



Защити созданное

Программно-аппаратный комплекс Dr.Web® Office Shield

Установка и настройка

Развертывание антивирусной сети

Тестирование продукта

Версия 7.00

Содержание

Краткое описание Dr.Web Office Shield	3
Модельный ряд Dr.Web Office Shield	4
1. Введение	5
2. Установка и настройка Dr.Web Office Shield	5
3. Настройка сервиса защиты почтовых сообщений	9
3.1. Настройка действий для зараженного входящего и исходящего почтового трафика	9
3.2. Настройка действий для спам-сообщений	11
3.3. Управление карантинном	13
4. Настройка сервиса защиты интернет-трафика	14
4.1. Настройка действий для зараженного трафика	15
4.2. Управление карантинном	16
5. Настройка системы защиты сети	17
5.1. Развертывание антивирусной сети Dr.Web Enterprise Suite	17
5.1.1. Установка с использованием веб-интерфейса	17
5.1.2. Установка с использованием дистрибутивов компонентов Dr.Web Enterprise Suite	22
5.2. Смена языка отображения	24
5.3. Управление параметрами защиты рабочих станций и серверов Windows	24
5.3.1. Просмотр параметров защиты рабочих станций и серверов Windows	25
5.3.2. 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	27
5.3.3. Настройка доступа к защищаемым каталогам и сменным носителям	29
5.3.4. Настройка доступа к ресурсам и узлам сети Интернет	30

5.3.5. Настройка проверки HTTP-трафика. Выбор приложений для проверки/исключения из проверки их трафика, выбор контролируемых портов	31
6. Контроль состояния сети	34
6.1. Сбор статистики. Формирование графиков активности вирусов, статистики по найденным типам вредоносных объектов, произведенных над ними действий	35
7. Статистика использования ресурсов сети Интернет	38
8. Сохранение и восстановление настроек	41
8.1. Сохранение настроек	41
8.2. Восстановление настроек	41
9. Тестирование производительности программно- аппаратного комплекса Dr.Web Office Shield	42
9.1. Процедура тестирования Dr.Web Office Shield	42
9.2. Тестирование производительности системы фильтрации почтового трафика	42
9.3. Тестирование функционирования системы фильтрации почтового трафика	44
9.4. Тестирование производительности системы фильтрации интернет-трафика	45
9.5. Тестирование функционирования системы фильтрации интернет-трафика	45
9.6. Тестирование функционирования системы Wi-Fi	47
10. Приложения	48
10.1. Приложение 1. Получение доступа через кросс-кабель	48
10.2. Приложение 2. Получение прямого доступа к операционной системе типа Linux	49
Гарантийный талон	51

Краткое описание Dr.Web Office Shield

Dr.Web Office Shield является высокопроизводительным и отказоустойчивым сервером централизованной антивирусной и антиспам-защиты рабочих станций и файловых серверов Windows, почтового и интернет-трафика. Модульность решения и гибкость системы лицензирования позволяет использовать устройство в самых различных конфигурациях локальных сетей предприятий и организаций, реализуя их внутреннюю политику безопасности. В частности, Dr.Web Office Shield может быть использован в качестве:

- внутреннего сервера антивирусной защиты — максимально изолированного от внутренней сети устройства, отвечающего за антивирусную и антиспам-защиту предприятия;
- прокси-сервера (шлюза доступа пользователей внутренней интранет-сети к ресурсам сети Интернет), предназначенного для обеспечения защиты почтового и интернет-трафика от вирусов, разного рода вредоносных объектов и спама. Использование Dr.Web Office Shield в качестве шлюза значительно снижает затраты компаний на организацию безопасного доступа пользователей корпоративной интранет-сети к ресурсам сети Интернет и позволяет существенно экономить интернет-трафик;
- внутреннего фильтра трафика в составе локальной сети в дополнение к шлюзу, уже установленному в сети.

В состав Dr.Web Office Shield входят:

- Dr.Web Enterprise Suite, обеспечивающий централизованную защиту рабочих станций и файловых серверов Windows;
- Dr.Web для интернет-шлюзов Unix, обеспечивающий защиту доступа пользователей внутренней интранет-сети к ресурсам сети Интернет;
- Dr.Web Mail Gateway, обеспечивающий антивирусную и антиспам-защиту почтового трафика;
- корпоративный межсетевой экран;
- VPN-сервер;
- DHCP&DNS-сервер;
- точка доступа Wi-Fi.

Внимание! Важной особенностью Dr.Web Office Shield является то, что он может быть установлен как в существующую сеть организации, так и использован в качестве основы для вновь создаваемой сети — наличие работающих сервисов DHCP и DNS позволит провести эту работу с минимальными усилиями.

Модельный ряд Dr.Web Office Shield

Модель корпуса

Neo



Формфактор

50x275x172

Системная конфигурация

Плата Ci945a-4rxx
Чипсет Intel 945
Процессор Intel CeleronM 1.86 ГГц
Память 2 x DDR II SDRAM (2 GB)
Накопитель SATA 160 GB
Сеть 4 x 100 Mb
Беспроводная сеть 802.11g

Рекомендуемое количество пользователей

от 10 до 50*

Модель корпуса

Twister



Формфактор

75x300x173

Системная конфигурация

Плата Ci945a-4rxx
Чипсет Intel 945
Процессор Intel Core 2 Duo 2.16 ГГц
Память 2 x DDR2 SODIMM (2 GB)
Накопитель SATA 160 GB
Сеть 4 x 100 Mb
Беспроводная сеть 802.11g

Рекомендуемое количество пользователей

от 50 до 250

* В случае использования Dr.Web Office Shield только для обеспечения защиты почтового и интернет-трафика максимальное рекомендуемое количество пользователей – 150.

1. Введение

Данный документ описывает процедуры установки и настройки системы антивирусной защиты локальной сети предприятия с помощью программного-аппаратного комплекса Dr.Web Office Shield. Все этапы развертывания, описанные в документе, сопровождаются примерами и рекомендациями по тестированию описанного функционала. Целью каждого из описанных этапов тестирования является проверка правильности функционирования конкретной подсистемы сервера.

Документ рассчитан на пользователей, имеющих достаточную для проведения тестирования квалификацию. В связи с этим в нем не рассматриваются вопросы установки необходимых для тестирования программ, их сборки и т. д.

2. Установка и настройка Dr.Web Office Shield

Для начала работы с Dr.Web Office Shield необходимо:

1. С любого локального компьютера, подключенного к Интернету, зарегистрировать серийный номер, указанный в лицензионном сертификате, на сайте компании «Доктор Веб» (<http://products.drweb.com/register>). Отсчет срока действия лицензии начинается с момента регистрации серийного номера и получения ключевого файла.

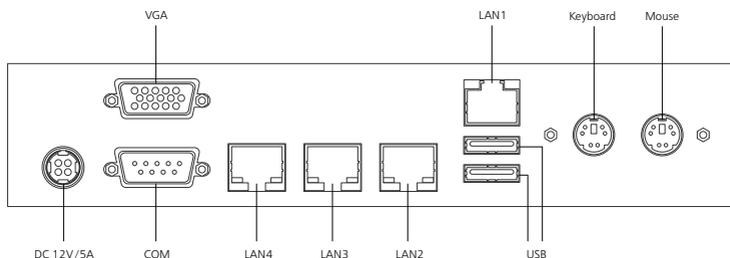
Полученные ключевые файлы необходимо разархивировать и сохранить на локальный диск или USB флеш-накопитель.

2. Подключить сервер Dr.Web Office Shield к корпоративной локальной сети.

Существующие разъемы предназначены для подключения:

- LAN1 — кабеля локальной сети (Local Area Network (**LAN**), интерфейс **eth0**),
- LAN3 — кабеля провайдера услуг глобальной сети (Wide Area Network (**WAN**), интерфейс **eth2**).

Разъем LAN2 (**DMZ**, интерфейс **eth1**) может быть использован для подключения к демилитаризованной зоне, в том случае если она существует в локальной сети, разъем LAN4 в данной версии устройства не используется.



Согласно настройкам по умолчанию сервер имеет IP-адрес **192.168.1.100**.

В том случае, если защищаемая сеть использует сетевые адреса типа 192.168.1.xxx и в сети не имеется адреса **192.168.1.100**, Dr.Web Office Shield может быть включен в локальную сеть без предварительной настройки и сразу после включения будет доступен как через веб-интерфейс, так и по протоколу SSH. В противном случае необходимо заменить используемый в Dr.Web Office Shield IP-адрес. Сделать это можно двумя способами — либо вручную с помощью утилит командной строки, либо через веб-интерфейс, подключившись к Dr.Web Office Shield через кросс-кабель. Ниже будет рассмотрен второй вариант. Порядок подключения через кросс-кабель рассмотрен в Приложении 1.

В случае использования Dr.Web Office Shield в качестве шлюза в разъем WAN подключается кабель, идущий от внешней сети (WAN), в разъемы DMZ и LAN подключаются кабели сегмента демилитаризованной зоны и LAN соответственно.

В случае подключения Dr.Web Office Shield между существующим шлюзом и сетью Интернет в разъем WAN подключается кабель, идущий от внешней сети (WAN), в разъем LAN подключается кабель, подключаемый к разъему WAN используемого шлюза.

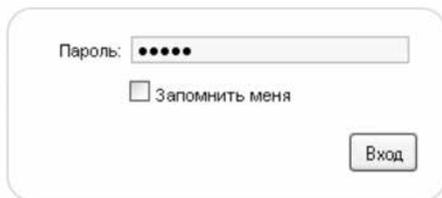
В случае подключения Dr.Web Office Shield между существующим шлюзом и локальной сетью в разъем WAN подключается кабель, идущий от разъема LAN (внутренней сети) шлюза, в разъемы DMZ и LAN подключаются кабели сегмента демилитаризованной зоны и LAN соответственно.

Внимание! В случае установки в дополнение к существующему шлюзу без специальной настройки маршрутизатора клиенты, использующие Wi-Fi, могут оказаться отделенными от сети LAN.

Сам запуск осуществляется путем нажатия кнопки  на лицевой панели. Загрузка Dr.Web Office Shield занимает порядка 1 минуты.

3. Обратиться к Dr.Web Office Shield для быстрой настройки с любого компьютера корпоративной локальной сети, используя браузер и сетевой адрес **https://192.168.1.100:10000**.

Логин по умолчанию — **root**, пароль по умолчанию — **drweb**.



Пароль:

Запомнить меня

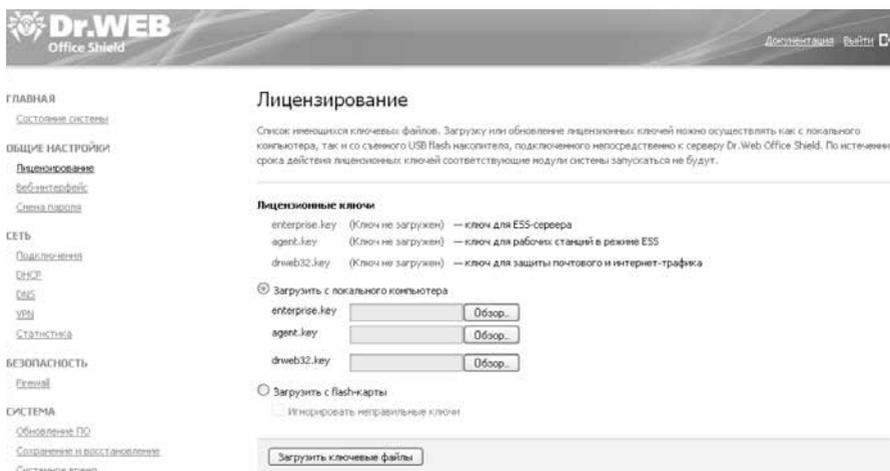
Внимание! Обязательно смените пароль администратора при первом заходе в систему. Смена пароля осуществляется на странице **Смена пароля**.

Внимание! Веб-интерфейс управления Dr.Web Office Shield реализован в виде дополнений к интерфейсу Webmin. Подробная информация об интерфейсе Webmin доступна на официальном сайте производителя: <http://www.webmin.com>.

4. Задать на странице **Подключения** веб-интерфейса параметры подключения: имя хоста Dr.Web Office Shield и настройки сети — локальной сети (**LAN**), глобальной сети (**WAN**), Wi-Fi-соединения (WEP KEY по умолчанию — **drweb**), а также в случае ее использования — демилитаризованной зоны (**DMZ**).

