

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 | |
| 2. Установка и настройка Dr.Web Office Shield | |
| 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 карантином | 13 |
| 4. Настройка сервиса защиты интернет-трафика | 14 |
| 4.1. Настройка действий для зараженного трафика | |
| 4.2. Управление карантином | 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 НТТР-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 | |
| 7. Статистика использования ресурсов сети Интернет | |
| 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 антиспамзащиту 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



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

1. Введение

Данный документ описывает процедуры установки и настройки системы антивирусной защиты локальной сети предприятия с помощью программно-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:

 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 | |
| | | |
| | | Вход |

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.

| Office Shield | | | Acconentation Dealthr D |
|-----------------------------|---|--|---|
| главная | Лицензирован | ие | |
| COCTORNHE CIRCTERED | Crucie and courses a resident | การสำคัญหา วิษาการการการการการการการการการการการการการ | กลายสติ หลายหลา กลางและ รอกสรร. หวด 1 การ สารเหตรก |
| ОБЩИЕ НАСТРОЙКИ | конпьютера, так и со съем | юго USB Rash накопителя, подключенного непосредо | твенно к серверу Dr.Web Office Shield. По истечения |
| Пиценонрование | срока действия лицензион | ых ключей соответствующие модули системы запуси | аться не будут. |
| <u>веб-интерфейс</u> | | | |
| Criena napona | Лицензионные ключи | | |
| CETH | enterprise.key (Ключэ agent.key (Ключэ | е загружен) — ключ для ESS-сереера е загружен) — ключ для рабочих станций в режине | ESS |
| Оодклюнения | drweb32.key (Knicks | вагружен) — ключ для защиты почтового и интер | нет-трафика |
| DHCE. | 0 | | 18 - 74 |
| 045 | Эагрузить с покального | компьютера | |
| <u>WPN</u> | enterprise.key | 063op | |
| GTATHCTHE@ | agent.key | 0630p | |
| БЕЗОПАСНОСТЬ | drweb32.key | 06sop. | |
| Exerval | O Загрузить с flash-карты | | |
| CACTEMA | Игнорировать непра | энльные ключен | |
| Обновление ПО | | | |
| Сохранение и восстановление | Sarrouterts concuersed | aŭmu | |
| Систенное вреня | Complyante cardeenard | and and a second s | |

- 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:ums_xocta_noчtoBoro_cepвера) 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



задать 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 вебинтерфейса 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 сохра**нить 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 выможете задать правила фильтрации почты и выбрать действия, которые будут применяться к обнаруженным угрозан. Карантин Ядро Отчеты Приемпочты Отправка почты Антислан Антисарус Сокет, через который антивирусный плагин Адрес сокета взаимодействует с демоном drwebd. подробнее pid:/var/drweb/run/drwebd.pid 🗙 8 Время ожидания Максимальное время ожидания исполнения команды денонон drwebd. минут 🖌 🏳 подробнее 1 Звристический анализ Настройка работы зеристического анализатора. подробнее Да 💌 Добавлять X заголовки Добавление заголовков X-Antivirus и X-Antivirus-Code к проверенным демоном drwebd Да 🛰 сообщениям. подробнее Параноидальное сканирование Настройка "параноидального" режима сканирования. Нет 🛩 подробнее Выражения для блокирования по имени файла Список регулярных выражений, используемых плагином при проверке имён файлов в отчёте, присылаеном деноном drwebd после сканирования сообщения. подробнее Зараженные Действие, совершаемое с сообщениями, заражёнными известными вирусами. Основное действие лечить × Дополнительные действия Обязательно должно быть задано одно из основных значений: излечить, удалить карантин 🗙 вложение, отклонить без уведоиления, отклонить с уведомлением. Также может быть задано одно или несколько перенаправить дополнительных значений: переместить в карантин, перенаправить, информировать. ньформировать CODENTE 🕂 добавить заголовок + добавить счет

| Подозрительные Основное действие опклонить У Дополнительные действия карантин X информировать X | Действие, совершаемое с сообщениями, которые могут быть заражены неизвестным вирусон. Обязательно должно быть задано одно из основных замачений: пропустить, удалить вложение, отклонить без уведонления, отклонить с уведонлением. Также |
|--|--|
| перенапазенть Асбаенть счет Асбаенть счет | ножет быть задано одно или несколько дополнительных значений: переместить в карантин, перемапраенть, информировать. SCENTE |
| Некалечимые Основное действие отклонить м | Действие, совершаеное с сообщеникани, заражённьани нензлечено. поддобнее |

3.2. Настройка действий для спам-сообщений

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

Для настройки через веб-интерфейс необходимо в разделе Расширенные настройки, доступном на странице Почтовый прокси, перейти на закладку Антиспам 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 вносимые 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

Основные настройки | Карантин | Расширенные настройки На этой вкладке выножете задать правила фильтрации почты и выбрать действия, которые будут применяться к обнаруженным угрозам. Карантин Ядро Отчеты Приенпочты Отправка почты Антислан Антивирус • Основные Полная проверка Производится полная проверка сообщения на наличие спана. Да 👻

Почтовый прокси

подробнее



| игнорировать встроенные домены Да 💌 | Игнорировать встроенные han-домены. Подообнев |
|--|--|
| Добавлять заголовок с версией Нет 💌 | Добавление к сообщению заголовка X-Drweb- SpanVersion, содержащего информацию о версии плагина VadeRetro. |
| Добавлять заголовок со статусом сообщения Нет 💌 | Добавление к сообщение заголовка X-Drweb- SpanSkate-Num. содообние |
| Добавлять заголовок с уровнем спама Нет 🐋 | Добавление к сообщению заголовка X-Span- Level, состоящего из символов "**. годобнее |
| Добавлять заголовки Да 💌 | Добавление к сообщению заголовков X-Drweb- SpamState и X-Drweb-SpamScore. подсобнее |
| Проверять уведомления о доставке | Возможность отдельной фильтрации уведсилений о доставки сообщений. |
| Tredexic Aus coase | Префикс, добевляеный к тене сообщения, если оно отнечено как спан. поддобная |
| Префикс для уведомлений | Префикс, добавляеный к тене сообщения, если оно является уведоплением о невозкожности доставки (и, соответственно, определено в 3 класстикен библикотекой VadeRetro). |
| Граница безусловного спама 1000 | Если оценка, полученная письном, равна значению данного параметра или превышает его, письно считается безусловным слаком. содообене |
| Префикс для безусловного спама | Префикс, добавляеный к тене сообщения, если оно отнечено как безусловный спан. одаробнее |
| Граница спама 100 | Если оценка, полученная письком, равна значенею данисго параметра или превышает его, писько считается спаком. родообние |
| Действие для безусловного спама Основное действие пропустить Дополнительные действия | Действие, совершаеное с безусловныя сланон. оздосбияв |

