

Dr.Web для MS Exchange 2007/2010 Dr.Web Mail Gateway

# Руководство по быстрой установке и развертыванию

Версия 6.0

Методическое пособие для практических занятий по курсу DWCERT-005

Централизованно управляемая защита почтовых сервисов для Microsoft Exchange 2007/2010 на базе решений Dr.Web для MS Exchange 2007/2010, Dr.Web Mail Gateway



#### ООО «Доктор Веб» Руководство по быстрой установке и развертыванию

# «Централизованно управляемая защита почтовых сервисов для Microsoft Exchange 2007/2010 на базе решений Dr.Web для MS Exchange 2007/2010, Dr.Web Mail Gateway»

Внимание! Материалы, представленные в настоящем документе, являются собственностью ООО «Доктор Веб». Защита авторских прав на данный документ осуществляется в соответствии с текущим законодательством РФ. Ни одна из частей данного документа не может быть сфотографирована, размножена или распространена другим способом без согласия ООО «Доктор Веб». Если вы собираетесь использовать, копировать или распространять материалы настоящего курса, свяжитесь, пожалуйста, с представителями ООО «Доктор Веб» через специальную форму, расположенную на официальном сайте <u>http://support.drweb.com/new/feedback/</u>

Dr.Web®, SpIDer Guard® и SpIDer Mail® – зарегистрированные товарные знаки ООО «Доктор Веб». Другие названия продуктов, упоминаемые в тексте курса, являются товарными знаками или зарегистрированными товарными знаками соответствующих фирм.

Программные продукты Dr.Web для MS Exchange 2007/2010 и Dr.Web Mail Gateway входят в группу продуктов Dr.Web Enterprise Security Suite, включающую элементы защиты всех узлов корпоративной сети и единый центр управления для большинства из них. Dr.Web для MS Exchange 2007/2010 принадлежит к коммерческому продукту Dr.Web Mail Security Suite, Dr.Web Mail Gateway (SMTP proxy) является дополнительным компонентом к нему.

Возможности Dr.Web для MS Exchange 2007/2010 и Dr.Web Mail Gateway не ограничиваются функционалом, описанным в данном документе. Для ознакомлением с возможностями Dr.Web для MS Exchange 2007/2010 и Dr.Web Mail Gateway используйте документацию к продуктам.

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

© ООО «Доктор Веб», 2006-2011 http://www.drweb.com

Версия программного обеспечения Версия документа Статус документа Дата последнего изменения 6.00**.01** 1.0 Утвержден <del>9</del> марта 2011 года

# Содержание

1. Введение	4
2. Базовые определения	6
3. Перед установкой	6
3.1. Развертывание и настройка антивирусной защиты почтовых сервисов MS Exchange	7
3.1.1. Установка сервиса защиты MS Exchange	7
3.1.2. Тестирование функционирования сервиса	12
3.2. Настройка параметров антивирусной защиты	
3.2.1. Настройка действий по отношению к различным типам сообщений. Настройка действий по отношению к различным типам проверяемых объектов	17
3.2.2. Добавление пользовательских фильтров	18
3.2.3. Настройки черных и белых списков проверяемых адресов	19
3.2.4. Сопроводительный текст	20
3.2.5. Настройки для отдельных пользователей и групп	20
3.2.6. Редактирование шаблонов уведомлений	22
3.2.7. Сохранение текущих настроек в конфигурационный файл	23
3.3. Управление карантином	24
3.3.1. Статистика работы сервиса. Получение отчетов о работе программы	24
3.4. Тестирование производительности	
3.4.1. Тестирование производительности системы фильтрации почтового трафика	26
3.4.2. Тестирование функционирования системы фильтрации почтового трафика	27
4. Настройка системы антивирусной фильтрации на почтовом шлюзе с помощью Dr.Web Mail Gateway	28
4.1. Установка сервиса	28
4.1.1. Настройка языка интерфейса	
4.2. Настройка параметров антивирусной защиты	34
4 2 1 Первоначальная настройка	34
4.2.2. Настройка параметров проверки сообщений по протоколам POP3/POP3S/IMAP4/IMAP4S	
4.2.3. Настройка действий для зараженного входящего и исходящего почтового трафика	
4.2.4. Настройка действий для спам-сообщений	
4.2.5. Управление черными и белыми списками отправителей	
4.2.6. Настройка параметров отчетов	43
4.2.7. Настройка параметров журналов	43
4.2.8. Управление карантином	44
4.2.8.1. Обработка писем с помощью управляющих писем	46
4.2.9. Архивирование и регистрация сообщений	47
4.2.10. Интерактивное управление сервисом	48
4.3. Управление защитой почтовых сервисов под ОС UNIX из Центра управления Dr.Web Enterprise Security Suite	49
4.3.1. Подключение почтового сервиса к Центру управления Dr.Web Enterprise Security Suite	49
4.3.2. Настройка запуска почтового сервиса из Центра управления Dr.Web Enterprise Security Suite	50
4.4. Проверка корректности настроек	51
5. Тестирование производительности	
5.1. Тестирование производительности системы фильтрации почтового трафика	52
5.2. Тестирование функционирования системы фильтрации почтового трафика	53
6. Последние замечания	



# 1. Введение

Настоящий документ служит руководством по быстрой установке и развертыванию решений Dr.Web для MS Exchange 2007/2010 и Dr.Web Mail Gateway, предназначенных для защиты почтовых сервисов, построенных на базе Microsoft Exchange 2007/2010.

Dr.Web для MS Exchange предназначен для:

- сканирования всех входящих и исходящих сообщений в реальном времени с учетом индивидуальных настроек групп и отдельных пользователей;
- фильтрации и блокировки спама, в том числе по белым и черным спискам адресов;
- изоляции инфицированных и подозрительных объектов в карантине;
- фильтрации электронных писем по различным критериям;
- отправки уведомлений о вирусных событиях;
- ведения журнала вирусных событий;
- сбора статистики и рассылки отчетов о работе программы.

Dr.Web для MS Exchange осуществляет проверку следующих элементов электронных писем:

- тело письма;
- вложения (включая архивированные и упакованные файлы);
- вложенные OLE-объекты.

Особенностями Dr.Web для MS Exchange являются:

- возможность установки для любых ролей Microsoft Exchange Server;
- наличие антиспама, что дает возможность существенно снизить нагрузку на сервер, увеличить производительность труда сотрудников компании;
- отсутствие необходимости обучения антиспама Dr.Web для MS Exchange 2007/2010 готов к фильтрации спама с момента установки;
- наличие черных и белых списков адресов, что позволяет исключать из проверки определенные адреса и увеличивать ее эффективность;
- возможность фильтрации по типам файлов, что позволяет снизить трафик компании;
- возможность группировки, что позволяет настроить продукт с учетом потребностей различных групп пользователей, а наличие системы наполнения состава групп из Active Directory существенно сокращает введение системы антивирусной защиты в строй и упрощает сопровождение продукта;
- наличие механизма обнаружения вирусов, скрытых неизвестными упаковщиками;
- наличие дополнительных механизмов обнаружения неизвестных вредоносных программ, что увеличивает вероятность обнаружения вирусов новейших типов;
- наличие подробной русскоязычной документации и круглосуточной технической поддержки.

Использование Dr. Web Mail Gateway в качестве почтового шлюза, проверяющего всю входящую и исходящую почту компании, позволяет:

- снизить нагрузку на внутренний почтовый сервер компании за счет фильтрации почтового трафика на почтовом шлюзе, что в свою очередь позволяет улучшить время отклика почтового сервера и уменьшить время получения сообщений сотрудниками компании;
- изолировать почтовый сервер компании от сети Интернет, что не дает злоумышленникам воспользоваться его известными уязвимостями.

Dr. Web Mail Gateway обеспечивает полную проверку почтовой корреспонденции по протоколам SMTP/ LMTP/POP3/IMAP4. В зависимости от набора подключенных плагинов Dr. Web Mail Gateway способен:

 осуществлять проверку и фильтрацию почтовых сообщений от вирусов, спама и прочей нежелательной корреспонденции. При этом производится проверка как самого письма, так и всех его компонентов, вне зависимости от уровня вложенности. В результате проверки сообщение может пропускаться, блокироваться или видоизменяться;



- увеличить эффективность фильтрации почтовых сообщений за счет наличия таких механизмов проверки подлинности подлинности IP-адреса, как:
  - аутентификация отправителей;
  - проверка вхождения хоста отправителя в список ProtectedDomains с помощью PTR и А-запросов;
  - проверка IP-адреса соединения на вхождение в белые и черные списки как IP-адресов, так и доменов;
  - проверка на наличие и соответствие в DNS А- и МХ-записей хостам и IP-адресам отправителя либо получателя;
  - сравнение IP-адреса хоста с хостом, с которого произошло соединение;
  - проверка адреса по черным спискам RBL/DNSBL;
- увеличить эффективность фильтрации почтовых сообщений за счет проверки правильности формирования почтовых сообщений;
- обеспечить возможность экономии трафика;
- архивировать все проходящие сообщения;
- модифицировать обрабатываемые сообщения в зависимости от имеющихся политик;
- применять белые и черные списки для фильтрации корреспонденции;
- разбирать почтовые сообщения любых форматов. При этом производится анализ как самого письма, так и всех его компонентов, вне зависимости от уровня вложенности;
- уведомлять как получателей, так и других лиц о результатах проверки. Уведомления составляются при помощи шаблонов, описанных в системе, что позволяет получать информацию в максимально удобном виде;
- вести статистику, учитывающую все аспекты работы системы;
- защищать работу собственных модулей от сбоев;
- лечить или удалять вредоносные объекты любых типов.

Данный документ в первую очередь предназначен для пользователей, впервые сталкивающихся с задачами обеспечения безопасности почтовых сервисов. Тем не менее предполагается, что пользователем, ответственным за развертывание Dr.Web на предприятии, является администратор, обладающий следующими знаниями:

- базовые знания по устройству компьютерной техники, находящейся в локальной сети предприятия;
- хорошие знания операционных систем и другого программного обеспечения (далее ПО), использующегося в локальной сети предприятия;
- базовые знания по администрированию локальных сетей;
- базовые знания по основам обеспечения информационной безопасности компаний и организаций;
- знание особенностей устройства и функционирования локальной сети, в которой предполагается развертывать антивирусную сеть;
- технический уровень английского языка (весьма желательно).

Данное руководство не претендует на полноту сведений о Dr.Web для MS Exchange 2007/2010 и Dr.Web Mail Gateway, а служит лишь отправной точкой для быстрой настройки полноценной AB-сети на предприятии.

Документ также служит руководством для практических занятий сертификационных курсов для специалистов информационной защиты предприятий на базе антивирусных продуктов компании «Доктор Веб».



### 2. Базовые определения

**Антивирусная сеть** — локальная сеть предприятия, в которой установлено, настроено и функционирует антивирусное ПО Dr.Web (далее — АВ-сеть).

**Антивирусный сервер** — компьютер, находящийся в локальной сети предприятия, на котором установлено ПО Dr.Web Enterprise Server (далее — ES-сервер). В функции антивирусного сервера входит координация работы антивирусной сети. В локальной сети предприятия может функционировать как один ES-сервер, так и несколько.

**Антивирусный агент** — компонент Dr. Web Enterprise Security Suite, устанавливаемый на всех защищаемых объектах сети. Антивирусный агент (далее — ES-агент) отвечает за прием и передачу всей необходимой для функционирования AB-сети информации, за правильное функционирование антивирусного комплекса на каждом защищаемом объекте, а также за выполнение заданий, назначенных сервером и пользователем, на защищаемом объекте.

**Веб-интерфейс администратора (Веб-администратор)** – компонент Центра управления Dr. Web Enterprise Security Suite, Dr. Web для MS Exchange 2007/2010 и Dr. Web Mail Gateway, с помощью которых можно управлять соответствующими продуктами. Веб-администратор может использоваться совместно с интернет-браузерами (Microsoft Internet Explorer 7 или выше, Mozilla Firefox 3.0 или выше, Opera, Safari или Chrome). При этом необходимо и достаточно наличия одного из этих браузеров, установка дополнительного ПО не требуется.

Администратор антивирусной сети — сотрудник предприятия, в котором расположена защищаемая антивирусная сеть, отвечающий за нормальное функционирование АВ-сети.

# 3. Перед установкой

До решения о приобретении Dr.Web для MS Exchange 2007/2010 и/или Dr.Web Mail Gateway предоставляется возможность заказать демонстрационный ключ. Сделать это можно в специальном разделе официального сайта <u>http://download.drweb.com/demo</u> либо через вашего поставщика антивирусного ПО.

Перед развертыванием системы защиты почтовых сервисов рекомендуется опробовать выбранные решения на небольшом участке локальной сети предприятия или использовать специализированное ПО (например, VMware — <u>http://www.vmware.com</u>).

Компания «Доктор Веб» также предоставляет возможность удаленного тестирования решений для защиты почтовых сервисов с помощью сервиса Dr.Web LiveDemo. Тестирование выбранных решений на виртуальных серверах, предоставляемых компанией «Доктор Веб», позволяет оценить выбранные решения до их приобретения, приобрести навык установки и внедрения до полномасштабного развертывания в составе локальной сети, отработать процедуры перехода на новые версии программного обеспечения.

Для тестирования рекомендуется использовать не менее 3 компьютеров для тестирования конфигурации без почтового прокси и 4 — с установленным почтовым прокси. При этом один компьютер используется в качестве почтового сервера, один — в качестве отправителя тестовых сообщений и один в качестве их получателя.

Для тестирования должны использоваться операционные системы со всеми доступными на момент начала тестирования обновлениями. Операционные системы должны устанавливаться на чистый компьютер — перед установкой должно производиться форматирование жесткого диска. После установки всех программ должна производиться дефрагментация жесткого диска для исключения влияния скорости чтения данных.

Для управления установленными продуктами через веб-интерфейс на операционных системах типа MS Windows должны быть установлены браузеры Internet Explorer или Mozilla Firefox. Браузер должен быть обновлен до последней рекомендуемой производителем версии.

Для чтения документации должна быть установлена программа Adobe Acrobat Reader (или аналогичная) со всеми необходимыми обновлениями.



В процессе планирования развертывания системы защиты почтовых сервисов необходимо, обладая информацией о структуре компании, уровне угроз, топологии локальной сети и ее текущей пропускной способности, решить вопросы о том, каким образом расположить на компьютерах локальной сети различные компоненты системы защиты.

Рекомендуется проводить планирование до приобретения ПО, т. к. от плана будущей АВ-сети существенно зависит состав лицензии и, соответственно, ее стоимость. На состав и стоимость лицензии на использование Dr.Web Enterprise Security Suite влияет:

- количество и структура защищаемых почтовых серверов;
- количество пользователей и объем трафика.

Эту информацию необходимо обязательно сообщать продавцу лицензии при покупке решения Dr.Web.

Необходимо определить схему обновления AB-сети. Идеальным вариантом считается наличие в локальной сети предприятия прокси-сервера, администрирующего доступ в Интернет для пользователей и ПО, которому необходим такой доступ. Тем не менее возможно обновление AB-сети вручную даже в том случае, если ни один компьютер внутренней локальной сети предприятия не имеет выхода в Интернет (в данном руководстве этот способ обновления не рассматривается).

Необходимо также учитывать минимальные системные требования, необходимые для функционирования антивирусных серверов и агентов управления.

Весьма желательно перед установкой ПО Dr. Web установить на всех компьютерах все актуальные критические обновления для ОС.

Перед непосредственной установкой и развертыванием AB-сети на базе Enterprise Security Suite в локальной сети предприятия необходимо:

- убедиться в том, что вы обладаете текущими версиями дистрибутивов устанавливаемого ПО, посетив соответствующий раздел официального сайта (http://download.drweb.com/esuite);
- отключить антивирусную сеть от Интернета для исключения проникновения инфекции извне в локальную сеть во время установки.