Внимание! В случае замены обязательно смените пароль администратора при первом заходе в систему. Смена пароля осуществляется на странице **Смена пароля**.

5. Загрузить действующие лицензионные ключи, используя локальный компьютер или съемный USB флеш-накопитель, подключив его непосредственно к серверу Dr.Web Office Shield.



6. В том случае, если с помощью Dr.Web Office Shield планируется осуществлять проверку почтового трафика на странице **Почтовый прокси**: выбрать виды осуществляемых проверок трафика (по умолчанию осуществляются проверки как на вирусы, так и на спам), а также указать адрес почтового сервера, используемого для отправки почты (в формате **mx:имя_хоста_почтового_сервера**) и имена защищаемых доменов через запятую.

7. В случае необходимости с помощью веб-интерфейса на странице:
 - **DHCP**: в случае использования Dr.Web Office Shield в качестве DNS-сервера

здать доменное имя и адрес DNS-сервера, выдаваемые DHCP-клиентам локальной сети. По умолчанию DNS-сервер отключен.

- **DNS:** указать используемый сторонний DNS-сервер, на который будут перенаправляться DNS-запросы. По умолчанию DNS-сервер отключен.
- **VPN:** настроить подключение VPN.
- **Системное время:** настроить время и часовой пояс.
- **Веб-интерфейс:** указать используемый язык интерфейса.
- **Сохранение и восстановление:** выбор места для хранения резервной копии всех настроек Dr.Web Office Shield.

Внимание! После переопределения имени хоста SSL-сертификат веб-интерфейса будет сгенерирован заново!

Внимание! Для корректной работы лицензионных ключей необходимо правильно задать локальное системное время.

8. Сделав все необходимые изменения, нажать на кнопку **Применить и сохранить изменения**.

Дальнейшая настройка производится через пункты меню, находящегося в левой части страницы:

- настройка фильтрации почты производится в пункте меню **Безопасность → Почтовый прокси**;
- настройка фильтрации интернет-трафика производится в пункте меню **Безопасность → Веб-прокси**;
- настройка VPN производится в пункте меню **Сеть → VPN**. Пароль пользователя **vpn_user** по умолчанию — **drweb**.

Внимание! После завершения настройки Dr.Web Office Shield рекомендуется провести обновление его компонентов. Сведения о наличии обновлений компонентов Dr.Web Office Shield выводятся в виде уведомления в верхней части всех страниц веб-интерфейса.

3. Настройка сервиса защиты почтовых сообщений

Настройка сервиса производится на странице **Почтовый прокси** раздела **Безопасность** главного меню. На странице настроек доступно три вкладки:

- **Основные настройки** — позволяет включить или выключить защиту от вирусов и спама, а также указать параметры подключения к почтовому серверу и имя защищаемого домена или доменов;
- **Карантин** — позволяет получить доступ к списку писем, отфильтрованных в процессе работы;
- **Расширенные настройки** — позволяет произвести тонкие настройки работы сервиса. Вкладка содержит следующие разделы:
 - **Карантин** — настройка времени хранения письма в карантине.
 - **Антиспам, Антивирус** — настройка компонентов антиспама и антивируса.
 - **Ядро** — настройка защищаемых сетей, доменов, включение поддоменов в список защищаемых доменов, адрес для отправки перенаправленных сообщений и т. п.
 - **Отчеты** — подключение отчетов о результатах обработки сообщений, график их отправки и т. п.
 - **Прием почты** — адрес для получения сообщений и действия, применимые к входящей почте, настройки для SMTP.
 - **Отправка почты** — адрес для отправки сообщения, подключение отчетов, задание правил маршрутизации, действия для застрявших писем и т. п.

3.1. Настройка действий для зараженного входящего и исходящего почтового трафика

Определить действия по отношению к зараженному трафику можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

Для настройки через веб-интерфейс необходимо в разделе **Расширенные настройки**, доступном на странице **Почтовый прокси**, перейти на закладку **Антивирус** и выставить необходимые значения для параметров **Зараженные** (Infected), **Подозрительные** (Suspicious), **Неизлечимые** (Incurable) и т. д.

Предлагаемый список действий различается для вредоносных программ различного типа. Так, для вирусов на выбор предлагаются действия **Лечить**, **Удалить**, **Отклонить** (отказаться от приема, уведомив отправителя (Discard)), **Отклонить без уведомления** (отказаться от приема, не уведомив отправителя (Reject)). Для троянских программ действие **Лечить** недоступно — программы такого типа не имеют механизма размножения, и их лечение невозможно. Кроме основного действия, возможны и дополнительные — **Карантин** (Quarantine — переместить письмо в карантин), **Информировать** (Notify), **Перенаправить** (Redirect — пере-

слать письмо на адрес) и т. д. Для добавления в список действий дополнительного действия необходимо нажать на кнопку , для его удаления из списка — .

Применить сделанные изменения можно, нажав кнопку **Применить и сохранить изменения**.

Почтовый прокси

[Основные настройки](#) | [Карантин](#) | [Расширенные настройки](#)

На этой вкладке вы можете задать правила фильтрации почты и выбрать действия, которые будут применяться к обнаруженным угрозам.

Карантин | Ядро | Отчеты | Прием почты | Отправка почты | Антиспам | **Антивирус**

▼ Основные

Адрес сокета Сокет, через который антивирусный плагин взаимодействует с демоном drwebd. [подробнее](#)

`pid:/var/drweb/run/drwebd.pid` ✕



Время ожидания Максимальное время ожидания исполнения команды демоном drwebd. [подробнее](#)

минут 

Зервистический анализ Настройка работы зервистического анализатора. [подробнее](#)

Да

Добавлять X заголовки Добавление заголовков X-Antivirus и X-Antivirus-Code к проверенным демоном drwebd сообщениям. [подробнее](#)

Да

Параноидальное сканирование Настройка "параноидального" режима сканирования. [подробнее](#)

Нет

Выражения для блокирования по имени файла Список регулярных выражений, используемых плагином при проверке имен файлов в отчете, присланном демоном drwebd после сканирования сообщения. [подробнее](#)

Зараженные Действие, совершаемое с сообщениями, зараженными известными вирусами.

Основное действие

Дополнительные действия

карантин ✕









[ссылка](#)



3.2. Настройка действий для спам-сообщений

Определить действия по отношению к спам-сообщениям можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

Для настройки через веб-интерфейс необходимо в разделе **Расширенные настройки**, доступном на странице **Почтовый прокси**, перейти на закладку **Анти-спам** и выставить необходимое значение для параметра **Действие для спама** (Action). Для большинства случаев достаточно использовать значения **Пропустить (Pass)** или **Отклонить без уведомления** (Discard — отказаться от приема, не уведомив отправителя). В том случае, если выбрано значение **Пропустить**, пользователь имеет возможность настроить фильтрацию на своей стороне, используя видимые при проверке отметки. В том числе по заголовку письма (message header) — скрытой в служебной области письма невидимой пользователю информации, и его теме (Subject). Система фильтрации по умолчанию всегда добавляет в служебный заголовок строку X-DrWeb-SpamState: Yes/No, где значение Yes показывает, что письму присвоен статус «спам». Определить префикс, добавляемый к теме письма, вы можете, используя параметр **Префикс для спама** (SubjectPrefix).

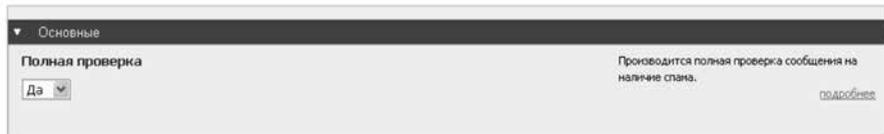
Применить сделанные изменения можно, нажав кнопку **Применить и сохранить изменения**.

Почтовый прокси

[Основные настройки](#) | [Карантин](#) | [Расширенные настройки](#)

На этой вкладке вы можете задать правила фильтрации почты и выбрать действия, которые будут применяться к обнаруженным угрозам.

Карантин | Ядро | Отчеты | Прием почты | Отправка почты | Антиспам | Антивирус



Игнорировать встроенные домены <input type="button" value="Да"/>	Игнорировать встроенные ham-домены. подробнее
Добавлять заголовок с версией <input type="button" value="Нет"/>	Добавление к сообщению заголовка X-Drweb-SpamVersion, содержащего информацию о версии плагина YadeRetro.
Добавлять заголовок со статусом сообщения <input type="button" value="Нет"/>	Добавление к сообщению заголовка X-Drweb-SpamState-Num. подробнее
Добавлять заголовок с уровнем спама <input type="button" value="Нет"/>	Добавление к сообщению заголовка X-Spam-Level, состоящего из символов "M". подробнее
Добавлять заголовки <input type="button" value="Да"/>	Добавление к сообщению заголовков X-Drweb-SpamState и X-Drweb-SpamScore. подробнее
Проверять уведомления о доставке <input type="button" value="Нет"/>	Возможность отдельной фильтрации уведомлений о доставке сообщений.
Префикс для спама <input type="text" value="*[SPAM]"/>	Префикс, добавляемый к теме сообщения, если оно отмечено как спам. подробнее
Префикс для уведомлений <input type="text"/>	Префикс, добавляемый к теме сообщения, если оно является уведомлением о невозможности доставки (и, соответственно, определено в 3 класс писем библиотекой YadeRetro).
Граница безусловного спама <input type="text" value="1000"/>	Если оценка, полученная письмом, равна значению данного параметра или превышает его, письмо считается безусловным спамом. подробнее
Префикс для безусловного спама <input type="text" value="*[SPAM]"/>	Префикс, добавляемый к теме сообщения, если оно отмечено как безусловный спам. подробнее
Граница спама <input type="text" value="100"/>	Если оценка, полученная письмом, равна значению данного параметра или превышает его, письмо считается спамом. подробнее
Действие для безусловного спама Основное действие: <input type="button" value="пропустить"/> Дополнительные действия: <input type="text"/> <input type="button" value="Скачать"/> <input type="button" value="Перенаправить"/> <input type="text"/> <input type="button" value="Добавить заголовок"/> <input type="text"/>	Действие, совершаемое с безусловным спамом. подробнее

Действие для спама Действие, совершаемое со спамом. [подробнее](#)

Основное действие:

Дополнительные действия

карантин

перенаправить

добавить заголовок

3.3. Управление карантином

В карантине содержатся поддиректории, названные именами компонентов, отвечающих за проверку почтовых сообщений. Письмо, отфильтрованное тем или иным компонентом, помещается в его «персональную» поддиректорию в директории карантина. Для каждого сообщения создается два файла: для самого письма и для его конверта. На странице **Карантин** представлен список писем с информацией об имени отфильтровавшего их подключаемого компонента, идентификаторе сообщения в базе данных, дате получения, адресе отправителя и получателя, теме письма и его размере.

Для просмотра карантина необходимо через веб-интерфейс выбрать пункт **Почтовый прокси** и щелкнуть по пункту меню **Карантин**.

Системный администратор имеет возможность просмотреть, удалить и отправить сохраненное письмо его получателям.

Почтовый прокси

[Основные настройки](#) | [Карантин](#) | [Расширенные настройки](#)

На данной вкладке вы можете просмотреть список заблокированных сообщений.

Отправить
 Переслать
 Удалить
 Не спам
 Сообщить о спаме

Отправитель:
 Получатель:
 Тема:

Дата:
 Размер:
 Статус:

-

Сообщений выбрано: 1

	Отправитель	Получатель	Тема	Дата	Размер
<input checked="" type="checkbox"/>	igorn@igorn-fedo...	igorn@igorn-fedo...		29/05/2012 12:46	231

— предыдущая следующая —

Элементов на странице:

 Показано: 1 — 1 из 1

4. Настройка сервиса защиты интернет-трафика

Настройка сервиса производится на странице **Веб-прокси** раздела **Безопасность** главного меню. На странице настроек доступно три вкладки:

- **Основные настройки** — отображает список защищаемых сетевых интерфейсов.
- **Карантин** — позволяет получить доступ к списку ссылок на файлы, отфильтрованные в процессе работы.
- **Расширенные настройки** — позволяет произвести тонкие настройки работы сервиса. Вкладка содержит следующие разделы:
 - **Действия над угрозами** позволяют задать действия для различных инцидентов, например для файлов с неизлечимым или подозрительным вирусом.
 - **Тематический фильтр** позволяет отсеивать веб-страницы по типу их содержимого.
 - **Системные настройки** позволяют задать адрес для отправления уведомлений, определить события для отправки уведомлений.
 - **Правила фильтрации трафика** определяют правила обработки файлов в зависимости от их MIME-типа.
 - **Черные и белые списки** ограничивают круг ресурсов в Интернете, доступных для просмотра пользователями.

