Dr.WEB®
Enterprise Security Suite

Защити созданное

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»

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 http://www.drweb.com.

Версия программного обеспечения	6.00.01
Версия документа	1.0
Статус документа	Утвержден
Дата последнего изменения	9 марта 2011 года

Содержание

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 A-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 A- и MX-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 АВ-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 АВ-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 http://download.drweb.com/demo 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 — http://www.vmware.com).

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 АВ-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 АВ-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 АВ-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.

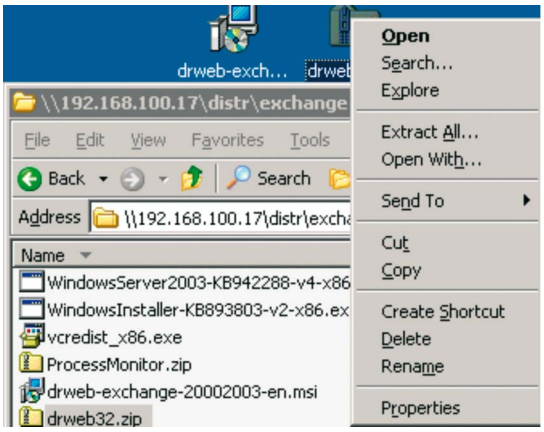
Актуальную версию дистрибутива можно получить здесь: http://download.drweb.com/esuite.

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.

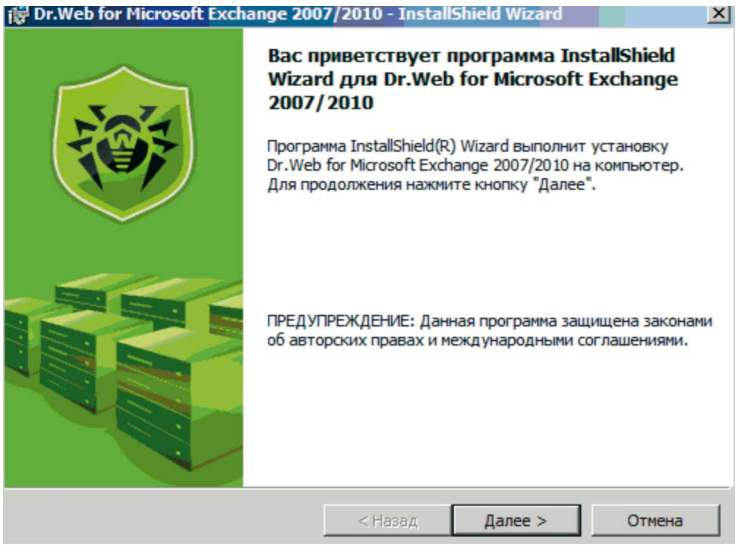
Внимание! Подробные системные требования и особенности установки на разных платформах описаны в «Руководстве администратора». В данной методике предполагается, что производится типовая установка как для MS Exchange 2007/2010, так и для Dr.Web для MS Exchange 2007/2010.

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

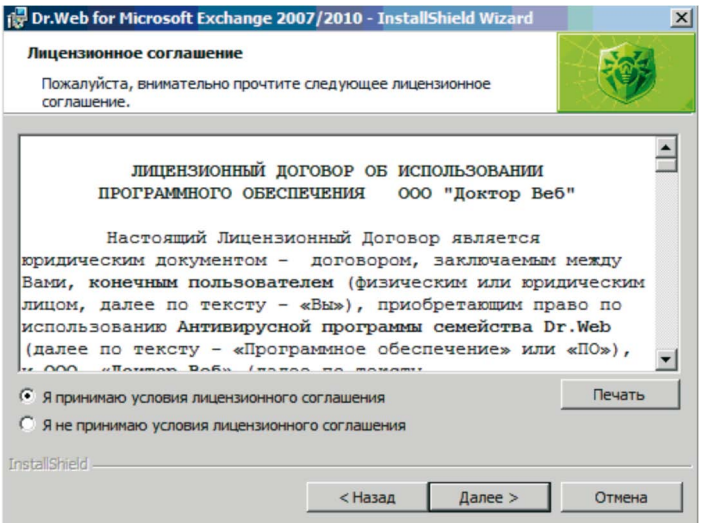
1. Скопируйте дистрибутив **Dr.Web для MS Exchange** `drweb-600-exchange-20072010-ru.msi` и файл `drweb32.zip`, содержащий актуальный ключ, на рабочий стол.
2. Распакуйте архив `drweb32.zip`, например, выбрав команду **Extract all** по щелчку правой кнопки мыши.



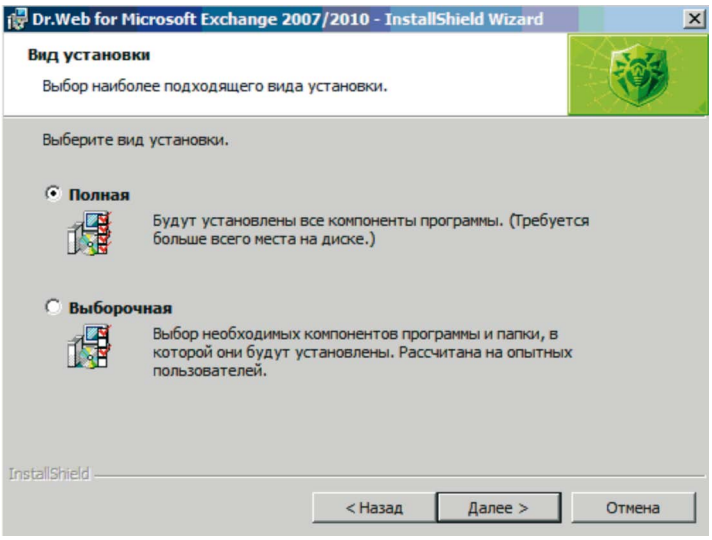
3. Запустите инсталляционный файл с рабочего стола и в открывшемся **Мастере установки** нажмите **Далее (Next)**.

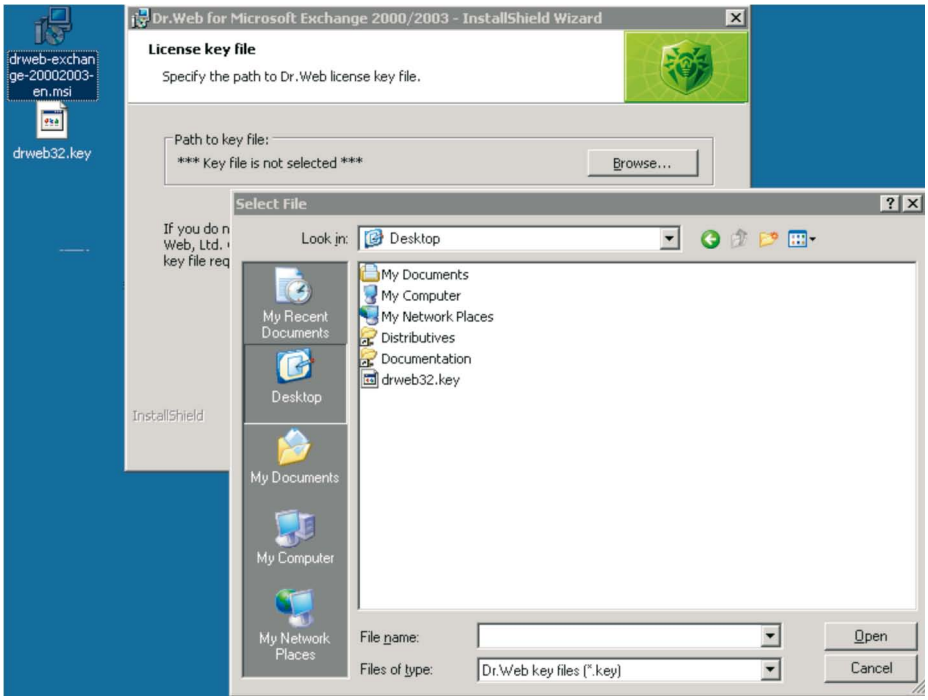


4. Ознакомьтесь с текстом лицензионного соглашения и примите его, выбрав пункт **Я принимаю условия лицензионного соглашения**. Нажмите **Далее (Next)**.

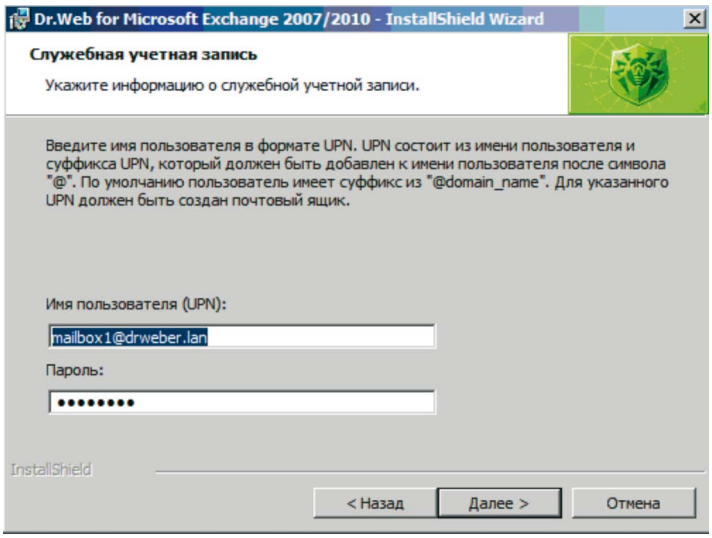


5. Укажите тип установки, выбрав **Полная** или **Выборочная**, и нажмите **Далее (Next)** для продолжения. Рекомендуется использовать полный вариант установки, устанавливая все необходимые компоненты.

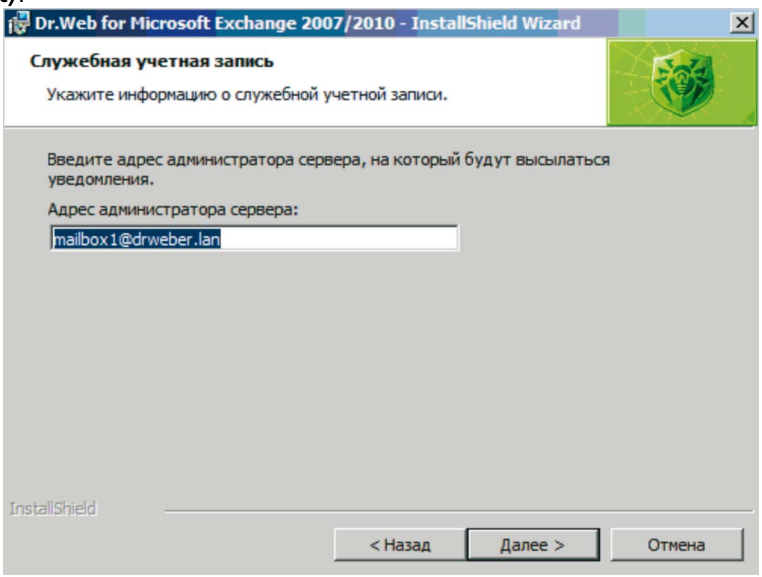




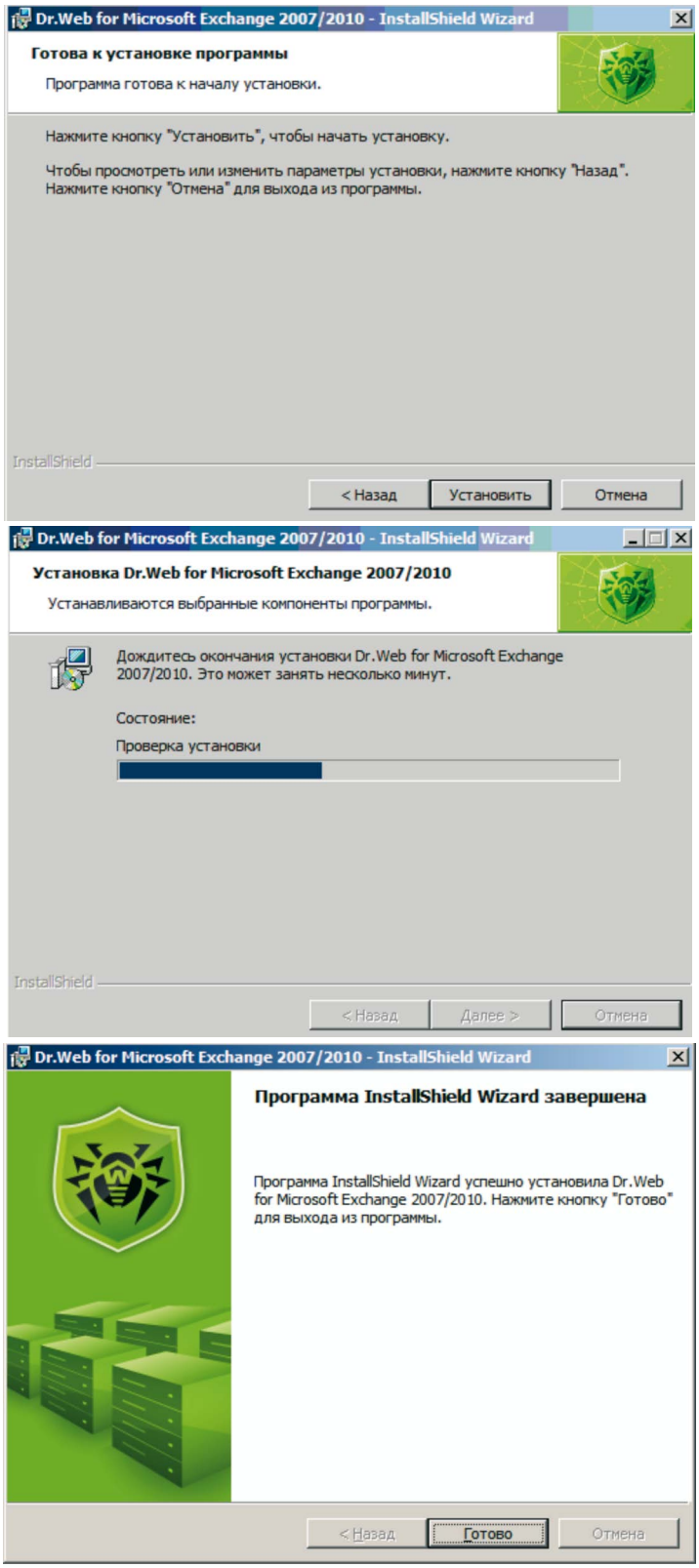
6. В окне **Лицензионный ключевой файл** укажите путь к вашему ключевому файлу и нажмите **Далее (Next)**.
7. В соответствующих полях ввода укажите электронный адрес и пароль учетной записи пользователя, с почтового ящика которой будут рассылаться уведомления. Указанная учетная запись должна обладать 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`.



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



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.

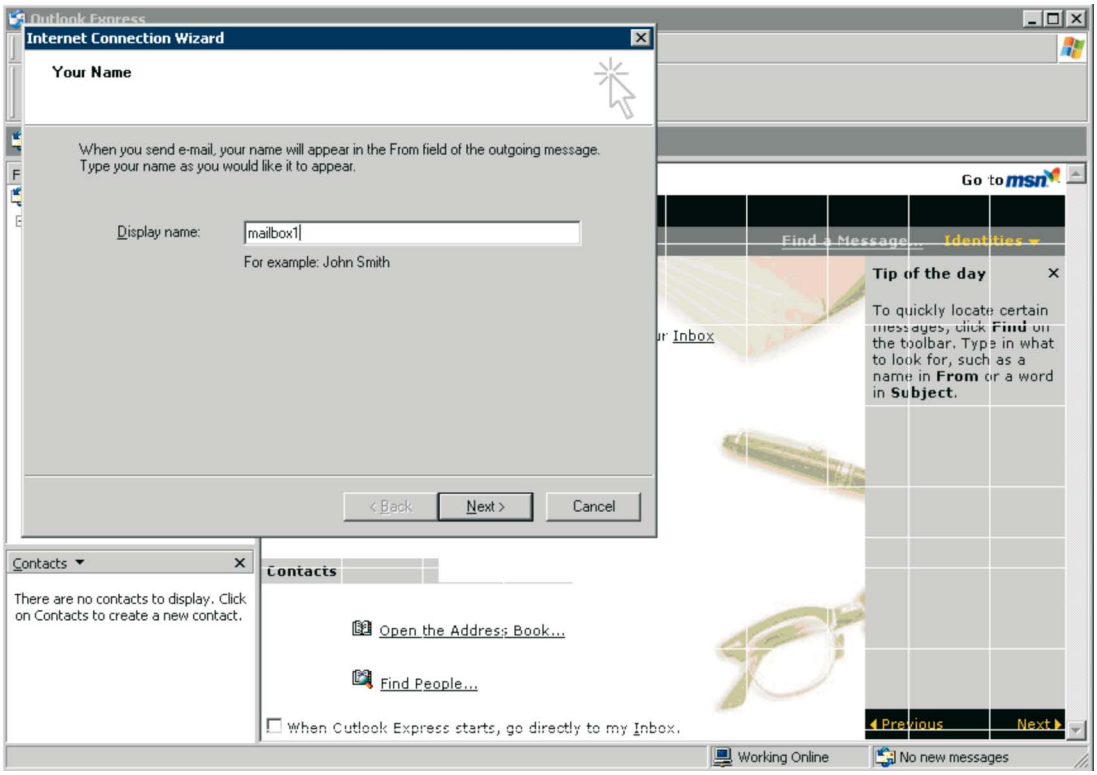
3.1.2. Тестирование функционирования сервиса