# 3.1. Развертывание и настройка антивирусной защиты почтовых сервисов MS Exchange

Развертывание АВ-сети включает следующие этапы:

- установка Центра управления антивирусной сети и агентов администрирования на серверы защиты (в данном документе развертывание Центра управления и антивирусной сети не рассматривается);
- установка и первоначальная настройка сервисов защиты MS Exchange;
- (в случае необходимости) установка и первоначальная настройка почтового прокси-сервера.

#### 3.1.1. Установка сервиса защиты MS Exchange

В состав дистрибутива входят следующие компоненты:

- ПО антивирусного сервера для соответствующей версии MS Exchange;
- вирусные базы;
- документация.

Кроме самого дистрибутива могут поставляться также лицензионный ключевой файл или серийный номер.

Актуальную версию дистрибутива можно получить здесь: http://download.drweb.com/esuite.

Dr.Web для MS Exchange требует наличия процессора Intel с поддержкой платформы x64 или AMD с поддержкой платформы AMD64, наличия установленных на компьютере 2 ГБ памяти, 20 МБ свободного дискового пространства для установки приложения, 50 МБ для журнала событий и опционально 512 МБ для архива журнала событий. Dr.Web для MS Exchange может быть установлен на Microsoft Windows Server 2003 R2 SP2 x64, Microsoft Windows Server 2008 x64.



**Внимание!** Подробные системные требования и особенности установки на разных платформах описаны в «Руководстве администратора». В данной методике предполагается, что производится типовая установка как для MS Exchange 2007/2010, так и для Dr.Web для MS Exchange 2007/2010.

Чтобы установить Dr.Web для MS Exchange 2007/2010, следуйте инструкциям ниже.

- 1. Скопируйте дистрибутив Dr.Web для MS Exchange drweb-600-exchange-20072010-ru.msi и файл drweb32.zip, содержащий актуальный ключ, на рабочий стол.
- 2. Распакуйте архив drweb32.zip, например, выбрав команду Extract all по щелчку правой кнопки мыши.



3. Запустите инсталляционный файл с рабочего стола и в открывшемся Мастере установки нажмите Далее (Next).



4. Ознакомьтесь с текстом лицензионного соглашения и примите его, выбрав пункт **Я принимаю** условия лицензионного соглашения. Нажмите Далее (Next).



🔂 Dr.Web for Microsoft Exchange 200	7/2010 - Install	Shield Wizard	×
Лицензионное соглашение Пожалуйста, внимательно прочтите соглашение.	следующее лице	нзионное	- <b>E</b>
ЛИЦЕНЗИОННЫЙ ДОЈ ПРОГРАММНОГО ОБЕСП Настоящий Лицензис кридическим документом - Вами, конечным пользовате:	ГОВОР ОБ ИСІ ВЧЕНИЯ ООО онный Догово договором, лем (физичес	ЮЛЬЗОВАНИИ ) "Доктор Ве р является заключаемым хим или юри	6" между дическим
лицом, далее по тексту – использованию Антивирусной (далее по тексту – «Програ С ОО «Полика» (порта) О я принимаю условия лицензионного С Я на портанизаю условия лицензионного	«Вы»), приоб й программы аммное обест соглашения	бретающим пр семейства D leчение» или	аво по r.Web «ПО»), т
InstallShield	< Назал	Лалее >	Отмена

5. Укажите тип установки, выбрав **Полная** или **Выборочная**, и нажмите **Далее (Next)** для продолжения. Рекомендуется использовать полный вариант установки, устанавливая все необходимые компоненты.



6. В окне Лицензионный ключевой файл укажите путь к вашему ключевому файлу и нажмите Далее (Next).

prise Security Suite

7. В соответствующих полях ввода укажите электронный адрес и пароль учетной записи пользователя, с почтового ящика которой будут рассылаться уведомления. Указанная учетная запись должна обладать правами локального системного администратора, электронный адрес должен быть основным (Default) для данной учетной записи и совпадать с основным именем пользователя (UPN), причем доменный суффикс UPN-имени не должен быть альтернативным для данной учетной записи. Нажмите **Далее (Next)**. Вы можете использовать полученные вами в письме адрес и пароль доступа к серверу установки. В данной методике тестирования в качестве домена используется drweb.test.

Pr.Web for Microsoft Exchange 200	7/2010 - Instal	lShield Wizard	×
Служебная учетная запись Укажите информацию о служебной у	четной записи.		- 🐯
Введите имя пользователя в формат суффикса UPN, который должен быт "@". По умолчанико пользователь им UPN должен быть создан почтовый я	е UPN. UPN состо ъ добавлен к име еет суффикс из † ащик.	ит из имени польз ени пользователя @domain_name". Д	ователя и после символа "ля указанного
Имя пользователя (UPN): mailbox 1@drweber.lan			
Пароль:			
•••••			
InstallShield			
	< Назад	Далее >	Отмена

8. Введите адрес администратора сервера, на который будут высылаться уведомления, и нажмите кнопку Далее (Next).

Dr.Web for Microsoft Exchange 2007/2010 - InstallShield Wizard
Служебная учетная запись Укажите информацию о служебной учетной записи.
Введите адрес администратора сервера, на который будут высылаться уведомления.
Адрес администратора сервера:
mailbox 1@drweber.lan
InstallShield
< Назад Далее > Отмена

9. Нажмите кнопку Установить (Install), чтобы начать установку Dr.Web для MS Exchange. По умолчанию файлы программы помещаются в папки C:\Program Files (x86)\DrWeb for Exchange и C:\Program Files\DrWeb for Exchange. Последующие действия Мастера установки не требуют вмешательства пользователя. По завершении установки нажмите кнопку Готово (Finish).





10. Перезагрузите сервер.



#### 3.1.2. Тестирование функционирования сервиса

Для тестирования сервиса защиты почты можно использовать установленный по умолчанию почтовый клиент Outlook Express. Для проведения тестирования рекомендуется завести как минимум два почтовых ящика. В данной методике используются почтовые ящики mailbox1 и mailbox2 с паролем доступа qwerty. Для добавления почтового ящика в Outlook Express необходимо:

Выбрать пункт Internet Accounts в меню Tools.

Нажать кнопку Add и выбрать Mail.

Ввести имя почтового ящика, например mailbox1, и почтовый адрес, например mailbox1@drweb. test.





Указать серверы для входящей и исходящей почты. В данном случае указывается адрес сервера, на котором была произведена установка. Тип сервера — IMAP.

🖸 Autlaak Express			_ 🗆 ×
Internet Connection Wizard	×		2
E-mail Server Names	×.		
My incoming mail gerver is a IMAP server.			Go to <b>msn<sup>M</sup> 🔺</b>
E Incoming mail (POP3, IMAP or HTTP) server:		Find a Mes	sage Identities <del>v</del>
192.168.100.27	-		Tip of the day ×
An SMTP server is the server that is used for your outgoin Outgoing mail (SMTP) server: 192.168.100.27	g e-mail.	ır <u>Inbox</u>	To quickly locate certain messages, click <b>Find</b> on the toolbar. Type in what to look for, such as a name in <b>From</b> or a word in <b>Subject</b> .
<u> </u>	Next > Cancel		
Contacts ▼ × Contacts			
There are no contacts to display. Click on Contacts to create a new contact.	the Address Book		
Find P	eople		4 Province North
L When Cutlook Exp	ess starts, go directly to my <u>I</u> nb	iox.	
		🖳 Working Online	

В качестве пароля и логина доступа необходимо указать имя ящика и пароль qwerty.

ternet Mail Logon	
Type the account nar	me and password your Internet service provider has given you.
Account name:	mailbox2
Password:	
	I Remember pass <u>w</u> ord
	provider requires you to use Secure Password Authentication
If your Internet service p (SPA) to access your m Authentication (SPA)' cl	heck box.
If your Internet service p (SPA) to access your m Authentication (SPA)' cl Log on using <u>S</u> ecur	all account, select the 'Log On Using Secure Password heck box. e Password Authentication (SPA)
If your Internet service ( (SPA) to access your m Authentication (SPA)' cl Log on using Secur	a account, select the 'Log On Using Secure Password heck box. e Password Authentication (SPA)

Внимание! В том случае, если вы используете такие почтовые клиенты, как MS Outlook 2003:

- Поддержка этих почтовых клиентов должна быть включена при инсталляции MS Exchange.
- Опции шифрования должны иметь одинаковое значение как на стороне сервера, так и на стороне клиента. В противном случае при старте клиента будет выдано сообщение Unable to open your default e-mail folders. По умолчанию в Outlook 2007/2010 опция шифрования между Outlook и Exchange включена, а в Outlook 2003 нет:



onfiguring Outlook Accounts reating Welcome Message	Type a question for h
	Microsoft
Microsoft Office Outlook Unable to open your defau Exchange Server computer folders with your offline fo	ilt e-mail folders. You must connect to your Micros with the current profile before you can synchroni Ider file.
Copyright @ 19	5-2003 Microsoft Corporation. All rights reserved.

Для включения опции шифрования необходимо отметить пункт Шифровать данные, пересылаемые между Microsoft Office Outlook и Microsoft Exchange (Encrypt data between...) на закладке Security (Сервис — Учетные записи — Другие настройки — Безопасность по умолчанию).

eneral	Advanced	Security	Connection	Remote	Mail
Encryp Enc	rypt data be Microsoft E	etween Mic Exchange S	rosoft Office	Outlook	٦
User id	lentification vays prompt	for user na	ame and passv	vord	
ogon ne	etwork secur	rity:			
Kerbero	s/NTLM Pas	sword Auth	nentication		~

Для проверки работоспособности сервиса можно использовать тестовый файл EICAR, определяющийся антивирусными программами как вирус. Загрузите его с веб-сайта EICAR (<u>http://www.eicar.org</u>) или создайте самостоятельно, сохранив строку

X50! P%@AP[4\PZX54(P^)7CC)7}\$EICARSTANDARD-ANTIVIRUS-TEST-FILE!\$H+H\* в файл с любым именем.

После этого прикрепите этот файл к электронному письму и отправьте на любой тестовый адрес. Полученное на этот адрес письмо должно содержать текстовый файл с суффиксом \_infected.txt, имеющий следующее содержание:

Инфицированный вирусом файл eicar.com был удален Dr.Web для MS Exchange. Имя вируса: EICAR Test File (NOT a Virus!).



From:	test			
Date:	Monday, November 02, 2009 7:19 AM		Received	$\Delta$
To:	mailbox2@drweb.test		11/2/2009 7	7:19 A
Subject:	test antivirus			
Attach:	EICAR.txt_infected.txt (265 bytes)			
	-			
📑 EIC/	AR.txt_infected.txt - Notepad		_ [	X
<u>File</u>	dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp			
File Virus	EICAR.txt was infected with a virus and has been deleted by name:EICAR Test File (NOT a Virus!)	/ Dr.Web for	Exchange	2 🔺

Кроме этого, **Dr.Web для MS Exchange** отправит уведомление с таким же текстом на адрес администратора, указанный во время установки.

Для того чтобы проверить качество обнаружения спама, отправьте письмо с тестовой строчкой GTUBE: XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARDANTI-UBE-TEST-EMAIL\*C.34X по протоколу SMTP на любой тестовый адрес.

Откройте утилиту Windows Просмотр событий → Приложение (Event Viewer → Application) и найдите сообщение о том, что Dr.Web для MS Exchange обнаружил спам.

😽 Event Viewer						-	
<u>File Action View Help</u>							
← → 🗈 🖬 😭 💀 🖆	ş						
Event Viewer (Local)	Application 1,011 event(s) Type Date	Time	Source	Category	Event	User	<b></b>
Security	Warning 11/2/2009	7:21:34 AM 7:20:39 AM	Dr.Web Core Services LoadPerf	Spam None	1003 1000	N/A N/A	
DNS Server     File Replication Service	nt Properties		? ×	None Infected OMA Pus Monitoring	1001 1001 10302 9096	N/A N/A N/A	
	Date: <u>117272009</u> <u>S</u> ource: Time: 7:21:34 AM Category: Typ <u>e</u> : Warning Event <u>I</u> D:	Dr.Web Lore So Spam 1003		Monitoring None None	9095 1000 1001	N/A N/A N/A	
	User: N/A Computer: WIN2003MAIL101			None None None	1000 1001 1704	N/A N/A N/A	
	<u>D</u> escription: Dr.Web for Exchange detected spa Message subject: test antispam	am.		X.400 Se General	9298 1001	N/A N/A	
	Sent from: mailbox1@drweb.test Recipients: mailbox2@drweb.test Carbon Copy Recipients: nknown r	ecipient		Exchang General General	9600 9523 9523	N/A N/A	-
	Date: 🕫 Bytes 🕫 Words						



### 3.2. Настройка параметров антивирусной защиты

Начиная с версии 6.0 управление **Dr.Web для MS Exchange** возможно как с традиционной консоли управления, так и через веб-интерфейс. Возможности и внешний вид консоли управления и вебинтерфейса одинаковы, в связи с чем в данной методике для иллюстрации действий будет использоваться консоль управления.

Запустить Консоль администратора Dr.Web для Microsoft Exchange можно, зайдя в меню Пуск → Программы → Doctor Web → Dr.Web for Microsoft Exchange и выбрав Консоль управления Dr.Web для Exchange или щелкнув дважды на файле запуска консоли (файле drwexch.msc, который по умолчанию находится в папке C:\Program Files\DrWeb for Exchange).

Dr.Web for Exchange Administrative	Console	_ 🗆 ×
файл Действие Вид Справка		
🗢 🔿 🔰 💼 🛛 🖬		
Dr.Web for Exchange           Image: Image and the second	<b>Dr.WEB</b> ® для Microsoft Exchange Server	S
🖃 🖂 Почта		Почта
<ul> <li>Вылеченные</li> <li>Невылеченные</li> <li>Спам</li> </ul>	Вылеченные письма	
Подозрительнь Подозрительны Подозрительны Подозрительны	Невылеченные письма	
Канирование Антислам Фильтрация	О Спам-письма	
Сопроводительный теї Пруппы Карантин	Отфильтрованные письма	
🚹 Статистика 🌐 Отчеты 🍄 Настройки	Подозрительные письма	
Версия	Повреждённые письма	
•		

Запустить веб-интерфейс управления можно как через меню Пуск → Программы → Doctor Web → Dr.Web for Microsoft Exchange, так и непосредственно из браузера, набрав

https:// адрес сервера /DrWebAccess/DrWebForExchange.aspx И указав логин и пароль доступа.

Требуется ауте	нтификация	
0	Введите имя пользователя и пароль для https://localhost	
Имя пользовате	19:	
-		
Lapo	ъ:	
	ОК Отмена	
WIN2K8-64 - Mozilla Firefox		<u>_</u> _×
<u>р</u> айл Правка <u>В</u> ид <u>Ж</u> урнал <u>З</u> акладки <u>И</u> нстру	иенты <u>С</u> правка	
C X 🏠 🚺 localnost https	://localhost/DrWebAccess/DrWebForExchange.aspx 🖒 - Яндекс	٩
O Outlook Web App	NXR.64 Y	
для Microsoft Exchange Server		Русский 💌 🕐
🖃 🎯 WIN2K8-64		
🖃 💽 Профили		
🖃 🖲 Default		
🖃 📢 Уведомления		
🖃 🔤 Почта		
Нарыданные	8 Профили	
Спам		
У Отфильтрованные	🚳 <u>группы</u>	
🔞 Подозрительные	😴 Карантин	
🔞 Поврежденные	Company Learning	
🕑 Журнал событий	Статистика	
Сканирование	Отчеты	
Фильтрания	Настройки	
Сопроводительный текст		
🕮 Группы	Версия	
🕃 Карантин	-	
1 Статистика		
🕑 Отчеты		
💥 Настройки		
😈 Версия		
2010 «Доктор Веб»		
отово		

### 3.2.1. Настройка действий по отношению к различным типам сообщений. Настройка действий по отношению к различным типам проверяемых объектов

Используя Консоль управления Dr.Web для MS Exchange, администратор может определить правила проверки объектов различного типа на наличие вредоносных объектов. Для настройки параметров сканирования необходимо открыть консоль управления, выбрать интересующий профиль и пункт меню Сканирование.

