ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky Anti-Spam 2.0
Enterprise Edition / ISP Edition

РУКОВОДСТВО АДМИНИСТРАТОРА

KASPERSKY ANTI-SPAM 2.0
ENTERPRISE EDITION / ISP EDITION

Руководство администратора

Тел., факс: +7 (095) 797-87-00
http://www.kaspersky.ru

Тел., факс: +7 (095) 422-71-98
http://www.ashmanov.com

Дата редакции: июнь 2004 года

Содержание

ГЛАВА 1. KASPERSKY ANTI-SPAM 2.0 ENTERPRISE EDITION / ISP EDITION

Kaspersky Anti-Spam Enterprise Edition / ISP Edition версии 2.0 является программным комплексом, который осуществляет фильтрацию электронной почты с целью защиты пользователей почтовой системы от нежелательных анонимных массовых рассылок – спама.

Kaspersky Anti-Spam осуществляет фильтрацию входящей электронной почты в процессе ее приема по SMTP-протоколу, т. е. до того, как письма попадут в почтовые ящики пользователей. На основании правил, заданных администратором, Kaspersky Anti-Spam обрабатывает сообщение, а именно: доставляет получателю в неизменном виде, блокирует, генерирует сообщение о невозможности приема письма, добавляет или изменяет заголовок, и т. п.

Каждое входящее электронное письмо проверяется на присутствие в нем признаков нежелательного сообщения (спама).

Во-первых, проверяются всевозможные атрибуты письма: адреса отправителя и получателя (envelope), размер письма, его заголовки (включая заголовки *From* и *To*). В частности, фильтр обнаруживает следующие "подозрительные" ситуации:

- наличие e-mail отправителя и получателей в "черных" списках; их отсутствие в "белых" списках;
- наличие IP-адреса отправителя в "черных" списках; его отсутствие в "белых" списках;
- наличие IP-адреса отправителя в том или ином DNS-based real time black hole list (RBL);

RBL (**real time black hole list**) – база данных IP-адресов почтовых серверов с неконтролируемыми рассылками. Такие почтовые сервера принимают почту от кого угодно и отправляют ее далее кому угодно.

Если с какого-либо адреса постоянно рассылается спам, и администрация сервера, через который идет рассылка, не принимает никаких мер, можно сообщить о спамере в RBL. Спамера занесут в базу данных, что дает возможность автоматически запрещать прием почты с этого почтового

сервера.

Некоторые из служб RBL заносят в базу данных бесплатные почтовые сервисы и другие "добропорядочные" сервера; поэтому во избежание ложных срабатываний фильтра их данными необходимо пользоваться с осторожностью.

- отсутствие сервера отправителя в DNS;
- соответствие одного из заголовков письма заданному шаблону (regular expression);
- слишком большой размер письма.

Подробнее об анализе почтовых сообщений см. в п. 4.3.1 на стр. 28.

Во-вторых, используется *контентная фильтрация*, т. е. анализируется содержание самого письма (включая заголовок *Subject*) и файлов вложений[1]. Применяются лингвистические алгоритмы, основанные на сравнении с письмами-образцами и на поиске характерных терминов (слов и словосочетаний).

Письма, не подпадающие под параметры какого-либо правила и алгоритма контентной фильтрации, отправляются адресатам в неизменном виде.

Над письмами, в которых обнаружены те или иные признаки нежелательной корреспонденции, выполняются действия, указанные в *правилах фильтрации* (см. п. 4.3 на стр. 27).

Профили (наборы правил) фильтрации, а также списки адресов, на которые они ссылаются, и другие настройки Kaspersky Anti-Spam редактируются администратором почтового сервиса при помощи программы веб-конфигуратор.

[1] Проверяются вложения форматов Plain text, HTML, Microsoft Word, RTF; подробнее см. п. 4.3.2 на стр. 29.

Kaspersky Anti-Spam поставляется вместе с предустановленными профилями (наборами правил) фильтрации, обеспечивающими эффективное обнаружение спама и несколько вариантов его обработки. Прежде, чем приступить к использованию Фильтра, ознакомьтесь с предлагаемыми схемами фильтрации (см. п. 4.4 на стр. 38) и выберите оптимальные для вас.

Если вы хотите отредактировать предустановленные профили фильтрации или создать новые, внимательно прочитайте главы данного Руководства, посвященные логике работы Фильтра (см. п. 4.3 на стр. 27) и его настройке с помощью программы веб-конфигуратор (Глава 5 на стр. 52).

Отнеситесь к настройке Фильтра с максимальным вниманием. Неправильная настройка может привести:

- к неэффективности работы Фильтра (большинство нежелательных сообщений пропускается);
- к потере "нормальной" (желательной) почты.

Компания "Ашманов и Партнеры" постоянно ведет работу по совершенствованию и пополнению лингвистических данных, используемых для обнаружения спама. Для эффективной борьбы со спамом необходимо регулярно получать последнюю версию таких данных с помощью скрипта получения обновлений (см. Глава 6 на стр. 96).

Мы настоятельно рекомендуем настроить автоматический запуск обновления данных из cron с частотой не менее 4-6 раз в день.