4.1. Настройка действий для зараженного трафика

Определить действия по отношению к зараженному трафику можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

Для настройки через веб-интерфейс необходимо в разделе **Расширенные настройки**, доступном на странице **Веб-прокси**, перейти на закладку **Действия над угрозами** и выставить необходимые значения для параметров **Зараженные** (Infected), **Подозрительные** (Suspicious), **Неизлечимые** (Incurable) и т. д.

Предлагаемый список действий различается в зависимости от типа вредоносных программ. Так, для вирусов на выбор предлагаются действия **Информировать** (report — вывести html-страницу с соответствующим сообщением), **Отсечь** (truncate — обрезать файл до нулевой длины и вернуть его получателю), **Лечить** (cure/pass — пропустить вылеченный файл), **В карантин** (move — переместить файл в карантин и вывести html-страницу с соответствующим сообщением). Для троянских программ действие **Лечить** недоступно — программы такого типа не имеют механизма размножения, и их лечение невозможно.

Веб-прокси

[Основные настройки](#) | [Карантин](#) | [Расширенные настройки](#)

На этой вкладке вы можете задать правила фильтрации трафика и выбрать действия, которые будут применяться к обнаруженным угрозам.

Действия над угрозами ▼	Тематический фильтр	Системные настройки	Правила фильтрации трафика	Черный и Белый списки
Подозрительные Информировать ▼	Действие, совершаемое с подозрительными (потенциально зараженными) файлами.			подробнее
Зараженные Лечить ▼	Действие, совершаемое с зараженными файлами, которые, возможно, удастся вылечить.			подробнее
Неизлечимые Информировать ▼	Действие, совершаемое с файлами, содержащими неизлечимые вирусы.			подробнее
Рекламные программы Информировать ▼	Действие, совершаемое с рекламными программами.			подробнее

Применить сделанные изменения можно, нажав кнопку **Применить и сохранить изменения**.

4.2. Управление карантинном

На вкладке **Карантин** представлен список заблокированных веб-адресов. Подозрительные файлы помещаются в карантин целиком, а имена их создаются по специальным правилам из адресов тех веб-страниц, откуда файл был скачан.

Для просмотра карантина необходимо через веб-интерфейс выбрать пункт **Веб-прокси** в разделе **Безопасность** (или нажать на иконку **Проверка HTTP и FTP трафика** на странице просмотра состояния комплекса) и щелкнуть по пункту меню **Карантин**.

Веб-прокси

[Основные настройки](#) | [Карантин](#) | [Расширенные настройки](#)

На данной вкладке содержится список ссылок на заблокированные файлы в директории карантина. Имена соответствующих файлов создаются из адресов тех веб-страниц, с которых данные файлы были загружены.

Файлы карантина			Очистить	Удалить
<input type="checkbox"/>	URL	Размер	Дата	
<input type="checkbox"/>	http://eicar.org/download/eicarcom2.zip	308 б	13 07 2012 09:22	
<input type="checkbox"/>	http://eicar.org/download/eicar_com.zip	184 б	13 07 2012 09:22	
<input type="checkbox"/>	http://eicar.org/download/eicar.com.txt	68 б	13 07 2012 09:22	
<input type="checkbox"/>	http://eicar.org/download/eicar.com	68 б	13 07 2012 09:22	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/vchost.exe	53.2 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/vchost.url	167.97 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/vchost.exe	20 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/vchost(0).exe	53.2 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/mzsm32.url	92 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/nod	41 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/msocks.url	155 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/man.jpg	789 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/gamet.dll.url	76 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/grfp.url	36.07 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/lsd.url	147.96 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/ldr.url	660 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/dns1.dll	22.73 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/algesteyes.url	56 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan2.url	128 кБ	13 07 2012 09:21	
<input type="checkbox"/>	http://10.4.0.36/augtrojan/backdoor/trojan/algestwebs.url	56 кБ	13 07 2012 09:21	

1-20 21-35

Чтобы удалить URL из директории карантина, нужно выделить его и нажать кнопку **Удалить**.

5. Настройка системы защиты сети

5.1. Развертывание антивирусной сети Dr.Web Enterprise Suite

Система антивирусной защиты рабочих станций и серверов Dr.Web Enterprise Suite имеет в своем составе большое количество средств развертывания. В зависимости от структуры локальной сети, политик безопасности, действующих в компании, системный администратор может использовать возможности веб-интерфейса, Active Directory. В данном руководстве будут рассмотрены варианты развертывания через веб-интерфейс и утилиту инсталляции компонентов. Последний способ рекомендуется использовать в случае недоступности (невидимости) защищаемых станций с центрального сервера.

5.1.1. Установка с использованием веб-интерфейса

Для того чтобы соединиться с помощью веб-интерфейса с антивирусным сервером, необходимо либо, перейдя на страницу **Защита рабочих станций**, нажать на кнопку **Перейти к Dr.Web Enterprise Security Suite**, либо в адресной строке браузера ввести его имя или адрес (по умолчанию используется адрес 192.168.1.100) и указать порт 9080 (в случае использования протокола http) или 9081 (в случае использования протокола https).

Пример адресной строки: **http://192.168.1.100:9080**.

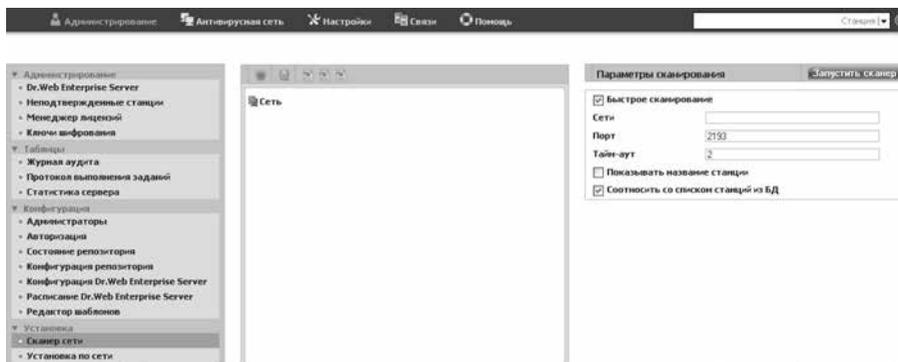
Логин по умолчанию — **admin**, пароль — **root**.

Внимание! Пароль доступа к Dr.Web Office Shield никак не связан с логином и паролем, используемым для доступа к Центру управления Dr.Web ES. Логин и пароль доступа к Центру управления Dr.Web ES задаются в Центре управления Dr.Web ES.

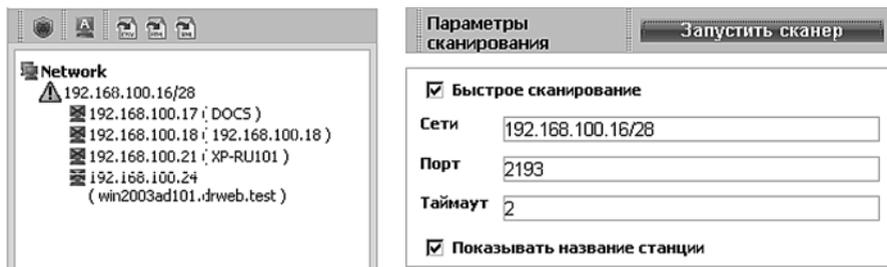
В случае необходимости системный администратор может использовать средства шифрования и сжатия трафика, встроенные в Dr.Web Enterprise Suite, заменить адрес по умолчанию.

Внимание! Веб-консоль, входящая в состав Dr.Web Enterprise Suite, поддерживает только браузеры Internet Explorer и Mozilla Firefox.

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

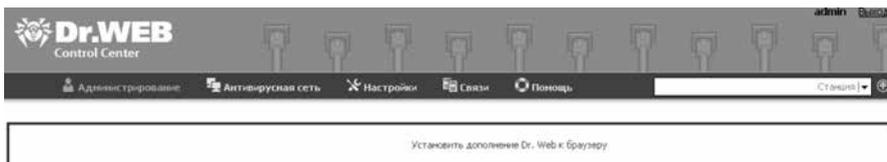


В поле **Сети** введите параметр вашей сети (в данном примере это 192.168.1.100/28) и нажмите **Запустить сканер**.



Внимание! Для отображения данной страницы может потребоваться установка дополнительного плагина к браузеру. Сообщение о необходимости установки появится автоматически.

Плагин доступен для браузеров, работающих под операционными системами Windows и Linux.

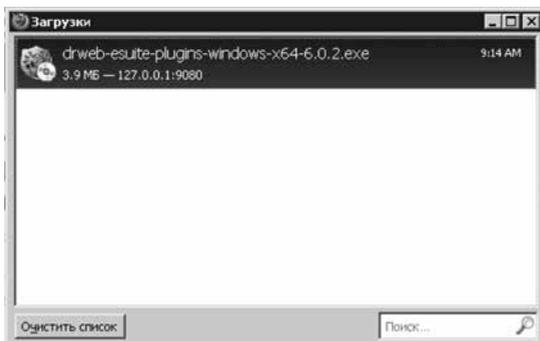
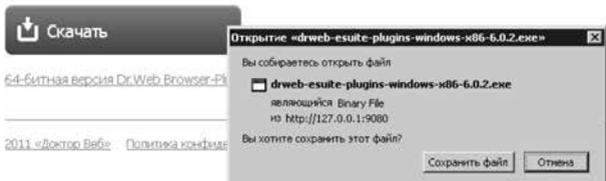


На появившейся странице предлагается начать скачивание плагина или (в случае, если тип плагина определен неверно) выбрать для скачивания необходимый тип плагина.

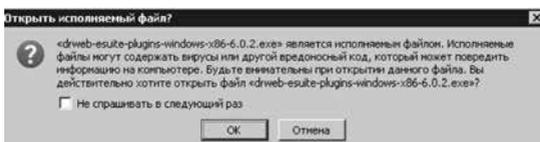
Внимание! При использовании неанглоязычного браузера Firefox на англоязычной операционной системе Windows необходимо убедиться, что в названии папки загрузки по умолчанию не используются неанглийские символы (должна быть только латиница). Настройка папки скачивания производится на странице **Основные**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



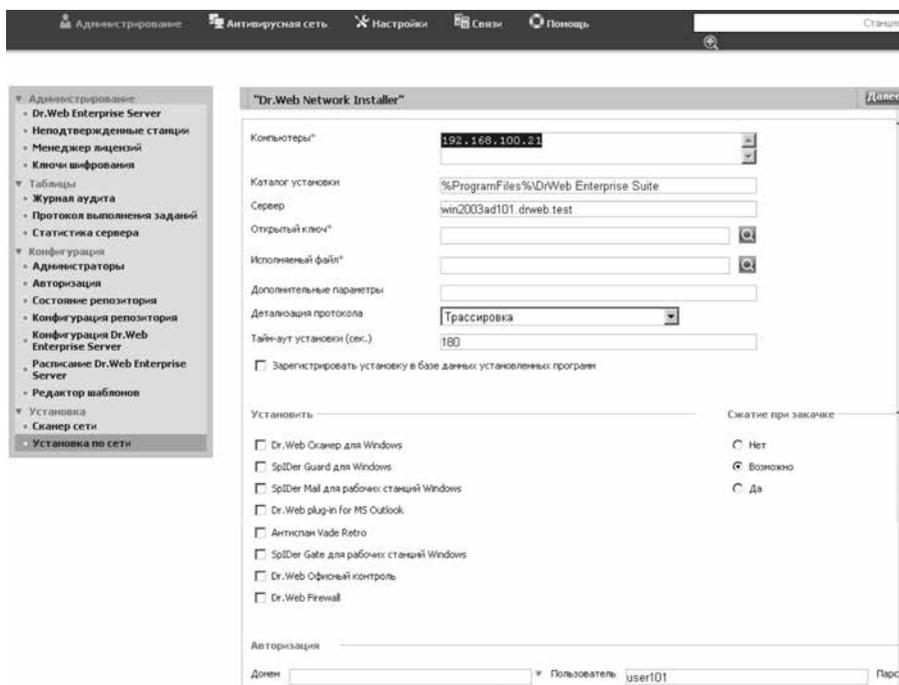
Dr.Web Browser-Plugin для Firefox 4 (x86)



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. Для начала процедуры установки выберите станцию из сформированного списка и нажмите .