На данной странице администратор может определить:

• действия, применяемые к объектам различного типа;

Для неизлечимых и поврежденных объектов можно блокировать сообщения с объектами таких типов, посылать запросы на их удаление с сервера (результат будет зависеть от настроек Microsoft Exchange), удалять их самостоятельно или перемещать прикрепленные файлы в карантин. Для подозрительных объектов также предусмотрена возможность пропускать их и доставлять получателю нетронутыми. Дополнительным действием является возможность прикреплять файл с информацией о зараженном сообщении. В поле **Текст** администратор может задать содержимое прикрепленного текстового файла. Для добавления макросов в тело файла необходимо нажать на кнопку **Макрос** и выбрать необходимый.

- какие типы потенциально опасных объектов следует искать в проверяемом трафике (потенциально опасные, дозвона, взлома, рекламные, шутки);
- следует ли искать вредоносные объекты в архивах;
- использовать ли при проверке эвристический анализатор.

**Внимание!** Исключение объектов из проверки может снизить нагрузку на сервер, но одновременно понизит безопасность защищаемой сети. Отказ от использования эвристических механизмов не позволит обнаруживать новые модификации вредоносных программ.

Dr.Web for Exchange Administrative	Console			
Файл Действие Вид Справка				
🗢 🔿 🙍 🖬 🛛 🖬				
<ul> <li>Dr.Web for Exchange</li> <li>WIN2(8-64</li> <li>Профили</li> <li>Тандартный</li> <li>Стандартный</li> <li>Уведоиления</li> <li>Почта</li> <li>Вылеченные</li> </ul>	🕑 Включить звристиче	<b>для М</b> ский анализатор	Dr.WEB® licrosoft Exchange Server C Время ожидания: 1000 ис	канирование
невылеченные Спам Г Отфильтрован Одозрительнь	Проверять архивы Обнаруживать		Рассматривать архивы с паролем ка	к поврежденные
Повреждённые Журнал событий Сканирование Антислам	Потенциально опасны Программы дозвона Программы взлома	не программы	<ul> <li>Рекламные программы</li> <li>Программы-шутки</li> </ul>	
у чиль грация	Выберите действия Для неизлечимых и повр Удалить вложенный фа	ежденных объектов: йл 💌	Для подозрительных объектов: Поместить в карантин	
енстройки Ф Версия	Прикреплять следую Суффикс имени Текст:	ций файл к зараженным писи _infected.txt Инфицированный вирусом фай Exchange%NewLine%%Viruses	ьмам: iл %FileName% был %State% Dr.Web для %	Макрос
				Сохранить
	1			

Для сохранения изменений необходимо нажать кнопку Сохранить.

Для настройки параметров фильтрации трафика на спам необходимо выбрать пункт **Антиспам** настраиваемого профиля.



Strate for Exchange Administrative	Console
файл Действие Вид Справка	
🗢 🔿 🔰 🖬 🛛 🖬	
<ul> <li>Dr.Web for Exchange</li> <li>WIN2K8-64</li> <li>Профили</li> <li>Тандартный</li> <li>Тандартный</li> <li>Уведомления</li> </ul>	Dr.WEB® для Microsoft Exchange Server Антиспам
<ul> <li>Вылеченные</li> <li>Невылеченные</li> <li>Спам</li> </ul>	✓ Включить антиспам ☐ Добавлять предопределенные SMTP-заголовки
<ul> <li>Старильтрован</li> <li>Подозрительнь</li> <li>Повреждённые</li> <li>Журнал событий</li> </ul>	Префикс в теме: *** SPAM ***
Сканирование О Антиспам Фильтрация Сопроводительный тек	Сочно спам — Действие: Удалить письмо Добавлять префикс в тему
<ul> <li>Группы</li> <li>Карантин</li> <li>Статистика</li> <li>Отчеты</li> </ul>	Возможно, спам
Версия	Маловероятно, что спам Действие: Пропустить Добавлять префикс в тему
×>	Сохранить

В данном окне администратор может определить действия программы по отношению к сообщениям в зависимости от вероятности их принадлежности к спаму (Точно спам, Возможно спам, Маловероятно, что спам). Действия определяются выбором элементов выпадающих меню Действия для соответствующих типов сообщений. Доступные действия: удалять письма, перемещать их в папку docted and e-mail, пропускать или не принимать и оставлять их на сервере.

Кроме этого, администратор может задавать префикс, добавляемый в тему письма после проверки на спам.

В том случае, если необходимо осуществлять дополнительную фильтрацию проверенных писем сторонними программами, администратор может задать добавление к проверяемым письмам заголовка вида X-AntiVirus, выбрав Добавлять предопределенные SMTP заголовки.

Для сохранения настроек необходимо нажать на кнопку Сохранить.

#### 3.2.2. Добавление пользовательских фильтров

Для настройки параметров сканирования необходимо открыть консоль управления, выбрать интересующий профиль и пункт меню **Фильтрация**.

Dr.Web for Exchange						~~
🖻 📲 WIN2K3ST					Dr W	
🖻 🏢 Профили						
🖻 🔡 Стандартный				для Місто	soft Exchange S	erver
🖃 🌄 Уведомления						
🖻 🖂 Почта						Фильтрация
Вылеченные						
Невылеченные						
Спам	-					
Отфильтровани	I Включ	нить фильтрации	0			
Подозрительны	-					
Поврежденные	Суффикс	имени файла:	_filtered.txt			
журнал сооытии			1			
Антиспам	Текст:	Файл %FileNa	ре% отфильтрован	и сейчас удалён. %NewLine%/	Істали фильтрации:	Mascoor
Фильтрация		%FilteringDeta	ils%			manpoorm
Сопроводительный тег						
Пруппы						
Карантин						
Статистика						-
Отчеты		1				100
— 🌺 Настройки	Правила	-				
Версия			2	0	1	
	ФИЛЬТР		значе	Описание		
				Импорт правил Экспорт	правил Создать	Изменить Удалить
						Covperson
						Сохранитв



Для создания нового правила необходимо отметить пункт **Включить фильтрацию** и нажать на кнопку **Создать**.

В появившемся меню необходимо выбрать из выпадающего списка **Тип** один из доступных типов правил: **Расширение**, **Маска**, **Максимальный размер файла**, **Максимум получателей писем с вложениями** и **Максимум получателей писем без вложений**, в поле значение ввести соответствующий параметр.

Правило				
Тип	Значение	Описание		
Расширение:				
Расширение:		Г		
Маска:			ОК	Отмена
Максимальный размер файла:				
- максимум получателей для писем с приложениями:				
Максимум получателей для писем с приложениями: Максимум получателей:				

Для сохранения настроек необходимо нажать на кнопку Сохранить.

В дальнейшем имеющиеся правила можно как редактировать, так и удалять. Соответствующие действия доступны по кнопкам **Изменить** и **Удалить**.

#### 3.2.3. Настройки черных и белых списков проверяемых адресов

Для того чтобы задать списки черных и белых адресов, необходимо выбрать закладку **Черные/белые** списки на странице **Настройки** консоли управления.

Or.Web for Exchange → ₩IN2K3ST → Профили → Стандартный		Dr.WEB® для Microsoft Exchange Server	No.
— Уведомления	Настройки прокси Черные/Белые списки	Ha	стройки
<ul> <li>Вылеченные</li> <li>Невылеченные</li> <li>Спам</li> <li>Отфильтрован</li> <li>Подозрительны</li> <li>Повреждённые</li> <li>Журнал событий</li> </ul>	E-Mail		
Сканирование	Добавить в белый список	Добавить в черный список	
	e-mail	e-mail	
⊞- 🔝 Группы 🔊 Карантин	Убрать из белого списка	Убрать из черного списка	
Статистика		10.21	_
Отчеты Мастройки Версия		Импорт Экспорт Сохранить	ь

Для добавления адреса в тот или иной список необходимо, отметив для включения фильтрации пол спискам пункт **Включить**, ввести адрес в поле **E-Mail** и нажать либо на кнопку **Добавить в белый список**, либо на кнопку **Добавить в черный список**.

Кроме этого, списки адресов можно импортировать непосредственно из файла, нажав кнопку Импорт.

Для сохранения настроек необходимо нажать на кнопку Сохранить.



### 3.2.4. Сопроводительный текст

Для того чтобы задать сопроводительный текст к проверенным сообщениям, администратор должен в консоли управления зайти на страницу **Сопроводительный текст** настраиваемого профиля и, включив данную функцию, задать соответствующий текст в одном из двух доступных форматов.

Dr.Web for Exchange			~1
🗄 📓 WIN2K3ST		Dr WED®	( )
🖻 🏢 Профили		DI.WED	2
😑 📲 Стандартный		для Microsoft Exchange Server	F
🖻 📢 Уведомления		0	
🖻 🖂 Почта		Сопроводитель	ный текст
Вылеченные			
Невылеченные			
	🔲 Включить сопроводительный текст		
Подозрительны			
	Параметры		
	HTML.		
— 🧱 Сканирование	HIPL:		-
О Антиспам			
— ү Фильтрация			
Сопроводительный тег			
🕀 📠 Группы			
Карантин			
Статистика			-
	Unctrue Torest		1921
	HICTOR TENET.		_
Версия			
			-
	1		
	-		
			Сохранить

Для сохранения настроек необходимо нажать на кнопку Сохранить.

#### 3.2.5. Настройки для отдельных пользователей и групп

Для упрощения организации антивирусной защиты среды Exchange в консоли **Dr.Web для MS Exchange** реализована возможность создания групп пользователей и присвоения им определенных профилей. При этом профиль представляет собой набор настраиваемых параметров обработки сообщений.

Чтобы создать новый профиль, выберите пункт **Профили** в дереве консоли и нажмите **Создать (Add new)**.

Dr.Web for Exchange Administrative	Console					_D×
Файл Действие Вид Справка						
🗢 🔿 🔰 🖬 🚺 🖬						
Слан Слан Стандартный Стандартный Стандартный Стандартный Стандартный Стандартный Стандартный Стандартный Вылеченные Спан Спан Спан Спан Спан Стандартные	Создать	/далить Переи	для Micros	Dr.\ soft Exchange	NEB® Server	<b>Вофили</b>
🕅 Подозрители				1	1	
С Повреждённ	Профиль	Фильтрация	Антислам	Сопроводительны.		
Курнал событи	Профильт	-	+	-		- 1
Сканирование	Стандартный	-	+	-		V
	1					
Сопродолитольный						
Профить 1						
Н К Увеломления						
Сканирование						
Антиспам						
Фильтрация						
Сопроводительный						
Са Группы						
🔊 Карантин						
Статистика						
Отчеты						
🔅 Настройки 💌						

Будет создан новый профиль с именем **Профиль1 (Profile1)**, который появится в дереве консоли под пунктом **Профили**. Если профиль с таким именем уже существует, то имя нового профиля будет **Про-филь2**, и т. д.





Чтобы изменить имя профиля, выберите его в списке, расположенном в области сведений раздела **Профили**, и в меню, открывающемуся по клику правой кнопки мышки, выберите **Переименовать** (Rename).

У каждого профиля есть определенный уровень приоритета, назначаемый администратором. В случае если клиент состоит в нескольких группах, которым назначены разные профили, то при обработке сообщений, получаемых или отправляемых этим клиентом, будет использован профиль с наибольшим уровнем приоритета. Приоритет изменяется в области сведений раздела **Профили** перемещением существующих профилей вверх или вниз по списку при помощи кнопок и справа от списка. Чем выше профиль расположен в списке, тем выше уровень его приоритета. **Стандартный** профиль всегда обладает самым низким уровнем приоритета, и его нельзя переместить выше нижней строчки в списке профилей.

Для назначения профиля группе пользователей нужно в консоли управления выбрать в списке групп интересующую и в выпадающем списке **Профиль** выбрать необходимый.

Dr.Web for Exchange     WIN2K3ST     Пофили     Пофили			для Microsoft Exch	Dr.WEB <sup>®</sup> ange Server	ST.
					Группа
- Вылеченные - Невылеченные - © Спам	Имя гоуппы:	deu			
- 2 Подозрительны		u			
Повреждённые	Тип группы:	Группы Active Directory	Выбрать		
— 🚺 Журнал событий — 🔳 Сканирование	Параметры:	Группы Active Directory Указать адреса клиентов			
О Антиспам			<u>^</u>		
— 🍸 Фильтрация					
Сопроводительный тег					
н на Профиль1 — 🔝 Группы			~		
Карантин	Профиль:	Стандартный			
Статистика					
Настройки	-				
Версия					Сохранить

В этом же окне администратор должен указать тип группы, выбрав его в выпадающем списке Тип группы. Если выбран тип Указать адреса клиентов, то проверяемые адреса нужно ввести вручную в поле Параметры. Если выбран тип Группы Active Directory, то для выбора интересующих групп надо нажать на кнопку Выбрать.



Dr. Web for Exchange     WIN2K3ST     Профили     Стандартный     Software Provided Addressed		Dr. для Microsoft Exchang	WEB® e Server
Спраника Спраника Спраника Спраника Спраника Спраника Спраника Спраника Спраника Сопроводительный тек Сопроводительный тек Сопроводитек Сопро	Има группы: drw Тип группы: Группы Activ Пар Выбор: "Группы" Выберите тип объект "Труппь" или "Встро В сдедующем месте: dw.test Про Введите умена выби; Дополнительно	е Directory Выбрать  Выбор: "Группы" Выберите тип объекта:  Группы" или "Встроенные участники безопасности" В следующем месте:  drw.test Общие запросы  Mma: начинается  Плисание: наченается  Пароли с неограниченным сроком действия.  Число дней со времени последнего входа в систему:  Результаты поиска: Има (RDN) Описание В папке	? × ипы объектов Размещение Столдцы Воиск Столдцы Воиск Отмена

### 3.2.6. Редактирование шаблонов уведомлений

Для того чтобы настроить уведомления для различных типов пользователей, администратор должен в выбранном профиле консоли управления в пункте меню **Почта** выбрать интересующий его тип уведомления (**Вылеченные**, **Невылеченные**, **Спам**...) и в открывшемся окне настроить параметры информирования администратора, получателей и отправителей сообщения.

© Dr.Web for Exchange □-	Dr.WEB <sup>®</sup> для Microsoft Exchange Server				
<ul> <li>Эка Областия</li> <li>Эка Областия</li> <li>Эка Оказа</li> <li>Эк</li></ul>	Администратору	Отправително Получателно Вылече истратору уведоиления по почте	нные письма		
— Санирование — Сканирование — Оканирование — Оканирование	Настройте параметр Тема уведомления:	ы уведонлений для администратора Dr. Web для Exchange обнаружил вирус!			
<ul> <li></li></ul>	Текст	Dr.Web для Exchange обнаружил, что %ObjectType% заражен вирусом. %ObjectType% %State%, %NewLine%Имя файла: %FileName%%NewLine%%Viruses%%NewLine%Tema письма: %MessageSubject%%NewLine%OT; %MessageSender%%NewLine%Komy;	Макрос,		
Отчеты	Кому:	user1@drw.test			
Версия	От кого:	user1@drw.test			
	Имя сервера:	WIN2K3ST			
			Сохранить		

Кроме этого, администратор может задать текст, выводимый в журнал событий системы при возникновении событий различного типа. Тексты задаются на странице **Журнал событий** выбранного профиля.