Мы желаем вам успешной работы с Kaspersky Anti-Spam и надеемся, что вы оцените его важные преимущества:

- использование методов искусственного интеллекта для анализа содержания почтовых сообщений (контентной фильтрации);
- объединение всех методов фильтрации в едином модуле, возможность их комбинирования;
- централизованное управление всеми правилами фильтрации через единый веб-интерфейс.

1.1. Что нового в версии 2.0

В версии 2.0 Kaspersky Anti-Spam по сравнению с предыдущей версией существенно доработаны и расширены следующие возможности:

- *Интеграция в почтовые системы*. При **стандартной установке** Kaspersky Anti-Spam 2.0 интегрируется в почтовую систему, уже установленную у пользователя, в качестве фильтрующего модуля. Поддерживаются почтовые системы: Postfix, Sendmail, Qmail, Exim, Communigate Pro
- *Реализован новый инсталлятор*. Kaspersky Anti-Spam 2.0 распространяется в виде стандартных пакетов: *rpm*, *deb* для Linux и *tgz* для FreeBSD, которые устанавливаются при помощи штатных инсталляторов, входящих в состав операционных систем Linux и FreeBSD.
- *Улучшены пользовательские свойства*:
    - Улучшена система записи в журнал системных событий (syslog), появилась возможность собирать статистические данные о количестве обработанных писем и о процентном соотношении спама и не спама стандартными для unix-систем средствами анализа отчетов.
    - Разметка писем, признанных спамом, стала более удобной: метка ставится в начало темы письма.
- *Повышена стабильность работы приложения*:
    - Решены проблемы функционирования приложения на операционных системах Linux Red Hat 9, Suse 9, Red Hat Enterprise Edition и пр.
    - Из состава приложения сключена устаревшая утилита проверки лицензий (*kavuccsf*). Новый лицензионный модуль стабильно работает на различных версиях Linux и FreeBSD.
    - Из состава приложения исключен устаревший http-сервер (*_httpd*). Для работы с веб-конфигуратором используется стандартный сервер *thttpd* (возможно также использование сервера apache).
- *Повышена производительность работы приложения в два раза*, а также *оптимизирована работа со службами RBL*: повышена скорость выполнения запросов.
- *Повышено качество распознавания спама*:
    - Улучшено качество распознавания спама со вложенными картинками; внедрена технология GSG-2.
    - Добавлена возможность проверки IP-адресов не только последнего транспортного агента (relay), но и всех предыдущих (на основе разбора заголовков **Received**).

- Улучшено качество разбора писем в формате HTML: алгоритмы фильтрации "невидимого" текста, случайных последовательностей и пр.
- Добавлен анализ писем в формате UUE-Encoded.

- *Разработана OEM-версия приложения*. Наряду с готовыми решениями (Kaspersky Anti-Spam 2.0 Enterprise и Kaspersky Anti-Spam 2.0 ISP) сформирован SDK для интеграции механизмов фильтрации спама в OEM-решения.

1.2. Лицензионная политика

Kaspersky Anti-Spam 2.0 имеет два вида лицензирования:

- лицензирование по трафику (объему почты, прошедшему через фильтр) за определенный период времени;
- по почтовым адресам.

Во втором случае контроль за использованием Kaspersky Anti-Spam ведется по количеству и именам обрабатываемых почтовых адресов в течение периода действия лицензии.

В программе веб-конфигуратор на закладке **settings** в соответствии с ключевым файлом формируется список лицензированных почтовых адресов (см. п. 5.2.7.2 на стр. 93). Общее количество адресов не должно превышать число, оговоренное лицензией. Почтовые сообщения, содержащие адреса, заведенные сверх лицензированного объема или не указанные вообще, фильтроваться не будут (почтовые сообщения будут доставляться в неизменном виде).

Не забудьте перед началом использования Фильтра отредактировать список лицензированных получателей!

1.3. Аппаратные и программные требования к системе

Для корректной работы Kaspersky Anti-Spam необходимо соответствие системы следующим аппаратным и программным требованиям:

- Операционная система Linux или FreeBSD 4.x, работающая на платформе Intel x86.

- Процессор Intel Pentium III с частотой не менее 500 MHz.
- Оперативная память не менее 256 МБ.
- Наличие установленных программ **wget**, **bzip2**.
- Наличие одной из почтовых систем: Sendmail, Postfix, Exim, Qmail, Communigate Pro.

1.4. Комплект поставки

Программный продукт вы можете приобрести у наших дистрибьюторов (коробочный вариант), а также в одном из интернет-магазинов (например, www.kaspersky.ru, раздел **Электронный магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта;
- руководство пользователя;
- лицензионный ключ, записанный на установочный компакт-диск;
- регистрационная карточка (с указанием серийного номера продукта);
- лицензионное соглашение.

Перед тем как распечатать конверт с компакт-диском, внимательно ознакомьтесь с лицензионным соглашением.

При покупке продукта в интернет-магазине вы копируете продукт с веб-сайта "Лаборатории Касперского", в дистрибутив которого помимо самого продукта включено также данное руководство. Лицензионный ключ либо включен в дистрибутив, либо отправляется вам по электронной почте по факту оплаты.

1.4.1. Лицензионное соглашение

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО "Лаборатория Касперского", в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение!