В открывшемся окне выберите параметры установки, включая устанавливаемые компоненты.

Начиная с версии 5.0 в состав Dr.Web Enterprise Suite входят компоненты **SpIDer Gate** и **Офисный контроль**, для использования которых необходимо, чтобы они были указаны в вашей лицензии (Антивирус+Антиспам). Если данные продукты не указаны в лицензии, рекомендуется настроить список устанавливаемых компонентов на рабочих станциях, установив значение **Не может** для компонентов SpIDer Gate и Офисный контроль. Аналогично необходимо поступить в случае отсутствия лицензии на Антиспам.

Если вы изменили название папки с дистрибутивами (по умолчанию это \\192.168.1.100\public), последовательно нажмите значки  напротив полей **Открытый ключ** и **Исполняемый файл**, введите путь к открытой папке и выберите файлы drwcsd.pub и drwinst.exe. По умолчанию вводимые значения – \\appliance\drwesi\$\drwinst.exe и \\appliance\drwesi\$\drwcsd.pub.

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

Открытый ключ
 Исполняемый файл

Используемый сервер Dr.Web Office Shield указывается в поле **Сервер** (по умолчанию **192.168.1.100**).

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 .

Внимание! В том случае, если в сети, в которой производится установка Dr.Web Enterprise Suite, отсутствует доменная организация, необходимо на каждый компьютер, на который производится установка компонентов Dr.Web Enterprise Suite, завести учетную запись администратора, совпадающую по логину и паролю с учетной записью администратора компьютера, с которого производится установка.

Авторизация

Домен Пользователь Пароль

drweb.test\user101
 drweb.test\user101
 user106

В открывшемся окне выберите параметры установки.

Dr.Web Enterprise Agent для Windows Назад Установить

Шифрование Сжатие

Нет Нет
 Возможно Возможно
 Да Да

Авторизация

Установить параметры
 Идентификатор
 Пароль

Нажмите **Установить**.



Выберите пункт **Неподтвержденные станции**, отметьте станции, на которых была произведена установка, и нажмите на значок или .

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

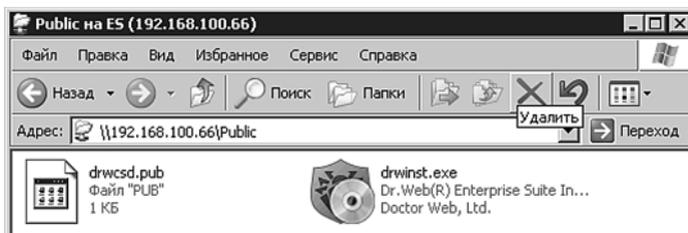
5.1.2. Установка с использованием дистрибутивов компонентов Dr.Web Enterprise Suite

Необходимо открыть папку на сервере Enterprise Suite (в данном примере это **192.168.1.100**), содержащую файлы, необходимые для установки компонентов Dr.Web Enterprise Suite. Адрес папки по умолчанию – **\\192.168.1.100\public**.

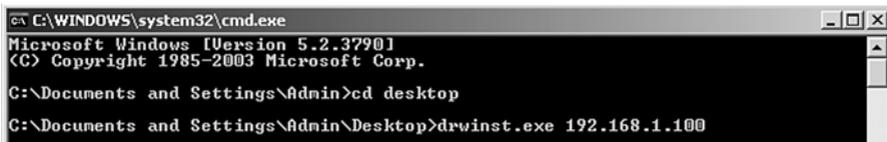
Внимание! После настройки Dr.Web Office Shield данный адрес может измениться.



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



Для установки компонентов Dr.Web Enterprise Suite на рабочую станцию или файловый сервер Windows необходимо либо просто запустить файл drwinst.exe, кликнув на него, либо запустить его в командной строке с указанием адреса сервера Enterprise Suite.



Свидетельством удачного завершения установки является появление значка в трее.



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

Для завершения процесса установки необходимо будет перезагрузить станцию, на которой она была проведена.



5.2. Смена языка отображения

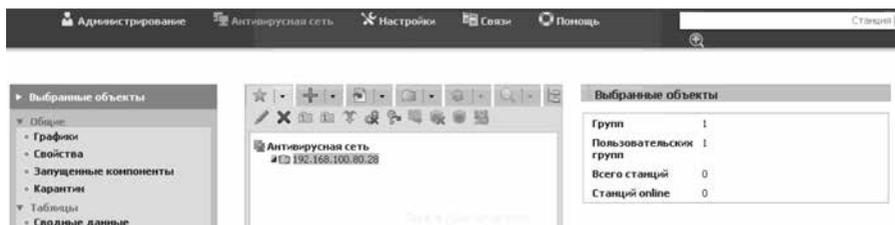
В связи с тем, что Dr.Web Enterprise Suite позволяет использовать для управления системой более одного системного администратора, каждый из которых может иметь свой предпочтительный язык отображения, этот параметр задается в профиле администратора. Для его редактирования надо перейти в раздел **Администрирование** (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**.



5.3. Управление параметрами защиты рабочих станций и серверов Windows

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.

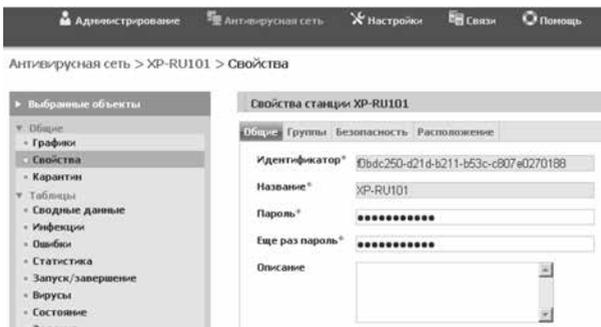


5.3.1. Просмотр параметров защиты рабочих станций и серверов Windows

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



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



Антивирусная сеть > XP-RU101 > Свойства



Выбрав пункт **Права** в группе **Конфигурация**, 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.



Антивирусная сеть > Everyone > Права



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

Антивирусная сеть > Everyone > Устанавливаемые компоненты



5.3.2. 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

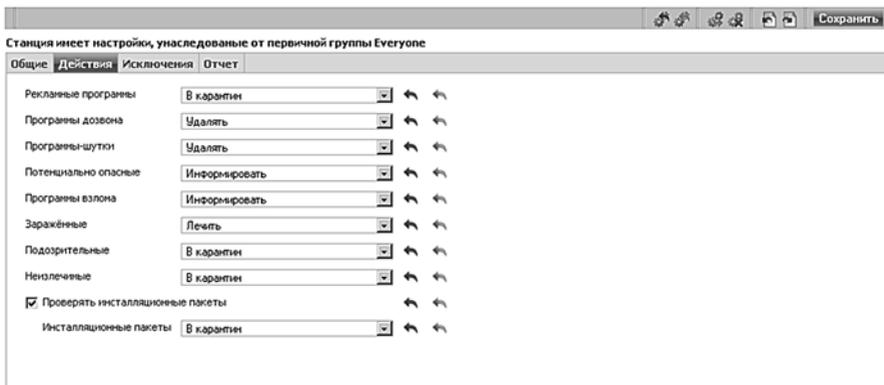
Настроить параметры защиты рабочих станций и серверов, а также групп станций можно, выделив соответствующий объект в дереве антивирусной сети и выбрав соответствующий пункт в группе настроек **Конфигурация**.

Конфигурация



Так, для компонента SpIDer Guard администратор может задать действия программы в зависимости от типов вредоносных объектов.

Антивирусная сеть > VISTA-RU104 > SpIDer Guard® для Windows XP



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.

Максимальный размер распакованных файлов (КБ)

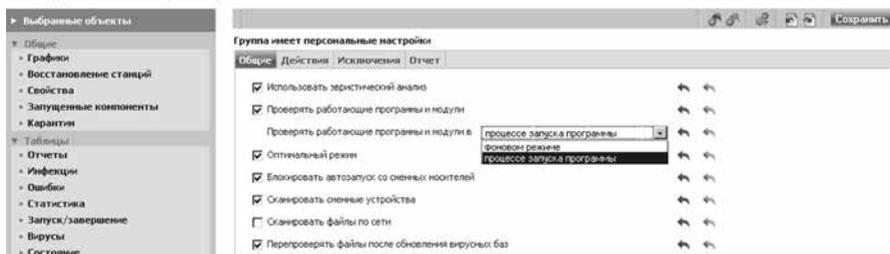
Максимальная степень сжатия

Проверять степень сжатия при размере (КБ)

Отключить режим расширенной защиты

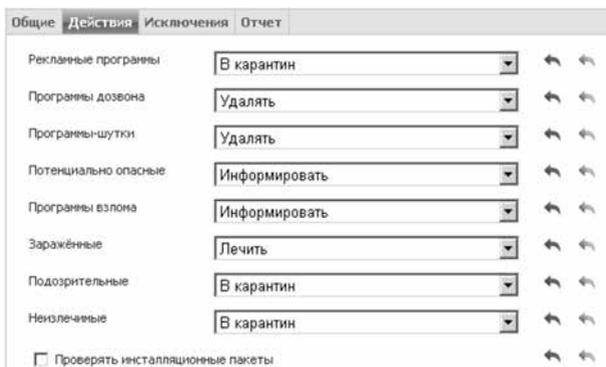
Аналогично на странице SpIDer Guard® G3 можно выбрать режим проверки файлов.

Антивирусная сеть > Everyone > SpIDer Guard® G3 for Windows Servers



Использование значков ↶ ↷ справа от параметров позволяет вернуть редактируемые значения либо в значение до редактирования, либо в значение по умолчанию.

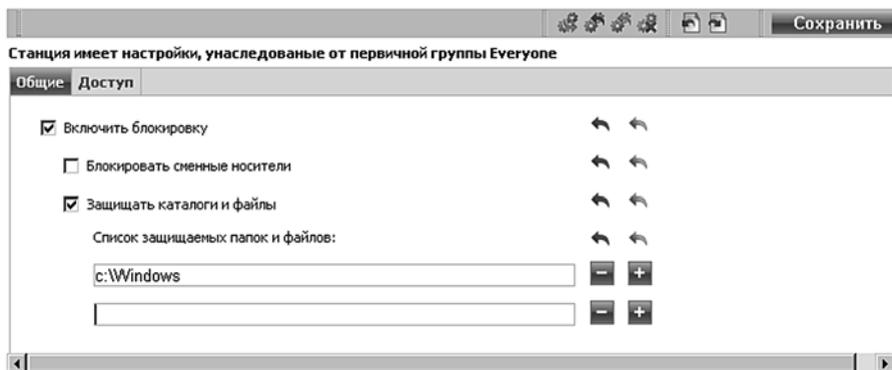
Действия программы для различных типов вредоносных объектов:



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

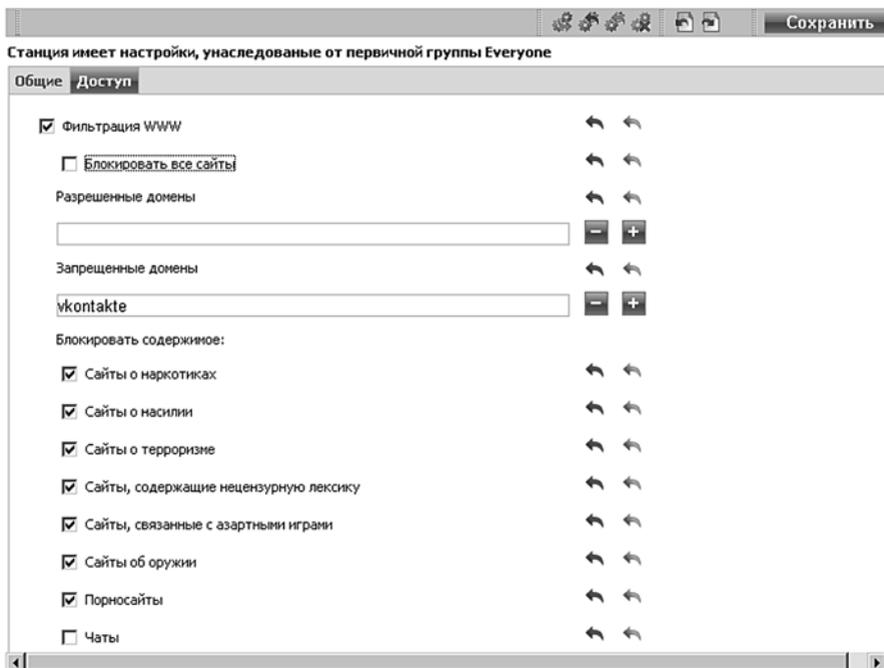
5.3.3. Настройка доступа к защищаемым каталогам и сменным носителям

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 этого надо выбрать пункт **Офисный контроль** и, отметив **Включить блокировку**, указать тип защиты — например, вручную добавив защищаемые каталоги.