С Dr.Web for Exchange ☐- Ш WIN2K3ST ⊡- Ш Профили □- Ш Стандартный	Dr. для Microsoft Exchang	WEB® e Server	S.
— Уведомления — Уведомления		Журна	л событий
Вылеченные Невылеченные О Спам Подозрительные Подозрительные Журнал событий Журнал событий	Вылеченные Вылеченные Включить Текст сообщения: МаssageSubject%%MewLine%Получатели копии: %MessageCcR	иля 🔺 omy: ecipients% 💌	Макрос
Фильтрация	Невылеченные		
— 📻 Сопроводительный теі ⊞ 🔝 Группы — 🖋 Карантин — 🚹 Статистика	Включить Текст сообщения: Инфицированный вирусом файл %FileName% был %State% Dr.Web / Exchange%NewLine%%CV/Uses%%NewLine%KTexa писсия: %MessageSubject%%NewLine%TC, %MessageSeder%%NewLine%KT %MessageRecipients%%NewLine%Получатели колии: %MessageCCR	ля 📕 owy: ecipients% 💌	Макрос
Отчеты	Спам		
— У Настронки — Версия	Включить Текст сообщения: %MessageSubject%%NewLine%OT: %MessageSender%%NewLine%C %MessageRecipients%%NewLine%Получатели копии: %MessageCCR	omy: ecipients%	Макрос
	Отфильтоованные		
	Включить текст сообщения: Удален. %NewLine%Имя файла: %FileName%%NewLine%Подробност %FilteringDetails%%NewLine%Teмa письма: %MessageSubject%%New %MessageSender%%NewLine%Kowy:	и фильтрации: /Line%От:	Макрос
	Полозоительные		
	Включить Текст сообщения: "МезsageSubject%%NewLine%Ot; MessageSender%%NewLine%K	зрительным.	Макрос
• <b>•</b>	Повреждённые		

Для сохранения настроек необходимо нажать на кнопку Сохранить.

### 3.2.7. Сохранение текущих настроек в конфигурационный файл

Для сохранения настроек администратор должен выбрать пункт **Dr.Web for Exchange** в консоли управления и, выбрав в таблице имя сервера, нажать на кнопку **Сохранить настройки**.



### 3.3. Управление карантином

Управление карантином доступно на странице **Карантин** консоли управления. На данной странице администратор может просматривать список объектов, находящихся в карантине, удалять их, сохранять в виде файла, очищать карантин.

По умолчанию объекты, которые находились в карантине больше 20 дней, удаляются автоматически.

😂 Dr.Web for Exchange				~1	
🖻 📓 WIN2K3ST			Dr WE		
🗄 🌐 Профили			DI.VVE		
😑 📲 Стандартный		Дл	19 Microsoft Exchange Serve	er le	
🚊 📢 Уведомления				If an average	
🖻 🖂 Почта				карантин	
Вылеченные Невылеченные Спам Спам Э Отфильтроване Подозрительные З Журнал событий Сканирование Антислам Чильтрация Сопроводительный тег	Тип фильтра: Дата 💌 = 💌 09:07.2010 💌 10:43:39 🚎 🚰				
	Очистка списка Удалить файлы старше 7 📑 дней Автоматически удалять файлы старше 20 📑 дней				
Карантин	ПЛата	Вирус	Отправитель	Тема	
			Обновить Сканировать Уда	лить Копировать	
				Сохранить	

#### 3.3.1. Статистика работы сервиса. Получение отчетов о работе программы

Просмотр статистики доступен на странице Статистика консоли управления. На закладке Статистика администратору доступна информация об общем количестве событий различного типа.

Для очистки статистики необходимо нажать на кнопку Очистить.

Подробная информация о событиях различного рода доступна на закладке События этой же страницы.

C Dr.Web for Exchange 			<b>Dr.WEB</b> <sup>®</sup> для Microsoft Exchange Server	S
Уведонления Почта Вылеченные Спам Отфильтрован Одозрительны Курнал событий Курнал событий Курнал событий Сканирование Антиспам Фильтрация Сопроводительный тен Группы Статистика	Статистика События Проверено объектов: Зараженных объектов: Подозрительных объектов: Спан-писеи: Вылечено объектов: Чистых объектов: Удалено объектов: Заблокировано распространений: Заблокировано распространений:	23549 674 18 0 22857 692 0 0		Статистика
Отчеты Мастройки Версия	Отфильтровано объектов: Поврежденных объектов:	0	Очистить	Обновить



С Dr.Web for Exchange → WIN2K3ST → Пофили → Стандартный		для Мі	Dr.WE	B®
<ul> <li>Уведомления</li> <li>Уведомления</li> <li>Очта</li> <li>Вылеченные</li> <li>Стам</li> <li>Отфильтровани</li> <li>Одозрительнь</li> </ul>	Статистика События Фильтр Тип фильтра: Отправител	b. V Macka		Статистика Применить
— 🔀 Повреждённые — 🔃 Журнал событий	Отправитель	Получатели	Тема	
Сканирование	user1@druptect	user1@druutect	uixicos in attach!	000107
Антиспам	user1@drw.test	user1@drw.test	virises in attacht	удален
	user1@drw.test	user1@drw.test	virises in attach!	VAanet
	user1@drw.test	user1@drw.test	virises in attach!	удален
Сопроводительный тег	user1@drw.test	user1@drw.test	virises in attach!	удален
н ма группы	user1@drw.test	user1@drw.test	virises in attach!	удален
Карантин	user1@drw.test	user1@drw.test	virises in attach!	удален
Статистика	user1@drw.test	user1@drw.test	virises in attach!	удален
Отчеты	user1@drw.test	user1@drw.test	virises in attach!	удален
Настройки	user1@drw.test	user1@drw.test	virises in attach!	удален
Версия	user1@drw.test	user1@drw.test	virises in attach!	удален
	user1@drw.test	user1@drw.test	virises in attach!	удален
	user1@drw.test ◀	user1@drw.test	virises in attach!	V/aner
			Эксп	орт Обновить
	Очистка списка Удалить записи старше Автоматически удалять за	09.07.2010 💌 лиси старше 30 📑 дней		Очистить
	-			Сохранить



### 3.4. Тестирование производительности

Для тестирования производительности рекомендуется использовать следующую методику:

- 1. Восстановление системы из образа с установленным и настроенным антивирусом.
- 2. Останов антивирусного монитора.

terprise Security Suite

- 3. Измерение свободных системных ресурсов в состоянии покоя.
- 4. Посылка потоков тестовых сообщений с отдельного компьютера. Рекомендуется повторять процесс посылки тестовых потоков не менее 3-х раз. Окончание приема сообщений необходимо отслеживать с помощью оснастки MS Exchange Средства просмотра очереди. Окончание загрузки операционной системы необходимо отслеживать как с помощью Process Explorer, так и с помощью оснастки MS Exchange Системного монитора. После посылки каждого потока база сообщений должна очищаться либо с помощью средств MS Exchange, либо из почтового клиента, например, из Microsoft Office Outlook.

Рекомендуется повторить данную процедуру не менее 3 раз.

Во время работы должно проводиться измерение:

- объема потребляемой оперативной памяти в состоянии покоя и при сканировании по требованию тестовой коллекции при помощи утилиты Process Explorer;
- уровня использования процессора и жесткого диска в состоянии покоя и во время сканирования по требованию;
- времени посылки и приема тестового потока.

Как правило, определяющим временем работы можно считать первое измерение, что позволяет избежать влияния кэширования.

# 3.4.1. Тестирование производительности системы фильтрации почтового трафика

Для проведения тестирования кроме самого почтового сервера рекомендуется использовать дополнительно еще две рабочие станции: для отправки потока сообщений и для их приема.

В случае использования на этих рабочих станциях операционных систем типа Linux для генерации и приема потока почтовых сообщений рекомендуется использовать пакет postal, содержащий две утилиты:

- bhm для приема почты «в никуда» (т. е. реализующий smtp-сессию без сохранения где-либо принятого письма, что минимизирует влияние принимающего сервера на общую производительность системы тестирования). Данная утилита запускается с указанием адреса (интерфейса) и порта на принимающей машине;
- 2. postal для отправки автоматически генерируемого потока сообщений с заданными параметрами (размером сообщения и списком параллельных потоков сообщений) по списку адресов. Данная утилита запускается вручную на отсылающей машине с указанием длительности теста, количества одновременных потоков, диапазона размеров сообщений, списка получателей, IP-адреса и порта, на который нужно производить отсылку. В качестве адреса получателя указывается адрес почтового сервера. Как правило, размер писем находится в диапазоне 1–10 КБ, поэтому рекомендуется для тестирования задавать диапазон 3–5 КБ.

Пример запуска postal на запускающей машине:

Postal -t 10 -m 1 -M 1 -r 1200 192.168.1.100 ./user\_url\_list

Выводимые значения покажут время, количество и объем переданных сообщений, количество возникших ошибок.

**Внимание!** Особенностью работы команды postal является то, что в течение первой минуты работы выводимые значения производительности не являются достоверными. В качестве достоверных значений необходимо использовать данные по работе, начиная со второй минуты.



**Внимание!** Отправляющая и принимающая машины не должны самостоятельно проверять тестируемый почтовый поток. В том случае, если на эти машины была установлена защита от спама, ее необходимо отключить.

**Внимание!** По особому запросу может быть предоставлена доработанная версия утилиты postal, позволяющая проводить более детальное тестирование, в частности формировать письма.

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

#### 3.4.2. Тестирование функционирования системы фильтрации почтового трафика

Для проведения тестирования кроме самого почтового сервера рекомендуется использовать дополнительно еще две рабочие станции: для отправки потока сообщений и для их приема.

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). Приведем пример отправки 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:

file_with_viruses	— файл с вложенными вирусами
root@localhost	– адрес, от кого придет сообщение
192.168.1.100	– адрес почтового сервера
toaddress	– адрес, на который должно прийти тестовое сообщение

Для тестирования работы антиспама необходимо отправить письмо, содержащее в теле письма 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: 30 минут с учетом установки и настройки необходимых утилит, сбора и формирования тестового набора файлов.

# 4. Настройка системы антивирусной фильтрации на почтовом шлюзе с помощью Dr.Web Mail Gateway

#### 4.1. Установка сервиса

**Внимание!** Установка продукта возможна как из инсталляционного пакета, предназначенного для конкретной операционной системы, так и с помощью универсального пакета, подходящего для установки на любой совместимой операционной системе. В данной методике описывается использование универсального пакета, имеющего расширение run.

Установка сервиса возможна как из командной строки, так и с помощью графического инсталлятора. Процедура установки с помощью графического инсталлятора подробно описана в документации на продукт, поэтому ниже будет рассмотрена процедура установки и настройки из командной строки.

Скопируйте инсталляционный файл во временную директорию и распакуйте его. Для распаковки можно просто запустить инсталляционный файл с ключом noexec:

sh ./drweb-gateways-av-as\_6.0.1.0-1102281538~linux\_x86.run

Сразу после запуска необходимо подтвердить согласие на установку.

This installation script will help you install DrWeb for Mail Gateways Antivirus+Antispam
Do you want to continue? (YES/no) _
Укажите тип установки. Для продолжения установки выбираем 1.
Select the installation type:

select	τne	installation type:
	1	Dr.Web for Mail Gateways (Antispam+Antivirus)
	2	Custom Configuration
Choose	one	configuration to install [1] : _

После этого вам будет показан текст лицензии. Вы можете ознакомиться с ней, нажимая пробел для прокрутки текста, либо прервать показ, нажав клавишу Q.

Dr.Web(R) SOFTWARE USAGE LICENSE AGREEMENT

The present License agreement is concluded between you (either a legal entity or home user) and Doctor Web ("the right holder"), that possesses intellectual property rights with regard to usage of Dr.Web(R) software ("software") including usage of technologies and software from other vendors where corresponding rights are acquired under law of the Russian Federation and International Law, as follows:

3.2. You are entitled to create as many copies of the key file as required to install the software on the number of computers (workstations, servers, etc.) defined in the key file. In addition you can store no more than two copies of the license key file. You may not give these copies to a third party or place them on tangible media accessible to a third party or make the files accessible to the public over the Internet or by any other means. If necessary you can specify your legally acquired Software <u>-More--(50%)</u>

Подтвердите согласие с текстом лицензии, введя Yes.

3.2. You are entitled to create as many copies of the key file as required to install the software on the number of computers (workstations, servers, etc.) defined in the key file. In addition you can store no more than two copies of the license key file. You may not give these copies to a third party or place them on tangible media accessible to a third party or make the files accessible to the public over the Internet or by any other means. If necessary you can specify your legally acquired Software Do you agree with the terms of this license? (yes/NO)

После завершения установки продукта инсталляционный скрипт предлагает настроить параметры работы программы. Введите Yes и ответьте на вопросы, задаваемые в ходе настройки.



This installation script will help you to configure DrWeb for Mail Gateways Antivirus+Antispam Do you want to continue? (YES/no) \_ Enter path to key file for Dr.Web MailD If you don't have the key yet you can leave this value unspecified, but you must set LicenseFile parameter value in configuration file agent.conf, and parameter Key in configuration file drweb32.ini before MailD is launched or any plugin is installed. [default=]: Enter list of plugins to process message before placing it to queue/DB. Possible values: (vaderetrolheadersfilterIdrwebImodifier). Values are delimited with commas. [default=]: Enter list of plugins to process message after placing it to queue/DB. Possible values: (vaderetrolheadersfilterIdrwebImodifier). Values are delimited with commas. [default=]: Enter email address to send notifications to. [default=postmaster@localhost]: Enter email address to send notifications from. [default=DrWEB-MAIL-DAEMON@localhost]: Enter list of protected networks (e.g. 127.0.0.0/8). Values are delimited with commas. [default=127.0.0.0/8]: Enter list of protected domains. Values are delimited with commas. [default=localhost]: Enter language(s) to use in reports. Possible values: (enljalru). Values are delimited with commas. [default=en]: \_\_\_\_ Configuration: Plugins directory = /opt/drweb/maild/plugins lng files directory = /etc/drweb/maild/lng Before queue plugins = After queue plugins = Administrator email address = postmaster@localhost Filter email address = DrWEB-MAIL-DAEMON@localhost Protected networks = 127.0.0.0/8 Protected domains = localhost Language(s) for reports = en Press 1 to Save updated configuration,

**Внимание!** В ходе настройки обязательно должен быть указан список подключаемых плагинов (например, vaderetro, drweb, modifier — разделенных запятыми и без пробелов), списки защищаемых доменов и сетей.

В дальнейшем список подключаемых плагинов может быть изменен путем редактирования параметра BeforeQueueFilters конфигурационного файла /etc/drweb/maild smtp.conf Например:

BeforeQueueFilters = vaderetro, drweb, headersfilter

После завершения настройки проверьте выбранную конфигурацию и сохраните ее, нажав 1.

После завершения процесса настройки сервис антивирусной фильтрации будет автоматически загружен и готов к работе.



Loading /var/drweb/bases/drwnasty.vdb - Ok, virus records: 28348 Total virus records: 1743213 Key file: /opt/drweb/drweb32.key - loaded. License key number: 0012826730 License key activates: 2010-10-25 icense key expires: 2011-01-25 License for Internet gateways: 5 users. License for file-servers: 5 users. License for mail-servers: 5 e-mail addresses. Daemon is enabled for protecting 5 e-mail's: username10example.com username10foo.example.com username1 username20example.com username20domain.tld Daemon is installed, active interfaces: /var/drweb/run/.daemon 127.0.0.1:3000 Done. Configuring startup of drweb-monitor... Starting Dr.Web Monitor... Done. Configuration completed succesfully. Press Enter to finish.

Если в дальнейшем возникнет необходимость дополнительной настройки Dr.Web Mail Gateway в соответствии с конкретными требованиями, то это можно сделать как через веб-интерфейс, так и напрямую — через конфигурационные файлы. Все настройки содержатся в конфигурационных файлах, расположенных в директории /etc/drweb/. В файле maild\_smtp.conf содержатся общие настройки Dr.Web MailD, в файле agent.conf — настройки компонента Dr.Web Agent, а в файле monitor.conf — настройки компонента Dr.Web Monitor. Настройки плагинов находятся в файлах plugin\_drweb.conf, plugin vaderetro.conf, plugin modifier.conf и plugin headersfilter.conf.

Базовую настройку можно также осуществить с помощью скрипта configure.pl, по умолчанию располагающегося в директории /opt/drweb/maild/scripts/. После запуска скрипт запросит значения основных параметров и запишет их в конфигурационные файлы maild\_MTA.conf, agent.conf и monitor.conf. Остальные параметры, необходимые для взаимодействия с почтовой системой, нужно будет настроить отдельно, вручную отредактировав конфигурационный файл Dr.Web MailD.