| DOADOOHee |
|-----------|
| |
| |
| |
| |
| |
| |
| |
| |
| |

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

| По Отправить | 🕼 Переслат | ъ 🗱 Удалить | 🖼 Не спам 🛛 | 🕲 Сообщить о спаме | | | |
|--------------|-----------------|----------------------|-------------|--------------------|---------|--------------|----------|
| Отправитель: | | | Получатель: | | Тема: | | |
| Дата: | весь период | | Размер: | байт 💌 | Статус: | любой статус | |
| | 01-01-2000 00:0 | 00 - 29-05-2012 23:5 | 5 | | | Сбросить | рименить |
| Сообщений в | абрано: 1 | | | | | | |
| Отп | равитель | Получатель | <u>Тема</u> | | | Дата 🔺 | Размер |
| | | | | | | | |



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 МІМЕ-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 ножете задать правила фильтрации трафика и выбрать действия, которые будут приненяться к обнаруженным угрозан.

| Действия над угрозами 🔻 🛛 Те | натический фильтр | Систенные настройки | Правила фильтрации трафика | Черный и Белый списки |
|--|-------------------|--------------------------|--------------------------------------|--|
| Подоэрительные Информировать | | Действие, с файлани. | овершаеное с подозрительными (потен | инально заражёнными) подробнее |
| Зараженные Лечть 🗸 | | Действне, с вылечить. | сеершаеное с заражёнными файлани, ки | оторые, возножно, удастся подробное |
| Неизлечимые Информировать | | Действие, с | звершаеное с файланн, содержашнын н | еколечиные вирусы. подробнее |
| Рекламные программы Информировать 👻 | | Действие, с | звершаеное с рекланными програннами | подробнее |

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

4.2. Управление карантином

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 **Вебпрокси** в разделе **Безопасность** (или нажать на иконку **Проверка НТТР** 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.

| айлы карантына | () Observ | VANNES |
|---|-----------|------------------|
| URL | Размер | Дата 🔅 |
| http://eicar.org/download/eicarcom2.zip | 308 b | 13.07.2012 08:22 |
| http://wicar.org/download/wicar_com.ap | 184 b | 13.07.2012 08:22 |
| http://eicar.org/download/eicar.com.txt | 68 b | 13.07.2012 08:22 |
| http://eicar.org/download/eicar.com | 68 b | 18 07 2012 08:22 |
| http://10.4.0.16/aug/troian/backdoor/troian/sychost.wx | 53.2 kB | 13.07.2012 08:21 |
| http://10.4.0.36/augtrojar/backdoor/trojar/split.urp | 167.37 kB | 13.07.2012 08:21 |
| http://10.4.0.36/aug/trojar/backdoor/trojar/svchost.ex_ | 20 kB | 13 07 2012 08 21 |
| http://10.4.0.36/aug/trojan/backdoor/trojan/suchozt(0).ex | 53.2 kB | 13.07.2012 08:21 |
| http://10.4.0.36/aug/trojar/backdoor/trojar/mszsm32.unp | 92 kB | 13 07 2012 08 21 |
| http://10.4.0.%%/aug/trojan/backdoor/trojan/nod | 41 kB | 13 07.2012 08:21 |
| http://10.4.0.36/aug/trojan/backdoor/trojan/misocks.unp | 155 kB | 13 07 2012 08 21 |
| http://10.4.0.36/aug/trojar/backdoor/trojar/msn.jpg | 789 kB | 13 07 2012 08 21 |
| http://10.4.0.36/aug/trojar/backdoor/trojar/gametdil.unp | 76 kB | 13.07.2012 08:21 |
| http://10.4.0.36/augtrojan/backdoor/trojan/hgghp.unp | 36.07 kB | 13 07 2012 08 21 |
| http://10.4.0.36/aug/trojar/backdooc/trojar/fol.unp | 147.96 kB | 13.07.2012 08:21 |
| http://20.4.0.36/aug/trojar/backdoor/trojar/dfh.unp | 660 k8 | 13 07 2012 08:21 |
| http://10.4.0.36/aug/trojan/backdoor/trojan/drop1.dll | 22.73 kB | 13.07.2012 08:21 |
| http://10.4.0.36/aug/trojan/backdoor/trojan/algesteryes.unp | 56 kB | 13.07.2012 08:21 |
| http://10.4.0.36/aug/trojan/backdoor/trojan/2.unp | 128 kB | 13.07.2012 08:21 |
| http://10.4.0.36/aug/trojan/backdoor/trojan/algestelebs.unp | 56 kB | 13.07.2012 08:21 |

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 вебинтерфейса, 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.

| 👗 Аднонистрорование | Б Антивируская сеть | 🛠 Настройки | EBCentre | О Понощь | | | Станана (+ С |
|--|----------------------------|-------------|-----------|----------|--|--|--------------|
| Адлениистрорование Ох.Web Enterprise Server Ox.Web Enterprise Server Ox.Web Enterprise Server Nency, web paratemic Server subponsione Converting Server Server subponsione Server subponsione | Server | X Hactpolie | Fig Caror | U Ronage | Параметры сил Бактрое ская Сетя Порт Тайн аут Показывать е Соотносоть со | анерованов орованов 2193 2 2 а спискон станцой из | Crawel • E |
| Редактор шаблонов Установка Становка Становка по сети | | | | | | | |



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

| | Параметры Запустить сканер |
|--|-------------------------------|
| ■ Network ▲ 192.168.100.16/28 | 🗹 Быстрое сканирование |
| 2 192.168.100.17 (DOCS) | Сети 192.168.100.16/28 |
| 翌 192.168.100.21 (XP-RU101) 受 192.168.100.24 | Порт 2193 |
| (win2003ad101,drweb.test) | Таймаут 2 |
| | 🔽 Показывать название станции |

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.

| ачать | Открытие «drweb-esuite-plugins-windows-x86-6.0.2.ex |
|-----------------------|--|
| і версия Dr. Web Brov | Bei coõispaetecis ortsperts dailin COT-P1 drweb-esuite-plugins-windows-x86-6.0.2.exe sennouvika Bray Féo u base//res o succes |
| ор Веб» — Политика к | нфыле Вы хотите сохранить этот файл? Сохранить файл] |
| | |
| Загрузки | |
| 🕵 drweb-esuite- | plugins-windows-x64-6.0.2.exe 9:14 |
| 3.9 MB — 127.0.0 | 0.1:9080 |

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

Поиск...