5.3.4. Настройка доступа к ресурсам и узлам сети Интернет

Ограничение доступа к ресурсам сети Интернет позволят 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 или запрещать все, кроме отдельно оговоренных ресурсов, отметкой **Блокировать все сайты**.

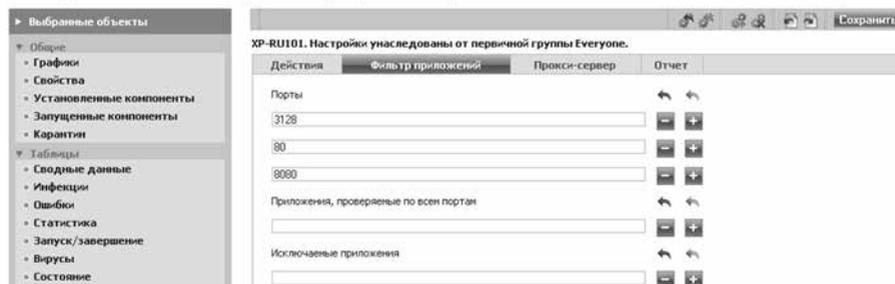


5.3.5. Настройка проверки HTTP-трафика. Выбор приложений для проверки/исключения из проверки их трафика, выбор контролируемых портов

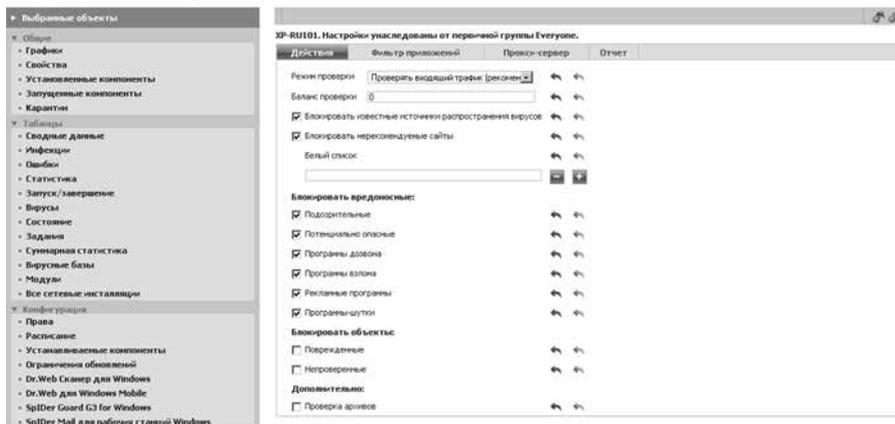
Используя возможности компонента **Dr.Web® SpiDer Gate**, администратор имеет возможность гибко управлять защитой HTTP-трафика, настраивая уровень контроля различного типа программ, определяя проверяемые порты и приложения, действия при обнаружении вредоносных объектов.



Антивирусная сеть > XP-RU101 > SpiDer Gate для рабочих станций Windows



Антивирусная сеть > XP-RU101 > SpiDer Gate для рабочих станций Windows

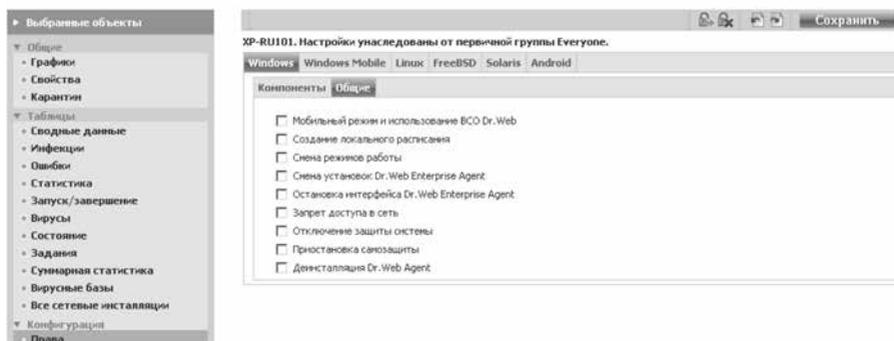


5.3.6. Настройки для мобильных пользователей

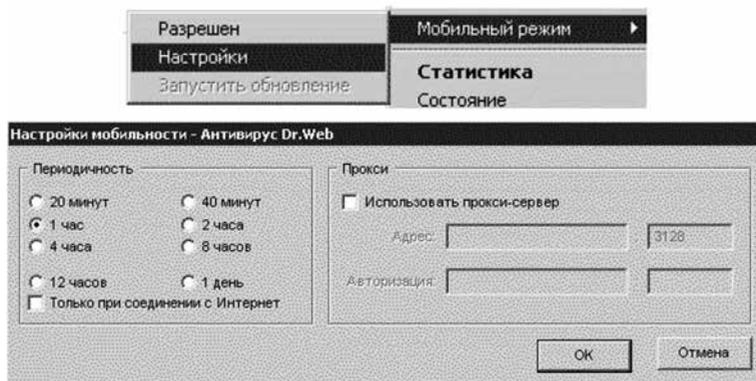
Наличие режима для мобильных пользователей позволяет обеспечить антивирусную защиту пользователя даже в том случае, если соединение его компьютера с сервером обновлений компании затруднено или является невозможным. Для таких пользователей администратор может как определять режим подключения компонента Dr.Web® Enterprise Agent, так и включать специальный мобильный режим работы с возможностью прямого подключения к серверам обновлений.

Для включения мобильного режима работы необходимо выбрать станцию и затем в разделе **Права** из группы настроек **Конфигурация** перейти на вкладку **Общие** и отметить **Мобильный режим использования**.

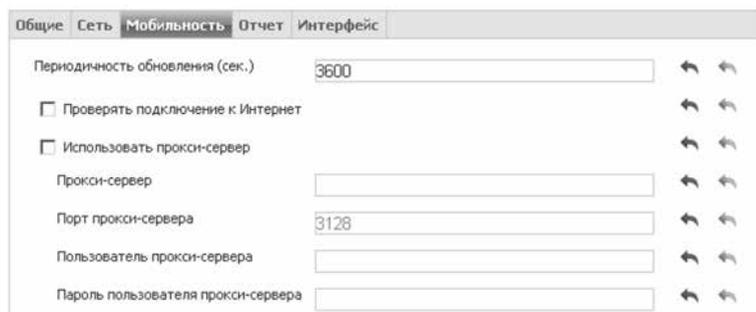
Антивирусная сеть > XP-RU101 > Права



После включения мобильного режима на стороне пользователя в контекстном меню появляется пункт **Мобильный режим**. Пользователь, если его компьютер долгое время не будет иметь связи с антивирусным сервером, для своевременного получения обновлений с серверов BCO Dr.Web может самостоятельно включать и выключать мобильный режим работы антивирусного Агента. Для этого в контекстном меню значка  в области уведомлений Панели задач необходимо выбрать **Мобильный режим**, а затем **Активировать**. Цвет значка в системном трее изменится на желтый .



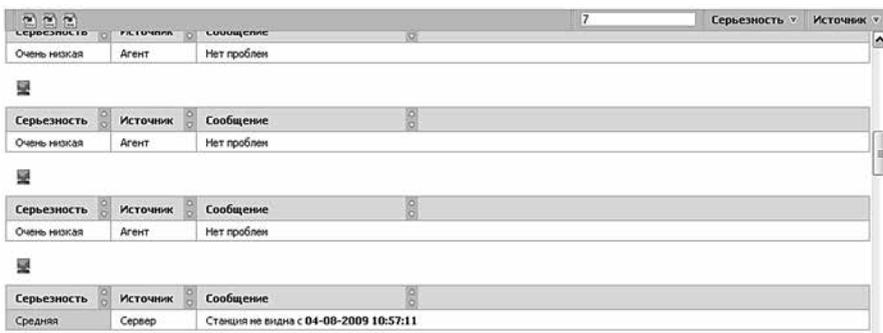
Для настройки параметров подключения к Интернету для конкретной станции или группы необходимо выбрать пункт Dr.Web Enterprise Agent для Windows, перейти на закладку **Мобильность** и настроить режим подключения к Интернету.



6. Контроль состояния сети

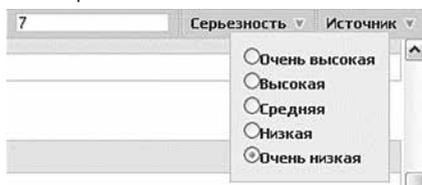
Следить за состоянием антивирусной сети, построенной на базе Dr.Web Enterprise Suite, можно с помощью таблицы состояния станций, а также отчетов и оповещений, формируемых антивирусным сервером.

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

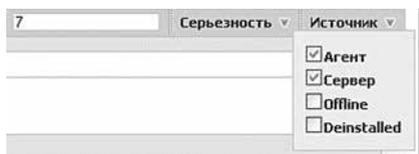


Серьезность	Источник	Сообщение
Очень низкая	Агент	Нет проблем
Очень низкая	Агент	Нет проблем
Очень низкая	Агент	Нет проблем
Средняя	Сервер	Станция не видна с 04-08-2009 10:57:11

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 серьезности сообщений **Очень высокая**, то будут выведены только сообщения с очень высоким уровнем серьезности (критичные).



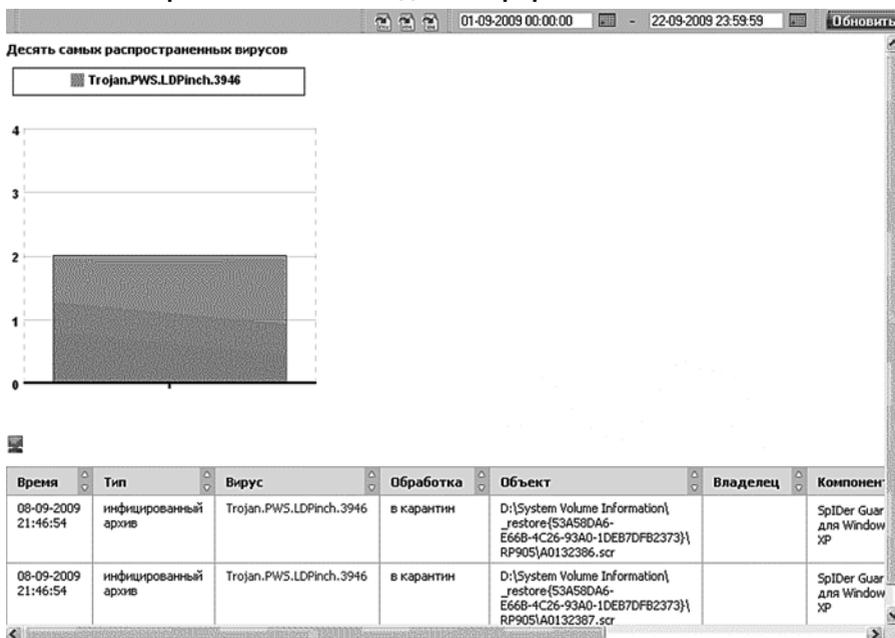
Также можно выбрать типы источников, информация от которых будет отображаться, с помощью группы настроек **Источник**. В качестве источников могут выступать антивирусные агенты и антивирусные серверы. Также может выводиться информация по станциям, которые в данный момент не подключены к антивирусному серверу, или станциям, с которых к настоящему моменту был удален антивирусный агент.

