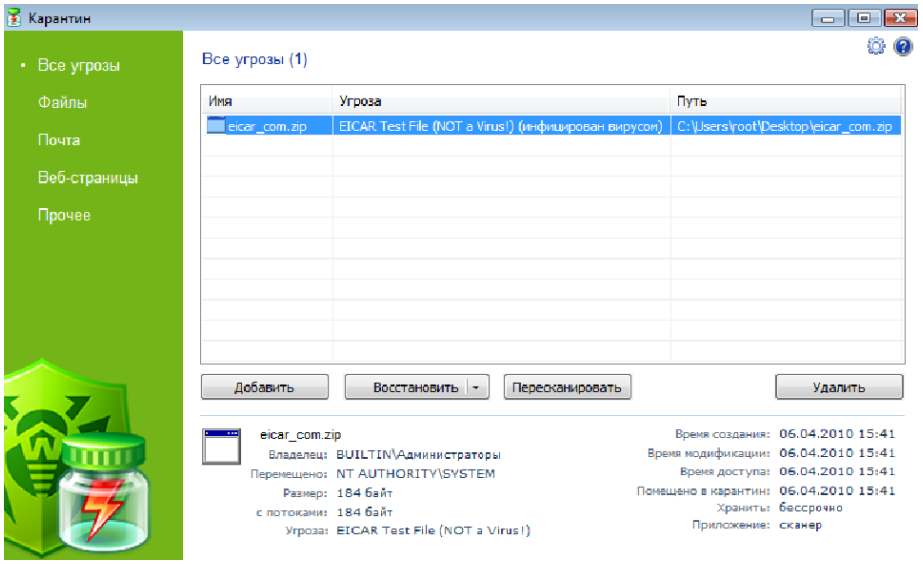
Файлы карантина, размещаемые на жестком диске, хранятся в зашифрованном виде.

Файлы карантина, размещаемые на съемном носителе, хранятся в незашифрованном виде.

Для просмотра и редактирования содержимого карантина выберите в контекстном меню пункт **Карантин** — откроется окно, содержащее табличные данные о текущем состоянии карантина.

В окне карантина пользователи могут видеть только те файлы, к которым имеют права доступа.

В нижней части окна карантина отображается подробная информация о выбранных объектах карантина.



Чтобы настроить отображение столбцов, необходимо выбрать контекстное меню заголовка таблицы объектов, щелкнув правой кнопкой мыши по заголовку, и в нем выбрать **Настроить колонки**. В открывшемся окне необходимо установить флаги напротив тех пунктов, которые необходимо включить в таблицу. Для сохранения изменений в настройках необходимо нажать кнопку **OK**, для закрытия окна без сохранения изменений — кнопку **Отменить**.

Для настройки свойств карантина необходимо нажать на кнопку **Настройки**. В открывшемся окне **Свойства карантина** можно определить размер карантина, возможность показа резервных копий.

Чтобы отобразить скрытые объекты, запустите под учетной записью с административными правами либо файл карантина dwqrui.exe, расположенный в каталоге установки, либо интерфейс Dr.Web Агента.

Если необходимо добавить файл в карантин, то в окне **Карантина**, нажав кнопку **Добавить**, можно выбрать интересующий файл.

Если необходимо переместить или восстановить файлы, то, нажав кнопку **Восстановить**, можно переместить файл из карантина и восстановить его первоначальное местоположение на компьютере (восстановить файл под тем же именем в папке, в которой он находился до перемещения в карантин). В выпадающем меню доступен вариант **Восстановить в** — переместить файл под заданным именем в папку, указанную пользователем.

Пользователь также имеет возможность проверить файлы повторно, нажав **Пересканировать**. Если при повторном сканировании файла обнаружится, что он не является зараженным, **Карантин** предложит восстановить данный файл.

Нажав кнопку **Удалить**, можно удалить файл из карантина и из системы.

Для работы одновременно с несколькими объектами необходимо выбрать их в окне **Карантина**, удерживая клавиши **SHIFT** или **CTRL**, затем щелкнуть правой кнопкой мыши по любой строчке таблицы и в выпадающем меню выбрать необходимое действие.

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.

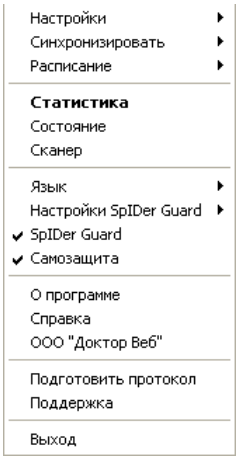
При переполнении карантина и невозможности его автоматической очистки перемещение файлов в карантин будет завершаться с ошибкой. В этом случае вы можете увеличить размер карантина в разделе **Свойства карантина / Задать размер карантина** или удалить файлы карантина вручную.

Для удаления всего содержимого **Карантина** необходимо выделить все файлы в окне **Карантина** и нажать кнопку **Удалить**.

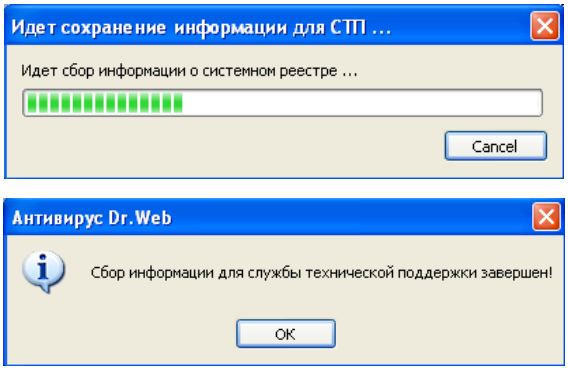
7.12. Сбор информации для служб технической поддержки

Немаловажным преимуществом продукта является простота сбора необходимой информации для служб технической поддержки. Пользователю не нужно собирать все необходимые файлы и данные — за него это делает сама система.

Для сбора информации необходимо щелкнуть правой кнопкой мыши значок  в системном трее и в появившемся меню



выбрать пункт Подготовить протокол. Антивирус автоматически соберет все данные и создаст в папке по умолчанию архив, который в дальнейшем можно будет передать в службу технической поддержки либо системному администратору.



8. 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 http://download.drweb.com;
- прочитать раздел часто задаваемых вопросов по адресу http://support.drweb.com/show_faq;
- посетить форумы Dr.Web по адресу http://forum.drweb.com.

Если после этого вам не удалось решить проблему, то вы можете заполнить веб-форму вопроса в соответствующей секции раздела http://support.drweb.com.

Контактные данные партнера, с которым вам удобно работать, вы можете найти по адресу http://partners.drweb.com. Контакты центрального офиса «Доктор Веб» доступны на странице http://company.drweb.com/contacts/moscow, а региональных представительств компании — на http://company.drweb.com/contacts/offices.

«Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Антивирусная защита Dr.Web позволяет информационным системам клиентов эффективно противостоять любым, даже неизвестным угрозам.

«Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги и по сей день продолжает оставаться безусловным лидером российского рынка интернет-сервисов безопасности для поставщиков ИТ-услуг. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.