Очистить список



После завершения установки рекомендуется обновить страницу браузера.

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



| | Taxaaa | | | Dane | |
|---|--------------------------------|--------------------------------------|------------------|---------|--|
| Dr.Web Enterprise Server | Dr.web Network Installer | | | (A Same | |
| Неподтвержденные станции Менеджер лицензий Ключи шифрования | Конпьютеры" | 192.168.100.21 | | | |
| r Таблицы | Каталог установки | %ProgramFiles%\DrWeb Enterprise Su | te | | |
| Журнал аудита Протокол выполнения заланий | Сервер | win2003ad101 drweb.test | | | |
| » Статистика сервера | Открытый ключ* | | 0 | | |
| Конфегурация Аднинистраторы | Исполняеный файл* | | | | |
| Авторизация Гостояние рерозитория | Дополнительные параметры | | | | |
| Конфигурация репозитория | Деталюация протокола | Трассировка | • | | |
| Конфигурация Dr.Web Enterprise Server | Тайн-аут установки (сек.) | 160 | | | |
| Pacnicanie Dr.Web Enterprise Server | Зарегистрировать установку | в базе данных установленных программ | | | |
| Редактор шаблонов | 1 | | | | |
| • Сканер сети | Установить | | Сжатие при закач | ace | |
| Установка по сети | □ Dr.Web Сканер для Windows | | C Her | | |
| | SpiDer Guard gra Windows | | Возможно | | |
| | SpiDer Mail для рабочно: стани | uni Windows | С Да | | |
| | Dr.Web plug-in for MS Outlook | | | | |
| | Arrivicinani Vade Retro | | | | |
| | SpIDer Gate для рабочих стан | щий Windows | | | |
| | Dr.Web Офисный контроль | | | | |
| | Cr.Web Firewall | | | | |
| | | | | | |
| | Авторизация | | | | |

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 | \\192.168.100.24\drwesi\$\drwcsd.pub |
|------------------|---------------------------------------|
| Исполняемый файл | \\192.168.100.24\drwesi\$\drwinst.exe |

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 | | | |
|--------------------|--------------|--------|---|
| Донен | Пользователь | Пароль | 4 |
| drweb.test\user101 | | | |
| drweb.test/user101 | | | |
| user106 | | | |

В открывшемся окне выберите параметры установки.

| Dr.Web Enterprise Agent для Windows | | Назад Установиз |
|-------------------------------------|----------|-----------------|
| Шифрование | Сжатие | |
| С Нет | C Her | |
| Возможно | Возможно | |
| С Да | СДа | |
| Авторизация | | |
| Установить паранетры | | |
| Идентификатор | | |
| | | |

Нажмите Установить.

| Прот | токол установки | e - 1 | | | | | | | Отмена |
|------|----------------------------|---------------------------|-------------|-------|---|----|-----|-----------|--------|
| | | | | | - | t. | + | | |
| | | | | | | * | | | |
| | TO THE NEW AND | 192.16 | 8.100.21 | 08 | | | | | |
| Конт | ыютеры Состоя | ие операции / сооб | бщение об с | ш-бке | - | 1 | | | |
| De | | DBM4 | | | | | | | Назад |
| 1.11 | | | | | | | | | |
| Про | цесс установ | вки завершён | | | | | | | |
| Про | цесс установ Компьютеры | яки завершён Результат | | Этап | | | Coo | бщение об | ошибке |

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

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.

| en C:\WINDOWS\system32\cmd.exe | _ 🗆 🗙 |
|---|----------|
| Microsoft Windows [Version 5.2.3790] (C) Copyright 1985-2003 Microsoft Corp. | ^ |
| C:\Documents and Settings\Admin>cd desktop | _ |
| C:\Documents and Settings\Admin\Desktop>drwinst.exe 192.168.1.100 | |

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 Пили Па.

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**.

| Адинностророванов | Учетная запись администратора а | denin | Ø Korpusa |
|------------------------------------|--|---|-----------|
| : Макуустина закол. • Интерфейс | Регстрацияние ная * Толжа чтелне Ина Отнаство Фаннов Язан интерфейса Состояне Дата содания Дата содания Дата значенныя Относание | ladim James Dow Bycosh is Erodoh Erodoh Erodoh Produ Redo Frodoh Produ Frodoh Produ Frodoh Produ Frodoh Produ Frodoh Produ Frodoh Frodo | |

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.

| Выбранные объекты | ☆ · + · ● · □ · ● · Q · 日 | | | |
|---|--|--|--|--|
| ▼ Общие | /×自由下设多喝收#照 | | | |
| - Графики | B. C. M. | | | |
| - Свойства | 1 П 192.168.100.80.28 | | | |
| Запущенные компоненты | J □ Everyone | | | |
| - Карантин | MP-RU101 | | | |
| ▼ Таблецы | | | | |
| - Сводные данные | | | | |
| - Инфекции | | | | |
| • Ошибки | | | | |
| Статистика | | | | |
| Запуск/завершение | | | | |
| = Вирусы | | | | |
| • Состояние | | | | |
| • Задания | | | | |
| Сунмарная статистика | | | | |
| Все сетевые инсталляции | | | | |
| 🔻 Конфигурация | | | | |
| = Права | | | | |
| = Расписание | | | | |
| "Устанавливаемые компоненты | | | | |

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

| 🍰 Аднинистрировани | е 📲 Антивирусная сеть | 🛠 Настройки | Ба связи | Опонощь |
|--|---|--------------------------|---------------------------|------------|
| Антивирусная сеть > XP-R | :U101 > Свойства | | | |
| Выбранные объекты | Свойства станции | XP-RU101 | | |
| • Общие • Графико • Графико • Сообства • Карактов • Тоблицы • Соодлые данные • Инфекции • Опибок | Общись Группы Бе Иденгификатор* Название* Пароль* Еще раз пароль* | Dbdc250-d21d XP-RU101 | повожение b211-b53c-c8 | 97e0270188 |
| • Статистика • Запуск/завершение • Вирусы • Состояние • Завлика | Описание | | | * |



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.