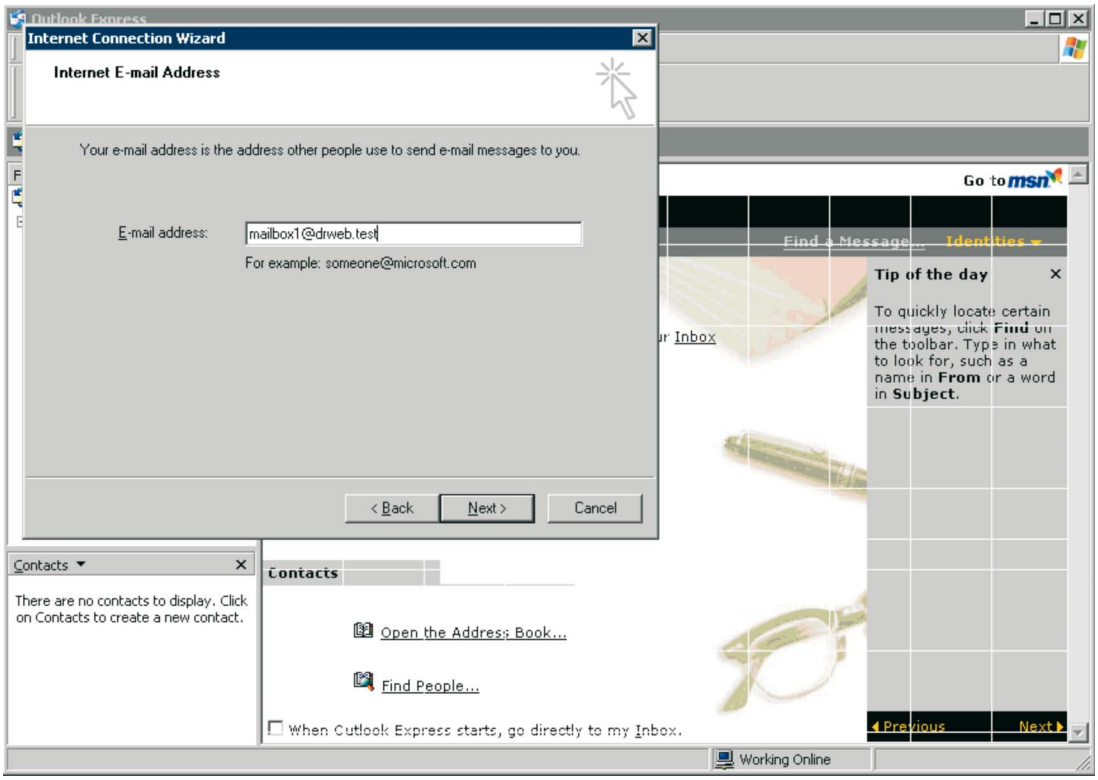
Для тестирования сервиса защиты почты можно использовать установленный по умолчанию почтовый клиент Outlook Express. Для проведения тестирования рекомендуется завести как минимум два почтовых ящика. В данной методике используются почтовые ящики mailbox1 и mailbox2 с паролем доступа qwerty. Для добавления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

Выбрать пункт **Internet Accounts** в меню **Tools**.

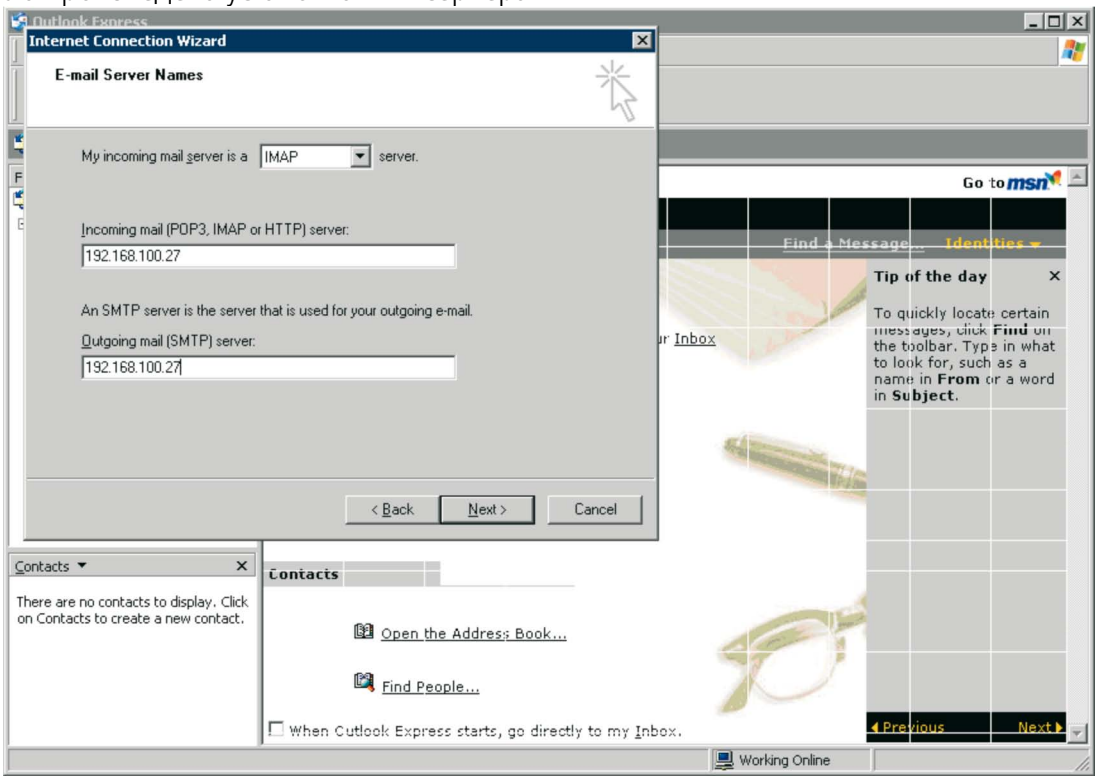
Нажать кнопку **Add** и выбрать **Mail**.

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

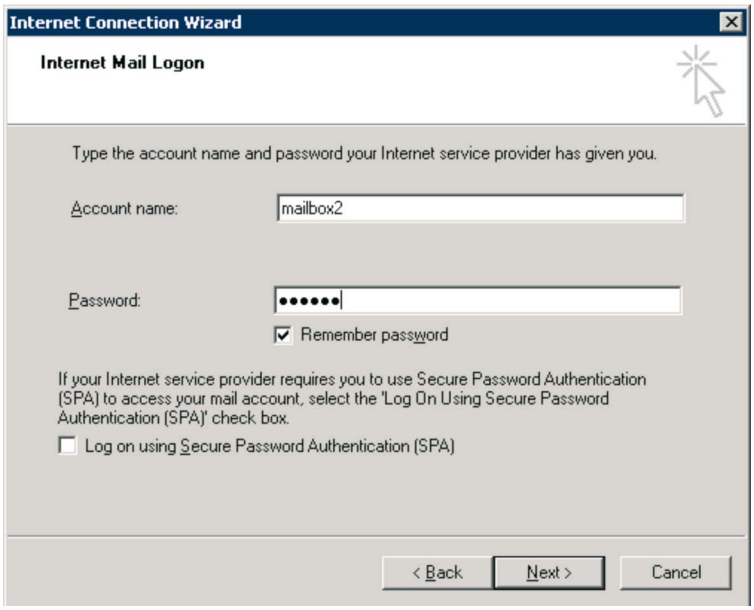




Указать серверы для входящей и исходящей почты. В данном случае указывается адрес сервера, на котором была произведена установка. Тип сервера — `IMAP`.

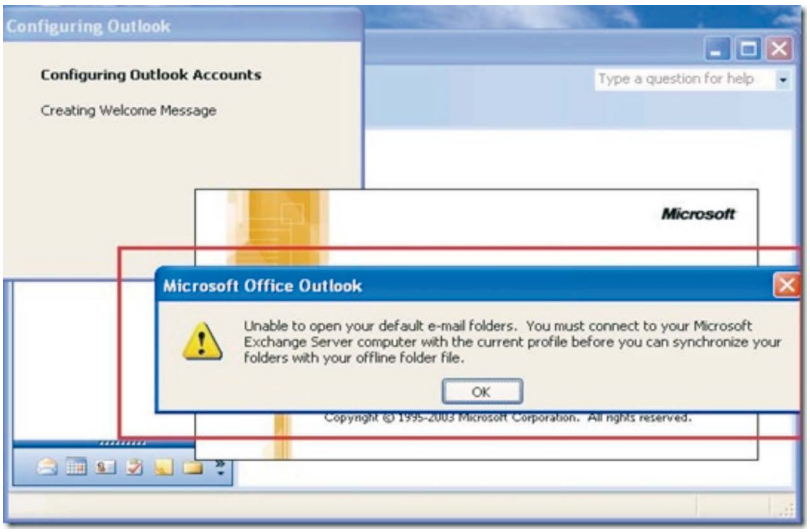


В качестве пароля и логина доступа необходимо указать имя ящика и пароль `qwerty`.

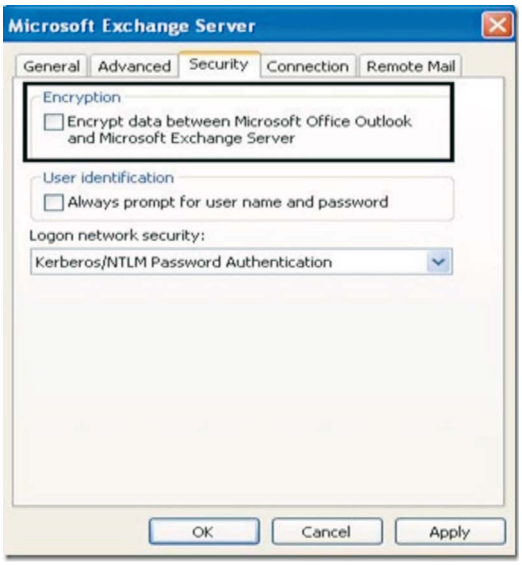


Внимание! В том случае, если вы используете такие почтовые клиенты, как MS Outlook 2003:

- 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:



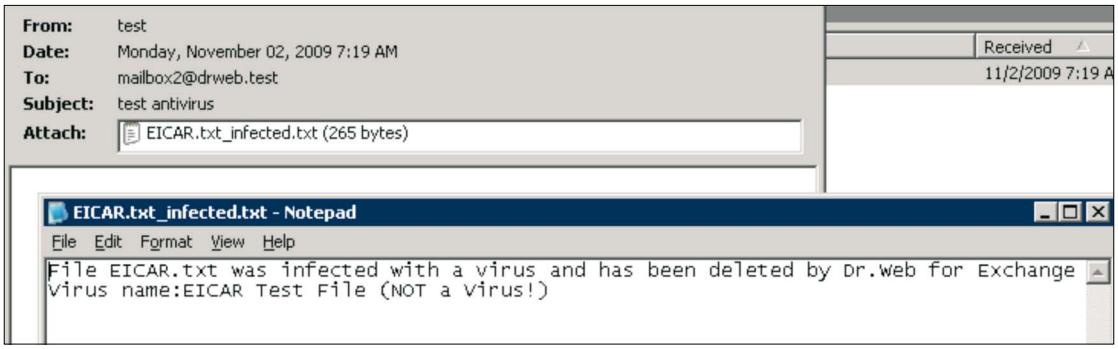
Для включения опции шифрования необходимо отметить пункт **Шифровать данные, пересылаемые между Microsoft Office Outlook и Microsoft Exchange (Encrypt data between…)** на закладке **Security (Сервис — Учетные записи — Другие настройки — Безопасность по умолчанию)**.



Для проверки работоспособности сервиса можно использовать тестовый файл `EICAR`, определяющийся антивирусными программами как вирус. Загрузите его с веб-сайта EICAR (http://www.eicar.org) или создайте самостоятельно, сохранив строку
`X5O!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:

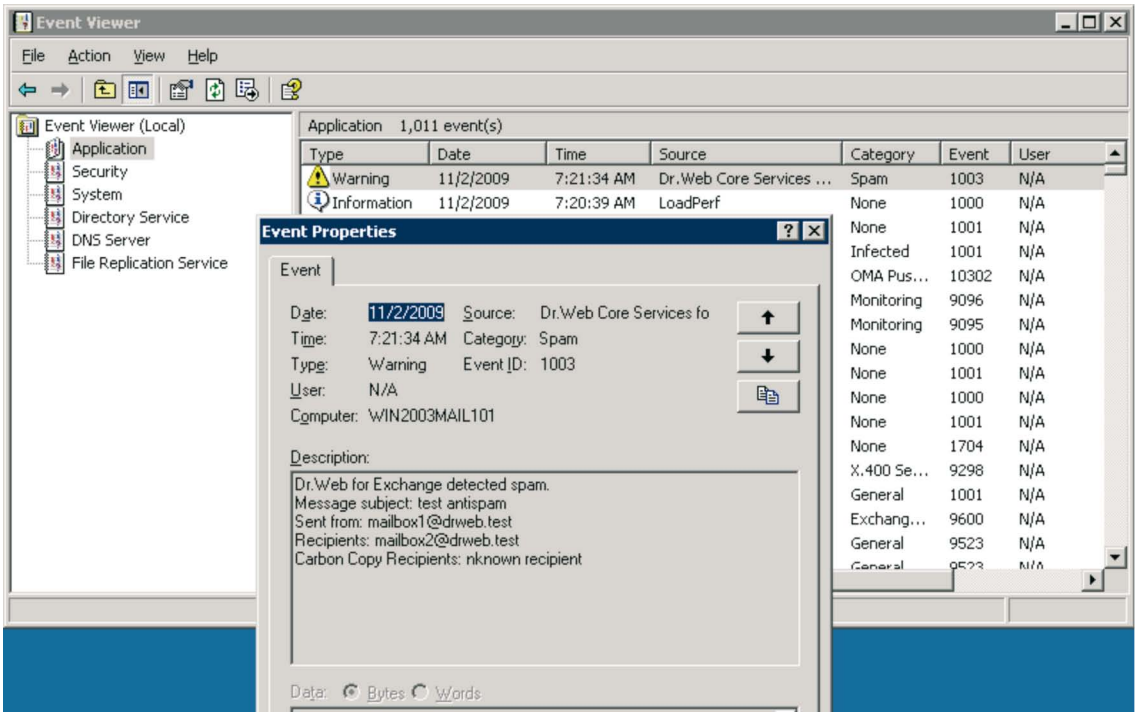
Инфицированный вирусом файл `eicar.com` был удален Dr.Web для MS Exchange. Имя вируса: `EICAR Test File (NOT a Virus!)`.



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.

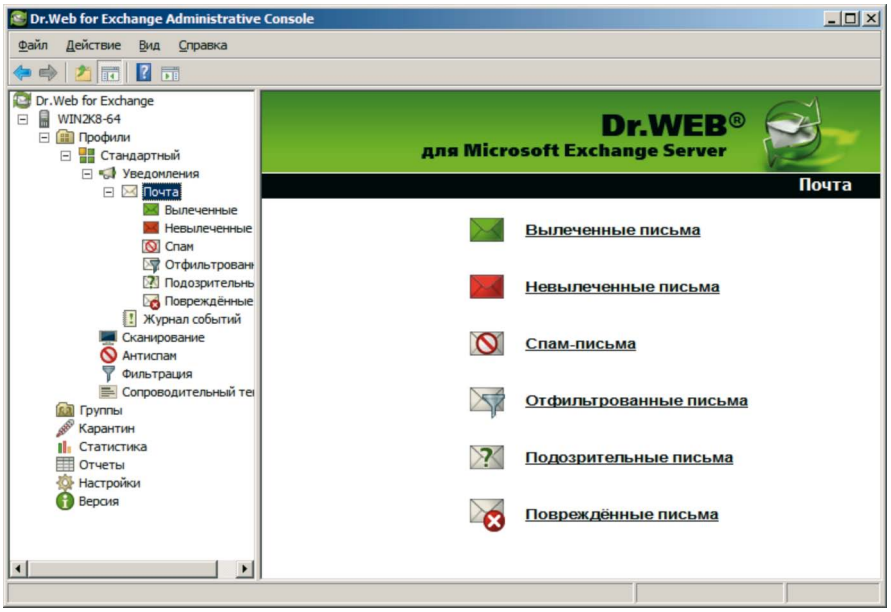
Откройте утилиту Windows **Просмотр событий ➔ Приложение (Event Viewer ➔ Application)** и найдите сообщение о том, что **Dr.Web для MS Exchange** обнаружил спам.