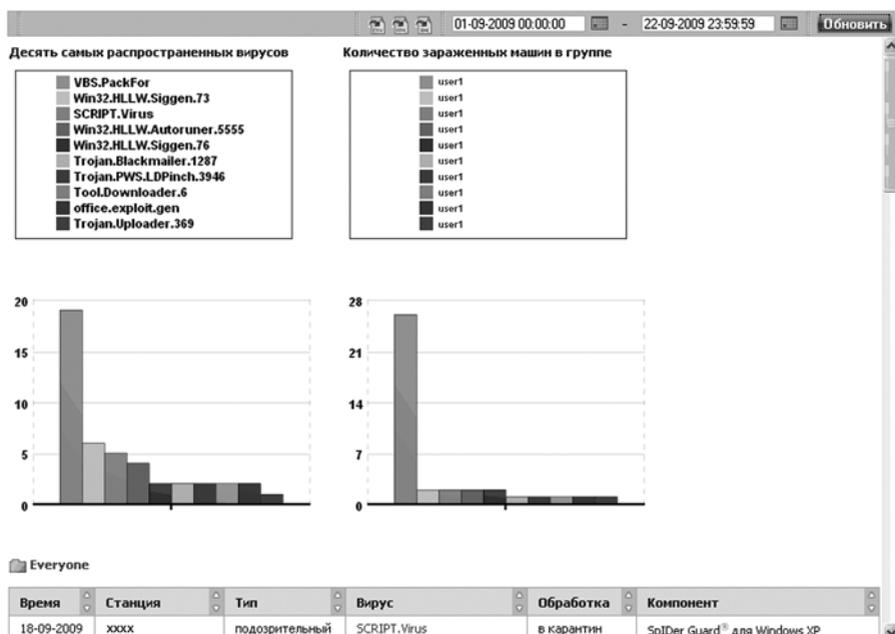


6.1. Сбор статистики. Формирование графиков активности вирусов, статистики по найденным типам вредоносных объектов, произведенных над ними действий

Используя возможности веб-интерфейса, администратор может формировать отчеты о состоянии антивирусной защиты, в том числе о количестве пойманных вредоносных объектов и произведенных над ними действиях. 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 также для групп и сети в целом.

Настройка видов собираемой статистики производится в разделе **Конфигурация Dr.Web® Enterprise Server** (меню **Администрирование**).





Полученную статистику администратор может экспортировать в удобный для себя формат.



Для администратора доступны также суммарная статистика в виде таблицы по пользователям и группам и возможность построения графиков активности вирусов.

Общая статистика

Группа	Искать	Свойства	Сортировка	Фильтр	Справка	Печать	Выход	Справка	Печать	Выход	Справка	Печать	Выход
Everyone	74998485	636	2	18	0	35	189	0	62	5	31551	2668	
74998485	636	2	18	0	35	189	0	62	5	31551	2668		

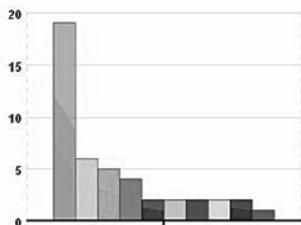
Everyone

Станция	Искать	Свойства	Сортировка	Фильтр	Справка	Печать	Выход	Справка	Печать	Выход	Справка	Печать	Выход
sotrudnik_1	1204849	12	1	0	0	6	4	0	3	0	16	1642	
sotrudnik_2	43402	0	0	0	0	0	0	0	0	0	0	4728	
sotrudnik_3	846066	0	0	0	0	0	0	0	0	0	0	1923	
sotrudnik_4	327916	0	0	0	0	0	0	0	0	0	0	4287	
sotrudnik_5	811789	2	0	0	0	2	0	0	0	0	0	15907	
sotrudnik_6	989452	3	0	0	0	1	0	0	0	1	875	3841	
sotrudnik_7	569822	0	0	0	0	0	0	0	0	0	0	917	
sotrudnik_8	1114224	48	0	0	0	0	1	0	0	0	0	13972	
sotrudnik_9	586905	2	0	0	0	2	0	0	0	0	0	3454	
sotrudnik_10	7684380	150	0	0	0	0	0	0	3	0	28434	16307	
sotrudnik_11	321273	5	0	0	0	2	0	0	3	0	0	7606	
sotrudnik_12	934736	0	0	0	0	0	0	0	0	0	0	1996	
sotrudnik_13	3136036	2	0	0	0	0	1	0	0	1	1	18964	
sotrudnik_14	1226774	1	0	0	0	0	0	0	1	0	77	154	
sotrudnik_15	1344515	4	0	0	0	3	0	0	1	0	0	2341	
sotrudnik_16	1554143	54	0	7	0	1	1	0	7	0	0	12528	
sotrudnik_17	852988	0	0	1	0	0	0	0	1	0	0	1441	

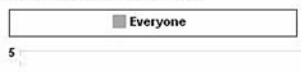
01-09-2009 00:00:00 - 22-09-2009 23:59:59 Обновить

Десять самых распространенных вирусов

- VBS.PackFor
- Win32.HLLW.Siggen.73
- SCRIPT.Virus
- Win32.HLLW.Autoruner.5555
- Tool.Downloader.6
- Win32.HLLW.Siggen.76
- Trojan.PWS.LDPinch.3946
- office.exploit.gen
- Trojan.Blackmailer.1287
- Trojan.Uploader.369



Суточная активность вирусов



Десять наиболее зараженных машин

- sotrudnik_10
- sotrudnik_8
- sotrudnik_11
- sotrudnik_6
- sotrudnik_16
- sotrudnik_1
- sotrudnik_15

7. Статистика использования ресурсов сети Интернет

Для просмотра статистики использования ресурсов сети Интернет необходимо перейти на страницу **Статистика**, нажав соответствующий пункт в группе **Сеть**.

Статистика



Чтобы просмотреть статистику за конкретный год или месяц, необходимо выбрать интересующий год и месяц в календаре, а затем выбрать тип интересующей статистики и период. Например, для просмотра суммарной информации за месяц необходимо выбрать кнопку **МЕСЯЦ** в столбце **Всего**.

Статистика

целиком МЕСЯЦ

Отчётный период: Июль 2012

№	Время	График	МЕСЯЦ	Пользователь	Соединений	Скачано	%
1			[M]	192.168.3.201	14	9 7936	100.0%
2			[M]	192.168.3.5	1	06	0.0%
Всего						9 7936	

Для просмотра информации о времени посещения необходимо выбрать в появившейся таблице значок .

Статистика

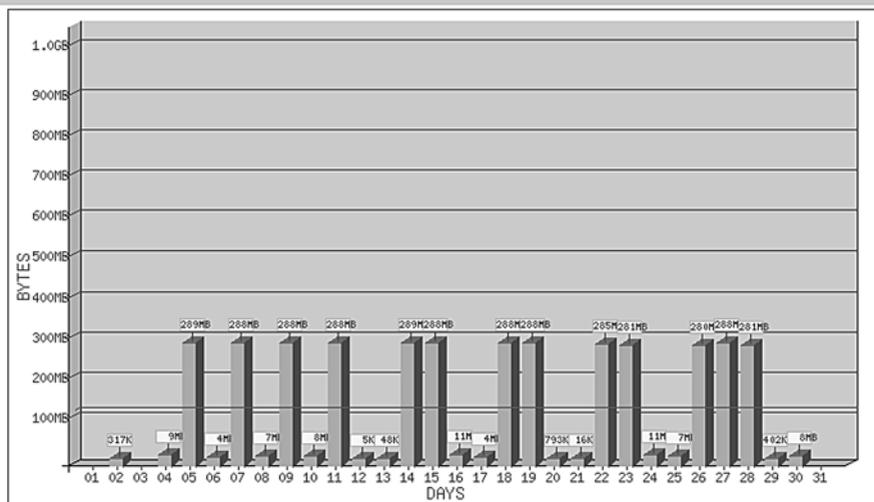
Пользователь: 192.168.3.201
 Дата: целиком МЕСЯЦ - 2012 Июль

№	Посещённые сайты	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Всего
	Всего	0.0	.	0.0	0.0	9 793Б
1	192.168.3.200	0.0	0.0	4 035Б
2	192.168.3.156	0.0	.	0.0	3 052Б
3	192.168.3.157	0.0	2 706Б
	Всего	0.0	.	0.0	0.0	9 793Б

Для просмотра информации в виде графика необходимо выбрать значок .

Отчётный период: Сен 2010

Пользователь "192.168.1.1"



Для просмотра информации по дням недели необходимо напротив интересующего пользователя выбрать значок [M].

Пользователь: 192.168.3.201
 Отчётный период: Июль 2012
 Всего: 9 793Б



Дата	Скачано	За неделю	Итого
13 Июль 2012	362Б		362Б
12 Июль 2012	1 345Б		1 707Б
11 Июль 2012	8 086Б		9 793Б
Всего	9 793Б		

Для просмотра информации по посещенным сайтам необходимо выбрать интересующего пользователя.

Пользователь:	192.168.100.10 (?)
Дата:	целиком МЕСЯЦ - 2010 Авг

Всего		6.0 М			
№	Посещённые сайты	Соединений	Байт	Итого	%
1	www.mobile-review.com	30	4.4 М	4.4 М	73.6%
2	fc05.deviantart.net	1	717 406	5.1 М	11.4%
3	mrmurtazin.com	34	219 184	5.3 М	3.5%
4	img-fotki.vandex.ru	2	171 151	5.4 М	2.7%
5	mediacdn.disqus.com	34	137 598	5.6 М	2.2%
6	h6.qqgpt.com	1	62 749	5.6 М	1.0%
7	s.lurkmore.ru	8	59 516	5.7 М	0.9%
8	static.ak.fbcdn.net	6	58 228	5.7 М	0.9%
9	i.imgur.com	1	40 930	5.8 М	0.6%
10	lurkmore.ru	15	40 342	5.8 М	0.6%

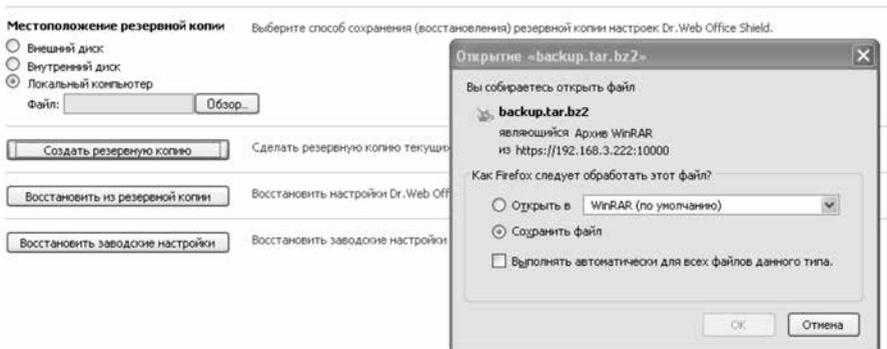
8. Сохранение и восстановление настроек

8.1. Сохранение настроек

Для сохранения настроек необходимо открыть закладку **Сохранение и восстановление** и выбрать **Создать резервную копию**. По умолчанию копия сохраняется на жестком диске.

Сохранение и восстановление

На этой странице вы можете сделать резервную копию настроек модулей Dr.Web Office Shield и восстановить их при необходимости. Резервная копия содержит конфигурационные файлы основных модулей Dr.Web Office Shield.



8.2. Восстановление настроек

Для восстановления настроек необходимо открыть закладку **Сохранение и восстановление**.

Если необходимо восстановить настройки по умолчанию, то необходимо выбрать **Восстановить заводские настройки**. Если необходимо восстановить ранее сохраненные настройки — **Восстановить из резервной копии**.

Внимание! После обновления образа системы **Dr.Web Office Shield** ранее сохраненные настройки могут оказаться несовместимы. В этом случае их загрузка будет невозможной.

Если вы настроили антивирусную сеть предприятия при помощи **Dr.Web Enterprise Suite**, входящего в состав комплекса, а восстанавливаемые настройки не содержат настроек антивирусной сети **Dr.Web ES**, то восстановление настроек может привести к тому, что антивирусная сеть **Dr.Web ES** окажется недоступной — в этом случае необходимо выполнить восстановление антивирусной сети.

9. Тестирование производительности программно-аппаратного комплекса Dr.Web Office Shield

9.1. Процедура тестирования Dr.Web Office Shield

Процедура тестирования включает:

1. Тестирование функционирования системы фильтрации почтового трафика.
2. Тестирование функционирования системы фильтрации интернет-трафика.
3. Тестирование функционирования брандмауэра.
4. Тестирование функционирования системы защиты рабочих станций Windows.
5. Тестирование функционирования системы Wi-Fi.