Если вы не согласны с условиями лицензионного соглашения, вы можете вернуть коробку с Антивирусом Касперского дистрибьютору, у которого она была приобретена, и получить назад сумму, уплаченную за подписку. При этом конверт с установочным компакт-диском должен оставаться запечатанным.

Открывая запечатанный пакет с установочным компакт-диском или устанавливая продукт на компьютер, вы тем самым принимаете все условия лицензионного соглашения.

1.4.2. Регистрационная карточка

Пожалуйста, заполните отрывной корешок регистрационной карточки, по возможности наиболее полно указав свои координаты: фамилию, имя, отчество (полностью), телефон, адрес электронной почты (если она есть), и отправьте ее дистрибьютору, у которого вы приобрели программный продукт.

Если впоследствии у вас изменится почтовый/электронный адрес или телефон, пожалуйста, сообщите об этом в организацию, куда был отправлен корешок регистрационной карточки.

Регистрационная карточка является документом, на основании которого вы приобретаете статус зарегистрированного пользователя нашей компании. Это дает вам право на техническую поддержку в течение срока подписки. Кроме того, зарегистрированным пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского", высылается информация о выходе новых программных продуктов.

1.5. Сервис для зарегистрированных пользователей

ЗАО "Лаборатория Касперского" предлагает своим легальным пользователям большой комплекс услуг, позволяющих увеличить эффективность использования Антивируса Касперского.

Приобретя подписку, вы становитесь зарегистрированным пользователем программы и в течение срока действия подписки получаете следующие услуги:

- предоставление новых версий данного программного продукта;

- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией данного программного продукта, оказываемые по телефону и электронной почте;
- оповещение о выходе новых программных продуктов Лаборатории Касперского и о новых вирусах, появляющихся в мире (данная услуга предоставляется пользователям, подписавшимся на рассылку новостей ЗАО "Лаборатория Касперского").

Консультации по вопросам функционирования и использования операционных систем, а также работы различных технологий не проводятся.

1.6. Принятые обозначения

Текст документации выделяется различными элементами оформления в зависимости от его смыслового назначения. В расположенной ниже таблице приведены используемые условные обозначения.

Оформление	Смысловое назначение
Жирный шрифт	Названия меню, пунктов меню, окон, элементов диалоговых окон и т. п.
 Примечание.	Дополнительная информация, примечания.
 Внимание!	Информация, на которую следует обратить особое внимание.
 *Чтобы выполнить действие,* 1. Шаг 1. 2. …	Описание последовательности выполняемых пользователем шагов и возможных действий.
 Задача, пример	Постановка задачи, примера для реализации возможностей программного продукта

Оформление	Смысловое назначение
 Решение	Реализация поставленной задачи
[ключ] – назначение ключа.	Ключи командной строки.
`Текст информационных сообщений и командной строки`	Текст конфигурационных фай, информационных сообщений программы и командной строки.

ГЛАВА 2. СОСТАВ И АРХИТЕКТУРА KASPERSKY ANTI-SPAM

Начиная с версии 2.0, Kaspersky Anti-Spam не является полнофункциональным почтовым агентом (MTA), способным принимать почту, пересылать ее или доставлять сообщения в почтовые ящики конечных пользователей. Эти функции выполняет почтовая система (MTA), установленная на сервере.

Kaspersky Anti-Spam 2.0:

1. интегрируется в почтовую систему;
2. получает от нее письма;
3. производит проверку на наличие в них признаков спама;
4. в зависимости от полученного результата производит модификацию писем (проставляет и модифицирует заголовки, меняет список получателей);
5. возвращает письма почтовой системе для дальнейшей доставки.

Внутренняя архитектура Kaspersky Anti-Spam представлена на рис. 1.

Клиентские модули предназначены для интеграции Kaspersky Anti-Spam в различные почтовые системы. Каждый клиентский модуль учитывает особенности конкретной почтовой системы и выбранного способа интеграции.

В поставку Kaspersky Anti-Spam включены клиентские модули для почтовых систем Sendmail, Postfix, Exim, Qmail и Communigate Pro.

Как правило, клиентский модуль устанавливается в MTA в качестве фильтра и обеспечивает прием от почтовой системы писем, подлежащих фильтрации, и возврат в нее модифицированных писем.

Запуск клиентских модулей осуществляется почтовой системой. MTA может запустить несколько клиентских процессов для параллельной обработки нескольких писем. Подробнее о клиентских модулях и способах их интеграции в почтовые системы см. раздел А.3 на стр. 105.