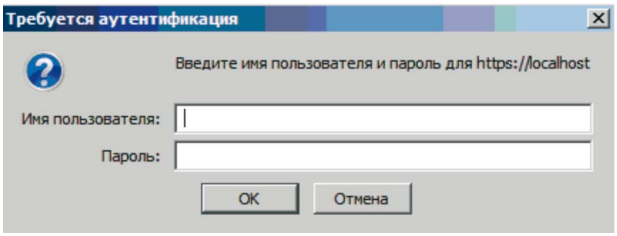
3.2. Настройка параметров антивирусной защиты

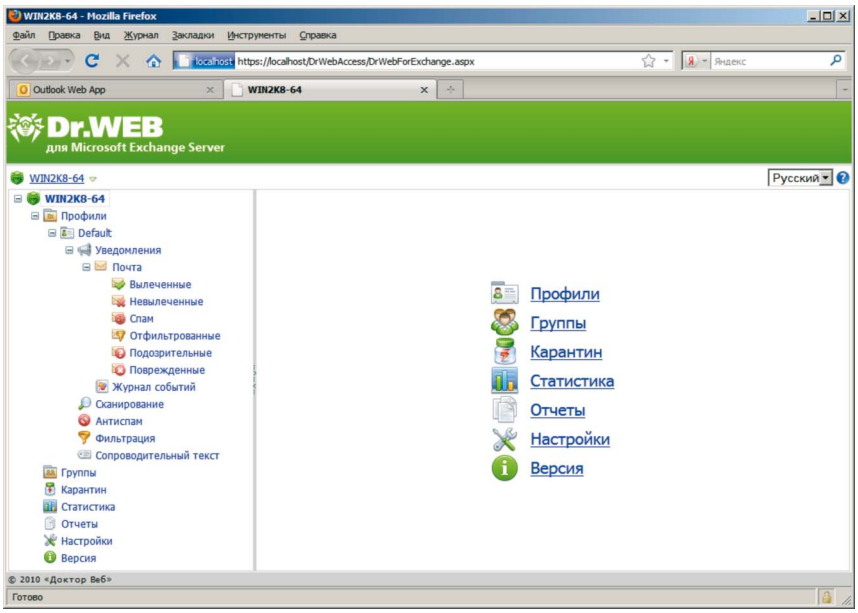
Начиная с версии 6.0 управление **Dr.Web для MS Exchange** возможно как с традиционной консоли управления, так и через веб-интерфейс. Возможности и внешний вид консоли управления и веб-интерфейса одинаковы, в связи с чем в данной методике для иллюстрации действий будет использоваться консоль управления.

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`).



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.





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

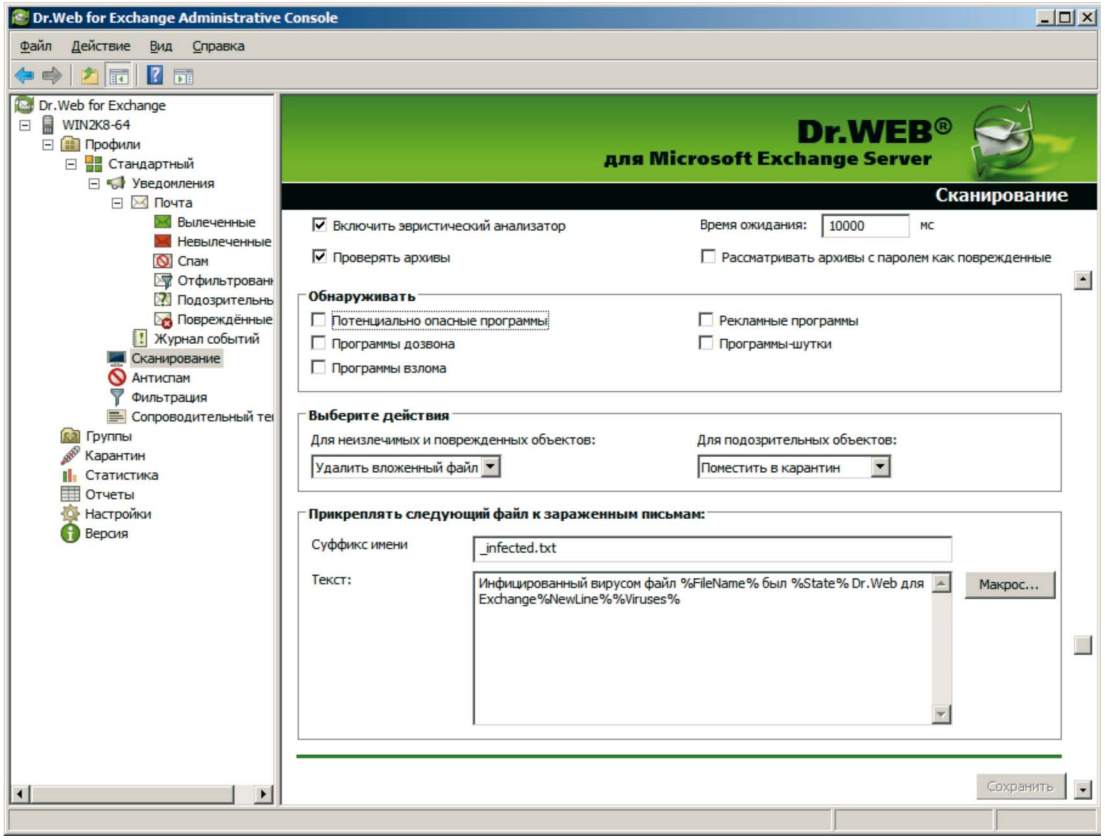
Используя **Консоль управления Dr.Web для MS Exchange**, администратор может определить правила проверки объектов различного типа на наличие вредоносных объектов. Для настройки параметров сканирования необходимо открыть консоль управления, выбрать интересующий профиль и пункт меню **Сканирование**.

На данной странице администратор может определить:

- действия, применяемые к объектам различного типа;

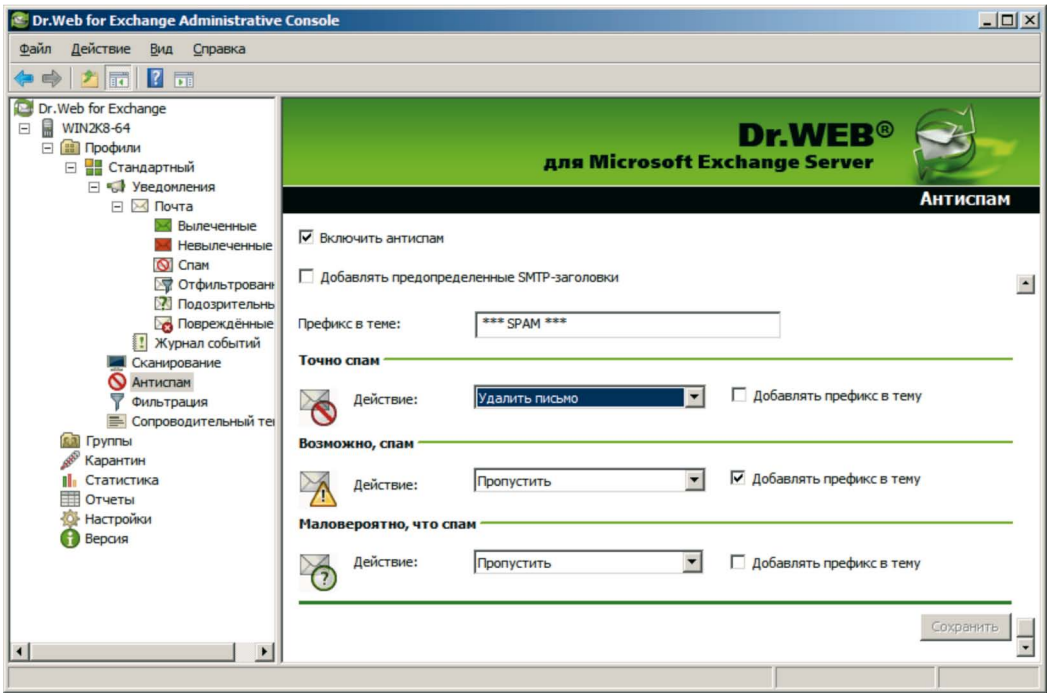
  Для неизлечимых и поврежденных объектов можно блокировать сообщения с объектами таких типов, посылать запросы на их удаление с сервера (результат будет зависеть от настроек Microsoft Exchange), удалять их самостоятельно или перемещать прикрепленные файлы в карантин. Для подозрительных объектов также 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.



Для сохранения изменений необходимо нажать кнопку **Сохранить**.

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



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~~ `Junk e-mail`, ~~пропускать или не принимать и оставлять их на сервере~~.

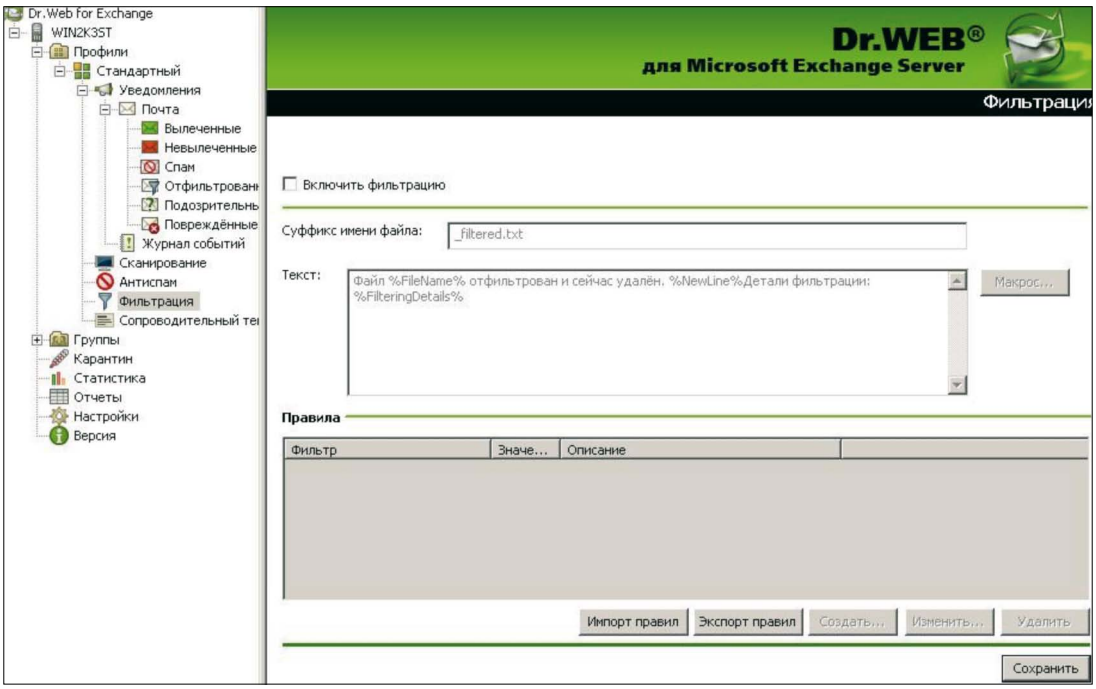
Кроме этого, администратор может задавать префикс, добавляемый в тему письма после проверки на спам.

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**.

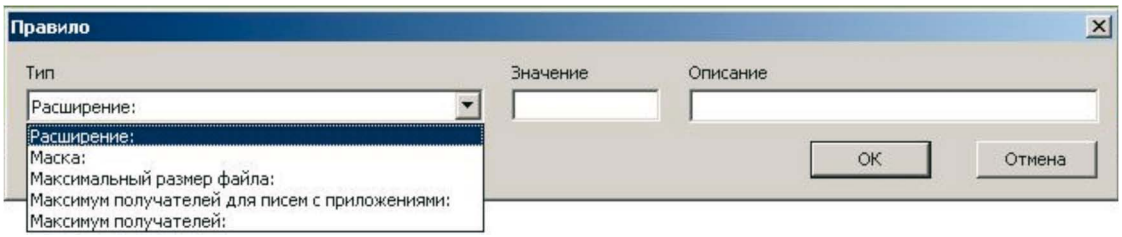
3.2.2. Добавление пользовательских фильтров

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



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.

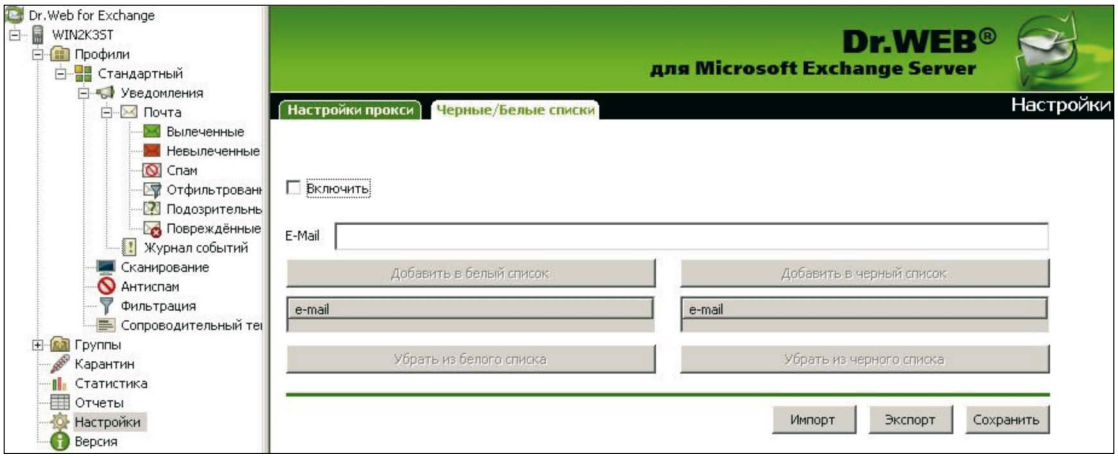


Для сохранения настроек необходимо нажать на кнопку **Сохранить**.

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.



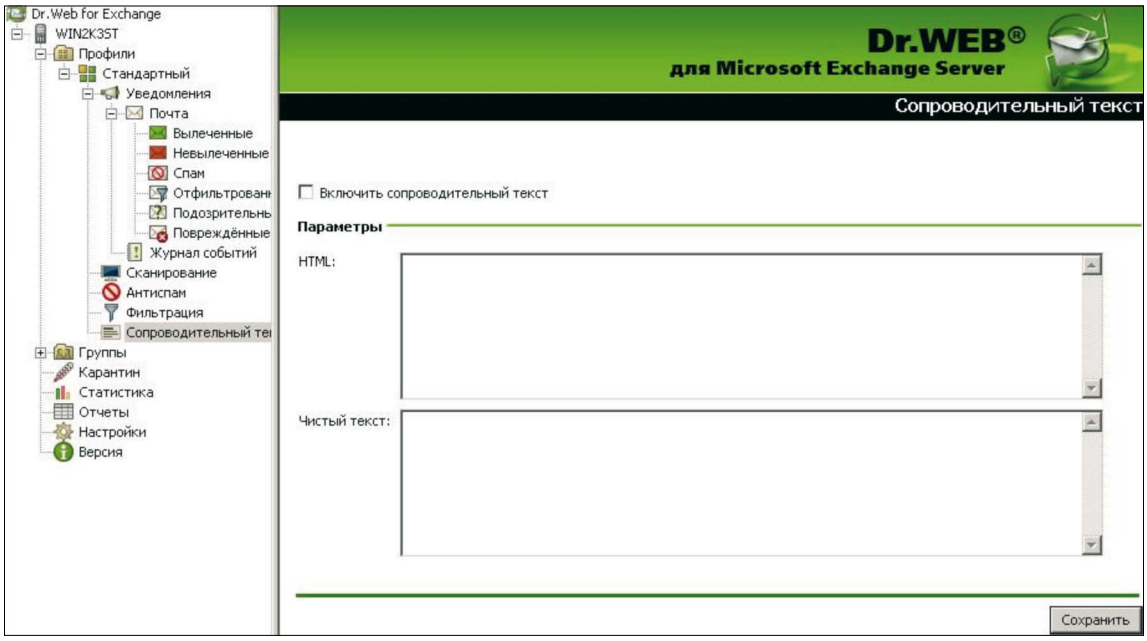
Для добавления адреса в тот или иной список необходимо, отметив для включения фильтрации пол спискам пункт **Включить**, ввести адрес в поле **E-Mail** и нажать либо на кнопку **Добавить в белый список**, либо на кнопку **Добавить в черный список**.

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.

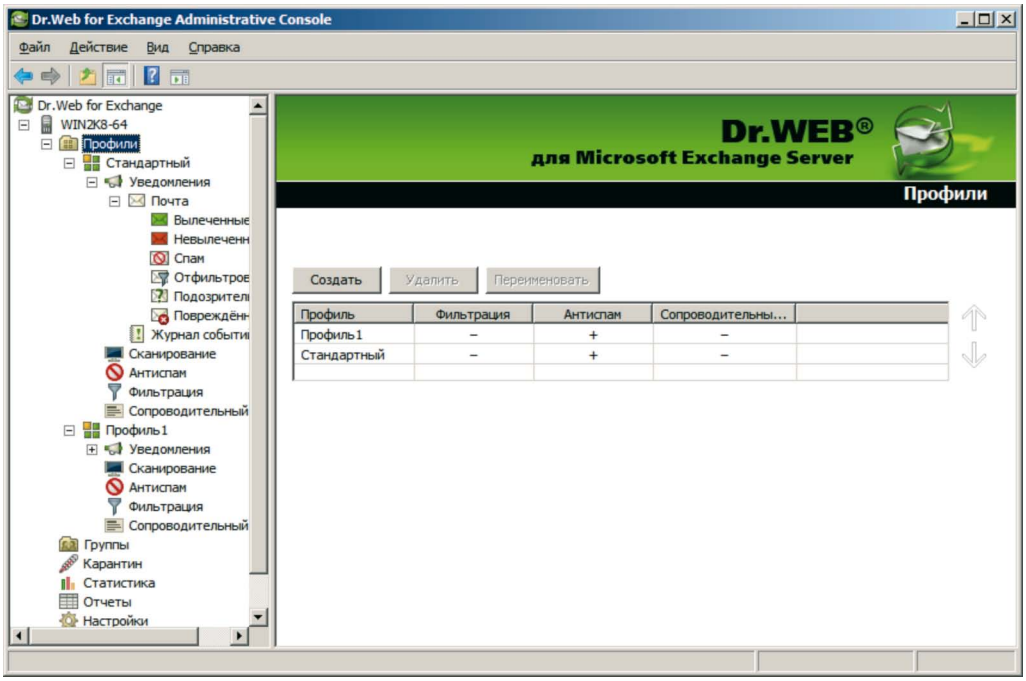


Для сохранения настроек необходимо нажать на кнопку **Сохранить**.