Рекомендуемая суммарная продолжительность тестирования — 4–8 рабочих часов.

В связи с тем, что отдельные этапы тестирования достаточно сильно нагружают сервер, что может привести к задержкам в работе пользователей локальной сети, рекомендуется либо проводить его тестирование в нерабочие дни, либо устанавливать его для тестирования в качестве внутреннего сервера локальной сети.

9.2. Тестирование производительности системы фильтрации почтового трафика

Для проведения тестирования кроме сервера Dr.Web Office Shield рекомендуется использовать дополнительно две рабочие станции: для отправки тестовых сообщений и для их приема.

Перед началом тестирования на Dr.Web Office Shield необходимо произвести следующие изменения:

1. Задать адрес принимающей машины (почтового сервера компании, осуществляющего доставку писем). Для этого необходимо в веб-интерфейсе Dr.Web Office Shield:
 - 1.1. Зайти на вкладку **Почтовый прокси**.
 - 1.2. Задать адрес принимающей машины в виде `inet:ip.address.bhm.receivever:port` в поле **Address**.
 - 1.3. Применить сделанные изменения.
 - 1.4. Указать адрес, по которому будут приходить уведомления о найденных вирусах и/или спаме. Сделать это можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

Для настройки через веб-интерфейс необходимо выбрать **Расширенные настройки** на странице **Почтовый прокси**, открыть закладку **Отчеты** и прописать адрес для параметра **Адрес администратора**. Применить сделанные изменения, нажав кнопку **Применить и сохранить изменения**.

- ГЛАВНАЯ
- Системные настройки
- ОБЩИЕ НАСТРОЙКИ
- Расширенные настройки
- Безопасность
- Сетевые настройки
- СЕТЬ
- Обновление
- DNS
- SMTP
- VPN
- Статистика
- БЕЗОПАСНОСТЬ
- Почтовый прокси
- Веб-прокси
- Защита рабочих станций
- Планшет
- СИСТЕМА
- Обновление ПО
- Сборщики и восстановление
- Системные файлы
- Диагностика и замедление работы
- Установленные пакеты
- КОМПОНЕНТЫ
- Настройка Webmail

Почтовый прокси

Системные настройки | Карантин | Расширенные настройки

На этой вкладке вы можете задать правила фильтрации почты и выбрать действия, которые будут применяться к обнаруженным угрозам.

Карантин	Адреса	Отчеты	Принимать почты	Отправка почты	Антиспам	Антивирус
Основные						
Отсылка отчетов		Отсылка отчетов.				
<input checked="" type="checkbox"/> Да						
Время отправки отчетов		График отправки отчетов.				
<input checked="" type="checkbox"/> Ежедневно						
Адреса		Адрес(а), на который(ые) высылаются отчеты. Подробнее				
<input type="text"/>						
Количество записей в списке часто блокируемых объектов		Показ в отчете списков часто блокируемых объектов и адресов, с которых присылается наибольшее количество блокируемых объектов. Подробнее				
<input type="text" value="20"/>						
Адрес администратора		Адрес системного администратора. Подробнее				
<input type="text" value="root@localhost"/>						

2. Для редактирования конфигурационных файлов необходимо зайти на сервер (локально или по ssh) и отредактировать файл /etc/drweb/maild_smtp.conf. В данном файле необходимо:

- 2.1. В секции [Notifier] для параметра AdminMail прописать адрес, по которому будут приходить уведомления.
- 2.2. Перезапустить сервис фильтрации почтового трафика с помощью команды /etc/init.d/drweb-monitor restart.

Для тестирования системы фильтрации необходимо организовать отправку писем, содержащих вредоносные программы или спам, с отправляющей машины, а также проконтролировать их получение или получение уведомлений об их доставке (найденных вирусах и спаме). В качестве примера рассмотрим отправку письма с тестовым вирусом.

```
echo "test mail with viruses" | mail -s "subject" -a __file_with_viruses__ -r root@localhost -S smtp=192.168.1.100 __to__address__
```

В данном примере:

- __file_with_viruses__ – файл с вложенными вирусами,
- root@localhost – адрес, с которого придет сообщение,
- 192.168.1.100 – адрес Dr.Web Office Shield,
- __to__address__ – адрес, на который должно прийти тестовое сообщение.

Для тестирования работы антиспама необходимо отправить письмо, содержащее в теле строчку XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X. Это так называемый GTUBE (Generic Test for Unsolicited Bulk

Email), некий аналог тестового вируса EICAR, применяемый для тестирования функций антиспама.

В качестве утилит отсылки писем можно использовать такие утилиты, как `nail`, `uencode` в связке с `mail`, `mpack`, `mutt`.

Например:

```
uencode __file1 __ __file2__ | mail -s «subject» __to__address__
```

В случае отсылки письма с тестовым вирусом на адрес, указанный в параметре `AdminMail`, должно прийти соответствующее уведомление.

Внимание! Отправляющая и принимающая машины не должны самостоятельно проверять тестируемый интернет-поток. В том случае, если на эти машины была установлена защита интернет-трафика, ее необходимо отключить.

Время тестирования — 60 минут с учетом установки и настройки необходимых утилит, сбора и формирования тестового набора файлов.

9.3. Тестирование функционирования системы фильтрации почтового трафика

Для проведения данного теста необходимо настроить локальную машину, с которой производится тестирование, на выход в Интернет через `Dr.Web Office Shield`. Для Linux в этом случае необходимо выполнить команды:

```
Route del default
```

```
Route add default gw 192.168.1.100
```

Проверить результат настройки можно через команду `route -n`.

Перед началом тестирования на `Dr.Web Office Shield` необходимо произвести следующие изменения:

1. Через веб-интерфейс `Dr.Web Office Shield` настроить выход в Интернет (напрямую или через какую-либо машину) и применить сделанные изменения.
2. Указать адрес, по которому будут приходить уведомления о найденных вирусах и/или спаме. Сделать это можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

Для настройки через веб-интерфейс необходимо выбрать пункт **Расширенные настройки** на странице **Веб-прокси**, перейти на закладку **Системные настройки** и прописать адрес для параметра **Адрес администратора**. Применить сделанные изменения, нажав кнопку **Применить и сохранить изменения**.

3. Для редактирования конфигурационных файлов необходимо зайти на сервер (локально или по `ssh`) и отредактировать файл `/etc/drweb/drweb_icapd.conf`. В данном файле необходимо:

3.1. В секции `[Icapd]` для параметра `Hostmaster` прописать адрес, по которому будут приходить уведомления.

3.2. Перезапустить сервис фильтрации интернет-трафика с помощью команды `/etc/init.d/drweb-icapd restart`.

Для проверки функционирования системы фильтрации достаточно скачать на машину, с которой производится тестирование, какой-либо файл с вредоносным кодом. Например:

ftp <http://www.eicar.com/download/eicarcom2.zip>

Результатом выполнения данного теста должно стать письмо, пришедшее на адрес, указанный в параметре Hostmaster, с уведомлением о зачке вируса.

Время тестирования — 40 минут с учетом установки и настройки необходимых утилит.

9.4. Тестирование производительности системы фильтрации интернет-трафика

Тестирование брандмауэра заключается в проверке наличия в нем уязвимостей, включая открытые неиспользуемые порты. Для тестирования можно использовать как сканеры уязвимостей типа Retina от eEye, так и сканеры портов типа hping. Желательно провести тестирование как со стороны внутренней сети, так и со стороны Интернета (icmp,udp, tcp).

Поскольку сканеры уязвимостей, как правило, работают в автоматическом режиме, подробно рассмотрим только работу с утилитой hping.

Пример тестирования 80-го порта:

```
hping -S 192.168.1.100 -p 80 -c 1
```

Здесь:

- S — указывает hping отослать SYN-пакет;
- 192.168.1.100 — адрес получателя, на который будет отправлен SYN;
- p 80 — порт на компьютере получателя, в нашем случае это порт 80;
- c 1 — количество отправляемых пакетов, в нашем случае это 1.

В том случае, если порт заблокирован, вся посланная информация должна быть потеряна.

Время тестирования — 60 минут с учетом установки и настройки необходимых утилит.

9.5. Тестирование функционирования системы фильтрации интернет-трафика

Для тестирования работы системы защиты рабочих станций с серверов Windows необходимо развернуть на одной или нескольких рабочих станциях Windows систему антивирусной защиты согласно вышеописанной инструкции.

Щелкните правой кнопкой мыши на значок  в системном трее. Выберите пункт **Статистика**. В открывшемся окне статистики запомните количество обнаруженных инфицированных объектов в строке с данными по компоненту SpiDer Gate.

Статистика - Антивирус Dr. Web

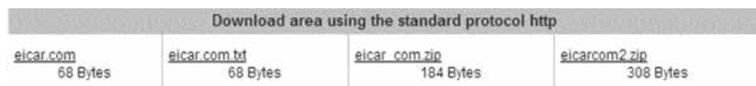
Компонент	Проверено	Инфицированных	Моди...	Подо...	Акти...	Исч
Dr. Web (R) Enterprise Scanner for Windows	674	0	0	0	0	0
SpiDer Gate (R) for Windows Workstations	0	0	0	0	0	0
SpiDer Guard (R) G3 for Workstations	1995	0	0	0	0	0
SpiDer Mail (R) for Windows Workstations	0	0	0	0	0	0
Bcero	2669	0	0	0	0	0

5 сек. 15 сек. 30 сек. 1 мин. 5 мин. Обновить ОК

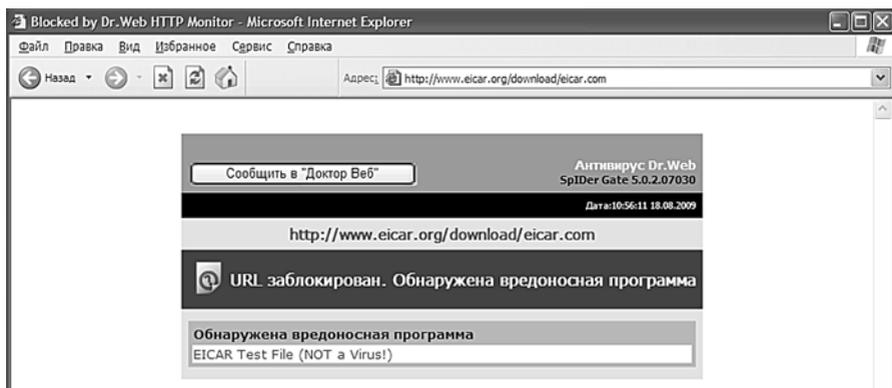
Откройте браузер, перейдите по адресу



На открывшейся странице опуститесь до текста



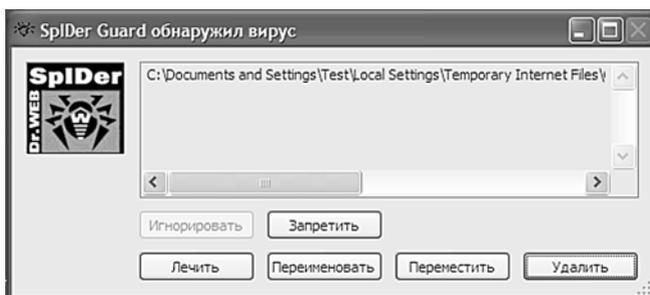
и выберите для скачивания любой из предложенных вариантов, например первый — eicar.com. В том случае, если ваша защита работает корректно, браузер должен показать следующее окно:



Щелкните правой кнопкой мыши по значку  в системном tree. Затем выберите **Статистика**. Количество обнаруженных инфицированных объектов 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 tree и снимите флаг SpiDer Gate.

Вернитесь на сайт eicar.org и снова попытайтесь загрузить тестовый вирус. Итогом попытки должно стать окошко типа:



После завершения проверки включите SpIDer Gate: щелкните правой кнопкой мыши значок  и установите флаг SpIDer Gate.

Внимание! Для тестирования функционирования защиты локальной станции желательно отключить проверку почтового и интернет-трафика для этой машины на сервере Dr.Web Office Shield.

Время тестирования – 60 минут с учетом установки и настройки системы защиты.

9.6. Тестирование функционирования системы Wi-Fi

Тестирование доступа по Wi-Fi заключается в проверке:

- 1) доступа к веб-интерфейсу Dr.Web Office Shield;
- 2) доступа к ресурсам сети Интернет для мобильных пользователей.