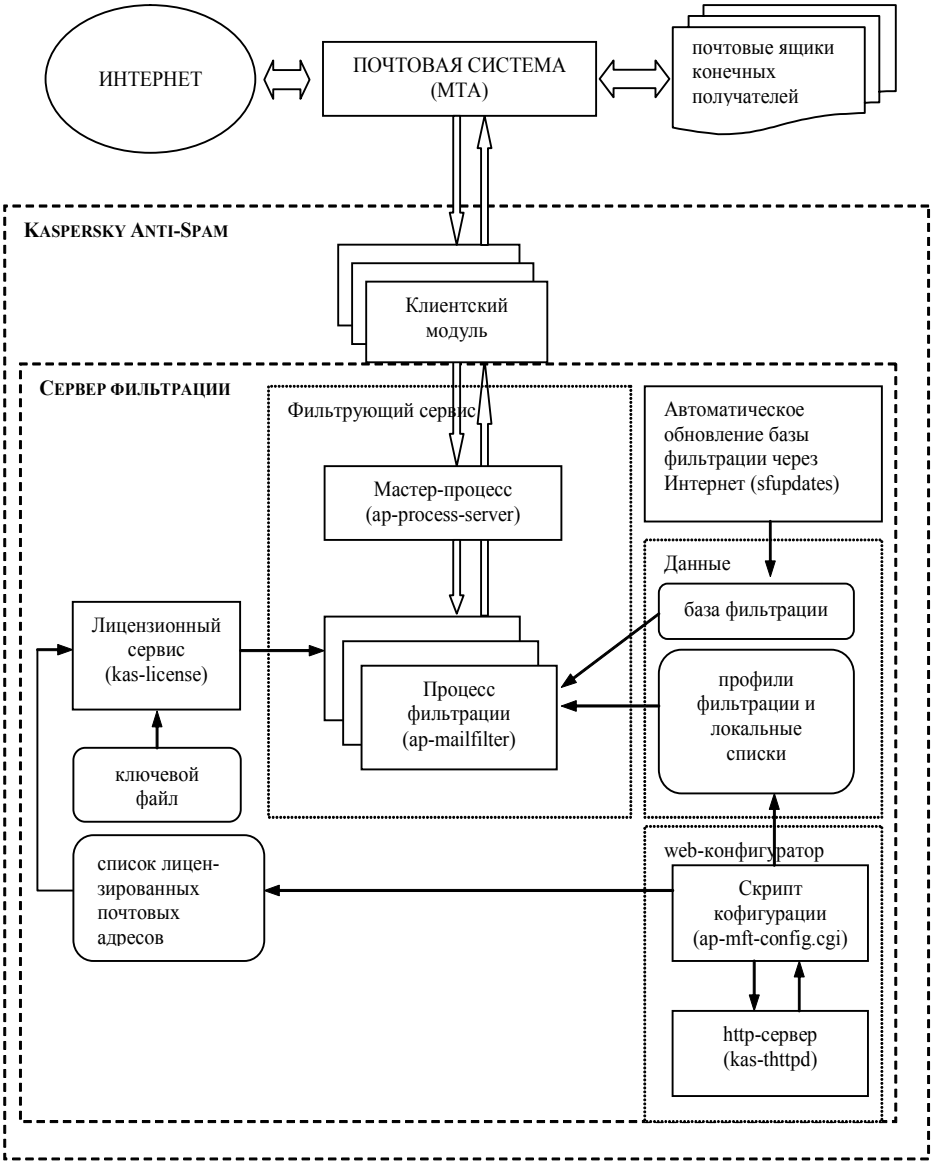

Рисунок 1. Внутренняя архитектура Kaspersky Anti-Spam

Вне зависимости от особенностей того или иного клиентского модуля, взаимодействие клиента и основной части Kaspersky Anti-Spam – сервера фильтрации – осуществляется единообразно с использованием внутреннего протокола обмена данными через сетевой или локальный сокет.

Сервер фильтрации отвечает на запросы обращающихся к нему клиентов, принимает от них письма для проверки и возвращает им результаты.

При использовании стандартной процедуры инсталляции почтовая система с интегрированным в нее клиентским модулем и сервер фильтрации устанавливаются на одной и той же машине.

Однако существует возможность установить сервер фильтрации Kaspersky Anti-Spam на отдельном сервере: в этом случае клиенты, работающие на другом компьютере (сервере), будут обмениваться данными с сервером фильтрации через локальную сеть по протоколу TCP.

Работая на выделенном компьютере, сервер фильтрации может обслуживать сразу несколько почтовых серверов при условии, что мощности используемого компьютера достаточно для обработки суммарного почтового трафика.

В состав **сервера фильтрации** входят:

- фильтрующий сервис, который, собственно, и осуществляет проверку писем;
- лицензионный сервис, проверяющий наличие действительного ключевого файла и работающий со списком лицензированных почтовых адресов;
- скрипт автоматической загрузки и компиляции обновлений базы фильтрации;
- веб-конфигуратор;
- вспомогательные программы и скрипты.

Работа **фильтрующего сервиса** осуществляется под управлением **мастер-процесса** (*ap-process-server*), который:

- отслеживает запросы на соединение с процессом фильтрации, поступающие от клиентов;
- при отсутствии свободных процессов фильтрации запускает новые;
- отслеживает статус запущенных процессов (свободен/занят);
- при поступлении сигналов (например, SIGHUP) передает их дочерним процессам.

При значительном объеме почтового трафика количество запущенных процессов фильтрации может доходить до нескольких десятков. При снижении нагрузки на почтовую систему свободные фильтрующие процессы прекращают работу. Максимальное и минимальное количество запущенных фильтрующих процессов определяется настройками в конфигурационном файле мастер-процесса (см. п. А.1.2 на стр. 101).

Процесс фильтрации при старте загружает профили (наборы правил) фильтрации и открывает базу фильтрации (набор данных для контентного анализа). После установления соединения с клиентом процесс фильтрации получает от него заголовки и тело письма, проводит анализ и возвращает клиенту полученные результаты.