За настройку взаимодействия между плагинами отвечают скрипты plugin\_drweb\_configure.pl, plugin\_vaderetro\_configure.pl и plugin\_headersfilter\_configure.pl, по умолчанию располагающиеся в директории /opt/drweb/maild/scripts. При запуске скрипта необходимо будет указать путь к лицензионному ключевому файлу, если он не найден автоматически (не указан в agent. conf), и порядок обработки писем конкретным плагином (до или после помещения письма в базу данных), а также задать адрес для доступа к Dr.Web Daemon.

Если необходимо произвести интеграцию с почтовым сервисом, то сделать это можно, запустив скрипт /opt/drweb/maild/scripts/configure\_mta.sh.

После завершения настройки сервиса его необходимо запустить или перезапустить, если он уже был запущен.

/etc/init.d/drwebd start

/etc/init.d/drweb-monitor start

Просмотреть результат запуска можно, введя команду ps -Af | grep drw или ps ax | grep drw

31319 ?	Ss	0:00 /opt/drweb/drwebd.real
31511 ?	S	0:00 /opt/drweb/drwebd.real
31979 ?	S	0:00 /opt/drweb/drwebd.real
32237 ?	Ss	0:00 /sbin/syslog-ng
32240 ?	Ss	0:00 /sbin/klogd -c 1 -x
32274 ?	S	0:00 /opt/drweb/drwebd.real
32399 ?	Ssl	0:00 /opt/drweb/drweb-monitor.real -c /etc/drweb/monitor.conf
32400 ?	Ssl	0:00 /opt/drweb/drweb-agent.real -c /etc/drweb/agent.conf
32408 ?	Ssl	0:01 /opt/drweb/drweb-notifier.real local:/var/drweb/ipc/.agent
32415 ?	Ssl	0:00 vopt/drweb/drweb-sender.real local:/var/drweb/ipc/.agent
32424 ?	Ssl	0:00 /opt/drweb/drweb-maild.real local:/var/drweb/ipc/.agent
32438 ?	Ssl	0:00 /opt/drweb/drweb-receiver.real local:/var/drweb/ipc/.agent



В качестве средства удаленного администрирования используется Webmin. Если вы хотите использовать для управления веб-интерфейс, вы должны установить его. Например:

rpm -i ./webmin-1.530-1.noarch.rpm.

Дистрибутив Webmin'а может быть загружен с www.webmin.com/download.html.

**Внимание!** В связи с тем, что используемый по умолчанию в Windows XP браузер Internet Explorer версии 6.0 имеет значительные проблемы с безопасностью и не рекомендуется к использованию своим производителем, дальнейшая демонстрация проводится с помощью браузера Firefox.

Для того чтобы получить доступ к консоли Вебмина, в строке браузера нужно указать адрес сервера Linux, на котором был установлен вебмин, и 10000. Например, <u>http://192.168.100.82:10000</u>. В качестве логина используется root, пароля — пароль доступа к серверу Linux.

Login failed. Please try again.

Login to Webmin		
You must enter a username and password to login to the Webmin server on 192.168.100.34.		
Username	ame root	
Password		
	Remember login permanently?	
	Login Clear	

Для установки консоли управления Dr. Web Mail Gateway необходимо в папке Webmin выбрать пункт Webmin Configuration и на открывшейся странице выбрать Webmin Modules.

Login: root Webmin Backup Configuration Files Observe Longerge and Theree	Module Config	Webmin Co Webm	onfiguration in 1.450
Change Language and Theme Webmin Actions Log Webmin Configuration Webmin Servers Index Webmin Users	IP Access Control	Ports and Addresses	
System			
Servers			يەلى
Others			
Networking		<b>V</b>	
Hardware	User Interface	Webmin Modules	Operating System and

На странице Webmin Modules необходимо выбрать вариант From local file и указать путь к файлу drweb-maild-web.wbm.gz. По умолчанию он находится в каталоге /opt/drweb/web.

Module Index	Webmin Modules	
Install Clone	Delete Export	
Webmin modules distributed in .wor installed from RPM	can be added after installation by using the form to the right. Modules a files, each of which can contain one or more modules. Modules can d files if supported by your operating system.	are typically also be
Install Module		
Install from	© From local file	
	C From uploaded file	Обзор
	C From ftp or http URL	
	C Standard module from www.webmin.com	
	C Third party module from	
lgnore dependencies?	C Yes © No	
Grant access to	Grant access only to users and groups : root     Grant access to all Webmin users	
Install Module		



Указав файл, необходимо на странице **Webmin Modules** нажать на кнопку **Install Module**. После завершения установки нужно перезагрузить **Webmin**. Консоль управления Dr.Web Mail Gateway находится в папке Servers.

Login: root			
Lugini. ruut	Module Index	Install Module	
🔟 Webmin		motan modale	
System	The following modules have be	an average fully installed and added to your approach control list :	
Servers	The following modules have be	en successiony instaned and added to your access control list .	
Others	Dr.Web console for U	Dr.Web console for Unix mail servers in /usr/libexec/webmin/drweb-maild (12080 kB) under categor	
Networking	Servers		
🔟 Hardware	📥 Boturn to modulos form. I	Beturn to Webmin configuration	
Cluster	The relation to modules form 1	Return to Webhini conliguration	
Un-used Modules			
Search:			

В том случае, если для работы консоли не хватает ряда дополнительных модулей, их список будет показан при попытке запуска консоли.



Недостающие модули можно установить как автоматически — нажав кнопку install modules, так и из командной строки. Рекомендуется устанавливать недостающие модули из командной строки. Имена модулей могут различаться, однако, как правило, они содержатся в пакетах perl-Convert-BinHex, perl-IO-stringy, perl-MIME-tools, perl-XML-Parser, perl-XML-XPath. Для установки в rpm-системах рекомендуется выбирать пакеты noarch.rpm.

🗞 Webmin 1.530 on Sles11Sp1 ( 💥	🗞 Install Module	×	÷
Module Index	Install I	Vodule	
Downloading http://www.cpan.org/modules Received 1024 bytes (0 %) Received 95 kB (10 %) Received 95 kB (20 %) Received 284 kB (30 %) Received 284 kB (30 %) Received 379 kB (40 %) Received 473 kB (50 %) Received 568 kB (60 %) Received 568 kB (60 %) Received 657 kB (80 %) Received 851 kB (90 %) Received 945.11 kB (100 %) download complete.	s/02packages. details. txt ;	gz (945.11 kB)	
Downloading http://www.cpan.org/authors. Received 1024 bytes (1 %)	/id/M/MA/MAKAMAKA/JS	SON-2.50.tar.gz (7	5.03 kB)



Module names	JSON 2.50		
	MIME::tools 5.428		
Source	http://www.cpan.org/authors/id/M/MA/MAKAMAKA/JSON-2.50.tar.gz		
	http://www.cpan.org/authors/id/D/DO/DONEILL/MIME-tools-5.428.tar.gz		
	http://www.cpan.org/authors/id/D/DO/DONEILL/MIME-tools-5.428.tar.gz		
	http://www.cpan.org/authors/id/D/DO/DONEILL/MIME-tools-5.428.tar.gz		
Dro roguisitos	The full www.cpan.org/authors/u/D/DO/DO/NETEL//WIME-tools-5.428.tal.gz		
Pre-requisites	MTME: : Pace 64 Mail: Field Eile: : Temp Eile: : Path Mail: Internet (Missing 4 modules)		
Install action	PIPIC. Baseo4 main. neid rite. reinprite. Patri main. memer (missing 4 modules)		
Install action	Make, test and install 🗘		
Makefile.PL			
arguments			
Makefile.PL	Name Value		
environment			
variables			
Continue With Install	Eetching Missing Pre-Requesites		
	······································		
두 Return to modules li	st		

После завершения установки модуля управления рекомендуется обновить страницу Webmin.

# 4.1.1. Настройка языка интерфейса

Для изменения языка отображения интерфейса необходимо выбрать пункт Change Language and Theme и выбрать необходимую кодировку.

Login: root Vebmin		Сменить	язык и тему				
Backup Configuration Files Change Language and Theme Webmin Actions Log	Этот модуль может быть использован для изменения язык, на котором отображаются модули и тема, которая контролирует внешний вид Webmin, только для вашей учетной записи Webmin.						
Webmin Configuration Webmin Servers Index	Язык интерфейса Webmin	С Глобальный язык (Engli	sh (US))				
Webmin Users		персональный выбор	Russian KOI8 (RU_SU)	<b>•</b>			
System	Тема интерфейса Webmin	<ul> <li>Глобальная тема (Blue)</li> </ul>	German (DE)	<b></b>			
Servers		Персональный выбор	Greek (EL) Hebrow (HE)				
Dr.Web console for Unix mail	C		Hungarian (HU)				
servers	сохранить изменения		Italian (IT)				
Fetchmail Mail Retrieval			Japanese (JA_JP.EUC)				
Postfix Mail Server			Japanese (JA_JP.UTF-8)				
PostgreSQL Database Server			Klingon (TL)				
Procmail Mail Filter			Korean (KO_KR.EUC)				
Read User Mail			Korean (UTF-8) (KU_KR.UTF-8)				
SSH Server			Littuarian (LT)				
Samba Windows File Sharing			Norwegian (NO)				
Sendmail Mail Server			Persian (FA)				
Dithers			Polish (PL)				
Networking			Portuquese (PT)				
Hardware			Portuguese (Brazilian) (PT_BR)				
Cluster			Romanian (RO)				
Un-used Modules			Russian CP1251 (RU_RU)				
Search:			Hussian Kolo (RU_SU)				



### 4.2. Настройка параметров антивирусной защиты

# 4.2.1. Первоначальная настройка

Для настройки через веб-интерфейс необходимо выбрать пункт Dr.Web консоль для почтовых серверов UNIX в меню Службы и перейти в меню Конфигурация.

Первоначальная настройка осуществляется на странице **Ядро (Engine)** меню **Конфигурация** (Configurations).

	Версия Dr.Web MailD: Версия веб-интерфейса Dr.Web: 6.0.0.0	6.0.0 .1011301406
консоль для почтовых серверов UNIX	© 2010	"Доктор Веб"
💓 Карантин 🔅 Конфигурация 📝 Шаблоны	MailD запуще	н
Базовые настройки Карантин Подключаемые	модули Правила Ядро Отчеты При	ем почты
Отправка почты Ітар РорЗ Ргоху		
▼ Основные		
ProtectedNetworks	Список защищаемых сетей.	подробнее
127.0.0.0/8 ×		
<b>H</b>		
Префикс: другое значение 💌 Значение:		
ProtectedDomains	Список защищаемых доменов.	
×		
localhost 🍆		
<b>±</b>		
Префикс: другое значение		
€ €		
Include Subdomains	Включение поддоменов в список защищаемых доменов.	
postmaster@localhost		
		_
OnlyTrustedControlMails ☐a	Возможность отправлять управляющие письма (например, дл: письма из карантина) только из защищаемой сети.	я получения
		подроонее
LicenseLimit	Действия над сообщениями, которые не были проверены из-за лицензионных ограничений.	
Основное деиствие пропустить  Дополнительные действия		
<ul> <li>нерегланравите</li> <li>информировать</li> </ul>		
+ добавить заголовок		
+ добавить счет		
		_
EmptyFrom Основное действие продолжить	Реакция на пустое поле From в заголовках письма.	подробнее
Дополнительные действия		
перенаправить		
+ добавить заголовок		
<b>+</b> добавить счет		



На данной странице рекомендуется задать параметры ProtectedDomains (например, drweber. test) и ProtectedNetworks.

В случае необходимости администратор может задать адрес, на который будут отправляться сообщения, на странице **Отправка почты (Sending Mail)** меню **Конфигурация (Configurations)**. В большинстве случаев задание данного параметра необязательно.

😹 Карантин 🔅 Конфигурация 📝 Шаблоны	MailD запущен
Базовые настройки Карантин Подключаемые модули	Правила Ядро Отчеты Прием почты
Отправка почты Ітар Рор3 Ргоху	
▼ Основные	
Address	Адрес, используемый компонентом Sender для отправки сообщения.
inet:3003@127.0.0.1 ×	подросное
SendDSN Her 🔽	Отправка DSN-отчета. подробнее
Router	Правила маршрутизации сообщений в зависимости от их получателей. подробнее
Префикс: другое значение     ✓ Значение:     ✓	
▶ Дополнительные	
Предпросмотр Сохранить Применить и сохранить изменения	

Если значение **Method**, задаваемое на этой же странице в разделе **Advanced**, равно pipe, то в данном параметре необходимо указать полный путь к почтовой системе, получающей сообщения. В остальных случаях в параметре **Address** задается сокет, через который отправляются сообщения. При работе программного комплекса в режиме SMTP-прокси кроме стандартных типов адресов можно также использовать тип mx: HOSTNAME, где HOSTNAME — имя хоста. В случае использования такого типа программный комплекс получает для HOSTNAME все MX-записи и отправляет сообщение в соответствии с ними. Указание имени хоста не является обязательным — оно будет взято из имени хоста почтового адреса. При отсутствии для указанного mx соответствующей записи в DNS используется запись А.

Адрес, используемый для получения сообщений, задается на странице Прием почты (Mail Receiving) меню Конфигурация (Configurations) в параметре Address.



😹 Карантин 🔅 Кон	нфигурация 📝 Шаблоны		▶	MailD запущен
Базовые настройки Каран	ітин Подключаемые м	одули Правила	Ядро Отчеты	Прием почты
Отправка почты Imap	Рор3 Ргоху			
▼ Основные				
Address inet:8025@127.0.0.1 ×		Адрес, используемый ко	мпонентом Receiver для по	лучения сообщений. подробнее
	]			
ProcessingErrors Основное действие отклонить	×	Действия, применяемые	к сообщениям в случае ог	иибок их обработки. подробнее
ę				
настройки для smtp				
▶ Дополнительные				
Предпросмотр Соуранить Г	Применить и соуранить изменен	1149		

В параметре Address указывается сокет — либо TCP-сокет в формате inet: порт@имя\_хоста, либо UNIX-сокет в формате local: путь\_к\_файлу\_сокета.

Применить сделанные изменения можно, нажав находящуюся внизу страницы кнопку **Применить** и сохранить изменения.

#### 4.2.2. Настройка параметров проверки сообщений по протоколам POP3/POP3S/ IMAP4/IMAP4S

Настройка параметров проверки протоколов POP3/POP3S/IMAP4/IMAP4S производится на страницах **Pop3** и **Imap** меню **Конфигурация (Configurations)**. Для примера рассмотрим настройку для протоко-лов POP3/POP3S.

В параметрах ServerAddress (по умолчанию inet:pop3@localhost) и ListenAddress (по умолчанию inet:5110@localhost) указываются адреса сокетов, по которым следует подключаться к серверу POP3 и на которых следует ожидать подключений клиентов. Для ListenAddress допустимы адреса вида inet: или inet-ssl:.

Внимание! Адрес вида inet-ssl требует использования протокола POP3S/IMAP4S.

В параметре **OnFilterErrors** необходимо задать действие, которое будет применяться к письму при ошибке, возникшей до его отправки.



	Версия Dr.Web MallD: 6.0.0 Версия веб-интерфейса Dr.Web: 6.0.0.0.1011301400
	© 2010 "Доктор Веб"
🏽 Карантин 🌣 Конфигурация 🏿 🖉 Шаблоны	МаіЮ запущен
Базовые настройки Карантин Подключаемые п	чодули Правила Ядро Отчеты Прием почты
Отправка почты Ітар Рор3 Ргоху	
▼ Общие	
CallbackPoolOptions Текущие значения: auto minimum minimum minimum c minimum c maximum c ma	Дополнительные параметры пула потоков, обрабатывающих сигналы от drweb-maild об окончании обработки письма.
ListenAddress inet:5110@0.0.0.0 ×	Список адресов сокетов, на которых следует ожидать подключений клиентов. подробнее
ClientTLSSettings	Настройки SSL/TLS для клиентской части РОРЗ протокола. подробнее
ServerTLSSettings	Настройки TLS/SSL для серверной части РОРЗ протокола. подробнее
ServerAddress inet:pop3@127.0.0.1 ×	Адрес, по которому следует подключаться к серверу РОРЗ.
OnFilterErrors Основное действие отклонить 💌	Действие, применяемое к письму при ошибке, возникшей до отправки письма модулю drweb-maild. подробнее

Предпросмотр Сохранить Применить и сохранить изменения

При необходимости проверки писем, передаваемых по протоколам POP3S/IMAP4S, необходимо настроить параметры ServerTLSSettings и ClientTLSSettings, задающие настройки серверной и клиентской части протоколов. Настройки задаются через запятую. Использование серверной части возможно, только если заданы сертификат (certificate) и закрытый ключ (private\_key\_file). Пример вида настроек для обоих параметров: use\_sslv2 no, private\_key\_file \_путь\_до\_ключа, certificate \_путь\_до\_сертификата.