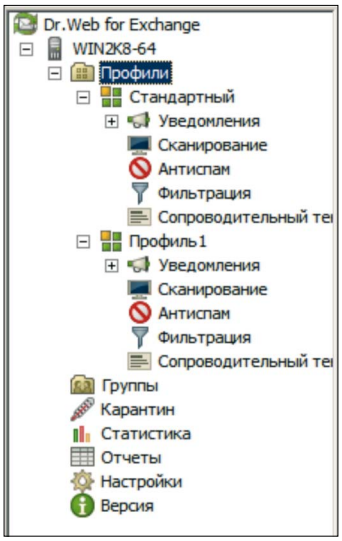
3.2.5. Настройки для отдельных пользователей и групп

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)**.



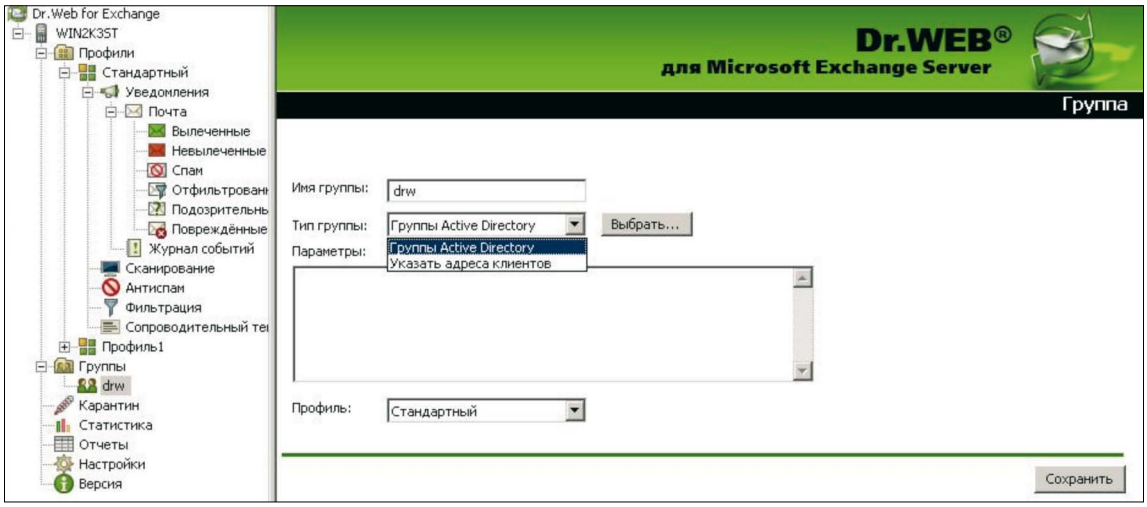
Будет создан новый профиль с именем **Профиль1 (Profile1)**, который появится в дереве консоли под пунктом **Профили**. Если профиль с таким именем уже существует, то имя нового профиля будет **Профиль2**, и т. д.



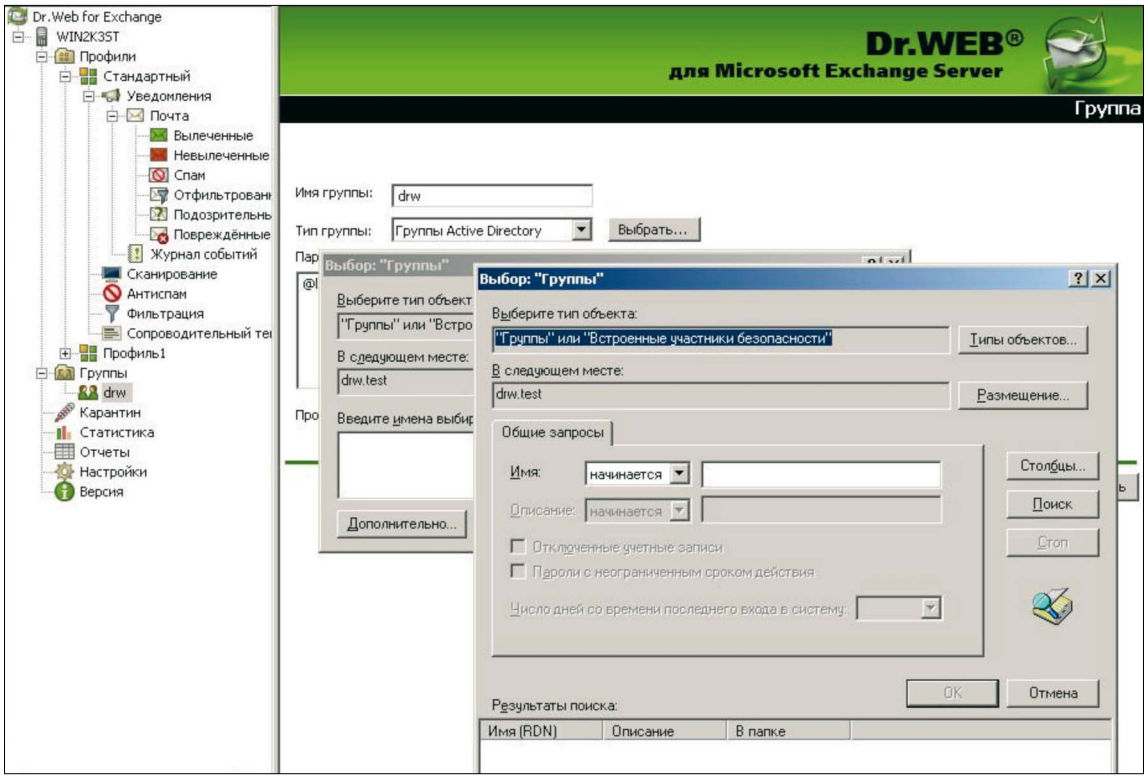
Чтобы изменить имя профиля, выберите его в списке, расположенном в области сведений раздела **Профили**, и в меню, открывающемуся по клику правой кнопки мышки, выберите **Переименовать (Rename)**.

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.

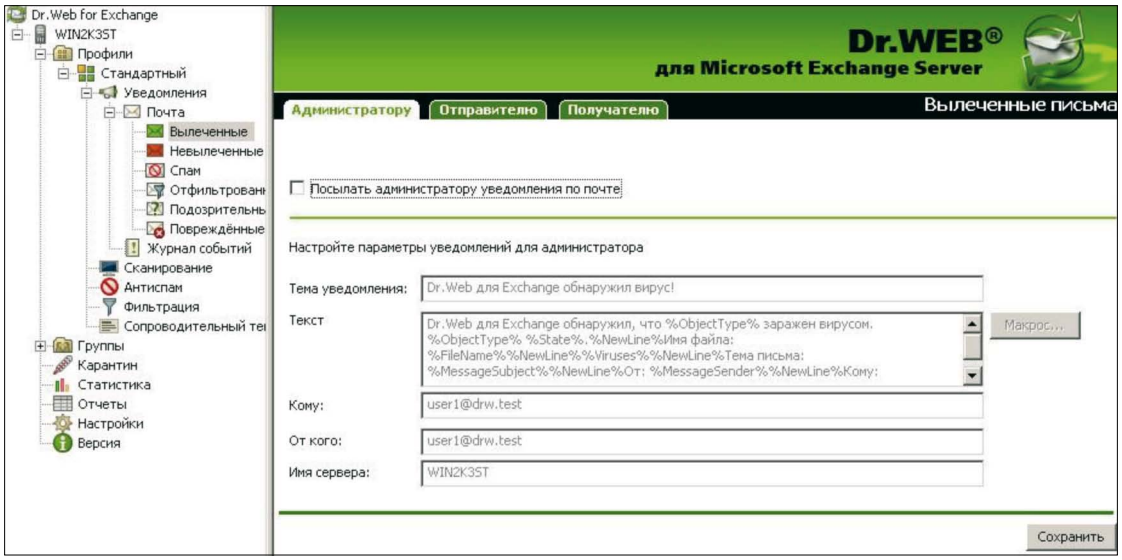


В этом же окне администратор должен указать тип группы, выбрав его в выпадающем списке **Тип группы**. Если выбран тип **Указать адреса клиентов**, то проверяемые адреса нужно ввести вручную в поле **Параметры**. Если выбран тип **Группы Active Directory**, то для выбора интересующих групп надо нажать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



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.



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

Для сохранения настроек необходимо нажать на кнопку **Сохранить**.

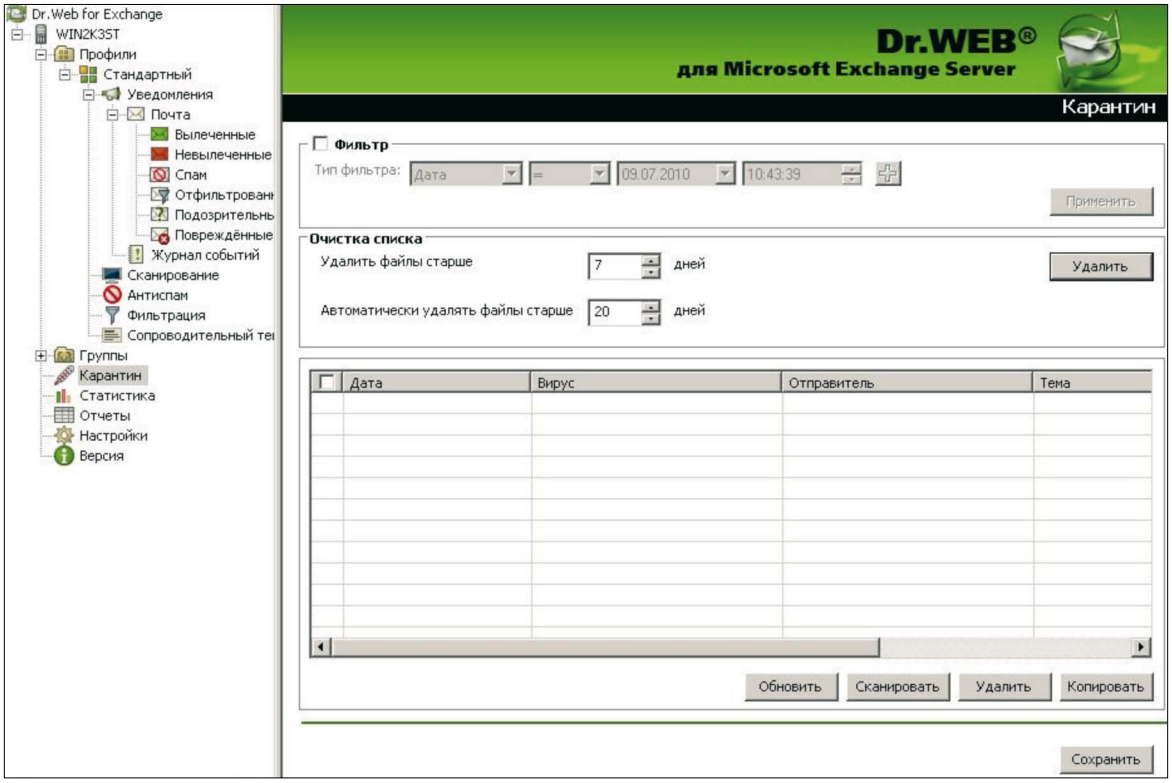
3.2.7. Сохранение текущих настроек в конфигурационный файл

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.

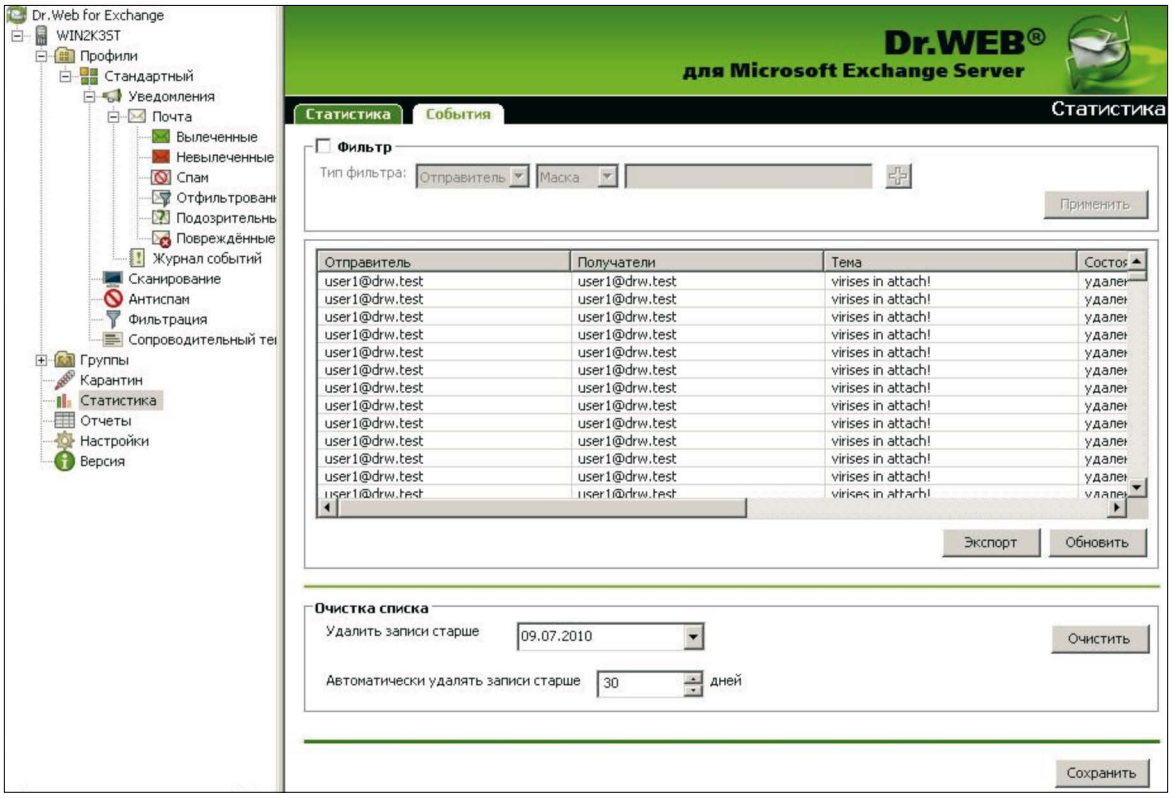


3.3.1. Статистика работы сервиса. Получение отчетов о работе программы

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.


Dr.Web for Exchange
WIN2K3ST
Профили
Стандартный
Уведомления
Почта
Вылеченные
Невылеченные
Спам
Журнал событий
Сканирование
Антиспам
Фильтрация
Группы
Карантин
Статистика
Отчеты
Настройки
Версия
Dr.WEB®
для Microsoft Exchange Server
Статистика
События
Статистика
Фильтр
Тип фильтра:
Отправитель
Маска
Применить
Отправитель
Получатели
Тема
user1@drw.test
virises in attach!
Экспорт
Обновить
Очистка списка
Удалить записи старше
09.07.2010
Очистить
Автоматически удалять записи старше
30
дней
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.
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:

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.

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

`__to__address__` – 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 с `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:
        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
--More--(50%)_
```

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: (vaderetro|headersfilter|drweb|modifier). Values are delimited with commas.
 [default=]:

Enter list of plugins to process message after placing it to queue/DB.
Possible values: (vaderetro|headersfilter|drweb|modifier). 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: (en|ja|ru). 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
License 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:
 username1@example.com
 username1@foo.example.com
 username1
 username2@example.com
 username2@domain.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 /opt/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
```

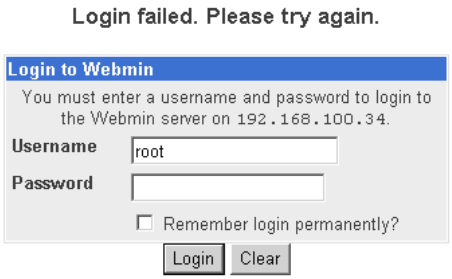
В качестве средства удаленного администрирования используется Webmin. Если вы хотите использовать для управления веб-интерфейс, вы должны установить его. Например:

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

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

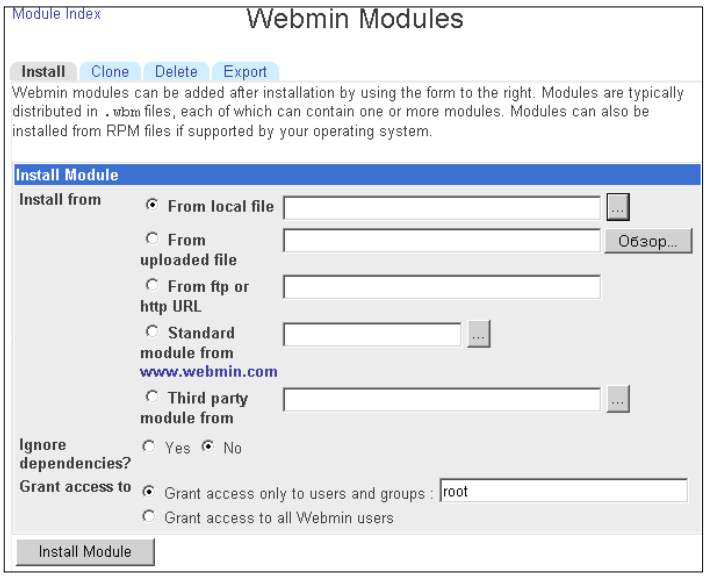
Внимание! В связи с тем, что используемый по умолчанию в Windows XP браузер Internet Explorer версии 6.0 имеет значительные проблемы с безопасностью и не рекомендуется к использованию своим производителем, дальнейшая демонстрация проводится с помощью браузера Firefox.