Анализ письма и применение к нему правил и профилей фильтрации производится только при наличии действующего лицензионного ключа. В случае, когда действует лицензия по почтовым адресам, проверка письма осуществляется только при наличии адреса получателя письма в списке лицензированных почтовых адресов.

Все проверки, связанные с лицензированием, осуществляются **лицензионным сервисом** (*kas-license*) по запросу от процесса фильтрации.

Закончив обработку письма, процесс фильтрации не прекращает работу, а ждет поступления нового запроса. Выполнение процесса фильтрации завершается после того, как он обработал максимальное для одного процесса количество писем (обычно 300) или долгое время находится в состоянии ожидания (idle).

Скрипт автоматической загрузки обновлений (*sfupdates*) запускается по расписанию (через crontab) и обеспечивает скачивание через интернет и компиляцию актуальной версии базы контентной фильтрации.

Веб-конфигуратор предоставляет администратору веб-интерфейс для редактирования профилей и правил фильтрации, ведения локальных белых и черных списков, а также списка лицензированных почтовых адресов.

ГЛАВА 3. УСТАНОВКА KASPERSKY ANTI-SPAM

Внимательно прочитайте данную главу, а также файл *readme-install*, в котором могут содержаться наиболее свежие рекомендации по установке программы.

3.1. Подготовка к установке

Прежде чем приступить к установке Kaspersky Anti-Spam:

- убедитесь, что система соответствует аппаратным и программным требованиям для установки Kaspersky Anti-Spam (см. п. 1.3 на стр. 12);
- убедитесь, что в вашем распоряжении имеется лицензионный ключ для продукта Kaspersky Anti-Spam 2.0 (Enterprise или ISP Edition);
- убедитесь, что установлены программы **wget**, **bzip2**, **perl**;
- убедитесь, что почтовая система, установленная на вашем сервере, функционирует корректно;
- сохраните резервные копии конфигурационных файлов почтовой системы.

Рекомендуем вам выполнять инсталляцию продукта в нерабочее время или тогда, когда поток почтовых сообщений наименьший!

Установка Kaspersky Anti-Spam производится в три этапа:

1. установка программ, входящих в состав Kaspersky Anti-Spam;
2. установка лицензионного ключа;
3. интеграция с почтовой системой.

3.2. Установка программ, входящих в состав Kaspersky Anti-Spam

Установка Kaspersky Anti-Spam должна осуществляться пользователем **root**.

Дистрибутив Kaspersky Anti-Spam 2.0 распространяется в нескольких вариантах:

- rpm-пакет для большинства версий операционной системы Linux (RedHat, SuSe, Mandrake, Fedora, ASP Linux, Alt Linux и др.);
- deb-пакет для Debian Linux;
- tgz-пакет для операционной системы FreeBSD;
- архив tar.gz с shell-инсталлятором для операционных систем без менеджера пакетов (например, Slackware).

Для установки Kaspersky Anti-Spam из rpm-пакета выполните команду:

```
rpm –i <имя_пакета>
```

Для установки Kaspersky Anti-Spam из deb-пакета выполните команду:

```
dpkg –i <имя_пакета>
```

Для установки Kaspersky Anti-Spam из tgz-пакета выполните команду:

```
pkg_add <имя_пакета>
```

Для установки Kaspersky Anti-Spam из архива tar.gz выполните команды:

```
tar xzvf <имя_архива>
cd <имя_распакованного_дистрибутива>
 ./install.sh
```

В процессе инсталляции будут выполнены следующие действия:

- создание пользователя и группы **mailflt**, необходимых для работы Kaspersky Anti-Spam;
- установка всех программ, входящих в состав Kaspersky Anti-Spam, в каталог */usr/local/ap-mailfilter*;
- создание и установка скрипта запуска фильтрующего сервиса (*ap-process-server*), лицензионного сервиса (*kas-license*) и http-сервера (*kas-thttpd*), который выполняется при перезапуске операционной системы;
- запуск необходимых программ и сервисов;
- создание записи в crontab пользователя **mailflt** для автоматического запуска скрипта загрузки обновлений базы контентной фильтрации.

В результате сервис фильтрации Kaspersky Anti-Spam будет установлен и запущен на вашем сервере, однако для того, чтобы осуществлялась фильтрация почтовых сообщений, необходимо выполнить установку лицензионного ключа и интеграцию Kaspersky Anti-Spam с почтовой системой.

3.3. Установка лицензионного ключа

Лицензионный ключ в соответствии с приобретенной лицензией поставляется вместе дистрибутивом Kaspersky Anti-Spam.

Если по каким-либо причинам в вашем распоряжении нет лицензионного ключа, обратитесь в службу поддержки Лаборатории Касперского (*support@kaspersky.com*).

Установка лицензионного ключа производится командой:

```
/usr/local/ap-mailfilter/bin/install-key
<имя_ключевого_файла>
```

В случае если лицензионный ключ не установлен или не действителен, Kaspersky Anti-Spam не осуществляет фильтрацию почты, однако работоспособность почтовой системы не нарушается: все письма доставляются получателям без проверки и соответствующей разметки.