На этой же вкладке в разделе Advanced можно задать ограничения. В том числе:

- Запрет клиенту передачи имени и пароля в незашифрованном виде (DisablePlainText использование данного параметра возможно при настроенном SSL). Настройка доступна только для протокола Imap.
- Обрывать соединение, если с одного IP приходит слишком много запросов на подключение, не возвращая клиенту сообщение о причине ошибки (Dos\_Blackhole). Настройка доступна только для протокола Imap.



- Максимальное количество входящих соединений и максимальное общее количество одновременных подключений с одного адреса (MaxConnections и MaxConnectionsPerlp). При значении, равном 0, ограничений нет.
- Максимально допустимое время обработки письма модулем и максимальное время ожидания для любых операций ввода и вывода с сокетом клиента для уже начавшейся операции (ProcessingTimeout и IoTimeout).

Применить сделанные изменения можно, нажав находящуюся внизу страницы кнопку **Применить** и сохранить изменения.

# 4.2.3. 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 выбрать пункт Dr.Web консоль для почтовых серверов UNIX в меню Службы и перейти на закладку Подключаемые модули, находящуюся в меню Конфигурация, открыть Антивирус и выставить необходимые значения для параметров Infected (инфицированные файлы), Suspicious (подозрительные), Incurable (неизлечимые) и т. д.

Предлагаемый список действий различается для вредоносных программ различного типа. Так, для вирусов на выбор предлагаются действия **Лечить** (Cure), **Удалять** (Remove), **Отклонить** (Reject — заблокировать отправку письма и вернуть ошибку клиенту), **Отклонить без уведомления** (Discard — блокировать отправку письма, но вернуть код успеха клиенту). 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 — перемести в карантин), **Информировать** (Notify), **Перенаправить** (Redirect), **Добавить заголовок**, **Добавить счет**. Для добавления дополнительного действия в список действий необходимо нажать на кнопку . его удаления из списка — Х. В отличие от основного действия, которое может быть только одно, и оно должно быть указано в списке действий конфигурационного файла первым, дополнительных может

быть несколько.

Применить сделанные изменения можно, нажав находящуюся внизу страницы кнопку Применить и сохранить изменения.



😹 Карантин 🔅 Конфигурация 📝 Шаблоны	🕨 🚺 MailD запущен
Базовые настройки Карантин Подключаемые м	одули Правила Ядро Отчеты Прием почты
Отправка почты Ітар Рор3 Ргоху	
Антиспам Фильтрация по заголовкам Антивирус	Фильтрация по элементам письма
• Основные	
Address	Сокет, через который антивирусный плагин взаимодействует с демоном drwebd.
pid:/var/drweb/run/drwebd.pid 🎽	подроонее
<b></b>	
Iimeout 30 секунд 💌	Максимальное время ожидания исполнения команды демоном drwebd. подробнее
HeuristicAnalysis	Настройка работы звристического анализатора. подробнее
AddXHeaders	Добавление заголовков X-Antivirus и X-Antivirus-Code к проверенным демоном drwebd сообщениям.
	подробнее
Paranoid	Настройка "параноидального" режима сканирования.
Нет	подроонее
RegexsForCheckedFilename	Список регулярных выражений, используемых плагином при проверке
	имён файлов в отчёте, присылаемом демоном drwebd после сканирования сообщения.
LicenseLimit	Действие, применяемое к сообщениям, которые не были проверены демоном drwebd по причине окончания срока действия лицензии.
Дополнительные действия	подробнее
нарантин	
<ul> <li>перенаправить</li> </ul>	
информировать	
+ добавить заголовок	
Infected	Действие, совершаемое с сообщениями, заражёнными известными
Основное действие лечить	вирусами. подробнее
карантин информировать	
на перенаправить	
• добавить заголовок	
Suspicious	Действие, совершаемое с сообщениями, которые могут быть заражены
Основное действие отклонить	неизвестным вирусом. подробнее
карантин 🔪 информировать 🔨	
теренаправить	
<ul> <li>добавить заголовок</li> <li>добавить счет</li> </ul>	

Система фильтрации по умолчанию добавляет в служебный заголовок информацию о проверке. Если необходимо модифицировать только те письма, которые являются спамом, а остальные пропускать без изменений, необходимо использовать параметры AddXHeaders, AddVersionHeader, AddXDrwebSpamStateNumHeader и AddXSpamLevel, установив их значение в no.



### 4.2.4. 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 выбрать пункт Dr.Web консоль для почтовых серверов UNIX в меню Службы и перейти на закладку Подключаемые модули, находящуюся в меню Конфигурация, открыть Антиспам и выставить необходимое значение для параметра Action. Для большинства случаев достаточно использовать значения Пропустить (Pass) или Отклонить без уведомления (discard). 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'y).

Система фильтрации по умолчанию 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 SubjectPrefix.

Если необходимо модифицировать только те письма, которые являются спамом, а остальные пропускать без изменений, необходимо использовать параметры AddXHeaders, AddVersionHeader, AddXDrwebSpamStateNumHeader и AddXSpamLevel, установив их значение в no.

В том случае, если необходимо задать различные действия над письмом в зависимости от того, насколько мы уверены, что письмо является спамом, можно использовать настройку UnconditionalAction. Например, для UnconditionalAction можно задать немедленное удаление письма, а для Action — сохранение в карантин и возвращение временной ошибки.

Применить сделанные изменения можно, нажав находящуюся внизу страницы кнопку Применить и сохранить изменения.

💽 Карантин 🏟 Конфигурация 📝 Шаблоны	NailD запущен
Базовые настройки Карантин Подключаемые мо Отправка почты Imap Рор3 Ргоху	дули Правила Ядро Отчеты Прием почты
Антиспам Фильтрация по заголовкам Антивирус	Фильтрация по элементам письма
• Основные	
FullCheck Да	Производится полная проверка сообщения на наличие спама. подробнее
NoHamFrom Да	Ипорировать встроенные ham-домены. подробнее
AddVersionHeader Her 💌	Добавление к сообщению заголовка X-Drweb-SpamVersion, содержащего информацию о версии платина VadeRetro.
AddXDrwebSpamStateNumHeader Her	Добавление к сообщению заголовка X-Drweb-SpamState-Num. подробнее
AddXSpamLevel Her	Добавление к сообщению заголовка X-Spam-Level, состоящего из символов "**". подробнее
AddXHeaders	Добавление к сообщению заголовков X-Drweb-SpamState и X-Drweb- SpamScore. подробнее
CheckDelivery Her	Возможность отдельной фильтрации уведомлений о доставке сообщений.
SubjectPrefix "[SPAM] "	Префикс, добавляемый к теме сообщения, если оно отмечено как спам. подробнее



NotifySubjectPrefix	Префикс, добавляемый к теме сообщения, если оно является уведомлением о невозможности доставки (и, соответственно, определено в 3 класс писем библиотекой VadeRetro).	
UnconditionalSpamThreshold 1000	Если оценка, полученная письмом, равна значению данного пара превышает его, письмо считается безусловным спамом.	метра или подробнее
UnconditionalSubjectPrefix "[SPAM] "	Префикс, добавляемый к теме сообщения, если оно отмечено ка безусловный спам.	к подробнее
SpamThreshold 100	Если оценка, полученная письмом, равна значению данного пара превышает его, письмо считается спамом.	метра или подробнее
UnconditionalAction Основное действие пропустить Дополнительные действия	Действие, совершаемое с безусловным спамом.	подробнее
<ul> <li>карантин</li> <li>перенаправить</li> <li>добавить заголовок</li> </ul>		
Action Основное действие пропустить 💌 Дополнительные действия	Действие, совершаемое со спамом.	подробнее
<ul> <li>карантин</li> <li>перенаправить</li> <li>добавить заголовок</li> </ul>		
NotifyAction Основное действие пропустить Дополнительные действия	Действие, совершаемое с письмом, если оно является уведомл невозможности доставки.	ением о подробнее
+ карантин       + перенаправить       - добавить заголовок		
SpamCustomReply "Dr.WEB vaderetro plu]	Настраиваемое сообщение в SMTP сессии для случаев, когда выполняется действие Action, UnconditionalAction, NotifyAction = r также если UseCustomReply = yes.	eject, а подробнее
WhiteList	Белый список отправителей.	подробнее
<ul> <li>Префикс: другое значение</li> <li>Значение:</li> </ul>		
BlackList	Черный список отправителей.	подробнее
Префикс: другое значение     Значение:		

Также на этой странице:

- С помощью параметров SubjectPrefix и/или UnconditionalSubjectPrefix можно задать префикс, добавляемый к теме письма, являющегося вероятно спамом и безусловно спамом. Модификацию темы можно использовать, если в качестве действия выбрано pass.
- С помощью параметров SpamThreshold и UnconditionalSpamThreshold можно задать уровни срабатывания как для вероятно спама, так и для безусловно спама.



Внимание! Письма, получившие оценку, превышающую порог UnconditionalSpamThreshold, относятся к системой к безусловному спаму, а письма, имеющие оценку между UnconditionalSpamThreshold и SpamThreshold, — к вероятному спаму.

В первом случае к письмам применяются действия, указанные в параметрах UncoditionalAction и UnconditionalSubjectPrefix, во втором — Action и SubjectPrefix. В связи с этим значение UnconditionalSpamThreshold должно быть больше SpamThreshold.

#### 4.2.5. Управление черными и белыми списками отправителей

Задать черные и белые списки отправителей можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

Для настройки через веб-интерфейс необходимо выбрать пункт Dr.Web консоль для почтовых серверов UNIX (Dr.Web Console for Unix mail Servers) в меню Службы (Servers) и перейти на закладку Подключаемые модули (Plugins), находящуюся в меню Конфигурация (Configurations), открыть Антиспам (Anti-spam) и заполнить списки для параметров WhiteList и BlackList, используя для добавления кнопку . При вводе допустимо использование как шаблонов адресов (например, для того, чтобы добавить в список все адреса, принадлежащие конкретному домену, достаточно указать символ \* вместо имени пользователя: \*@mycompany.com), так и путей к файлам со списками таких адресов. В последнем случае для параметра Prefix нужно выбрать значение file.

Применить сделанные изменения можно, нажав находящуюся внизу страницы кнопку **Применить и** сохранить изменения (Apply and Save Settings).

В ходе фильтрации адреса отправителей получаются из поля **From** в теле письма. Если тело письма не будет содержать полей **From**, либо, если перед полем **From** в теле письма будет стоять одна или несколько пустых строк, — то поиск отправителя в соответствующем списке производиться не будет. Если в теле содержатся два поля **From**, то адрес будет взят из первого найденного поля.

Внимание! Для уменьшения нагрузки на почтовый сервер можно всех получателей письма, идущего из защищаемой сети, заносить во временный белый список, используя параметры FromProtectedNetworkScoreAdd, UseReplyCache, ProtectedNetworkReplyCacheLifeTime и ReplyToProtectedNetworkScoreAdd.



#### 4.2.6. Настройка параметров отчетов

Настройка параметров получения отчетов выполняется на странице Отчеты меню Конфигурация.

🍺 Карантин	н 🔅 Конфигура	ация 📝 Шаблоны					MailD запуще	эн
Базовые настройки Отправка почты	Карантин Imap Pop3	Подключаемые Ргоху	модули	Правила	Ядро	Отчет	ы Пр	ием почты
▼ Основные		_						
Send Да 🔽			Отсылка	отчетов.				
SendTimes 00:00:00			График с	тправки отчётов				подробнее
Mail			Адрес(а)	і, на который(ые)	высылаютс	я отчеты.		подробнее
Names			Список п	лагинов, для кото	орых создае	тся отчет.		подробнее
<b>TopListSize</b> 20			Показ в і которых	отчете списков ч присылается наи	асто блокир юбольшее ко.	уемых объе личество бл	ктов и адрес юкируемых с	сов, с объектов. подробнее
MaxStoreInDbPeriod 31	дней 💌		Максима	льное время хра	нения стати	істики в баз	е отчетов.	подробнее
AdminMail postmaster@localhost	ę		Адрес си	істемного админи	истратора.			подробнее
FilterMail DrWEB-MAIL-DAEMO	Ą		Адрес, у	казываемый в за	головке Fror	п писем с о	гчетами.	
NotifyLangs en × ru ×			Язык(и), и	іспользуемые прі	и формирова	ании отчето	В.	
ia ₽								
<ul> <li>Дополнительные</li> </ul>								

Предпросмотр Сохранить Применить и сохранить изменения

Ha данной странице рекомендуется настроить время отправки отчетов (параметр SendTimes), указать адреса, на которые должны будут отправляться отчеты (параметр Mail; по умолчанию в системе доступны два адреса — mailbox1@drweb.test и mailbox2@drweb.test), задать адрес системного администратора (параметр AdminMail) и язык отчетов (параметр NotifyLangs). Для добавления языка в список необходимо нажать на кнопку

Размеры списков с наиболее частыми угрозами, отправителями и IP-адресами, включенными в отчет, настраиваются с помощью параметра TopListSize. С помощью параметра Names можно указать плагины, информация о работе которых будет включена в отчет. Порядок настройки шаблона отчета описан в документации.

#### 4.2.7. Настройка параметров журналов

Настройка подробности журналов отчетов осуществляется с помощью параметров Level и IPCLevel страницы Отчеты (Logging). Так, для установки отладочного режима нужно указать значение debug. При необходимости значение debug можно указать также для параметров RulesLogLevel и TemplatesParserLogLevel в страницах Notifier и Maild.

#### 4.2.8. Управление карантином

Карантин может быть создан как в файловой системе, так и в DBI-хранилище.

В карантине, созданном в файловой системе, 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 главной странице Карантина представлен список писем с указанием имени отфильтровавшего их плагина, идентификатора сообщения в базе данных, даты получения, адреса отправителя и получателя, темы письма и его размера.

Наименование сообщений в карантине контролируется параметрами FilenamesMode и FilenamesPrefix страницы Quarantine меню Configuration.

Права доступа к сохраненным файлам определяются параметром FilesMode страницы Quarantine меню Configuration.

Для просмотра карантина необходимо выбрать пункт **Dr.Web консоль для почтовых серверов** и щелкнуть по меню **Карантин**.

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



	headersfilter	15.03.2009 13:41	user@domain.com	user2@appliancetest	2097 Bytes		
M	headersfilter	15.03.2009	user@domain.com	user2@applancetest	2097 Bytes		
	П неа Отправить письма оригинальным получателям? Х						
	hea → C Bce	го сообщений	выбозно: 2		2097 Bytes		
	□ hea Вы действительно хотите отправить выбранные письма ?						
N	V drv						
	drv 0000005	13:40			2097 Bytes		
	drweb	15.03.2009 13:40	user@domain.com	user2@applancetest	2097 Bytes		
	drweb	15.03.2009 13:40	user@domain.com	user2@applancetest	2097 Bytes		

Карантин, организованный в файловой системе, можно ограничивать по времени хранения сообщений, размеру и числу сохраненных сообщений. Карантин, организованный в DBI-хранилище, можно ограничивать только по времени хранения сообщений в нем. Время хранения писем в карантине задается параметром StoredTime, задаваемом на закладке Карантин меню Конфигурация.