Office Shield

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

| Выбранные объекты | | | | 🔍 🖻 🖬 🛛 Сохранить |
|---|---|------------|----------|--------------------|
| * Dimue | Everyone. Заданы персональные настр | юйки. | | |
| • Графики | Dr.Web Enterprise Agent Ana Windows | должен | * | быть установлен |
| Свойства Запушенные компоненты | Dr. Web Enterprise Сканер для Windows | должен | Υ. | быть установлен |
| • Карантин | | | | |
| т Таблицы | | | | |
| - Сводные данные | Dr.Web Enterprise Agent для Unix | должен | * | быть установлен |
| • Инфекции • Ошибки | | | | |
| • Статистика | Dr.Web Ckanep Ans Windows | MOWET | | 6. m |
| Запуск/завершение | | | | opite yet anobien |
| • Вирусы | SpIDer Guard gna Windows | может | - | быть установлен |
| - Состояние | SpIDer Guard gna Windows ME | может | | быть установлен |
| Буммарная статистика | SpiDer Guard для Windows Servers | MOKET | | faire wrausanau |
| Все сетевые инсталляции | | | | derro y crandenen |
| Konderypages | Sptuer Мак для расочих станция windows | может | <u>·</u> | быть установлен |
| • Права | SpIDer Gate для рабочих станций Windows | должен | | FLIPL OF SLOPP REL |
| • Расписание | 4 | MOXET | | obite yet anobiten |
| Устанавливаеные компоненты | , etd. | The worker | | |
| Ограничения обновлений | | | | |
| - Почтовые адреса | | | | |
| - Dr.Web Сканер для Windows | | | | |
| - SoIDer Guard G3 for Windows | | | | |

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**.

| Конфигу | рация |
|--------------|---|
| | Права станции унаследованы от первичной группы Everyone |
| 10 11 | Расписание станции унаследовано от первичной группы Everyone |
| P= % | станция имеет ключ, унаследованный от первичной группы Everyone |
| • | Список устанавливаемых компонентов унаследован от первичной группы Everyone |
| ¢ ¢ | Dr.Web [®] Сканер для Windows имеет настройки, унаследованые от первичной группы Everyone |
| ¢ ¢ | SpIDer Guard [®] для Windows XP имеет настройки, унаследованые от первичной группы Everyone |
| <i>\$</i> \$ | Dr.Web [®] Enterprise Agent для Windows имеет настройки, |



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

| анция имеет настройки, у | унаследованые от первично | й группы Everyone | | 55 | \$P\$ \$\$ | 60 | Сохранить |
|--------------------------|---------------------------|-------------------|-----|----|------------|----|-----------|
| бщие Действия Исклю | чения Отчет | | | | | | |
| Рекланные програмны | В карантин | | h | | | | |
| Програнны дозвона | Удалять | | h | | | | |
| Програнны-шутки | Удалять | | h | | | | |
| Потенциально опасные | Информировать | | h | | | | |
| Програнны взлона | Информировать | | h | | | | |
| Заражённые | Лечать | | h | | | | |
| Подозрительные | В карантин | | h | | | | |
| Неизлечиные | В карантин | | h . | | | | |
| 🔽 Проверять инсталляцио | иные пакеты | * • | h | | | | |
| Инсталляционные паке | в карантин | | h | | | | |

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.

| Максинальный разнер распакованных файлов (КБ) | 0 |
|---|---|
| Максимальная степень сжатия | 0 |
| Проверять степень сжатия при размере (КБ) | 0 |
| Отключить режим расширенной защиты | |

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

| Выбранные объекты | | | 55 | \$2 | 66 | Сохранить |
|--|--|----|-----|-----|----|-----------|
| * Общие | Группа имеет персональные настройки | | | | | |
| • Графики | Общие Действия Исключения Отчет | | | | | |
| Восстановление станций Свойства | 🛱 Использовать зеристический акализ | * | + | | | |
| Запущенные компоненты | 😿 Проверять работающие программы и нодули | * | * | | | |
| • Карантия | | | 2 | | | |
| таблицы | Typolocie Sangera Ppolocie Sangera Ppolo | ۳. | - T | | | |
| • Отчеты | Процессе запуска программы | • | 44 | | | |
| Инфекции Ошибки | Елогоровать автозатую: со сненных носителей | * | 4% | | | |
| • Статистика | Сканировать сненные устройства | * | 44 | | | |
| Запуск/завершение | 🗖 Сканировать файлы по сети | * | ** | | | |
| • Вирусы • Состояние | 🗭 Перепроверять файлы после обновления вирусных баз | * | * | | | |

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.

| Рекламные программы | В карантин | • | * | |
|----------------------|---------------|---|---|---|
| Программы дозвона | Удалять | ٣ | * | ÷ |
| Программы-шутки | Удалять | • | * | ÷ |
| Потенциально опасные | Информировать | • | • | 4 |
| Программы взлома | Информировать | • | * | 4 |
| Заражённые | Лечить | • | * | 4 |
| Подозрительные | В карантин | • | ٠ | 4 |
| Неизлечиные | В карантин | • | * | 4 |

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.

| | ***** | Сохранить |
|---|------------|-----------|
| Станция имеет настройки, унаследованые от первичной группы Ем | veryone | |
| Общие Доступ | | |
| Включить блокировку | * * | |
| Блокировать сменные носители | * * | |
| 🔽 Защищать каталоги и файлы | * * | |
| Список защищаемых папок и файлов: | * * | |
| c:Windows | - + | |
| | - + | |
| | | Þ |

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**.

| | 🦸 🗳 🦑 🚔 🖻 📄 👘 Сохранить |
|---|-------------------------|
| Станция имеет настройки, унаследованые от первичной групп | ыEveryone |
| Общие Доступ | |
| Фильтрация WWW | * * |
| Блокировать все сайты | • • |
| Разрешенные домены | * * |
| | |
| Запрещенные домены | * * |
| vkontakte | - + |
| Блокировать содержимое: | |
| 🔽 Сайты о наркотиках | * * |
| 🔽 Сайты о насилии | * * |
| 🔽 Сайты о терроризме | * * |
| 🔽 Сайты, содержащие нецензурную лексику | * * |
| Сайты, связанные с азартными играми | * * |
| 🔽 Сайты об оружии | * * |
| 🔽 Порносайты | * * |
| 🗖 Чаты | * * |
| | |