Необходимо также учитывать, что в случае использования лицензии по почтовым адресам проверка осуществляется только для получателей, адреса которых входят в список лицензированных почтовых адресов (в пределах количества, оговоренного лицензией).

Не забудьте перед началом использования Фильтра ввести список лицензированных почтовых адресов!

3.4. Интеграция Kaspersky Anti-Spam с почтовой системой

Интеграция Kaspersky Anti-Spam с почтовой системой заключается в установке в почтовую систему клиентского модуля и внесении соответствующих изменений в ее конфигурационные файлы.

Эти действия выполняются автоматически при помощи универсального скрипта настройки MTA или при помощи скриптов настройки конкретной почтовой системы.

Подробная информация о способах интеграции клиентских модулей и об изменениях, которые вносятся в конфигурационные файлы почтовых систем, приведена в разделе А.3 на стр. 105.

Для интеграции Kaspersky Anti-Spam с почтовой системой, установленной на вашем сервере, запустите универсальный скрипт настройки MTA:

```
/usr/local/ap-mailfilter/bin/MTA-config.pl
```

В большинстве случаев этот скрипт определит тип используемого MTA и внесет необходимые изменения в его конфигурационные файлы.

Однако, если ваш MTA установлен или настроен нестандартно, то скрипт *MTA-config.pl* может не найти конфигурационных файлов. В этом случае нужно воспользоваться скриптом настройки конкретной почтовой программы:

Для интеграции Kaspersky Anti-Spam с почтовой системой Sendmail выполните команду:

```
/usr/local/ap-mailfilter/bin/sendmail-config.pl
```

Для интеграции Kaspersky Anti-Spam с почтовой системой Postfix выполните команду:

```
/usr/local/ap-mailfilter/bin/postfix-config.pl
```

Для интеграции Kaspersky Anti-Spam с почтовой системой Exim выполните команду:

```
/usr/local/ap-mailfilter/bin/exim-config.pl
```

Для интеграции Kaspersky Anti-Spam с почтовой системой Qmail выполните команду:

```
/usr/local/ap-mailfilter/bin/qmail-config.pl
```

Интеграция Kaspersky Anti-Spam с почтовой системой Communigate Pro осуществляется через веб-интерфейс почтовой системы (см. п. A.3.6.3 на стр. 120.

ГЛАВА 4. РАБОТА С KASPERSKY ANTI-SPAM И ПРИНЦИПЫ ФИЛЬТРАЦИИ

4.1. Настройка параметров фильтрации

Kaspersky Anti-Spam предоставляет вам мощный инструментарий для обнаружения спама в потоке входящей электронной почты. Действия с подозрительными письмами могут быть как самыми жесткими (отказ принять сообщение), так и достаточно мягкими (например, приписать сообщению дополнительный заголовок-"ярлык" для последующей обработки в почтовой программе получателя почты). Применение различных действий к различным типам спама – прерогатива администратора почтового сервиса.

Дистрибутив Kaspersky Anti-Spam включает набор предустановленных профилей фильтрации, обеспечивающих эффективную фильтрацию спама и альтернативные способы обработки распознанных спамерских писем (подробнее см. п. 4.4 на стр. 38).

Правила и профили фильтрации и порядок их применения могут быть отредактированы системным администратором через программу веб-конфигуратор (см. Глава 5 на стр. 52). Кроме того, при помощи веб-конфигуратора администратор имеет возможность включать и выключать использование тех или иных профилей.

Редактирование профилей фильтрации должно осуществляться с большой осторожностью, поскольку даже небольшие изменения могут привести к серьезным нежелательным последствиям: ложным срабатываниям Фильтра или снижению качества распознавания спама.

Настройка всех параметров работы Фильтра осуществляется через удобный веб-интерфейс, предоставляемый программой веб-конфигуратор.

Порядок работы с программой веб-конфигуратор и настройки параметров фильтрации описаны в Глава 5 на стр. 52.

Настоятельно рекомендуем вам прежде, чем приступать к настройке правил фильтрации, ознакомиться с принципами их применения, которые описаны в п. 4.3 на стр. 27.

4.2. Порядок обновления данных

Для анализа содержания писем Kaspersky Anti-Spam использует *Базу контентной фильтрации*, включающую образцы спамерских писем, характерные термины и другие данные. База постоянно обновляется и расширяется лингвистической лабораторией компании "Ашманов и Партнеры", поэтому для максимально эффективной борьбы со спамом вам необходимо регулярно скачивать ее обновление.

Доставка обновлений осуществляется через интернет *Скриптом получения обновлений*. Мы настоятельно рекомендуем включить скрипт получения обновлений в **crontab**. Периодичность его запуска желательно установить на уровне один раз в час.

По умолчанию обновления данных Фильтра скачиваются со следующего адреса: ftp://downloads1.kaspersky-labs.com/sfupdates; в случае необходимости этот адрес может быть заменен на альтернативный.

Обновления могут быть инкрементальными (добавление в базу новых записей) или полными (новая версия базы полностью заменяет старую); выбор и доставка необходимых для обновления файлов, компиляция Базы контентной фильтрации и перезапуск фильтрующего сервиса осуществляются автоматически.

Подробнее об обновлении Базы контентной фильтрации см. Глава 6 на стр. 96.