😹 Карантин 🔅 Конфигурация 📝 Шаблоне	1			MailD	запущен	
Базовые настройки Карантин Подключаемы Отправка почты Imap РорЗ Ргоху	ые модули	Правила	Ядро	Отчеты	Приег	м почты
▼ Основные						
AccessByEmail Да •	Запрос на г специальны	толучение писе ых управляющи	м, сохраненн іх писем.	ных в карантине	, через оті	правление подробнее
StoredTime 24 Yacob	Время хран	ения письма в	карантине.			подробнее
MaxSize О б 💌	Общий мак	симальный раз	мер сообщен	ий в карантине.		подробнее
MaxNumber 0	Максималь	ное число сооб	щений в кара	антине.		подробнее
MoveToDBI Her 💌	Перемещен DBI-хранил	ие писем, сохр ище.	аненных в ка	арантине, из фай	ілового хр	анилища в подробнее
MoveAll Her 💌	Перемещен /def/backup	ие всей входя "для архивиро	щей почты ск вания.	разу в директор	110 Quarant	ine/Path+" подробнее
Настройки хранилища						
Дополнительные						
Предпросмотр Сохранить Применить и сохранить изв	енения					

Системный администратор также может работать с карантином через drweb-qcontrol и интерфейс интерактивного управления.



#### 4.2.8.1. Обработка писем с помощью управляющих писем

Доступ к карантину можно получить через специальные управляющие письма, которые в поле **Subject** содержат команды, которые надо выполнить. Получив такое письмо, администратор имеет возможность получения заблокированного письма из карантина.

Для получения писем нужно поставить значение параметра AccessByEmail, задаваемого на закладке Карантин меню Конфигурация, в Yes.

💽 Карантин 🔅 К	онфигурация 📝 Шаблоны	▶ 88	MailD запущен
Базовые настройки Кара	антин Подключаемые модули П	равила Ядро Отчет	ъ Прием почты
Отправка почты Imap	Рор3 Ргоху		
▼ Основные			
AccessByEmail	Запрос на пол специальных *	јучение писем, сохраненных в кара управляющих писем.	нтине, через отправление
			подробнее
StoredTime	Время хранен	ия письма в карантине.	поллобнее
24 часов	•		подробнее
MaxSize	Общий максим	иальный размер сообщений в каран	тине. полробнее
MaxNumber	Максимальное	з число сооощении в карантине.	подробнее
MausTaDPI	Перемешение	RUCAM COVIDUALIUS P VORGUTINA	42 файлового уранилища в
Her	DBI-хранилище	писсии, сохранстных в карантинс, т 8.	ю факловото хранилища в
			подробнее
MoveAll	Геремещение /def/backup" дл	всеи входящеи почты сразу в дире ля архивирования.	екторию Quarantine/Path+"
			подробнее
<ul> <li>ปอดของมีของหลายและ</li> </ul>			
р пастрояки хранилища			
▶ Дополнительные			
Предпросмотр Сохранить	Применить и сохранить изменения		

Управляющее письмо может автоматически генерироваться сервисом при нажатии соответствующей ссылки в отчетах, высылаемых при помещении того или иного сообщения в карантин.

Письма будут отправляться на адрес, заданный значением параметра FilterMail на закладке Отчеты меню Конфигурация, либо в локальных правилах для данного письма.

Получаемые письма имеют следующий вид:

От: Дата: Кому: Тема:	DrWeb-MaiD 6 ноября 2009 г. 16:12 mailbox1@drweb.test Report from Dr.Web MailD per period of 05.11.09 16:12:39 - 06.11.09	16:12:38
	Защита почтовых серверов Dr.Web® for Unix mail servers	www.drweb.com
	MailD: отчет за период 05.11.09 16:12	2:39 - 06.11.09 16:12:38
	Плагин vaderetro	
	Пропущено:	З (6.57 КБ)
	Отказано:	0 (0 байт)
	Отклонено:	0 (0 байт)
	Временно отклонено:	0 (0 байт)
	Перемещено в карантин:	0 (0 байт)
	Перенаправлено:	0 (0 байт)
	Выслано отчетов:	0 (0 байт)
	~~ ·	a / c = 2 (c)



Если в качестве дополнительного действия выбрано уведомление о его блокировке (notify) и AccessByEmail выставлен в Yes, то в уведомлении, которое получит пользователь, будет содержаться ссылка, которая позволит самому пользователю получить сохраненное в карантине письмо.

**Внимание!** Так как о спаме, сохраненном в карантине, уведомления не высылаются, то этим способом спам из карантина получить нельзя.

#### 4.2.9. Архивирование и регистрация сообщений

Для резервного копирования всей проходящей почты в хранилище необходимо поставить значение параметра MoveAll, задаваемом на закладке Карантин меню Конфигурация, в Yes.

💽 Карантин 🌣 Конфигурация 🏼 🖉 Шаблоны	MailD запущен
Базовые настройки Карантин Подключаемые	модули Правила Ядро Отчеты Прием почты
Отправка почты Imap РорЗ Ргоху	
• Основные	
AccessBvEmail	Запрос на получение писем, сохраненных в карантине, через отправление
Да 💌	специальных управляющих писем.
	подроонее
StoredTime	Время хранения письма в карантине.
24 часов 💌	подробнее
MaxSize	Общий максимальный размер сообщений в карантине.
0 б 🔽	подробнее
MaxNumber	Максимальное число сообщений в карантине.
MoveloDBI	Перемещение писем, сохраненных в карантине, из фаилового хранилища в DBI-хранилище.
	подробнее
MoveAll	Перемещение всеи входящеи почты сразу в директорию Quarantine/Path+" /def/backup" для архивирования.
	подробнее
Настройки хранилища	
▶ Дополнительные	
Предпросмотр Сохранить Применить и сохранить измени	ения

**Внимание!** В связи с большим количеством проходящей почты рекомендуется перемещать ее в специальное хранилище. Настройка параметров хранилища подробно описана в документации.

A A A	Dr	.WEB	) ых серверов UNIX		Вер Версия веб-ин	сия Dr.Web MailD: 5.0.0 перфейса Dr.Web: 5.0.0 © 2008 Doctor Web
	💌 к	арантин 🔅 К	онфигурация 📝 Шаблонь			🕨 📕 MailD запущен
<b>v</b> 4	рильтр					
Кат	алог: Все Эильтровать		• От:	Кому:	Дата:	
	Письма в кара	нтине 💢	Удалить 🔀 Не спан	м 🕎 Сообщить о спаме	🟹 Отправить получателям 🙋	🔾 Переслать Вложением
	ID	Дата	От	Кому	Тема	Размер
	backup → 00000005.	2009/11/06 16:28	mailbox1@drweb.test	mailbox2@drweb.test	test as	01856 Bytes
	$backup \rightarrow$	2009/11/06 16:27	mailbox1@drweb.test	mailbox2@drweb.test	test as	1891 Bytes



#### 4.2.10. Интерактивное управление сервисом

Интерактивное управление позволяет производить тонкую настройку продукта, используя прямое подключение к нему. С помощью интерактивного управления можно:

- работать с текущей накопленной статистикой;
- работать с пользователями и группами;
- работать с внутренним карантином;
- управлять сообщениями, сохраненными во внутренней БД;
- управлять внутренней БД и очередями;
- получать текущие активные настройки;
- форсировать отправку отчетов;
- проверять генерацию уведомлений из шаблонов;
- и т. д.

Для включения модуля интерактивного управления необходимо включить параметр Control на закладке Ядро в Yes и перезапустить сервис командой /etc/rc.d/init.d/drweb-monitor restart.

Для управления сервисом необходимо подключиться к адресу, указанному в параметре ControlAdress на той же закладке. Также drweb-maild всегда открывает unix-coket по адресу /var/drweb/ipc/.ctl.



# >

Так, например, чтобы послать отчеты, необходимо ввести команду send-report.

send-report
success send report from 2009-Nov-05 16:12:38 date to Client.
> send-report
success send report from 20101228T084625 date to Client.

Полный список команд приводится в документации.



### 4.3. Управление защитой почтовых сервисов под ОС UNIX из Центра управления Dr.Web Enterprise Security Suite

# 4.3.1. Подключение почтового сервиса к Центру управления Dr.Web Enterprise Security Suite

Подключить почтовый сервер к Центру управления можно, создав учетную запись на сервере автоматически или вручную. Ниже будет рассмотрено автоматическое подключение.

Для запуска установленного продукта **Dr.Web Mail Gateway** в режиме **Enterprise** необходимо вручную внести изменения в локальные конфигурационные файлы компонентов **Агент** и **Монитор**. Для этого:

Зайдите на сервер, на котором установлен почтовый сервис (например, с помощью утилиты putty).

Откройте для редактирования (например, с помощью редактора vi) файл /etc/drweb/agent.conf и отредактируйте параметры UseEnterpriseMode и PublicKeyFile. Параметр PublicKeyFile должен указывать путь к файлу drwcsd.pub, созданному в процессе инсталляции сервера Enterprise Suite. В том случае, если сервис проверки почты развернут на одном сервере с Enterprise Suite, в данном параметре можно указать путь к месторасположению данного файла; в том случае, если сервисы расположены на разных серверах, файл необходимо скопировать:

UseEnterpriseMode = Yes;

PublicKeyFile = /opt/drwcs/Installer/drwcsd.pub

Параметры ServerHost и ServerPort должны содержать соответственно IP-адрес или имя хоста сервера Dr.Web Enterprise Security Suite и номер порта этого сервера (по умолчанию 2193). Если сервис проверки почты развернут на сервере Dr.Web Enterprise Security Suite, то можно оставить значения по умолчанию:

ServerHost = 127.0.0.1

```
ServerPort = 2193
```



Аналогичным способом откройте для редактирования файл /etc/drweb/monitor.conf и установите UseEnterpriseMode = Yes.

Значения ENABLE в файлах /etc/drweb/drwebd.enable и /etc/drweb/drweb-monitor.enable должны быть установлены в 1.

Перезапустите сервис:

/etc/init.d/drweb-monitor start

После подключения сервер Dr.Web Enterprise Security Suite автоматически не импортирует настройки подключенных компонентов. Если в эти настройки были внесены какие-либо изменения — их необходимо экспортировать на сервер с использованием параметра командной строки – export-config (или – e) с обязательным указанием названия компонента (DAEMON, MAILD):

/opt/drweb/drweb-agent -exportconfig MAILD



Внимание! При первом запуске в режиме Enterprise агент запрашивает регистрационные данные (идентификатор станции и пароль) у сервера Dr.Web Enterprise Security Suite. Если в Dr.Web Enterprise Security Suite установлен режим Ручное подтверждение доступа, действующий по умолчанию, то администратору в течение одной минуты с момента запроса необходимо подтвердить регистрацию новой станции через веб-интерфейс администратора Центра управления Dr.Web Enterprise Security Suite. Для подтверждения выберите пункт Неподтвержденные станции в меню Администрирование, отметьте интегрируемый сервер и нажмите на значок мили ими мено.

Через веб-интерфейс Центра управления можно управлять настройкой конфигурации компонентов Dr.Web Mail Daemon и Dr.Web Daemon (антивирусного модуля, входящего в базовый пакет Dr.Web). При запуске какого-либо из компонентов Агент запрашивает конфигурацию с сервера Dr.Web Enterprise Security Suite.

<ul> <li>Выбранные объекты</li> </ul>					đề 🖑 🌾 🕴	👌 🔁 👘 Сохранить
Общие	Станция имеет настройки, за	даные персонально для ст	танции			
• Графики			Общие			
• Свойства						
Таблицы	Общие FlyTrap DrWeb	Фильтр по заголовкам 🛛 Ұа	adeRetro Mod	lifier		
• Инфекции						
• Ошибки	Address	pid:/var/drweb/run/drwebc	d.pid			
• Статистика	Timeout	30s		•	<b>•</b>	
• Запуск/завершение						
• Вирусы	<ul> <li>HeuristicAnalysis</li> </ul>			•	•	
• Состояние	AddXHeaders			<b>•</b>	<b>*</b>	
• Задания						
<ul> <li>Суммарная статистика</li> </ul>	LocalScan			•	<b>•</b>	
• Вирусные базы	Parapoid			•	<b>•</b>	
• Модули						
<ul> <li>Все сетевые инсталяции</li> </ul>	RegexsForCheckedFilename			•	<b>*</b>	
Конфигурация	Licensel imit			<b>•</b>	<b>6</b>	
• Расписание		pass				
• Почтовые адреса	Infected	cure,quarantine		<b>•</b>	<b>*</b>	
Dr.Web® Mail Daemon для Linux	Suspicious				<u>_</u>	
• Dr.Web® Daemon для Linux	Juspicious	reject,quarantine,notify		<b></b>		

Для сохранения введенных параметров необходимо нажать кнопку Сохранить.

#### 4.3.2. Настройка запуска почтового сервиса из Центра управления Dr.Web Enterprise Security Suite

Для запуска необходимо:

 через веб-интерфейс Центра управления Dr.Web Enterprise Security Suite в настройках Монитора компонентов Dr.Web для Unix установить флаги Daemon и Maild для запуска соответствующих компонентов комплекса.

<ul> <li>Выбранные объекты</li> </ul>		🦸 🖑 🖑 😤 🕤 🖻 .	Сохранить
Общие	Станция имеет настройки, заданые персонально для станции		
• Графики	Список запущенных приложений		
• Свойства • Запущенные компоненты	✓ Daemon		
Таблицы	🔽 Maild		
• Инфекции			
• Ошибки			
• Статистика			
• Запуск/завершение			
• Вирусы			
• Lостояние			
• Задания			
• Суммарная статистика			
• Вирусные базы			
• Модули			
<ul> <li>Все сетевые инсталяции</li> </ul>			
Конфигурация			
• Расписание			
• Почтовые адреса			
• Dr.Web® Mail Daemon для Linux			
• Dr.Web® Daemon для Linux			
• Монитор компонентов Dr.Web® для Unix	4		

Запустить сервис на локальной станции командой /etc/init.d/drweb-monitor start.

Проверить наличие сервиса можно командой ps ax.

12668 ?	Ssl	0:00 /opt/drweb/drweb-monitor.real -c /etc/drweb/monitor.c
12669 ?	Sl	0:00 /opt/drweb/drweb-agent.real -c /etc/drweb/agent.conf



#### 4.4. Проверка корректности настроек

Для проверки корректности настроек необходимо запустить в консоли модуль управления drwebmonitor с параметром check. Можно также проверить корректность настроек отдельных компонентов, но при этом обязательно должен быть запущен **Агент**.

**Внимание!** В режиме проверки drweb-monitor не может произвести абсолютно все проверки, так как он должен работать и при запущенном продукте. Поэтому продукт может не запускаться, хотя проверка настроек не покажет ошибок. Так, например, продукт может не запуститься из-за того, что компоненты могут не инициализировать прослушивания на сокетах.



## 5. Тестирование производительности

# 5.1. Тестирование производительности системы фильтрации почтового трафика

Для проведения тестирования кроме почтового сервера рекомендуется использовать дополнительно две рабочие станции Linux: для отправки потока сообщений и для их приема.

Для генерации и приема потока почтовых сообщений рекомендуется использовать пакет postal, содержащий две утилиты:

- 1. bhm для приема почты «в никуда» (т. е. реализующий smtp-сессию без сохранения где-либо принятого письма, что минимизирует влияние принимающего сервера на общую производительность системы тестирования). Данная утилита запускается с указанием адреса (интерфейса) и порта на принимающей машине.
- 2. postal для отправки автоматически генерируемого потока сообщений с заданными параметрами (размером сообщения и списком параллельных потоков сообщений) по списку адресов. Данная утилита запускается вручную на отсылающей машине с указанием длительности теста, количества одновременных потоков, диапазона размеров сообщений, списка получателей, IP-адреса и порта, на который нужно производить отсылку. В качестве адреса получателя указывается адрес почтового сервера. Как правило, размер писем находится в диапазоне 1–10 КБ, поэтому рекомендуется для тестирования задавать диапазон 3–5 КБ.