5.3.5. Настройка проверки НТТР-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.

| 🔓 Аднинистрирование | 🚂 Антивирусная сеть | 🛠 Настройки | Ба Связи | 0 | юмощь | | | | | Станина]• 🛞 |
|---|----------------------------|--------------------------|---------------------|------------|-----------|----------|----------|-------|----|-------------|
| Антивирусная сеть > XP-RU1 | 01 > SpIDer Gate для | рабочих станци | าหั Windows | | | | | | | |
| Выбранные объекты | | | | | | | 55 | \$ \$ | 00 | Сохранить |
| * Общие | ХР-RU101. Настрой | ки унаследованы о | т первичной гр | улпы | Everyone. | | | | | |
| Графики Свойства | Действия | Фильтр приложе | лика П | рокси- | сервер | 014 | ет | | | |
| • Установленные компоненты | Порты | | | | | * | 45 | | | |
| Запущенные компоненты Карантин | 3128 | | | | | | 1.1 | | | |
| • Tafinana | 80 | | | | | | - | | | |
| • Сводные данные | 8080 | | | | | | 10 | | | |
| • Инфекции | Development and | | 2.2 | | | - | - | | | |
| • Ошибки | приложения, про | верженые по всен пор | Tan | | | <u> </u> | <u> </u> | | | |
| • Статистика | | | | | | | | | | |
| • Запуск/завершение | Исключаеные пр | поження | | | | * | 41 | | | |
| • Состояние | | | | | | 1 100 | 1710 | | | |
| Антивирусная сеть > XP-RU101 > Sp | IDer Gate для рабочих стан | แมงวั Windows | novoulu | | | | | | | |
| Выбранные объекты | | | | | | | | | | 53 |
| * Obspie | XP-RU101. Hactpo | йки унаследованы от ги | сраменой группы Е | veryone | | | | | | |
| • Графиях • Свойства | Reserves | Фильтр приложений | Прекси-с | cepsep | Orver | | | | | |
| • Установленные конпоненты | Режин проверки | Проверать входящий т | рафык (реконен 💌 | * | h | | | | | |
| • Запущенные конпоненты | Баланс проверко | 0 | | • | 6 | | | | | |
| • Карантин | 🖓 блогоровать | известные источники расп | ространения вирусов | | n | | | | | |
| • Сводные данные | F Encroiposana | нереконендуеные сайты | | • | 60 | | | | | |
| • Инфекции | Бельй списо | c | | • | n: . | | | | | |
| + Ogeface | 1 | | | a 1 | | | | | | |
| - Запуск/запершение | Emproperty (| INP BOUND IN IP- | | 100 | | | | | | |
| • Вирусы | | | | | <u>.</u> | | | | | |
| • Состояние | | 0.0000000 | | 2 | | | | | | |
| задания Сумнарная статистика | C December 2 | | | 2 | | | | | | |
| + Вирусные базы | N (bolbare) 1 | auguria. | | | | | | | | |

* *

* *

...

* *

* *

...

🔽 Програнны волона

Програнны-шутки

Поврежденные

П Непроверенные

Дополнительно:

Проверка архивов

Рекланные программы

Блокоровать объектые

- Модули

- Npasa

+ Pachicamie

Все сетевые инсталляции
 Конфигатion ин

Устаналляваеные кон
 Ограничения обновлен

+ Dr.Web Examp gas Windows

- Dr.Web gan Windows Mobile - SpIDer Guard G3 for Windows

SpiDer Mail для рабочня стан



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 обновления.

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**.

| Выбранные объекты | | B. B. | 10 | Сохранить |
|---|---|-------|----|-----------|
| * Ofmore | XP-RU101. Настройки унаследованы от первичной группы Everyone. | | | |
| - Графики | Windows Windows Mobile Linux FreeBSD Solaris Android | | | |
| Свойства Карантия | Компоненты Оптис | | | |
| Таблицы Сподные данные Инфекция Сшабки Статистика Запуск/уавершение Врусы Состояние Задани! Суняврива статистика Врусы базы Все сетевые инсталящии | MoSiria-exil pesser i i iccons.soeavee BCO Dr. Web Cosgavere noranevoro pacrecaves Greas pervesos padorai Creas ycrasecor. Dr. Web Enterprise Agent Ocrasioexa verrepóeñca Dr. Web Enterprise Agent Sanger accrysa is cers Processes autoraceuta is cers Processes autoraceuta is Revectanamaus Dr. Web Agent | | | |

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 **6**.

| | Разрешен | | Мобильный р | ежим | • |
|-----------------------------------|-------------------------------------|---------------|-------------------------|------|------|
| | Настройки Запустить обновление | | Статистика Состояние | 1 | |
| стройки мобиль | ности - Антивирус Dr.V | ₩eb | | | |
| Периодичность | | Прокси — | | | |
| С 20 минут С 1 час С 4 часа | С 40 минут С 2 часа С 8 часов | Г Испол Ар | рес | рвер | 3128 |
| П 12 часов Только при сов | С 1 день единении с Интернет | Авториза | ция: | | |

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.

| Общие Сеть Мобильность Отчет И | нтерфейс | | |
|------------------------------------|----------|---|----|
| Периодичность обновления (сек.) | 3600 | 4 | ÷1 |
| 🔲 Проверять подключение к Интернет | | 4 | 4 |
| 🔲 Использовать прокси-сервер | | 4 | 44 |
| Прокси-сервер | | ¢ | 41 |
| Порт прокси-сервера | 3128 | * | 4 |
| Пользователь прокси-сервера | | • | 41 |
| Пароль пользователя прокси-сервера | | • | 41 |

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**.

| 222 | | | | 7 | Серьезность у | Источник у |
|--------------|-----------|--------------------------|----------------|---------|---------------|------------|
| CEPBESHOLIB | PICTOMINA | COODULENNE | 10 | 111-6-1 | | |
| Очень низкая | Агент | Нет проблем | | | | |
| | | | | | | |
| Серьезность | Источник | Сообщение | 0 | | | |
| Очень низкая | Агент | Нет проблем | | | | |
| 2 | | | | | | Ľ |
| Серьезность | Источник | Сообщение | 0 | | | |
| Очень низкая | Агент | Нет проблен | | | | |
| | | | | | | |
| Серьезность | Источник | Сообщение | 0 | | | |
| 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.

| 7 | Серьезность 🔻 | Источник 🔻 |
|---|---------------|--|
| | | ✓Агент ✓Сервер Offline □Deinstalled |

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.