4.3. Принципы фильтрации

Обработка почтового сообщения заключается в последовательном применении к нему *правил фильтрации*.

Каждое правило фильтрации состоит из неупорядоченного множества *условий* и упорядоченного набора *действий*:

- обработка почтового сообщения начинается с *анализа*: проверяется выполнение условий, описанных в правиле;
- если хотя бы одно из условий не выполнено, обработка сообщения данным правилом прекращается без выполнения каких-либо действий;

- если все условия выполнены, над сообщением последовательно производятся действия, описанные в правиле (в том порядке, в котором они заданы).

Правила объединяются в группы – *профили фильтрации*. Профили фильтрации бывают двух типов:

- *общие* – для всех сообщений, независимо от их адресата;
- *персональные* – для сообщений, направленных отдельным адресатам.

4.3.1. Анализ адресов, заголовков и размера письма

В правилах фильтрации могут быть описаны условия следующих типов (а также их отрицания):

- IP-адрес сервера, с которого получено сообщение, (т. е. посылающего почтового relay'я) совпадает с указанным;
- IP-адрес сервера, с которого получено сообщение, входит в указанный список;
- какой-либо из сервисов DNS-based RBL, входящих в указанный список, выдает сообщение о "неблагонадежности" сервера, с которого получено сообщение;
- IP-адрес отправителя отсутствует в DNS;
- e-mail отправителя совпадает с указанным;
- e-mail отправителя входит в указанный список;
- e-mail получателя (одного из получателей, если их несколько) совпадает с указанным;
- e-mail получателя (одного из получателей, если их несколько) входит в указанный список;
- сообщение имеет какой-либо заголовок указанного типа (т. е. с указанным именем);
- сообщение имеет заголовок с указанным именем (например, *From* или *To*), соответствующий указанному шаблону (regular expression);
- общий размер письма превышает указанный предел;
- содержимое письма отнесено к определенной категории спама (см. п. 4.3.2 на стр. 29).

Списки, на которые ссылаются правила фильтрации, бывают следующих типов:

- **списки IP-адресов** – содержат IP-адреса в формате *aaa.bbb.ccc.ddd* или *aaa.bbb.ccc.ddd/nn*;
- **списки e-mail** – содержат адреса e-mail в формате *user@hostname.domain* или *@hostname.domain*, во втором случае подразумевается любой пользователь указанного домена;
- **списки служб DNS-based RBL** – содержат названия зон, которые используются для формирования запроса к DNS с целью проверки IP-адреса на его присутствие в "черном" списке (например, для проверки *IP=202.103.129.8* через *zone="blackholes.mail-abuse.org"* формируется запрос к DNS с именем домена *8.129.103.202.blackholes.mail-abuse.org*).

Проверка e-mail получателя производится:

- в общих профилях – по полному списку получателей;
- в персональных профилях – по списку тех из получателей исходного сообщения, для которых данный профиль применяется.

Правило фильтрации может содержать одновременно несколько условий различных типов. Например, могут блокироваться письма, у которых получатель принадлежит к списку A, а отправитель – списку B (B – "черный список" для получателей из списка A).

4.3.2. Анализ содержания письма – контентная фильтрация

Электронное письмо может не иметь никаких формальных признаков спама – быть направленным конкретному получателю с адреса, еще не попавшего ни в какие черные списки – и при этом содержать "сомнительную" информацию. Для того чтобы распознать и обработать такие письма (на русском и английском языках), используются алгоритмы *контентной фильтрации*.

С использованием технологий искусственного интеллекта анализируется содержание самого письма (включая заголовок *Subject*), а также вложений (прикрепленных файлов) в следующих форматах:

- текстовый: plain text (ASCII, не multibyte);
- HTML (2.0, 3.0, 3.2, 4.0, XHTML 1.0);
- Microsoft Word (версии 6.0, 95/97/2000/XP);

- RTF.

Задача Kaspersky Anti-Spam состоит в том, чтобы уменьшить поток нежелательной корреспонденции, засоряющей почтовые ящики пользователей. Стопроцентное обнаружение нежелательной корреспонденции не может быть гарантировано – в частности и потому, что слишком жесткие критерии неизбежно привели бы к "отфильтровыванию" части полезной корреспонденции.

Для обнаружения писем с "сомнительным" содержанием используются два основных метода:

- сравнение с письмами-образцами (путем сопоставления их лексических составов);
- обнаружение характерных терминов – слов и словосочетаний.

Все данные, используемые Kaspersky Anti-Spam для контентной фильтрации – *рубрикатор* (иерархический список категорий), образцы писем, характерные термины и т. п. – хранятся в *Базе контентной фильтрации*.

Лингвистическая лаборатория компании "Ашманов и Партнеры" ведет постоянную работу по пополнению и совершенствованию Базы контентной фильтрации. Поэтому рекомендуется регулярно обновлять данные Базы (см. Глава 6 на стр. 96). Системный администратор может также добавлять в Базу новые образцы спамерских писем (см. п. 5.2.6 на стр. 89).

По результатам контентного анализа почтовое сообщение может быть отнесено к одной или нескольким категориям рубрикатора Базы контентной фильтрации.