Перед началом тестирования необходимо произвести следующие изменения:

- 1. Задать адрес принимающей машины в конфигурационных настройках вашего почтового сервера.
- 2. Установить правило обработки найденного спама в значение Pass (пропускать). Настройку правил обработки спама можно произвести через веб-интерфейс. Для этого необходимо выбрать пункт Dr.Web консоль для почтовых серверов, перейти на закладку Плагины, открыть vaderetro и выставить значение Pass для параметра Action. Применить сделанные изменения, нажав кнопку Сохранить и применить изменения.
- 3. Перезапустить сервис фильтрации почтового трафика с помощью команды /etc/init.d/drweb-monitor restart.

Пример запуска postal на запускающей машине:

Postal -t 10 -m 1 -M 1 -r 1200 192.168.1.100 ./user\_url\_list

Выводимые значения покажут время, количество и объем переданных сообщений, количество возникших ошибок.

**Внимание!** Особенностью работы команды postal является то, что в течение первой минуты работы выводимые значения производительности не являются достоверными. В качестве достоверных значений необходимо использовать данные по работе, начиная со второй минуты.

Следить за загрузкой процессора почтового сервера можно через команду top, зайдя на сервер локально либо по ssh.

**Внимание!** Отправляющая и принимающая машины не должны самостоятельно проверять тестируемый почтовый поток. В том случае, если на эти машины была установлена защита от спама, ее необходимо отключить.

**Внимание!** По особому запросу может быть предоставлена доработанная версия утилиты postal, позволяющая проводить более детальное тестирование, в частности формировать письма.

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



# 5.2. Тестирование функционирования системы фильтрации почтового трафика

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

Перед началом тестирования на почтовом сервере необходимо произвести следующие изменения:

- 1. Задать адрес принимающей машины в конфигурационных настройках вашего почтового сервера.
- 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 **Dr.Web консоль для почтовых серверов**, перейти на закладку **Отчеты** и прописать адрес для параметра AdminMail. Применить сделанные изменения, нажав кнопку **Сохранить и применить изменения**.

🏾 Карантин 🌣 Конфигурация 📝 Шаблоны	MailD запущен
Базовые настройки Карантин Подключаемые м	одули Правила Ядро Отчеты Прием почты
Отправка почты Ітар Рор3 Ргоху	
▼ Основные	
Send	Отсылка отчетов.
SendTimes	График отправки отчётов.
00:00:00	подробнее
Mail	& nper(a) และเอาอาจได้(เมe) เรมเวมเสียวากๆ อานุครม
	подробнее
Names	Список плагинов, для которых создается отчет. подробнее
TopListSize	Показ в отчете списков часто блокируемых объектов и адресов, с которых присывается наибовышее количество блокируемых объектов
	которых присылается наибольшее количеет во олокируемых объектов. подробнее
MayStoralpDbBariad	Максимальное время уранения статистики в Безе отнетов
31 дней 💌	подробнее
AdminMail	Адрес системного администратора. подробнее
postmaster@localhost	
FilterMail	Адрес, указываемый в заголовке From писем с отчетами.

Для редактирования конфигурационных файлов необходимо зайти на сервер (локально или по ssh) и отредактировать файл /etc/drweb/maild\_smtp.conf. В данном файле необходимо секции [Notifier] для параметра AdminMail прописать адрес, по которому будут приходить уведомления. После завершения редактирования необходимо 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). Приведем пример отправки письма с тестовым вирусом с операционной системы Linux.

```
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:

file_with_viruses	— файл с вложенными вирусами
root@localhost	— адрес, от кого придет сообщение
192.168.1.100	— адрес почтового сервера, через который отправляется сообщение
toaddress	— адрес, на который должно прийти тестовое сообщение

Для тестирования работы антиспама необходимо отправить письмо, содержащее в теле письма 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.

Рекомендуемое время тестирования: 60 минут с учетом установки и настройки необходимых утилит, сбора и формирования тестового набора файлов.

Если вы используете для тестирования операционную систему типа Windows, то для тестирования сервиса защиты почты можно использовать установленный по умолчанию почтовый клиент Outlook Express. В предоставленной для тестирования системе заведены два почтовых ящика — mailbox1 и mailbox2. Пароль доступа — qwerty. Для добавления почтового ящика в Outlook Express необходимо:

Выбрать пункт Internet Accounts в меню Tools.

Нажать кнопку Add и выбрать Mail.

Ввести имя почтового ящика, например mailbox1, и почтовый адрес, например mailbox1@drweb.test.



	Outlook Express			
1	Internet Connection Wizard	12	×	n
	Your Name	×.		
Ľ	When you send e-mail, your i	name will appear in the From field of the outgoing message.		
F	Type your name as you woul	d like it to appear.		Go to msn 🖉 🖻
Ľ				
[	<u>.</u> Display name:	nailbox1	Find a Me	ssage Identities <del>-</del>
	F	or example: John Smith		Tin of the day of
				The or the day ~
				To quickly locate certain messages, click Find on
			In TUPOX	the toolbar. Type in what
				name in From or a word
				in Subject.
			54	
		(Rock Next) Cancel	1	
			]	
ľ	Toptacts 🔻 🛛 🗙			
Ľ,		Lontacts		
	on Contacts to create a new contact.	19 <b>0</b>		
		B2 Open the Address Book	Comments of	
		Find People		
L		$\square$ When Cutlook Express starts, go directly to my I	nbox.	Previous     Next
			具 Working Online	🕄 No new messages 🛛 🖉
1000				
5	Autlank Express			_ 🗆 ×
5	Internet Connection Wizard	×	3	_ D ×
	1 Dutlook Express Internet Connection Wizard Internet E-mail Address	×	J	_ I I ×
	Tutlook Express Internet Connection Wizard Internet E-mail Address	×		
	Outlook Express Internet Connection Wizard Internet E-mail Address Your e-mail address is the ad	Fress other people use to send e-mail messages to you.		X
	Outbook Express Internet Connection Wizard Internet E-mail Address Your e-mail address is the ad	ress other people use to send e-mail messages to you.		Go to <b>msi</b> 🎤
	Outbook Express Internet Connection Wizard Internet E-mail Address Your e-mail address is the ad	Iress other people use to send e-mail messages to you.		Go to msn 🖉
	Outbook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address <u>E</u> -mail address:	Iress other people use to send e-mail messages to you.	C Find a Me	Go to msile -
	Outbook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address           E-mail address:           R	Iress other people use to send e-mail messages to you.	Eind a Met	Go to msile -
	Outbook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address           E-mail address:           r           For	Itess other people use to send e-mail messages to you.	Eind a Mee	Go to msile Ssage Ident ties - Tip of the day ×
	Outbook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address           E-mail address:           r           Free	Itess other people use to send e-mail messages to you. nailbox1@drweb.test r example: someone@microsoft.com	Eind a Mes	Go to msile A
	Outlook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address           E-mail address:           r           Fr	ע tress other people use to send e-mail messages to you. nailbox1@drweb.test ווווווווווווווווווווווווווווווווווו	S Eind a Mee	Go to msn 2 Go to msn 2 SS age Ident files ~ Tip of the day × To quickly locate certain messages, click Find on the toolbar, Typs in what to look for, such as a
	Dutlook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address           E-mail address:           Fr	עליג tress other people use to send e-mail messages to you. nailbox1@drweb.test ור example: someone@microsoft.com	Eind a Mee	Go to msn 2 Go to msn 2 Ssage Idont tios - Tip of the day × To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	Dutlook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address           E-mail address:           T           Free	tress other people use to send e-mail messages to you.	Eind a Mea	Go to msn 2 2 So to
	Dutlook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address <u>E</u> -mail address:	Itess other people use to send e-mail messages to you.	Eind a Mea r Inbox	Go to msi X > So to msi X > Tip of the day × To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	Entronk Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address <u>E</u> -mail address: <u>F</u>	If ess other people use to send e-mail messages to you.	Find a Me	Go to msi X Seage Identifies - Tip of the day × To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	Dutlook Express           Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address:           E-mail address:           Fr	Itess other people use to send e-mail messages to you. hailbox1@drweb.tesf rexample: someone@microsoft.com	Tinbox	Go to meril a second se
	Internet Connection Wizard           Internet E-mail Address           Your e-mail address is the address:           E-mail address:           Fr	tress other people use to send e-mail messages to you. nailbox1@drweb.test or example: someone@microsoft.com	Eind Mer	Go to merit Figure 1 and the set Tip of the day × To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	Internet Connection Wizard Internet E-mail Address Your e-mail address is the address: E-mail address: Fr products	tress other people use to send e-mail messages to you.          valibox1@drweb.test         or example: someone@microsoft.com         < Back	C Find Me	Go to msile Tip of the day × To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	Internet Connection Wizard Internet E-mail Address Your e-mail address is the address is the address: E-mail address: Fr products There are no contacts to display. Click	tress other people use to send e-mail messages to you.          nailbox1@drweb.test         or example: someone@microsoft.com         < Back	S Find Mee	Go to msile Tip of the day × To quickly locate certain messages, click Find on the toolbar. Typa in what to look for, such as a name in From or a word in Subject.
	Internet Connection Wizard         Internet E-mail Address         Your e-mail address is the address         E-mail address:         mail address:         mail address:         mail address:         mail address:         mail address:         mail address:         Your e-mail address:         Mail address:         Mail address:         Your e-mail address         Your e-mail addres	tress other people use to send e-mail messages to you.          valibox1@drweb.test         valibox1@drweb.test         or example: someone@microsoft.com         <	S Find Mee	Go to msile Tip of the day × To quickly locate certain messages, click Find on the toolbar. Typ in what to look for, such as a in Subject.
	Internet Connection Wizard         Internet E-mail Address         Your e-mail address is the address         E-mail address:         mail address:         m	tress other people use to send e-mail messages to you.          nailbox1@drweb.test         nailbox1@drweb.test         or example: someone@microsoft.com         < Back	S Find Mee	Go to ment Seage Idont tion - Tip of the day × To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	Internet Connection Wizard Internet E-mail Address Your e-mail address is the address E-mail address: Free internet = mail address: Free internet = mail address = x	tress other people use to send e-mail messages to you.          nailbox1@drweb.test         nailbox1@drweb.test         or example: someone@microsoft.com         Cancel         Contacts         Image: Contacts         Image: Eind People	C Eind a Mee	Go to msile Tip of the day × To quickly locate certain messages, dick Find on the bolbar. Type in what to look for, such as a name in From or a word in Subject.
	Internet Connection Wizard         Internet E-mail Address         Your e-mail address is the address         E-mail address:         products         Frequencies         pontacts         X         here are no contacts to display. Click in Contacts to create a new contact.	tress other people use to send e-mail messages to you.          hailbox1@drweb.test         hailbox1@drweb.test         prexample: someone@microsoft.com         Cancel         Contacts         Image: Contacts         Image: Eind People         When Cutlook Express starts, on directly to my Image: Someone Someo	Eind Mes	Go to msile Tip of the day × To quickly locate certain messages, click Find on the bolbar. Type in what to look for, such as a name in From or a word in Subject.
	Internet Connection Wizard         Internet E-mail Address         Your e-mail address is the address         E-mail address:         m         Free         internet F         with the second se	tress other people use to send e-mail messages to you.  nailbox1@drweb.test pr example: someone@microsoft.com  Contacts	Find Met	Go to ment Tip of the day × To quickly locate certain the toolbar. Type in what to look for, such as a name in From or a word in Subject.

Указать серверы для входящей и исходящей почты. В данном случае указывается адрес сервера, на котором была произведена установка. Тип сервера — IMAP.



S Outlook Express		-1	_ 🗆 ×
Internet Connection Wizard	×		2
E-mail Server Names	×.		
My incoming mail server is a	IMAP server.		Go to <b>msn</b> 🖂
C E <u>I</u> ncoming mail (POP3, IMAP or 192.168.100.27	HTTP) server:	<u>Find a Me</u>	ssage Identities –
An SMTP server is the server I Outgoing mail (SMTP) server: 192.168.100.27	that is used for your outgoing e-mail.	r Inbox	To quickly locate certain messages, click Find on the toolbar. Type in what to look for, such as a name in From or a word in Subject.
	< <u>B</u> ack <u>N</u> ext > Cancel		
Contacts ▼ X	Contacts		
on Contacts to create a new contact.	🕲 Open the Addres; Book		
	🕅 Find People		
	$\Box$ When Cutlook Express starts, go directly to my Ir	box.	A Previous     Next ▶     ✓
		🖳 Working Online	1.

В качестве пароля и логина доступа необходимо указать имя ящика и пароль gwerty.

nternet Mail Logon	
Type the account nam	ne and password your Internet service provider has given you.
Account name:	mailbox2
Password:	•••••
	✓ Remember password
If your Internet service p (SPA) to access your ma Authentication (SPA)' ch	rovider requires you to use Secure Password Authentication ail account, select the 'Log On Using Secure Password neck box.
E Log on using <u>S</u> ecure	e Password Authentication (SPA)

Для проверки работоспособности сервиса можно использовать тестовый файл EICAR, определяющийся антивирусными программами как вирус. Загрузите его с веб-сайта EICAR (<u>http://www.eicar.org</u>) или создайте самостоятельно, сохранив строку

X50! P%@AP[4\PZX54(P^)7CC)7}\$EICARSTANDARD-ANTIVIRUS-TEST-FILE!\$H+H\* в файл с любым именем.

После этого прикрепите полученный файл к электронному письму и отправьте на любой тестовый адрес.

Пример отправки тестового сообщения:

```
grep X50 /opt/drweb/doc/readme.eicar | mail -s "virus" -r sender@sendhost -S
smtp=ip.address.of.testingserver toaddr@recepienthost
```



В ответ вы должны получить сообщение следующего вида:

От: Дата: Кому: Тема:	DrWeb-MailD 6 ноября 2009 г. 16:41 mailbox1@drweb.test Undelivered mail: test av		
	Защита почтовых серверов Dr.We	eb® for Unix mail servers www.drweb.com	
		Найденные вирусы Подробный отчет	
	У	′важаемый пользователь!!	
	Данное сообщение не Если Вы отправляли (	было доставлено, так как является зараженным данное сообщение, проверьте Ваш компьютер на наличие вирусов.	
	Отправитель (возможно, подделан):	mailbox1@drweb.test	
	Получатели:	mailbox2@drweb.test	
	Тема:	test av	
	IP клиента:	192.168.100.21	
	Сообщение сохранено в карант получить его, отправьте <u>запр</u>	тине под именем <b>def/drweb/6/0000006.maild.umwqAZ</b> . Чтобы <u>oc</u> по электронной почте. Время удаления из карантина: 30.11.09 16:41:32.	
	Ст Модио	атистика сканирования Dr.Web рикаций вируса: 1	

Администратор сервиса также получит уведомление об отправке пользователем вируса.

От: Дата: Кому: Тема:	DrWeb-MailD 6 ноября 2009 г. 16:41 System Administrator A VIRUS HAS BEEN DETECTED !		
	Защита почтовых серверов Dr.	Web® for Unix mail servers www.drweb.com	-
		Найденные вирусы Подробный отчет	
	Уважаемый администратор!		
	Данное сообщение не было доставлено, так как является зараженным.		
	Отправитель (возможно, подделан):	mailbox1@drweb.test	
	Получатели:	mailbox2@drweb.test	-
	Тема:	test av	
	IP клиента:	192.168.100.21	
	Сообщение сохранено в карантине под именем <b>def/drweb/6/00000006.maild.umwqA2</b> . Чтоби получить его, отправьте <u>запрос</u> по электронной почте. Время удаления из карантина: 30.11.09 16:41:32.		
	Мод	Статистика сканирования Dr.Web ификаций вируса: 1	
<u> </u>	Найденные вирусы		

Для того чтобы проверить качество обнаружения спама, отправьте письмо с тестовой строчкой GTUBE: xJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-STANDARDANTI-UBE-TEST-EMAIL\*C.34X



### 6. Последние замечания

Важно помнить о том, что после установки ПО необходимо сразу провести обновление всех установленных компонентов.

**Внимание!** После развертывания АВ-сети по данному руководству настоятельно рекомендуется тщательно изучить «Руководство администратора» по установленному продукту.

Этот документ можно загрузить со следующей страницы сайта компании «Доктор Веб»:

http://download.drweb.com/esuite.



© ООО «Доктор Веб», 2004-2011 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 www.freedrweb.com www.av-desk.com