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

| Общая статистика | | | | | | | | | | | | | |
|------------------|----------|----|-----|-----|-----|---|-----|------------|------|------|---|-------|------|
| Группа | à | | 0.0 | .00 | 200 | | V 8 | R : | IA 3 | 1 8 | 1 | 6 | |
| Everyone | 74998485 | 63 | 36 | 2 | 18 | 0 | 35 | 189 | 0 | 62 | 5 | 31551 | 2668 |
| | 74998485 | 63 | 6 | 2 | 18 | 0 | 35 | 189 | 0 | 62 | 5 | 31551 | 2668 |
| Everyone | | | | | | | | | | | | | |
| Станция | à | | 0.0 | | 1 | * | 2 | x 3 | TA 8 | 14 8 | 1 | 6 | |
| sotrudnik_1 | 1204849 | ্য | 2 | 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 | 192 |
| sotrudnik_4 | 327916 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 428 |
| sotrudnik_5 | 811789 | | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 1590 |
| sotrudnik_6 | 989452 | | 3 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 875 | 384 |
| sotrudnik_7 | 569822 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 91 |
| sotrudnik_8 | 1114224 | 4 | 18 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1397 |
| sotrudnik_9 | 586905 | | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 345 |
| sotrudnik_10 | 7684380 | 15 | 50 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 28434 | 1630 |
| sotrudnik_11 | 321273 | | 5 | 0 | 0 | 0 | 2 | 0 | 0 | 3 | 0 | 0 | 7606 |
| sotrudnik_12 | 934736 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 199 |
| sotrudnik_13 | 3136036 | | 2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1896 |
| sotrudnik_14 | 1226774 | | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 77 | 15 |
| sotrudnik_15 | 1344515 | | 4 | 0 | 0 | 0 | 3 | 0 | 0 | 1 | 0 | 0 | 234 |
| sotrudnik_16 | 1554143 | 5 | 54 | 0 | 7 | 0 | 1 | 1 | 0 | 7 | 0 | 0 | 1252 |
| sotrudnik_17 | 852988 | | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 144 |

Десять самых распространенных вирусов





Everyone

Суточная активность вирусов

5

Десять наиболее зараженных машин



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

| | | | | | | Kane | ндарь | | | | | | Посещённые сайты | Bcero |
|---|------------------|------------|----|----------------|-------------------------------------|------|-----------------------|--------------------------|----|------|------|------|--------------------------------------|-------|
| | | | | | | . 21 | 2012 | | | | | | COA | EOA |
| | 01 | 02 | 03 | 04 | 05 | 06 | 07. | 08 | 09 | 10 | 11 | 12 | MECHL | MECRU |
| | | | | | | | | | | | | | | |
| | | | _ | _ | | | | _ | _ | _ | _ | | | |
| | | | | | | | | | | | | | | |
| Дата | Пользо | зател | юй | Скач | ано | B | ред | нем | % | юш | (poe | анны | х страниц | |
| Дата 13 Июл 2012 | Пользо | зател ? | юй | Скач | нано 3625 | B | сред) 1 | нем 815 | % | KOWA | 4DO8 | анны | х страниц 0.00% | |
| Дата 13 Июл 2012 12 Июл 2012 | Пользо | sater ? | юй | Cicar 1 | нано 3626 3456 | B | среди 1 1 3 | нем 815 455 | % | юш | 4D08 | анны | страниц 0.00% 0.00% | |
| Дата 13 Июл 2012 12 Июл 2012 11 Июл 2012 | Пользо 2 1 | sater ? | юй | Скач 1 8 | нано 362Б 345Б 086Б | B | сред 1 13 80 | нем 815 455 866 | % | юш | (poe | анны | х страниц 0.00% 0.00% 0.00% | |

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

| | | | Отчётн | ный период: И | ол 2012 | | |
|------|-------|--------|--------|---------------|------------|---------|--------|
| N₽ | Время | График | месяц | Пользователь | Соединений | Скачано | % |
| 1 | Ø | il. | [M] | 192.168.3.201 | 14 | 9 7936 | 100.0% |
| 2 | Q | alla - | [M] | 192.168.3.5 | 1 | 06 | 0.0% |
| Bcer | ·0 | | | | | 9 7935 | |

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

| Ста | атистика | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----|------------------|----|------|----|----|-----|------|--------------|--------------|------|---------------------------|--------------|---------------|--------------|---------------|---------------------------------|------|----|------|-----|----|----|------|----|--------|--------|
| | | | | | | | no | пьзов Дат | атель: а: | | leuw | 192 ком № | 2.168 леся | 3.3.2 ц-2 | 201 1012 1 | люл | | | | | | | | | | |
| N9 | Посещённые сайты | 00 | 01 | 02 | 03 | 04 | 85 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | Bcero |
| | Bceno | | - 45 | 16 | 14 | 0.0 | 14 | 0.0 | | 10 | 5 | 14 | 16 | - 60 | 0.0 | 160 | - 24 | | - 82 | 84 | 14 | ÷ | - 63 | ÷. | \sim | 9 7936 |
| 1 | 192.168.3.200 | | 4 | 16 | 32 | 0.0 | - G. | 14 | + | 1 | 84 | 7¥ | 12 | 40 | 0.0 | $\mathbb{C}_{\mathbf{k}}^{(i)}$ | 12 | | 40 | 84 | ÷2 | ÷. | * | 24 | ÷2 | 4 0355 |
| 2 | 192.168.3.156 | | * | - | 22 | 0.0 | ÷. | 0.0 | ×. | - 11 | $\mathbb{G}_{\mathbb{C}}$ | 33 | 1 | - 25 | | 161 | 4 | | 20 | S., | 22 | - | - 20 | 14 | 12 | 3 0526 |
| 3 | 192.168.3.157 | | | | | | | | | | | | | | 0.0 | | | | | | | | | | | 2 7065 |
| | Bcero | | 5 | | | 0.0 | | 0.0 | | | | | | | 0.0 | | | | \$. | 3 | | | - 62 | | | 9 7935 |

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].

| Польз Отчётный | ователь: период: Всего: | 192.168.3. Июл 2 9 7 | 201 012 936 |
|-------------------|-------------------------------|----------------------------|-------------------|
| | sk | | |
| Дата | Скачано | За неделю | Итого |
| 13 Vion 2012 | 3625 | | 3626 |
| 12 Vion 2012 | 1 3455 | | 1 7075 |
| 11 Vion 2012 | 8 0865 | | 9 7935 |
| Bcero | 9 7936 | | |

Для просмотра информации по посещенным сайтам необходимо выбрать интересующего пользователя.