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

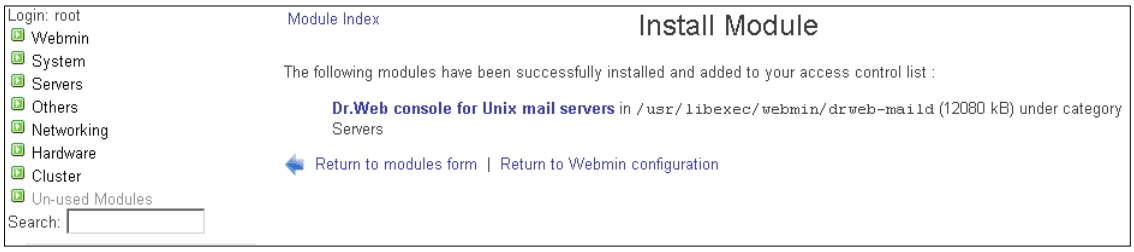


Для установки консоли управления Dr.Web Mail Gateway необходимо в папке **Webmin** выбрать пункт **Webmin Configuration** и на открывшейся странице выбрать **Webmin Modules**.

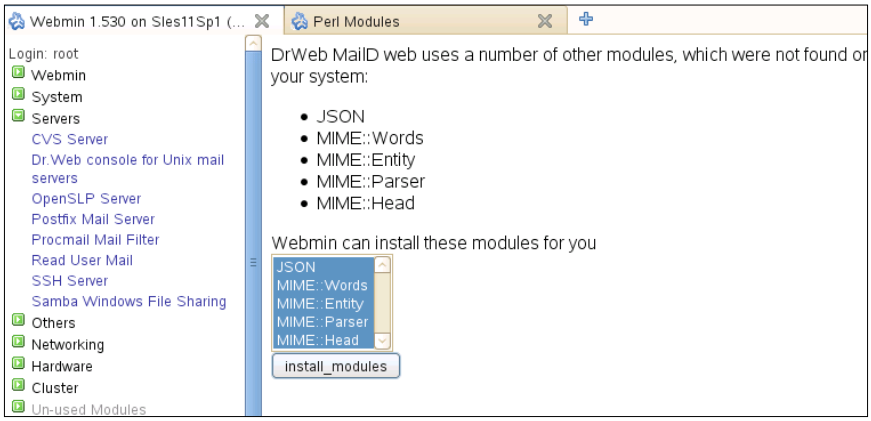
На странице **Webmin Modules** необходимо выбрать вариант **From local file** и указать путь к файлу `drweb-maild-web.wbm.gz`. По умолчанию он находится в каталоге `/opt/drweb/web`.



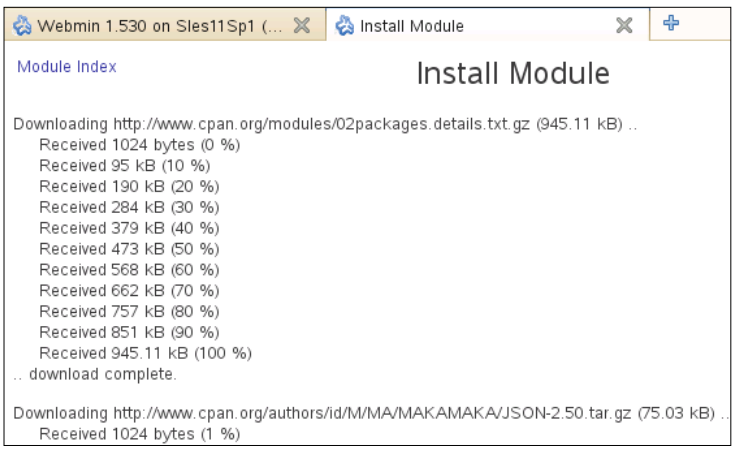
Указав файл, необходимо на странице **Webmin Modules** нажать на кнопку **Install Module**. После завершения установки нужно перезагрузить **Webmin**. Консоль управления Dr.Web Mail Gateway находится в папке `Servers`.

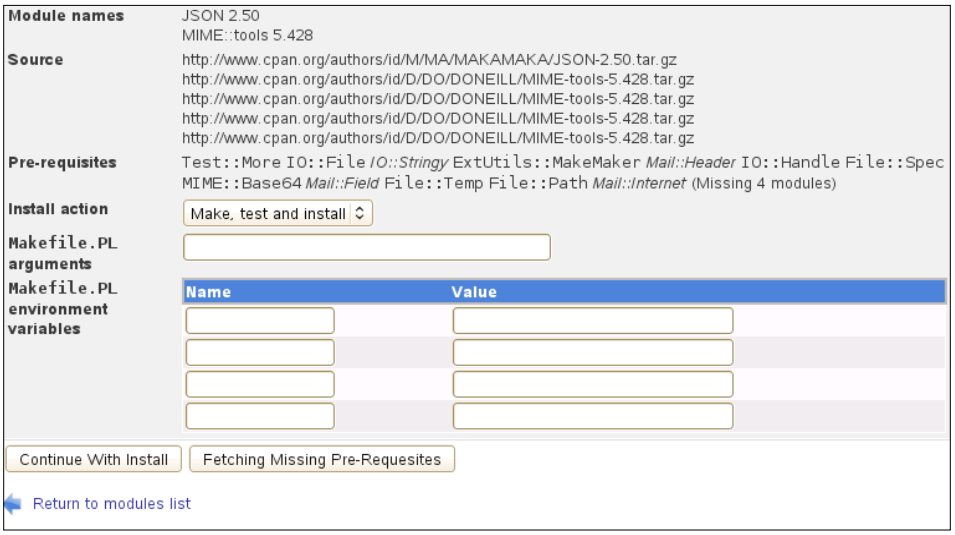


В том случае, если для работы консоли не хватает ряда дополнительных модулей, их список будет показан при попытке запуска консоли.



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`.

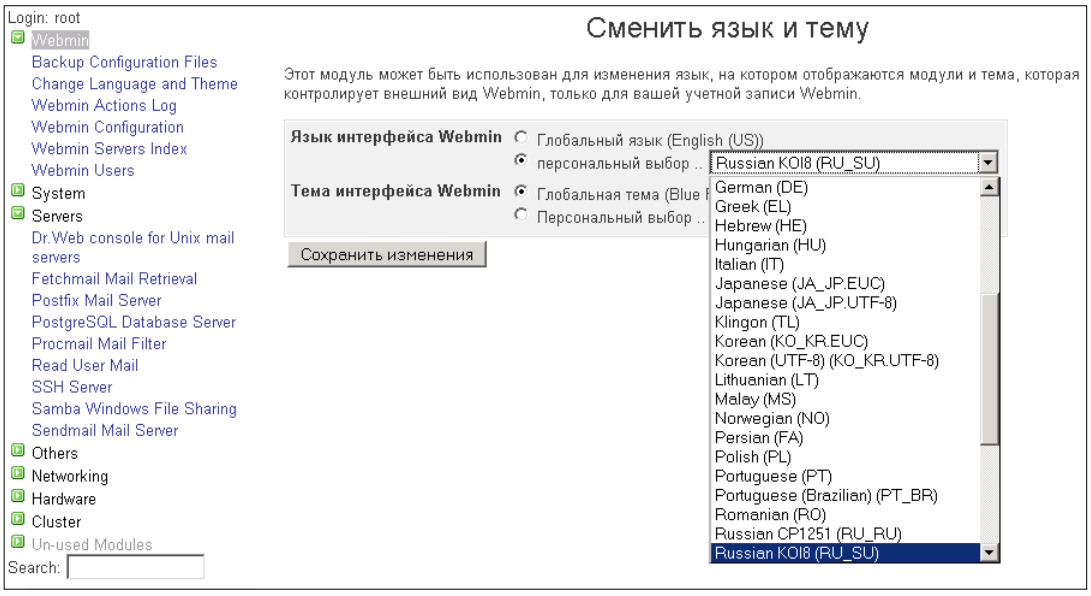




После завершения установки модуля управления рекомендуется обновить страницу **Webmin**.

4.1.1. Настройка языка интерфейса

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

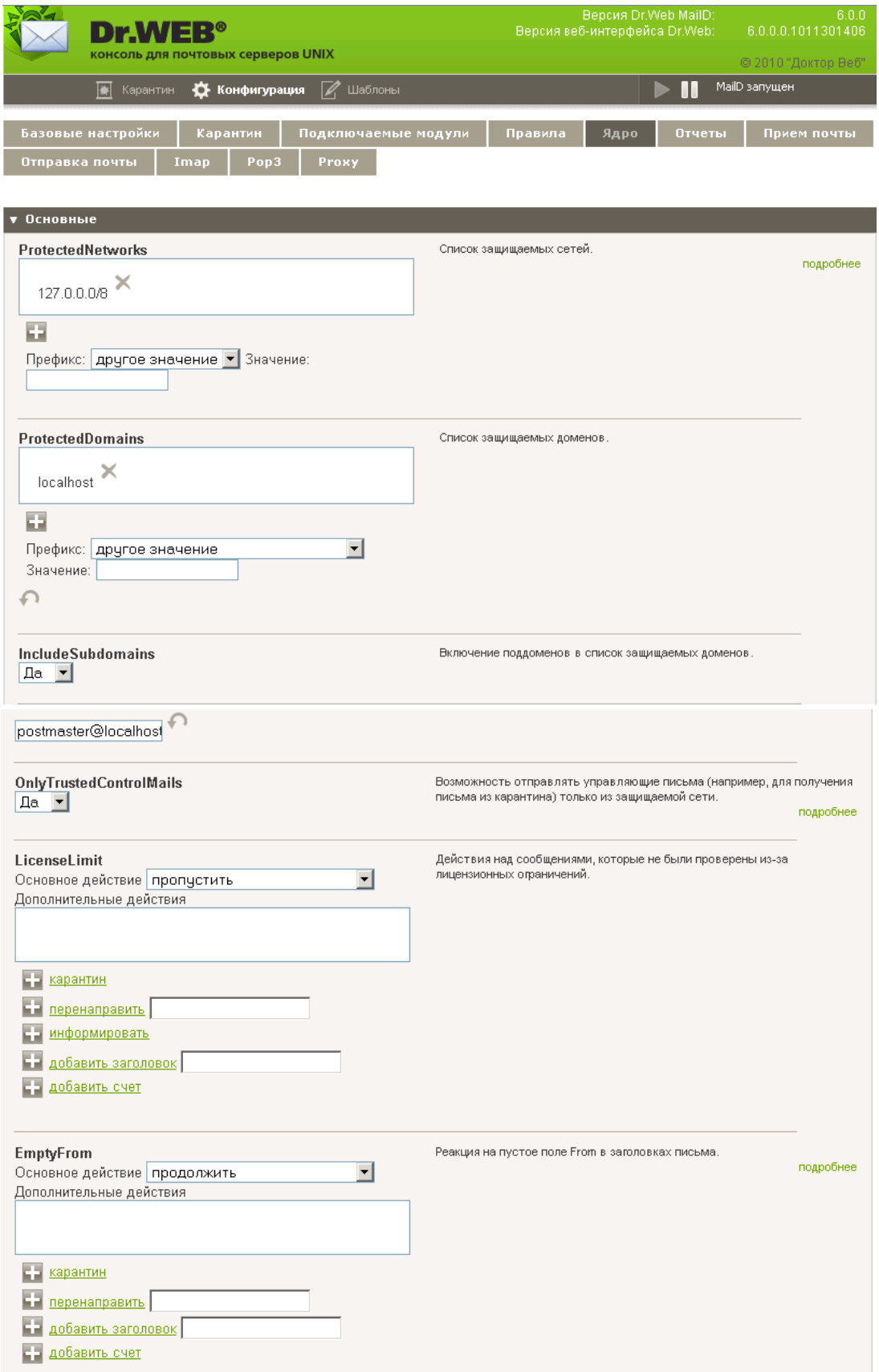


4.2. Настройка параметров антивирусной защиты

4.2.1. Первоначальная настройка

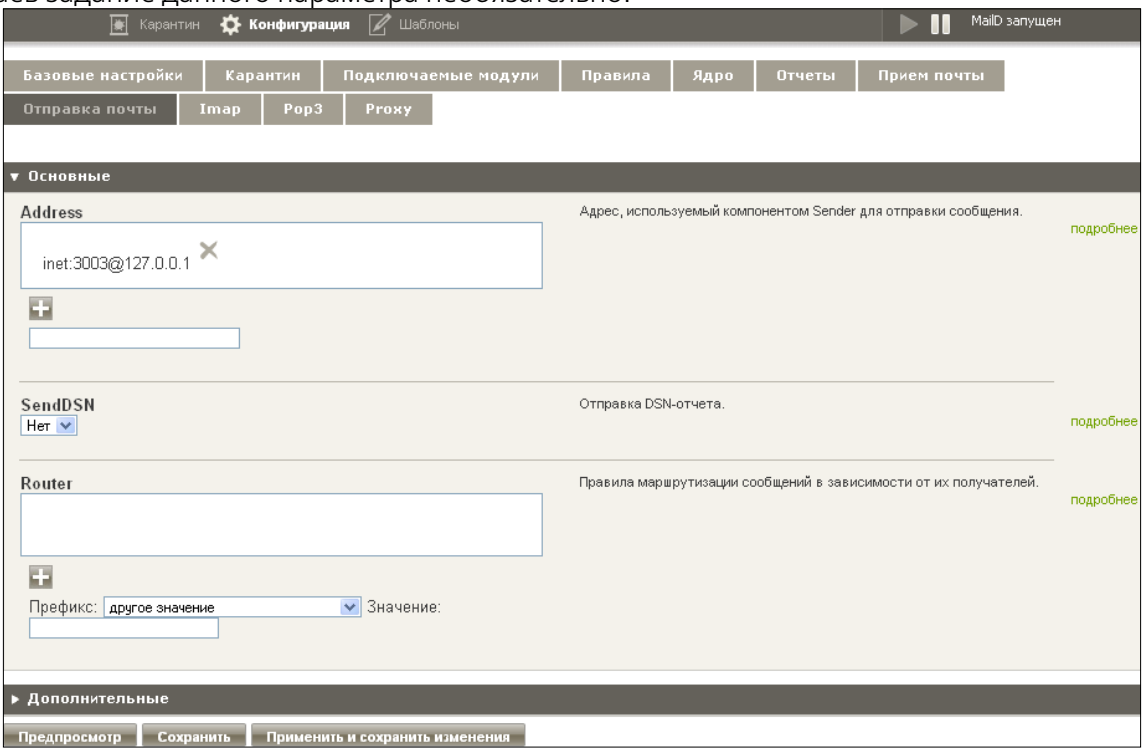
Для настройки через веб-интерфейс необходимо выбрать пункт **Dr.Web консоль для почтовых серверов UNIX** в меню **Службы** и перейти в меню **Конфигурация**.

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



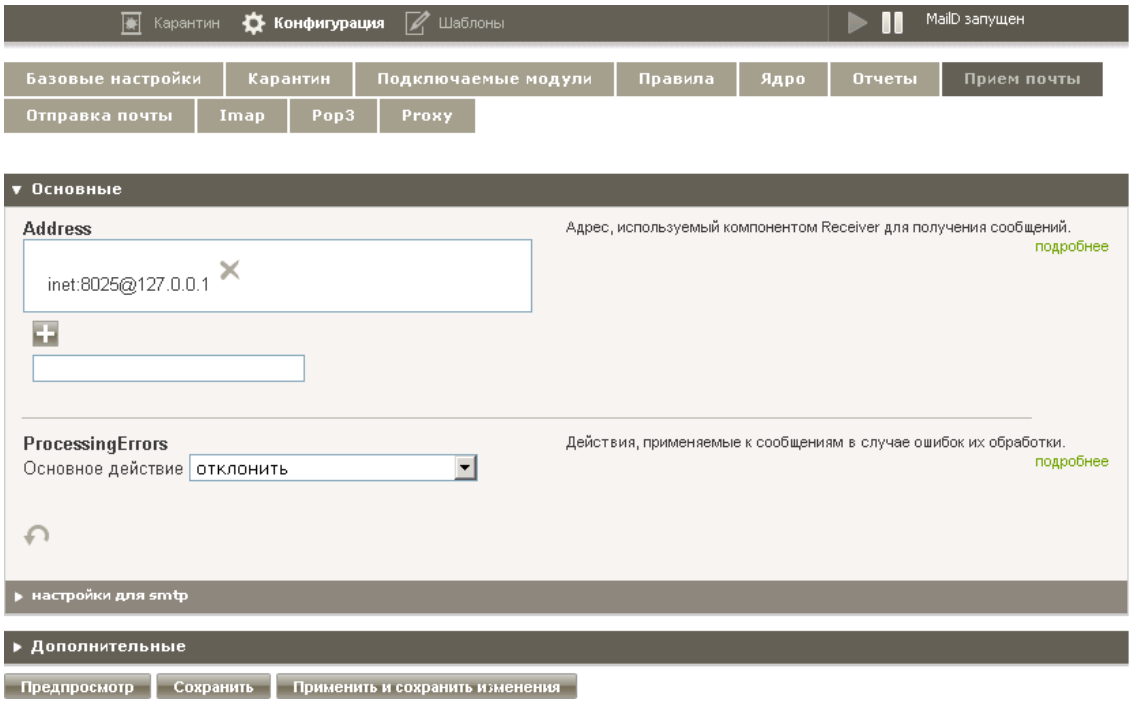
На данной странице рекомендуется задать параметры `ProtectedDomains` (например, `drweber.test`) и `ProtectedNetworks`.