Для тестирования работы системы защиты рабочих станций с серверов Windows необходимо с рабочей станции Windows:

- 1) настроить локальную машину, с которой производится тестирование, на выход в Интернет через Dr.Web Office Shield;
- 2) зайти на Dr.Web Office Shield по адресу <https://192.168.1.100:10000/officeshield-wizard>;
- 3) зайти на любой ресурс локальной сети. Например: [//192.168.1.100/public](http://192.168.1.100/public);
- 4) зайти на любой ресурс сети Интернет.

Время тестирования – 40 минут с учетом установки и настройки системы защиты.

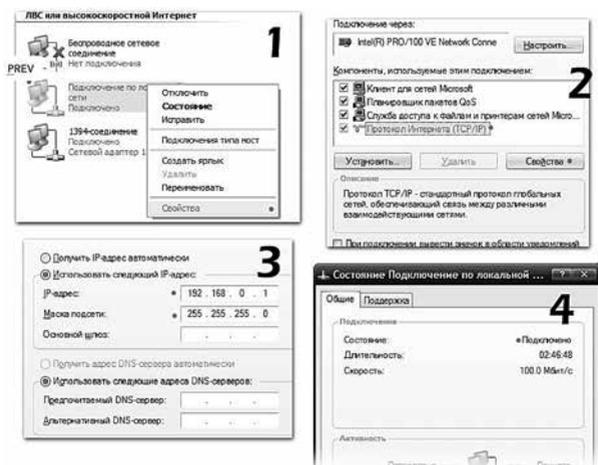
10. Приложения

10.1. Приложение 1. Получение доступа через кросс-кабель

Для получения доступа через кросс-кабель необходимо:

- Соединить используемый для настройки компьютер с Dr.Web Office Shield кросс-кабелем.
- В случае необходимости задать новый сетевой адрес используемого для настройки компьютера. Для этого выполнить **Start** (Пуск) → **Control Panel** (Панель управления) → **Network Connections** (Сетевые подключения) для Windows XP или **Start** (Пуск) → **Settings** (Настройки) → **Control Panel** (Панель управления) → **Network Connections** (Сетевые подключения) для Windows 2000.
- Выбрать в открывшем списке сетевых подключений используемую для подключения сетевую карту и, открыв по клику правой клавиши мышки меню, выбрать пункт **Properties** (Свойства).
- В открывшемся окне выбрать из списка в верхней части окна пункт **Internet Protocol (TCP/IP)** (**Протокол Интернета (TCP/IP)**) и нажать **Properties** (Свойства).
- В окне настроек сетевого адаптера на закладке **General** (Основные) отметить **Use the following IP address** (использовать следующий IP-адрес) и указать в поле **IP address** (IP-адрес) новый адрес. Например, 192.168.1.101. На соединяемых компьютерах последнее число в адресах не должно совпадать. **Маска подсети** (Subnet mask) по умолчанию 255.255.255.0.

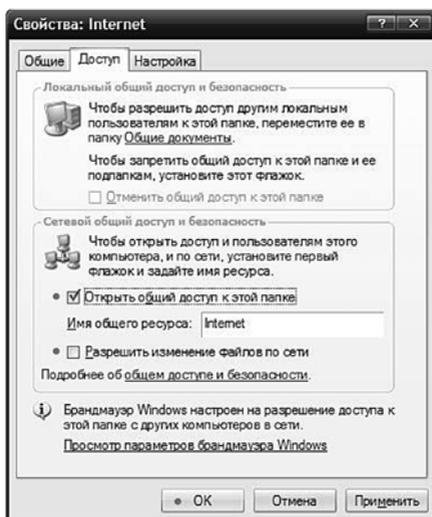
Нажимаем **OK**.



В окне **Сетевые подключения** щелкнуть два раза по значку **Соединение по локальной сети**. Если настройка была проведена верно, то напротив параметра **Состояние** появится надпись **Подключено**.

Проверить доступность компьютера можно, открыв любую папку на Dr.Web Office Shield. Для этого необходимо запустить командную строку (**Start → Run**) и ввести `\\192.168.1.100\public`.

Для того чтобы открыть папку для общего доступа, щелкните по ней правой кнопкой мыши и откройте в появившемся меню пункт **Общий доступ и безопасность**. В появившемся окне установите галочку **Открыть общий доступ к этой папке**. После этого вы сможете работать с этой папкой на другом компьютере через **Сетевое окружение**.



В том случае, если после проведения настроек невозможно установить общий доступ, рекомендуется:

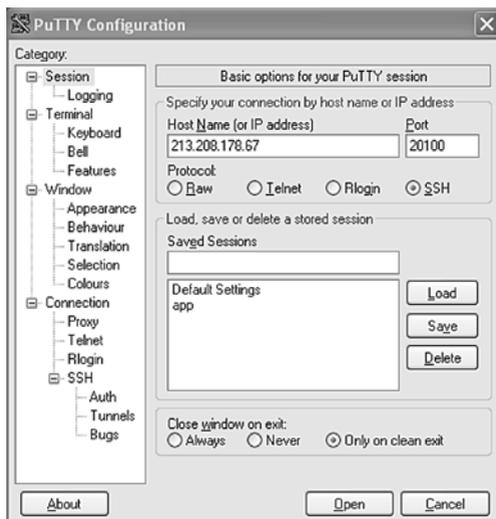
- временно отключить используемый брандмауэр;
- проверить, включен ли на компьютере **Простой общий доступ**. Для этого откройте любую папку, в меню **Сервис** выберите пункт **Свойства папки**. В открывшемся окне на вкладке **Вид** необходимо отметить пункт **Использовать простой общий доступ...** Если до этого пункт был не отмечен, то необходимо отметить его и перезагрузить используемый компьютер. После перезагрузки необходимо снять и заново поставить на всех открытых папках общий доступ;
- установить общее наименование для используемой рабочей группы в свойствах компьютера. После создания или переименования рабочей группы компьютер также потребует перезагрузить.

10.2. Приложение 2. Получение прямого доступа к операционной системе типа Linux

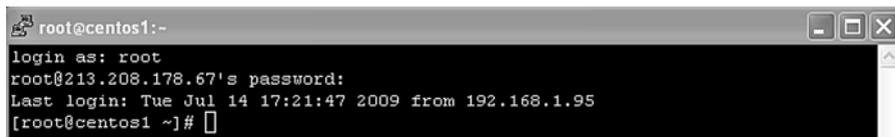
Для получения доступа к серверу Linux можно использовать любую утилиту, поддерживающую протокол SSH. Обычно в качестве такой утилиты используется PuTTY, которую, например, можно загрузить по адресу

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

Утилита не требует установки и может быть запущена сразу после загрузки. Для получения доступа необходимо ввести в соответствующие поля полученные в письме IP-адрес и порт. Введенные значения можно сохранить для использования в дальнейшем.



В открывшемся окне терминала необходимо ввести логин и пароль доступа. Для Dr.Web Office Shield это по умолчанию соответственно root и drweb.



В том случае, если для проведения тестирования необходимо поместить на сервер дополнительные файлы или дистрибутивы программ, скопировать их на сервер можно, например, с помощью команды pscp, также доступной на сайте проекта PuTTY. Запустить утилиту можно из командной строки. В качестве параметров ей передаются порт и адрес сервера, полный путь к файлам ключей и директория, куда должны быть помещены ключи. Например:

```
pscp -P 20100 agent.key enterprise.key root@213.208.178.67:/tmp
```



Гарантийный талон

Внимание! Пожалуйста, потребуйте от продавца полностью заполнить гарантийный талон, проверьте правильность указанного серийного номера и модели устройства

НАИМЕНОВАНИЕ УСТРОЙСТВА:

МОДЕЛЬ:

СЕРИЙНЫЙ НОМЕР:

ДАТА ПРОДАЖИ:

ФИРМА-ПРОДАВЕЦ:

ЮРИДИЧЕСКИЙ АДРЕС И ТЕЛЕФОН ФИРМЫ-ПРОДАВЦА:

ДАТА ЗАПОЛНЕНИЯ:

ПОДПИСЬ ПРОДАВЦА:

МЕСТО ДЛЯ
ПЕЧАТИ



Гарантийный талон № 1

Информация о ремонте:

Дата поступления в ремонт:

Дата выполнения ремонта:

Подпись владельца:

Принял:

МЕСТО ДЛЯ
ПЕЧАТИ



Гарантийный талон № 2

Информация о ремонте:

Дата поступления в ремонт:

Дата выполнения ремонта:

Подпись владельца:

Принял:

МЕСТО ДЛЯ
ПЕЧАТИ

Гарантийные обязательства

1. ООО «Доктор Веб» (далее – Производитель) несет ответственность по гарантийным обязательствам на Dr.Web Office Shield (далее – Устройство) в соответствии с действующим законодательством Российской Федерации.
2. Гарантия действительна только при предъявлении вместе с Устройством правильно и разборчиво заполненного гарантийного талона с проставленной датой продажи и печатью продавца.
3. Гарантийный срок исчисляется с момента приобретения устройства у официального дилера на территории России и стран СНГ и составляет:
 - 1) для всех устройств, блоков питания и систем охлаждения – один год;
 - 2) для Compact Flash, USB-накопителей, кабелей и прочих комплектующих – 180 дней.

В течение гарантийного срока Производитель обязуется бесплатно устранить дефекты Устройством путем его ремонта или замены на аналогичное при условии, что дефект присутствует по вине Производителя.

Устройство, предоставляемое Производителем для замены дефектного Устройством, может быть как новым, так и восстановленным, но в любом случае Производитель гарантирует, что его характеристики будут не хуже, чем у заменяемого Устройством.

4. Выполнение Производителем гарантийных обязательств по ремонту вышедшего из строя Устройством влечет за собой увеличение гарантийного срока на время ремонта.
5. Производитель не несет ответственности за совместимость своего программного обеспечения с любыми аппаратными или программными средствами, поставляемыми другими производителями, если иное не оговорено в прилагаемой к Устройством документации.
6. Ни при каких обстоятельствах Производитель не несет ответственности за любой ущерб, убытки, включая потерю данных, потерю прибыли и другие случайные, последовательные, прямые или косвенные убытки, возникший вследствие инсталляции, сопровождения, эксплуатации, либо связанные с выходом из строя и/или временной/постоянной неработоспособностью Устройством.
7. Производитель не несет ответственности по гарантии в случае, если произведенные им тестирование и/или анализ показали, что заявленный дефект в Устройством отсутствует, либо он возник вследствие нарушения правил инсталляции или условий эксплуатации, а также любых действий, связанных с попытками добиться от Устройством выполнения функций, не заявленных Производителем.
8. Условия гарантии не предусматривают чистку и профилактику Устройством силами и за счет Производителя.
9. Настоящая гарантия недействительна, если серийный номер на Устройством был изменен, удален или неразборчив.
10. Производитель не несет ответственности за дефекты и неисправности Устройством, возникшие в результате:
 - несоблюдения правил транспортировки и условий хранения, технических требований по размещению и эксплуатации;
 - неправильных действий, использования Устройством не по назначению, несоблюдения инструкций по эксплуатации;
 - механических воздействий (наличия явных механических повреждений, трещин, сколов на корпусе и внутри устройством, сломанных антенн и контактов разъемов);
 - ремонта, произведенного не уполномоченными на то компаниями либо частными лицами;
 - действия обстоятельств непреодолимой силы (таких как пожар, наводнение, землетрясение и др.) или влияния случайных внешних факторов (таких как падение напряжения в электрической сети и пр.).

ВАЖНО: до предоставления Устройством по гарантии либо предоставления Производителем услуг по Устройством вам необходимо убедиться, что вы произвели резервное копирование содержимого вашего жесткого диска, включая любые сохраненные данные или программное обеспечение, установленное на жестком диске. ООО «Доктор Веб» не несет ответственности за любой ущерб или потерю данных либо иной информации, имеющейся на любом носителе Устройством.

Подробные условия гарантийного обслуживания доступны на сайте ООО «Доктор Веб».

© 2013 ООО «Доктор Веб». Все права защищены. Товарные знаки являются собственностью их правообладателей. Программное обеспечение и спецификации могут изменяться без уведомления.



© ООО «Доктор Веб», 2003—2013

125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Телефон: +7 (495) 789-45-87 (многоканальный)

Факс: +7 (495) 789-45-97

www.drweb.com