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

| Всего | | | 6.0 M | | |
|-------|-----------------------|------------|---------|-------|-------|
| Nº | Посещённые сайты | Соединений | Байт | Итого | % |
| 1 | www.mobile-review.com | 30 | 4.4 M | 4.4 M | 73.6% |
| 2 | fc05.deviantart.net | 1 | 717 406 | 5.1 M | 11.4% |
| 3 | mrmurtazin.com | 34 | 219 184 | 5.3 M | 3.5% |
| 4 | imq-fotki.yandex.ru | 2 | 171 151 | 5.4 M | 2.7% |
| 5 | mediacdn.disgus.com | 34 | 137 598 | 5.6 M | 2.2% |
| 6 | h6.qapht.com | 1 | 62 749 | 5.6 M | 1.0% |
| 7 | s.lurkmore.ru | 8 | 59 516 | 5.7 M | 0.9% |
| 8 | static.ak.fbcdn.net | 6 | 58 228 | 5.7 M | 0.9% |
| 9 | i.imgur.com | 1 | 40 930 | 5.8 M | 0.6% |
| 10 | lurkmore.ru | 15 | 40 342 | 5.8 M | 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 кодулей Dr. Web Office Shield и восстановить их при необходимости. Резервная копия содержит конфигурационные файлы основных нодулей Dr. Web Office Shield.

| Внешний диск | Открытие «backup.tar.bz2» |
|--|--|
| Локальный компьютер Файл: Обзор. | Вы собираетесь открыть файл 🍒 backup.tar.bz2 |
| Создать резереную колию Сделать резереную колию текушию | являющийся Архие WinRAR из https://192.168.3.222:10000 Как Firefox следует обработать этот файл? |
| Восстановить из резервной копии Восстановить настройки Dr. Web Off | О открыть в WinRAR (по умолчанию) |
| Восстановить заводокие настройки. Восстановить заводокие настройки | Сохранить файл Вылолнять автоматически для всех файлов данного типа. |
| | ОК Отнена |

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 программноаппаратного 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:

 Задать адрес принимающей машины (почтового сервера компании, осуществляющего доставку писем). Для этого необходимо в веб-интефейсе 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**.

| ГЛАНАЯ Состояние окстание Окадуи настройки Раконскоемания Ребонствойскі Санан пасола | Почтовый прокси Основные настройка На этой волько в мальтирани Расширенные настройка На этой волько выкомете зыдать пракима фильтрации почты изверать действия, которые буд Карантинг Ядро Отчесты Приевы почеты. Отторанка почты. Ант | т ериненаться к обнаруженных угразан. еслина Антуненрус |
|---|--|--|
| Doarmoneuris | | |
| DHCP | Основные | |
| QNS . | Отсылка отчетов | Отсылка отчетов. |
| YEN | Да м | |
| Статистика | | |
| 6E30NACHOCT6 | | |
| Почтовый прокон | Время отправки отчетов | Графия: отправки отчётов. |
| Reg-ubovor | Ехерневно | |
| Защита собочно, станцей | | |
| Ermal | | |
| СИСТЕМА | Адреса | Адрес(а), на который(ые) высылаются отчеты. |
| Oferon nerver (RO | (The second sec | toacofens |
| Cost/weiterst H. BOCCT AND EITHERST | | |
| Getterroe.spens | | |
| Серезалиська и заексиение работи | Колчество зарисей в списке часто блоколичных объектов | Показ в отчете списков масто блокиочении |
| Vctavdbreveue navetui | | объектов и адресов, с которых присылается |
| KOMIDOREHTM | 120 | наибольшее количество блокоруеных объектов. |
| Hactpolica Webnin | | 0534555.0027 |
| | Аллес альенествотово | Anter curtanerra anneurrantea |
| | We are substituted a construction product of the | nogotivee |
| | rootpiccariost | |

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 недоставке (найденных вирусах и спаме). В качестве примера рассмотрим отправку письма с тестовым вирусом.

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

В данном примере:

| filewithviruses | — файл с вложенными вирусами, |
|-----------------|---|
| root@localhost | — адрес, с которого придет сообщение, |
| 192.168.1.100 | — адрес Dr.Web Office Shield, |
| toaddress | — адрес, на который должно прийти тестовое сообщение. |
| | C C |

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, uuencode в связке c mail, mpack, mutt.

Например:

uuencode __file1____file2__ | mail -s «sublect» __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-интефейс 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 настрой**ки 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 закачке 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; |

-с 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.



| Компонент | Проверено | Инфицированных | Моди | Подо | Акти | Ис |
|---|-----------|----------------|------|------|------|----|
| Dr.Web (R) Enterprise Scanner for Windows | 674 | 0 | 0 | 0 | 0 | |
| SpIDer Gate (R) for Windows Workstations | 0 | 0 | 0 | 0 | 0 | |
| SpIDer Guard (R) G3 for Workstations | 1995 | 0 | 0 | 0 | 0 | |
| 5pIDer Mail (R) for Windows Workstations | 0 | 0 | 0 | 0 | 0 | |
| 3cero | 2669 | 0 | 0 | 0 | 0 | |
| c] | | | | | | 6 |

Откройте браузер, перейдите по адресу

| Adpec: 🗿 http://www.eicar.org/anti_virus_test_file.ht | ~ |
|---|---|
|---|---|

На открывшейся странице опуститесь до текста

| Download area using the standard protocol http | | | | | | |
|--|---------------|---------------|---------------|--|--|--|
| eicar.com | eicar.com.txt | elcar com zip | eicarcom2.zip | | | |
| 68 Bytes | 68 Bytes | 184 Bytes | 308 Bytes | | | |