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.



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 `A`.

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



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**.

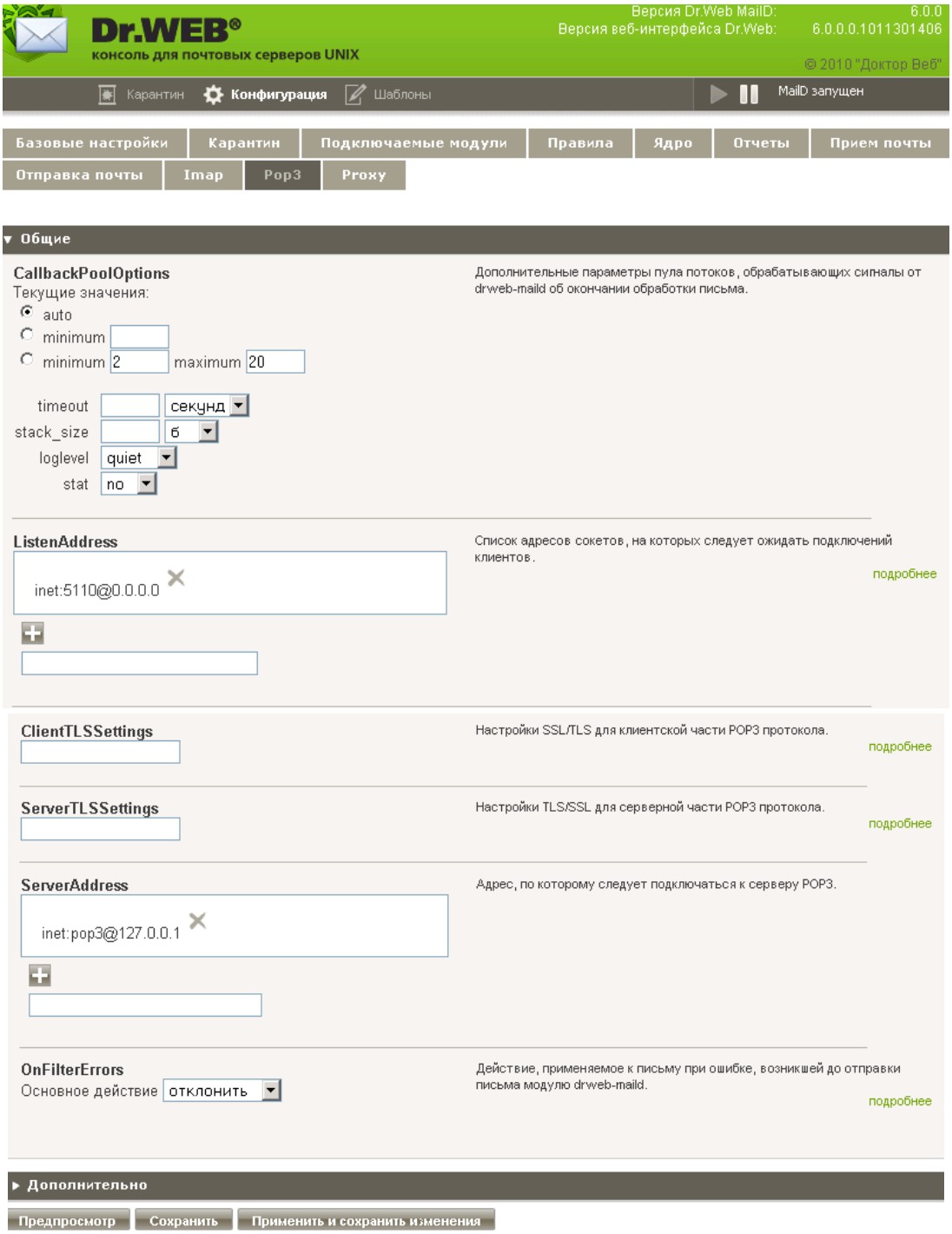
4.2.2. Настройка параметров проверки сообщений по протоколам POP3/POP3S/IMAP4/IMAP4S

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



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 `MaxConnectionsPerIp`). 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

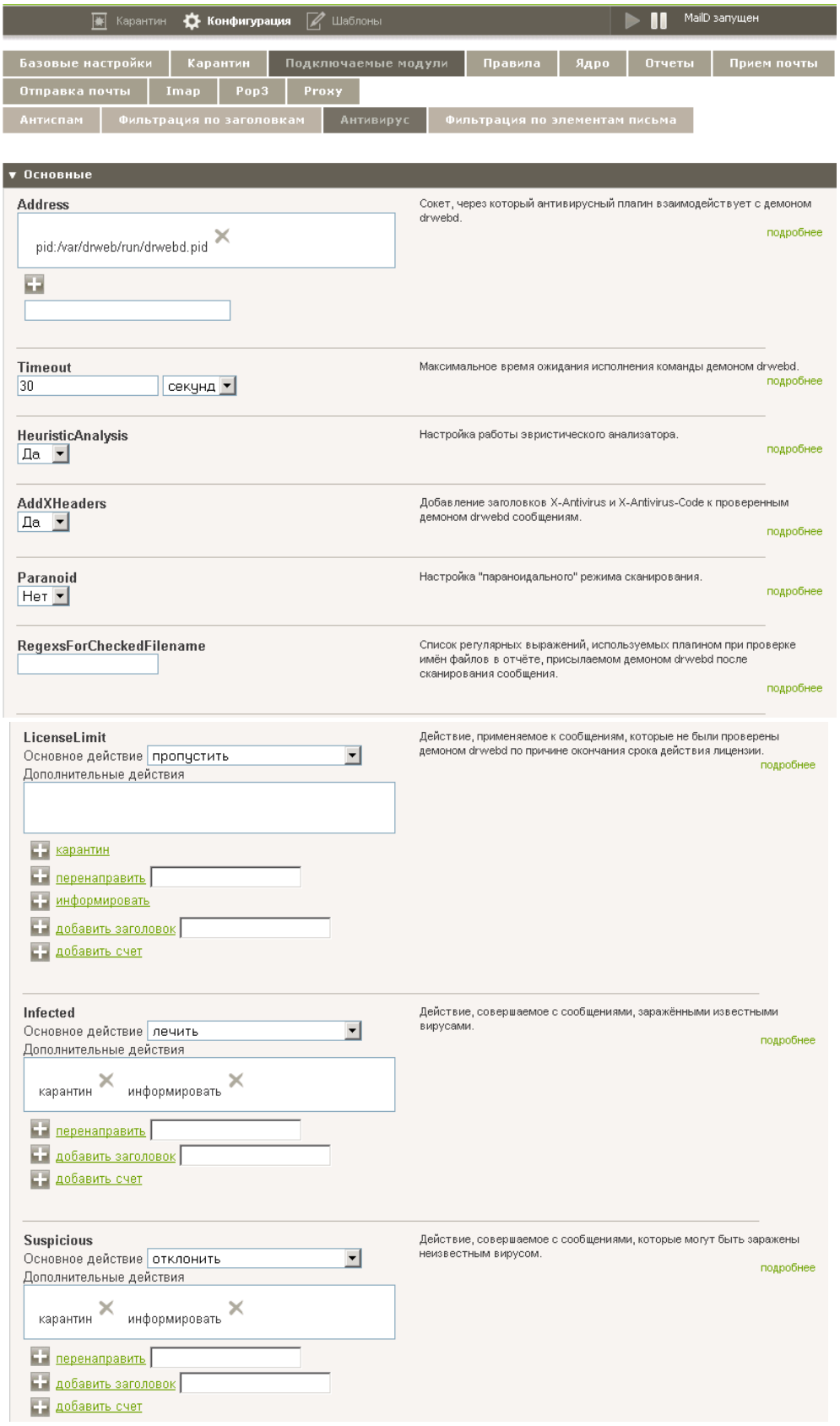
Определить действия по отношению к зараженному трафику можно либо через веб-интерфейс, либо напрямую — через редактирование конфигурационных файлов.

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  , для его удаления из списка —  . 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**.



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.

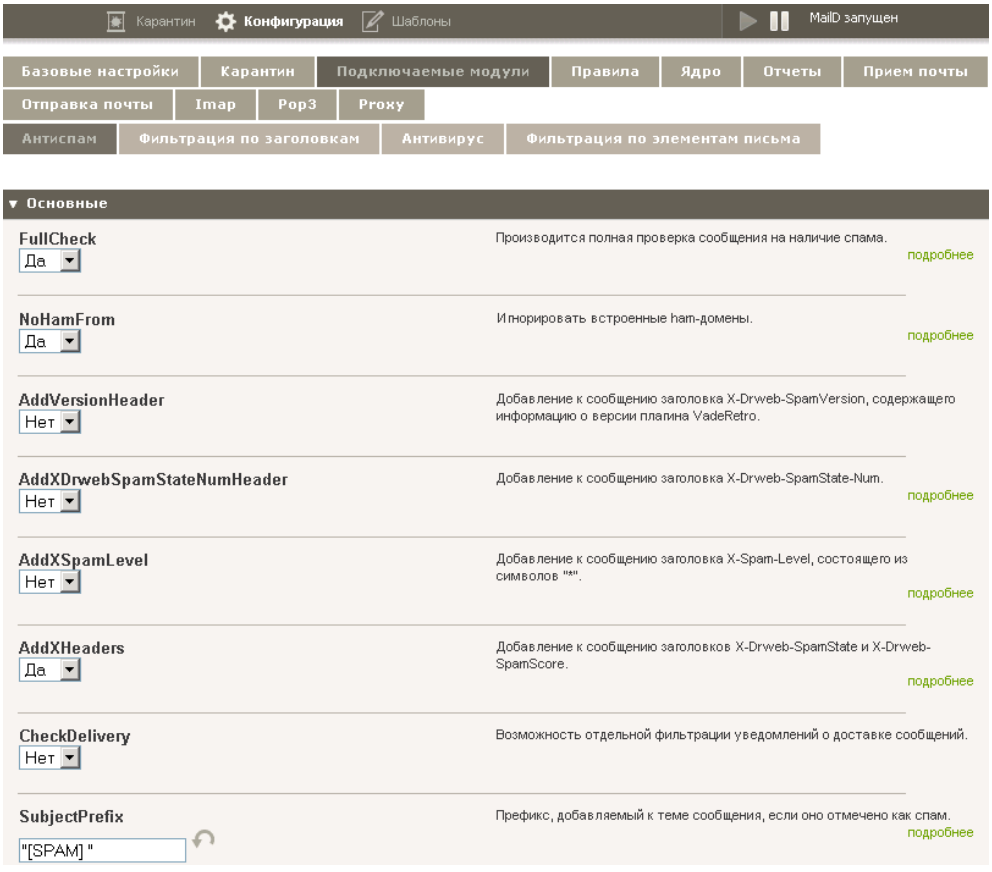
Для настройки через веб-интерфейс необходимо выбрать пункт **Dr.Web консоль для почтовых серверов UNIX** в меню **Службы** и перейти на закладку **Подключаемые модули**, находящуюся в меню **Конфигурация**, открыть **Антиспам** и выставить необходимое значение для параметра `Action`. Для большинства 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).

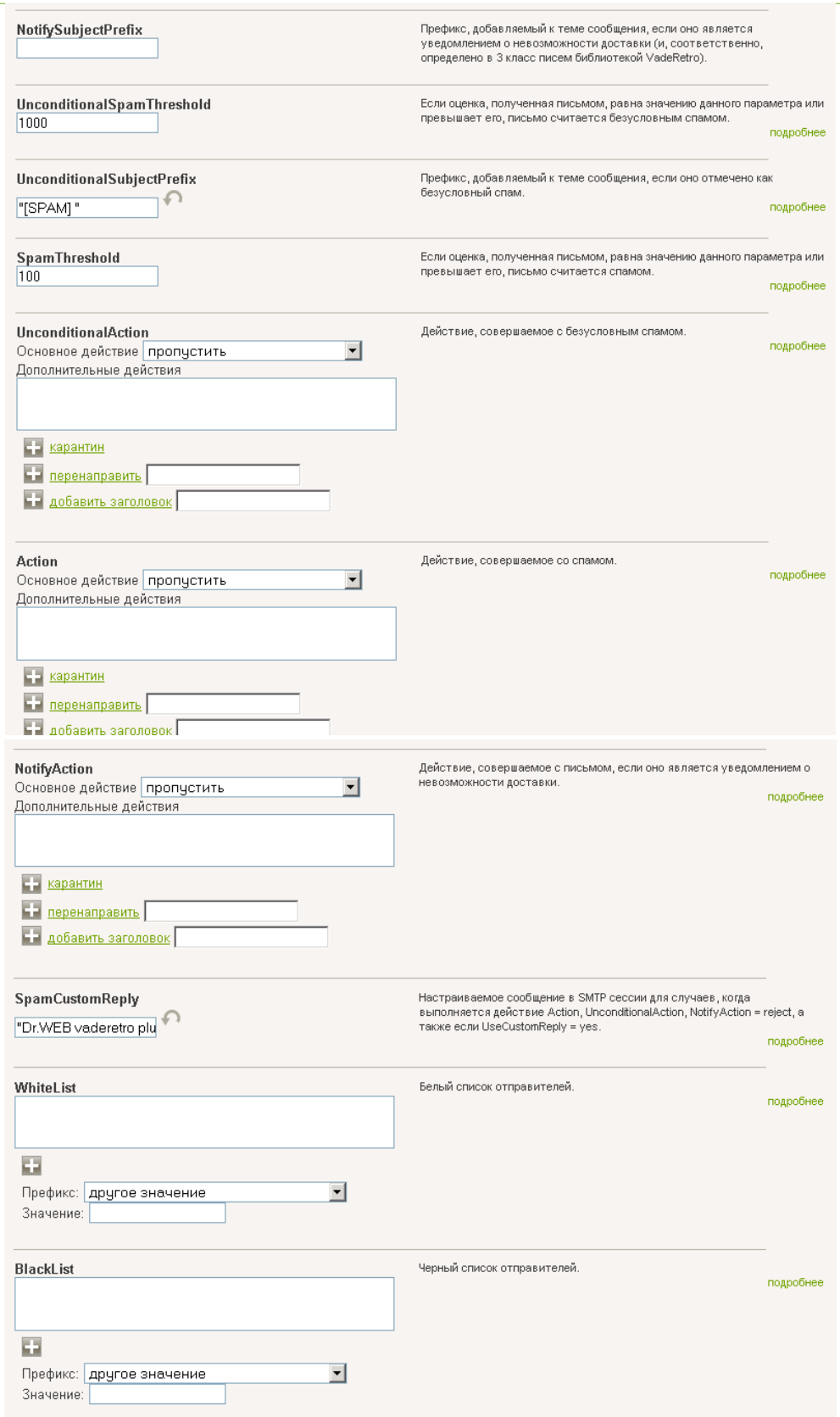
Система фильтрации по умолчанию добавляет в служебный заголовок строку `X-DrWeb-SpamState: Yes/No`, где значение `Yes` показывает, что письму присвоен статус «спам». Определить префикс, добавляемый к теме письма, вы можете, используя параметр `SubjectPrefix`.

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**.





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`.

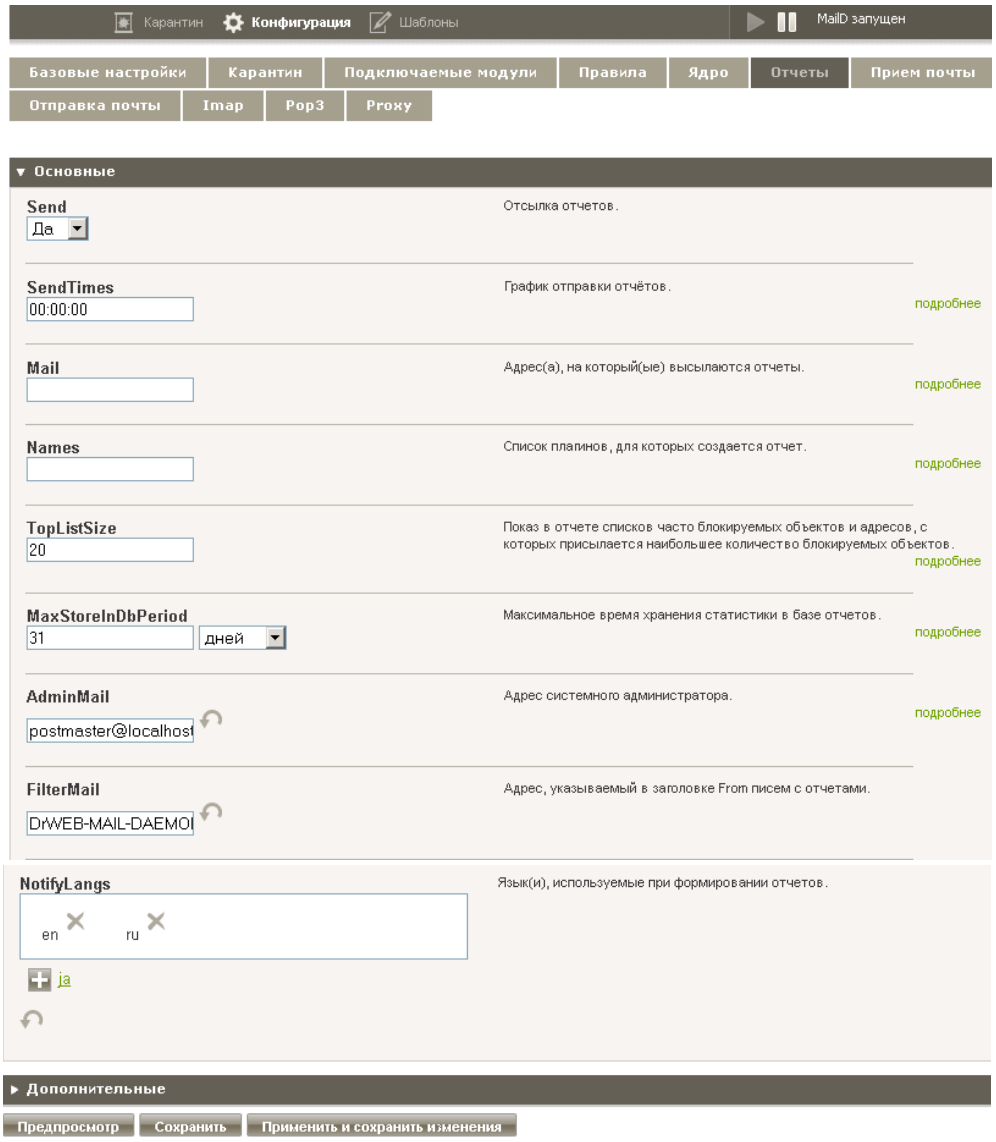
Применить сделанные изменения можно, нажав находящуюся внизу страницы кнопку **Применить и сохранить изменения (Apply and Save Settings)**.