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:

| Blocked by Dr.Web HTTP Monitor - Microsoft Internet Explorer | - DX |
|--|------|
| Файл Правка Вид Избранное Сервис <u>С</u> правка | AU . |
| Aspec: As | ~ |
| | ~ |
| | |
| Сообщить в "Доктор Веб" Антнанрус Dr. Web SpiDer Gate 5.0.2.07030 | |
| Дата:10:56:11 18.08.2009 | |
| http://www.eicar.org/download/eicar.com | |
| 🔯 URL заблокирован. Обнаружена вредоносная программа | |
| Обнаружена вредоносная программа | |
| EICAR Test File (NOT a Virus!) | |
| | |

Щелкните правой кнопкой мыши по значку 📾 в системном трее. 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 SplDer Gate: щелкните правой кнопкой мыши значок 📾 в системном трее и снимите флаг SplDer Gate.

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

| 🕸 SplDer Guar | d обнаружил вирус |
|---------------|---|
| SplDer | C: \Documents and Settings\Test\Local Settings\Temporary Internet Files \ |
| | |
| | Игнорировать Запретить |
| | Лечить Переименовать Переместить Удалить |

После завершения проверки включите SplDer Gate: щелкните правой кнопкой мыши значок 📾 и установите флаг SplDer 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-интефейсу 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;

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 кросскабелем.
- 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 adress (использовать следующий IP-адрес) и указать в поле IP adress (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 255.255.25.0.

Нажимаем ОК.



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**.

|) Suura | Лостип | Настойка | 1 |
|------------|-----------------------|--|---|
| ющие | Locijii | пастроика | |
| Лока | льный об | щий доступ | и безопасность |
| 3 | Пользо папку | разрешить вателям ка Общие доку | доступ другим локальным этой папке, переместите ее в <u>менты</u> . |
| | Чтобы подпаг | запретить о кам, устано | бщий доступ к этой папке и ее вите этот флажок. |
| | | енить общи | й доступ к этой папке |
| Сете | вой общи | і доступ и б | езопасность |
| • | компы флажо | отера, и по к и задайте ь о <u>бщ</u> ий доо | сети, установите первый имя ресурса. ступ к этой папке |
| 1 | <u>1</u> мя обще | го ресурса: | Internet |
| • [| Paspeu | ить измене | ние файлов по сети |
| Подр | обнее об | бщем дост | ите и безопасности. |
| 1) E | рандмауэ той папке | р Windows н с друпих ко | астроен на разрешение доступа к мпьютеров в сети. |

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 потребуется 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.

| PuTTY Configure | ation | × | | | | |
|--|--|------------------------|--|--|--|--|
| Category: | | | | | | |
| Session | Basic options for your PuTTY session | | | | | |
| Logging | Specify your connection by host name or IP address | | | | | |
| E I erminal | Host Name (or IP address) | Port | | | | |
| Bell | 213.208.178.67 | 20100 | | | | |
| Features ⊡-Window | Protocol: <u>Raw</u> <u>Ielnet</u> Rlogin | <u> </u> | | | | |
| Appearance Behaviour Translation Selection Colours Proxy Telnet Riogin SSH | Coad, save or delete a stored session | | | | | |
| | Default Settings app | Load Saye Delete | | | | |
| Tunnels Bugs | Close window on exit: Always Never O Dnly on | clean exit | | | | |
| About | <u></u> pen |] <u>C</u> ancel | | | | |

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
```

| C:\Program Files\Putty | >pscp.e> | ke −P | 20100 | agent. | key enterp | rise.key r | oot0213.208.1 |
|------------------------|------------|-------|-------|--------|------------|------------|---------------|
| agent key | | kB | 1.4 | kB∕s ¦ | ETA: 00:0 | D:00 100 |)× |
| enterprise.key | ; 1 | kB i | 1.3 | kB∕s ¦ | ETA: 00:0 | 0:00 100 | 1% |
| C:\Program Files\Putt | 1 > | | | | | | |

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: | МЕСТО ДЛЯ | |
| ПОДПИСЬ ПРОДАВЦА: | | - |
| Гарантийный талон № 1 Информация о ремонте: | | |
| Дата поступления в ремонт: | | |
| Дата выполнения ремонта: | ПЕЧАТИ | |
| Подпись владельца: | | |
| Принял: | | ÷ |
| Гарантийный талон № 2 Информация о ремонте: | | |
| Дата поступления в ремонт: | | |
| Дата выполнения ремонта: | МЕСТО ДЛЯ ПЕЧАТИ | |
| Подпись владельца: | | |
| Принял: | | |
| | | |

Гарантийные обязательства

- ООО «Доктор Веб» (далее Производитель) несет ответственность по гарантийным обязательствам на Dr.Web Office Shield (далее – Устройство) в соответствии с действующим законодательством Российской Федерации.
- Гарантия действительна только при предъявлении вместе с Устройством правильно и разборчиво заполненного гарантийного талона с проставленной датой продажи и печатью продавца.
- 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 Устройства путем его ремонта или замены на аналогичное при условии, что дефект присутствует по вине Производителя.

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

- Выполнение Производителем гарантийных обязательств по ремонту вышедшего из строя Устройства 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 Устройству 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 Устройства.
- 7. Производитель не несет ответственности по гарантии в случае, если произведенные им тестирование и/или анализ показали, что заявленный дефект в Устройстве отсутствует, либо он возник вследствие нарушения правил инсталляции или условий эксплуатации, а также любых действий, связанных с попытками добиться от Устройства выполнения функций, не заявленных Производителем.
- Условия гарантии не предусматривают чистку и профилактику Устройства силами и за счет Производителя.
- Настоящая гарантия недействительна, если серийный номер на Устройстве был изменен, удален или неразборчив.
- Производитель не несет ответственности за дефекты и неисправности Устройства, возникшие в результате:
 - несоблюдения правил транспортировки и условий хранения, технических требований по размещению и эксплуатации;
 - неправильных действий, использования Устройства не по назначению, несоблюдения инструкций по эксплуатации;
 - механических воздействий (наличия явных механических повреждений, трещин, сколов на корпусе и внутри устройства, 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 Устройств по гарантии либо предоставления Производителем услуг по Устройству 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 Устройства.

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