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**.



На 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  , для его удаления из списка —  .

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.

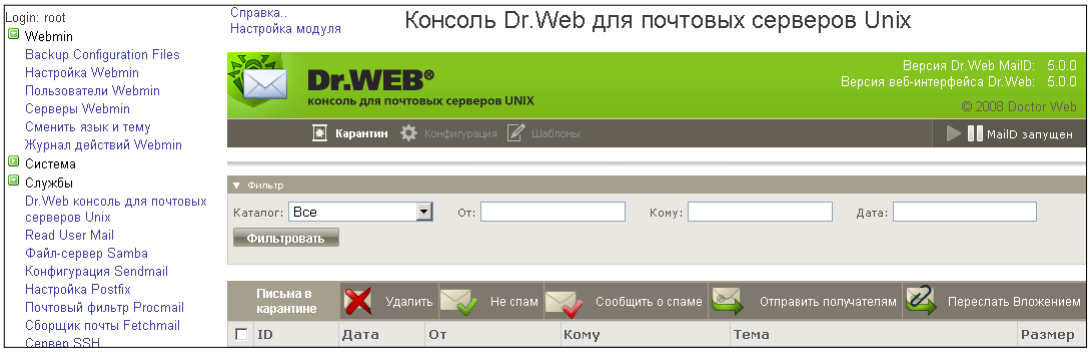
В карантине, созданном в файловой системе, содержатся поддиректории, названные именами компонентов, отвечающих за проверку почтовых сообщений. Письмо, отфильтрованное тем или иным компонентом, помещается в его «персональную» поддиректорию в директории карантина. Для каждого сообщения создается два файла: 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.

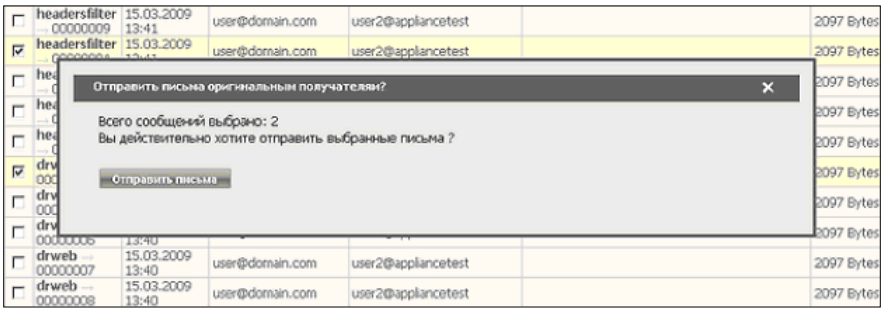
Наименование сообщений в карантине контролируется параметрами FilenamesMode и FilenamesPrefix страницы **Quarantine** меню **Configuration**.

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

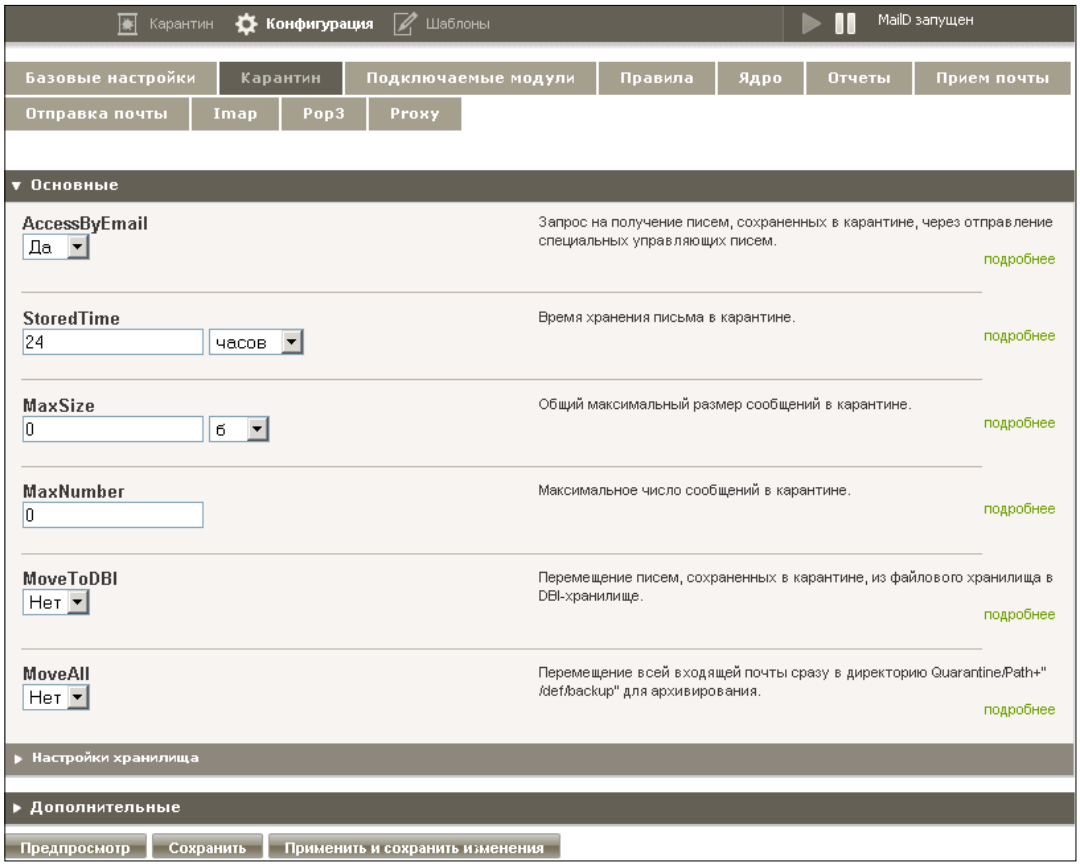
Для просмотра карантина необходимо выбрать пункт **Dr.Web консоль для почтовых серверов** и щелкнуть по меню **Карантин**.

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





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**.

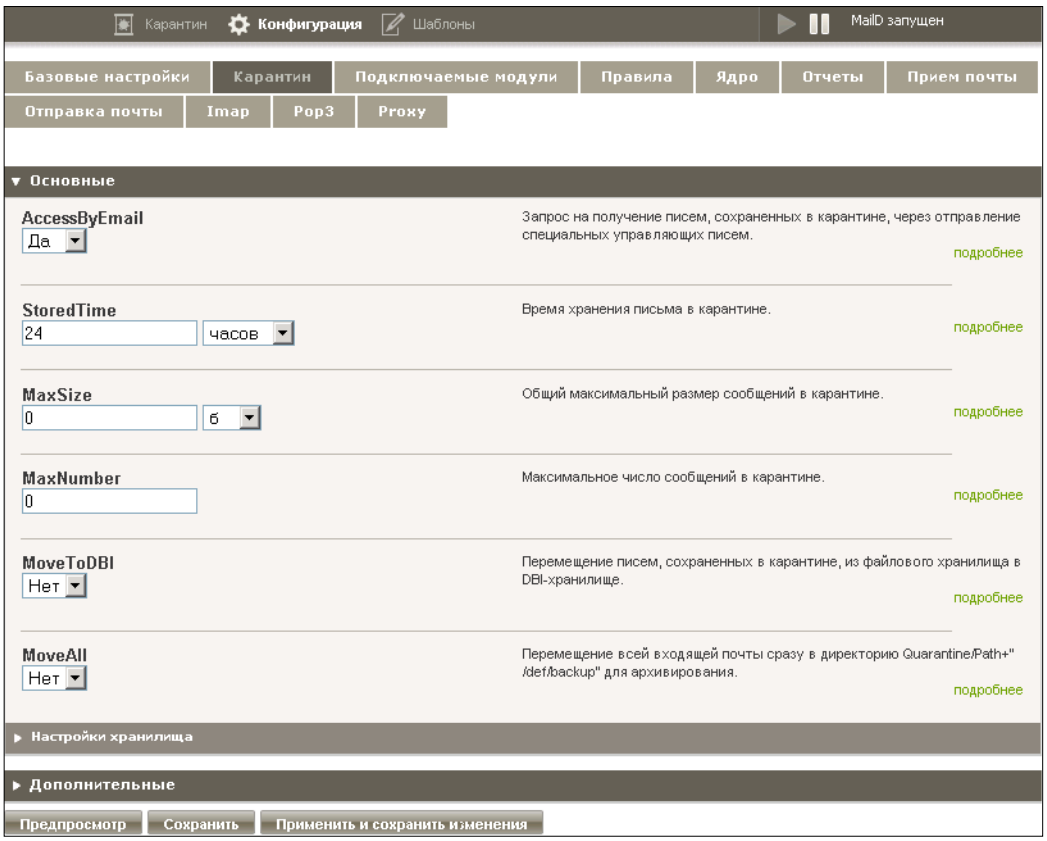


Системный администратор также может работать с карантином через `drweb-qcontrol` и интерфейс интерактивного управления.

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.

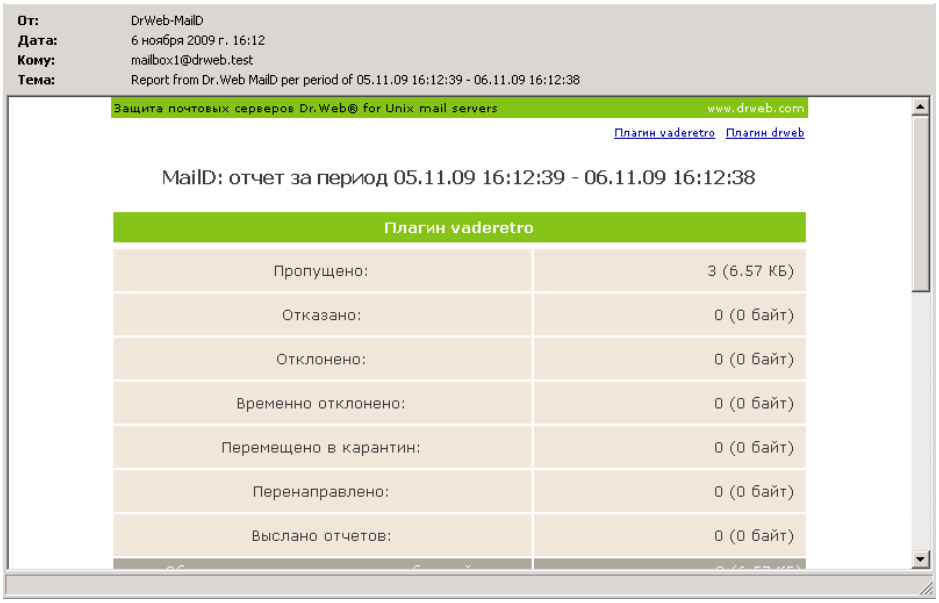
Для получения писем нужно поставить значение параметра `AccessByEmail`, задаваемого на закладке **Карантин** меню **Конфигурация**, в `Yes`.



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:

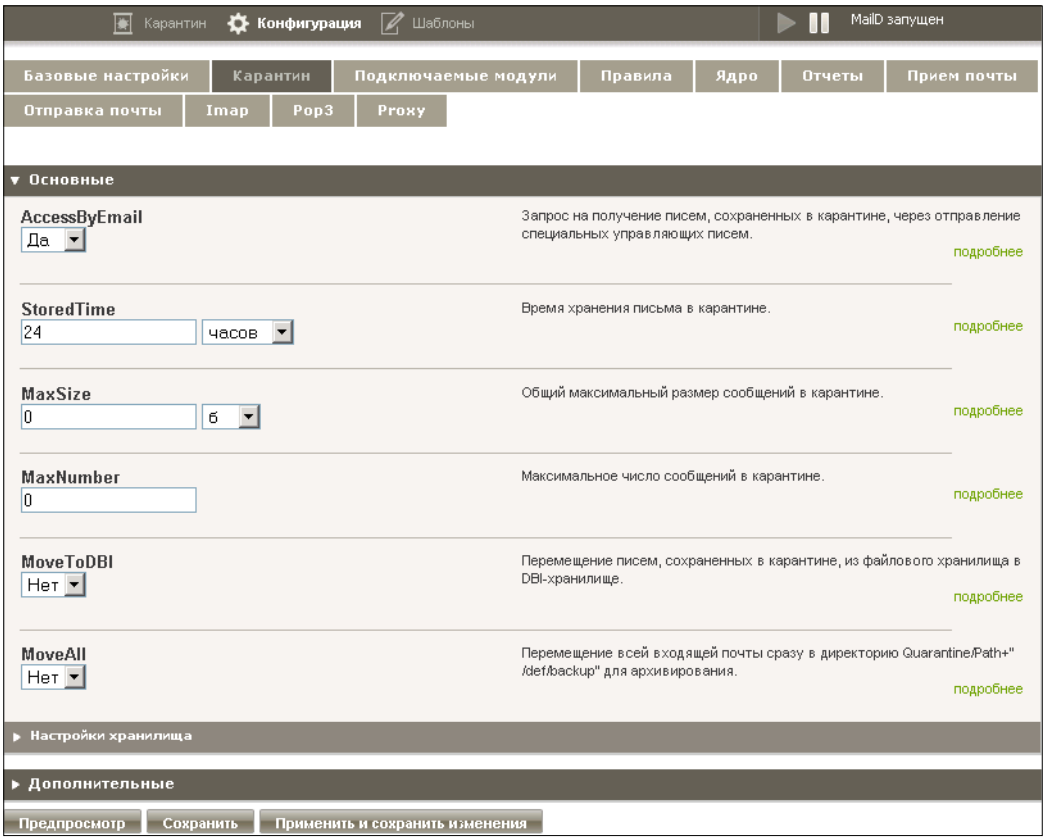


Если в качестве дополнительного действия выбрано уведомление о его блокировке (notify) и `AccessByEmail` выставлен в `Yes`, то в уведомлении, которое получит пользователь, будет содержаться ссылка, которая позволит самому пользователю получить сохраненное в карантине письмо.

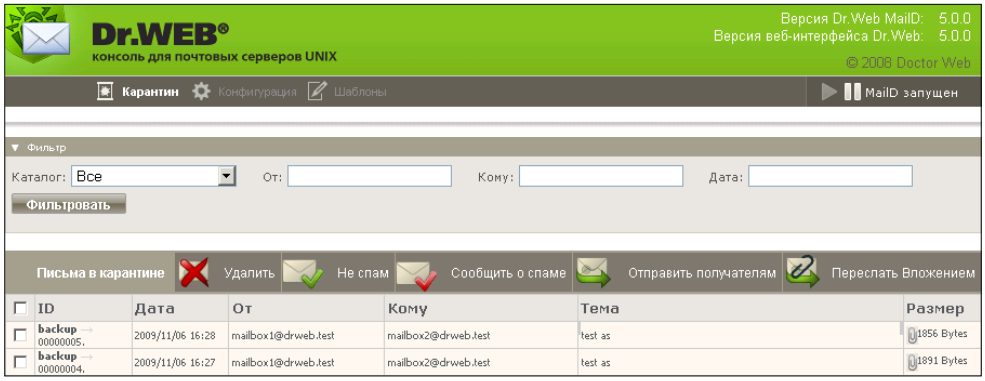
Внимание! Так как о спаме, сохраненном в карантине, уведомления не высылаются, то этим способом спам из карантина получить нельзя.

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`.



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



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`-сокет по адресу `/var/drweb/ipc/.ctl`.

```
[root@centos101 ~]# telnet 127.0.0.1 3009
Trying 127.0.0.1...
Connected to centos0.drweb.test (127.0.0.1).
Escape character is '^]'.
Dr.Web MailD v.5.0.0. Feci, quod potui, faciant meliora potentes.
```

```
Sles11Sp1:~/Desktop # telnet 127.0.0.1 3009
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Dr.Web MailD v.6.0.0.0. Welcome!

> 
```

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
```

```
# PublicKeyFile = {FilePath}
# public key file for accessing ES server.
PublicKeyFile = /opt/drwcs/Installer/drwcsd.pub

# ServerHost = {Address}
# IP-address of ES server
ServerHost = 127.0.0.1

# ServerPort = {Digital}
# Port for accessing ES server
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:

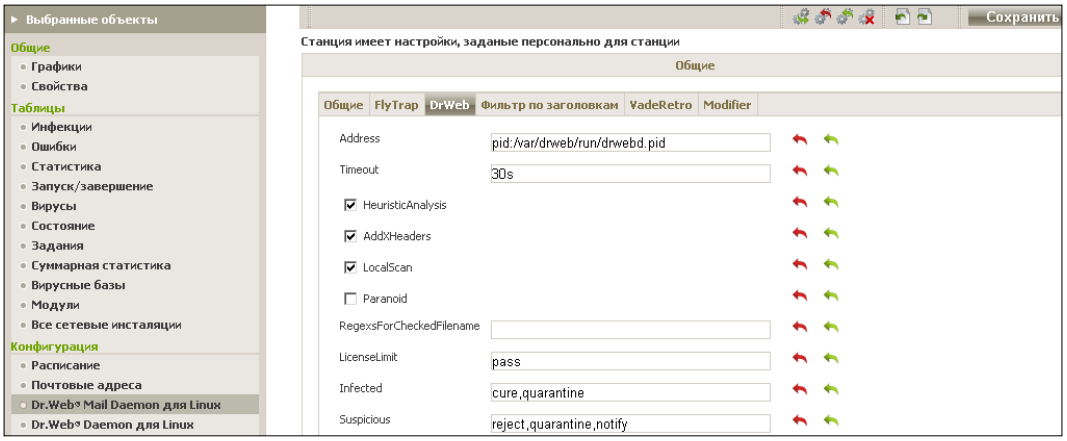
```
/etc/init.d/drweb-monitor start
```

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  или  .

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**.

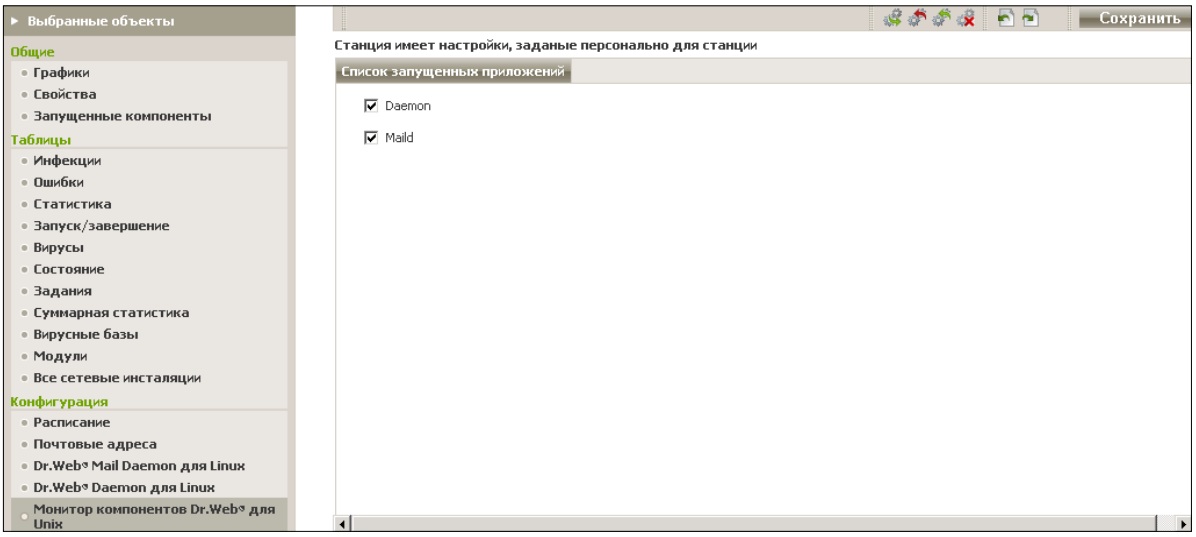


Для сохранения введенных параметров необходимо нажать кнопку **Сохранить**.

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.



- 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 `drweb-monitor` 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.

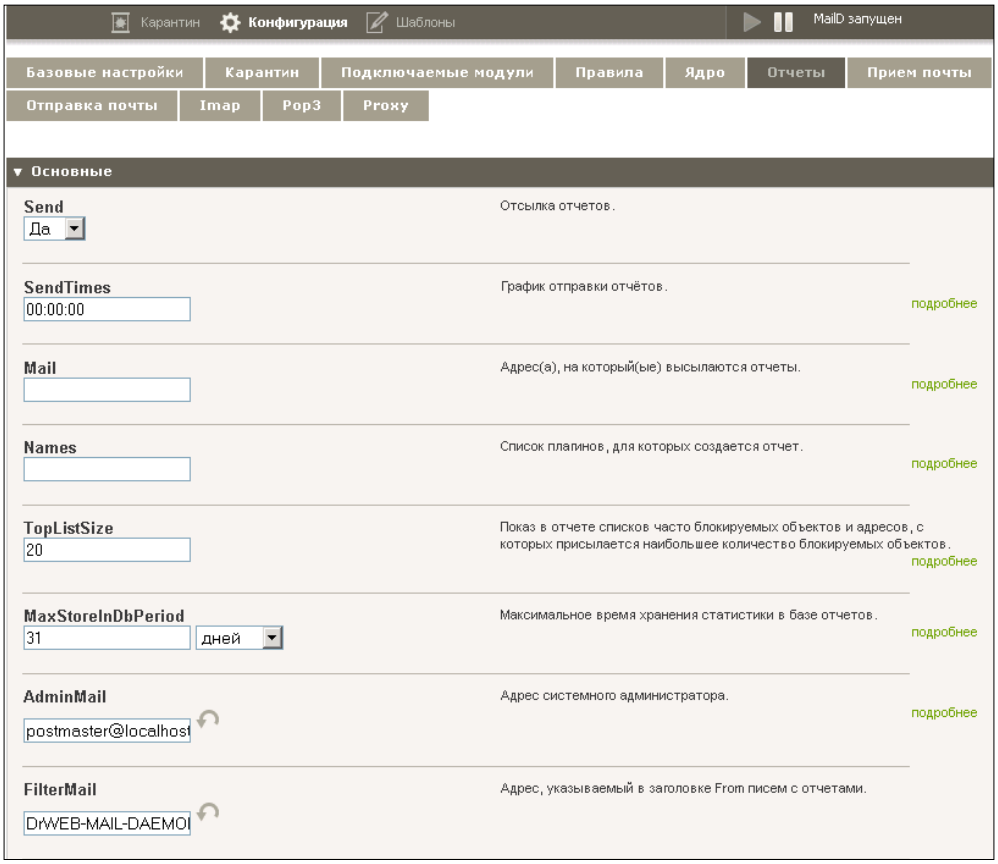
5.2. Тестирование функционирования системы фильтрации почтового трафика

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**.



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

`__to__address__` — 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 с `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.

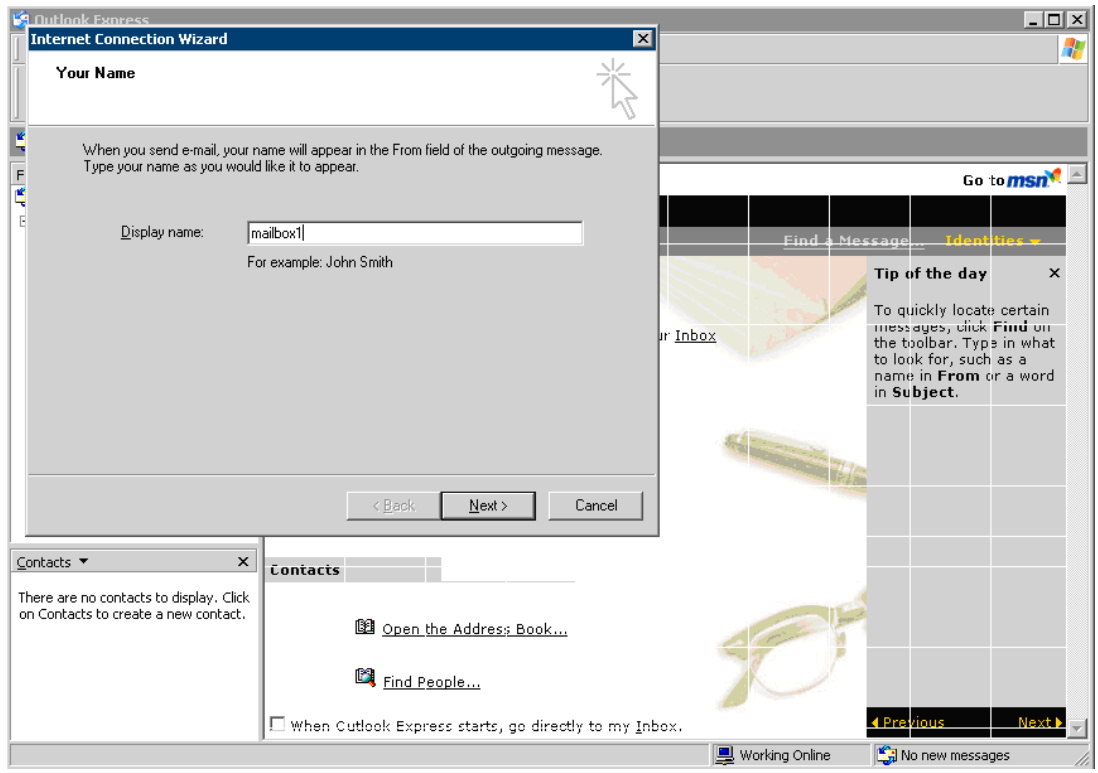
Рекомендуемое время тестирования: 60 минут с учетом установки и настройки необходимых утилит, сбора и формирования тестового набора файлов.

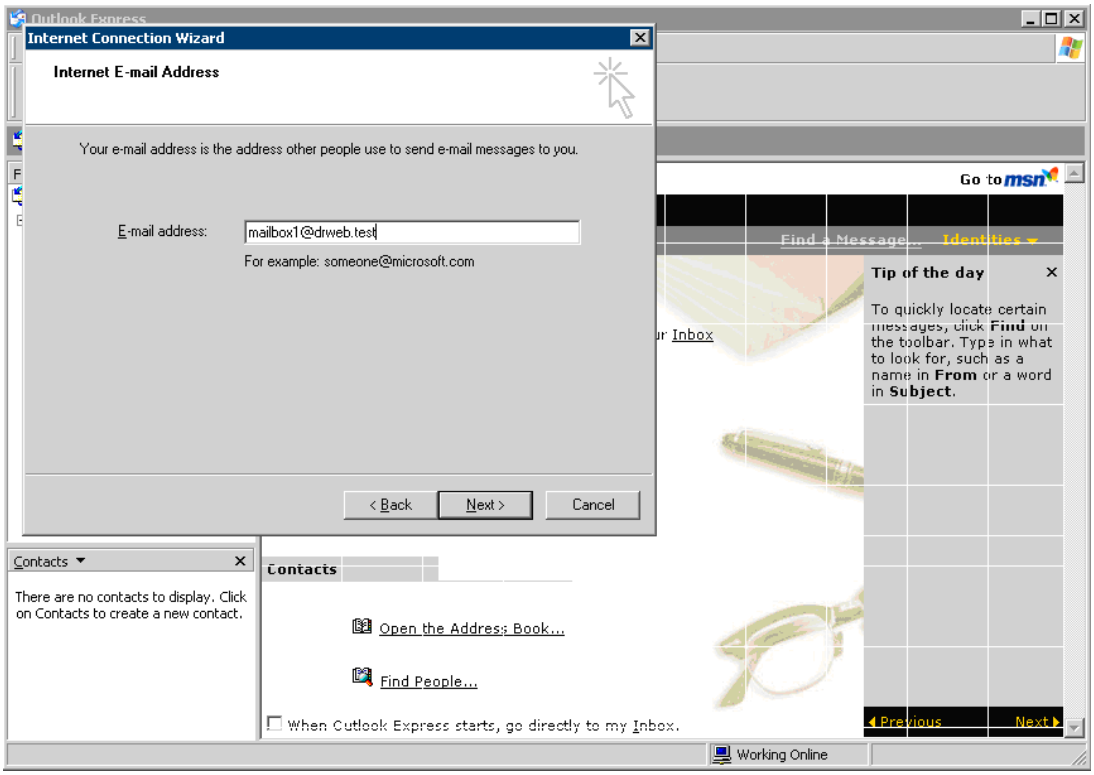
Если вы используете для тестирования операционную систему типа Windows, то для тестирования сервиса защиты почты можно использовать установленный по умолчанию почтовый клиент Outlook Express. В предоставленной для тестирования системе заведены два почтовых ящика — `mailbox1` и `mailbox2`. Пароль доступа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

Выбрать пункт **Internet Accounts** в меню **Tools**.

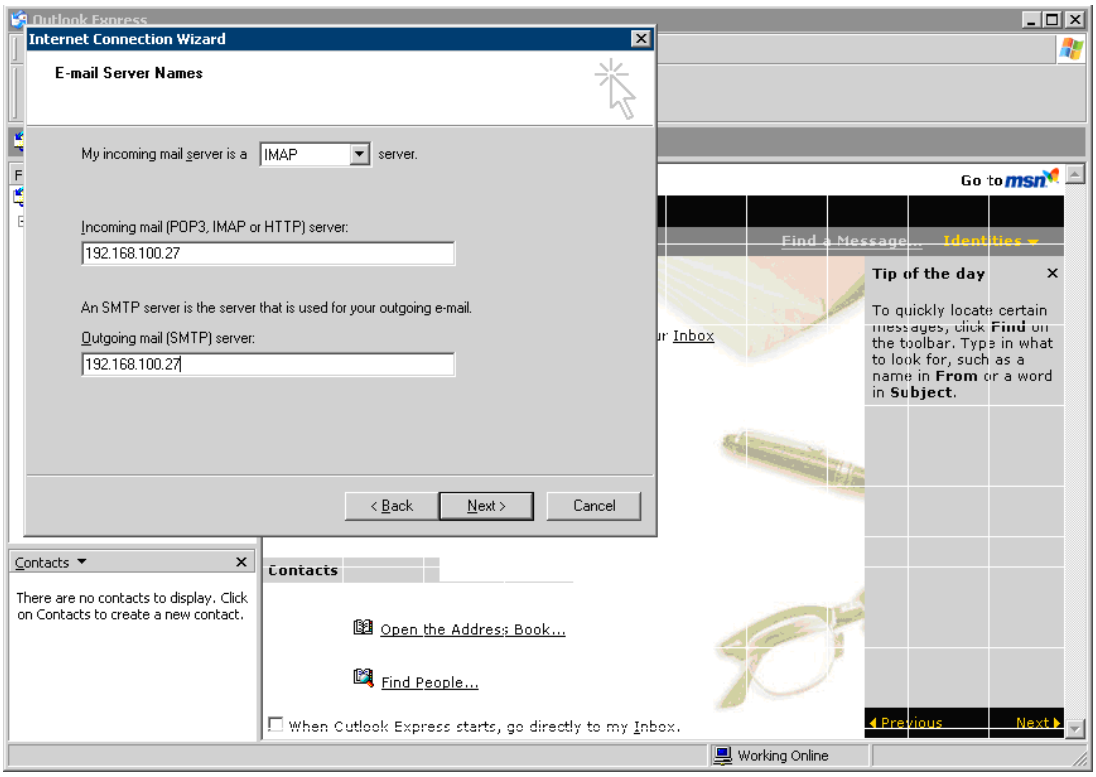
Нажать кнопку **Add** и выбрать **Mail**.

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

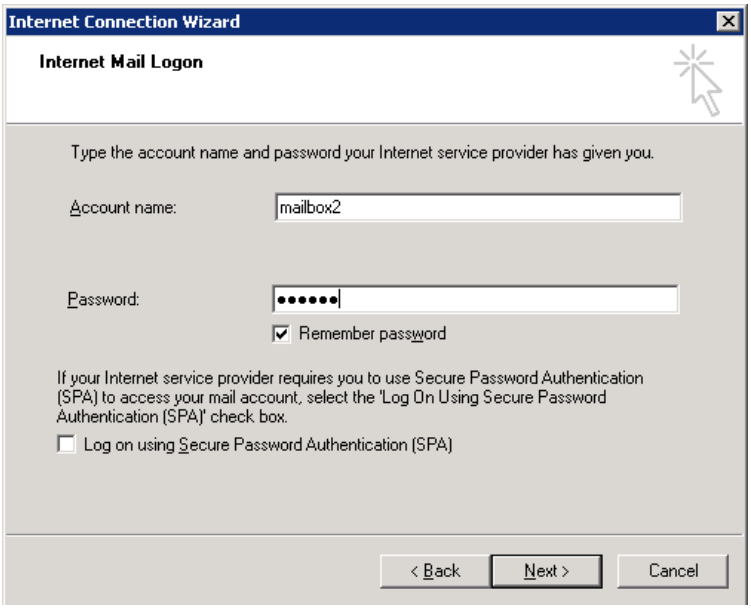




Указать серверы для входящей и исходящей почты. В данном случае указывается адрес сервера, на котором была произведена установка. Тип сервера — `IMAP`.



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



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

```
X5O!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 X5O /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:

Администратор сервиса также получит уведомление об отправке пользователем вируса.

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.

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