Устанавливая правила фильтрации с помощью программы веб-конфигуратор (см. Глава 5 на стр. 52), системный администратор должен задавать и правила обработки почтовых сообщений, отнесенных к различным категориям рубрикатора[2].

Безусловным приоритетом системного администратора при настройке Фильтра должно быть сохранение всей "полезной" корреспонденции, поскольку потеря одного важного письма может принести конечному пользователю значительно больший вред, чем получение десятков несанкционированных писем. Во избежание

[2] Отнесение письма к одной из категории рубрикатора необязательно означает, что письмо содержит спам. Например, письмо, содержащее нецензурную лексику, будет отнесено к категории *Obscene*. Эту категорию системный администратор при желании может просто игнорировать (не упоминать ее в условиях правил).

потери нужной корреспонденции рекомендуется применять к письмам, "отбракованным" по результатам контентного анализа, только мягкие способы обработки. Например:

- дописывать в заголовок *Subject* предупреждение "[Спам]";
- приписывать дополнительный заголовок *Keywords=...*, позволяющий получателям перенаправлять такие письма в специальные папки средствами своих почтовых клиентов.

4.3.3. Действия над письмами

Если для почтового сообщения выполнены условия, описанные в правиле фильтрации (см. п. 4.3.1 на стр. 28 и п. 4.3.2 на стр. 29), то к сообщению применяются описанные в этом правиле *действия*.

Действия бывают:

- *"жесткими"* – выполнение такого действия завершает обработку письма;
- *"полужесткими"* – выполнение такого действия завершает выполнение действий текущего правила и всех правил текущего профиля, однако к письму могут быть применены правила других профилей;
- *"нежесткими"* – после выполнения такого действия продолжается выполнение других действий текущего правила, а также других правил из того же и/или других профилей.

В одном правиле может быть описано несколько действий, но если какое-либо из них жесткое или полужесткое, то после его выполнения обработка письма данным правилом (а также всеми другими правилами текущего профиля) прекращается, и никакие последующие действия не "сработают".

Порядок действий внутри одного правила жестко задан.

В правилах фильтрации могут быть описаны действия следующих типов:

- "Жесткие" действия:
  - **reject** – отказаться принимать данное сообщение на уровне SMTP-chat. Фильтрующий сервер возвращает посылающему почтовому серверу ошибку 550 в процессе приема письма по протоколу SMTP. Текст сообщения об ошибке может быть задан с помощью программы веб-конфигуратор (см. п. 5.2.7 на стр. 91).

    В персональном профиле вместо действия *reject* выполняется комбинация действий **bounce + black hole**

(поскольку персональный профиль может действовать только для части адресатов, а "частичный" отказ от приема письма невозможен).

- **black hole** – уничтожить сообщение (не пересылать его дальше), не генерируя никаких уведомлений отправителю.

  

  Правилами с действием данного типа следует пользоваться с осторожностью: письмо полностью уничтожается и не может быть восстановлено.

  В общем профиле блокируется доставка сообщения всем получателям, в персональном – тем, для которых действует данный персональный профиль.

- **accept** – переслать сообщение адресату (адресатам) без изменения, т. е. в том виде, который оно получило в результате предшествующей обработки. При выполнении данного действия сообщение безотлагательно пересылается; никакие другие правила фильтрации к нему не применяются. Правила с действием **accept** используются для реализации "белых" списков.

  Кроме того, **accept** выполняется по умолчанию в конце обработки любого письма (копии письма), если только не было выполнено одно из действий **reject** или **black hole**:

  - в конце частного профиля для всех получателей данного частного профиля;
  - после выполнения всех частных профилей для всех необработанных получателей.

- "Полужесткое" действие **skip** – прекратить выполнение всех правил текущего профиля фильтрации и перейти к выполнению следующего профиля (если порядок выполнения профилей это предусматривает, см. п. 4.3.4 на стр. 34).

  В персональном профиле действие **skip** равнозначно действию **accept**.

- "Нежесткие" действия:

  - **bounce** – сгенерировать уведомление об отказе принять письмо для почтового сервера, от которого оно получено.

    Вместе с таким уведомлением посылается оригинальное сообщение в качестве вложения. Текст уведомления может быть задан с помощью программы веб-конфигуратор (см. п. 5.2.7 на стр. 91). Обработка сообщения продолжается, и,

если не сработало другое правило, блокирующее доставку, оно будет доставлено получателю (получателям).

- **change recipient** – изменить список получателей сообщения:
  - заменить адреса всех получателей на адрес (список адресов), указанный в правиле (**replace all**);
  - удалить указанный адрес получателя (**delete**);
  - добавить к списку получателей адрес (список адресов), указанный в правиле (**add**).

  При задании списка новых получателей, может использоваться макропеременная **${SMTP_FROM}**, обозначающая адрес отправителя сообщения, указанный в SMTP-envelope.

- **change header** – изменить указанный в правиле заголовок сообщения:
  - удалив старое значение заголовка с указанным именем (если он у сообщения уже был), дописать новое, указанное в правиле (**replace**);
  - оставив без изменения старое значение заголовка (если он у сообщения уже был), дописать к нему новое значение, указанное в правиле (**add**);
  - добавить новый заголовок с указанным именем и значением; заголовок добавляется в начало списка заголовков; наличие в письме других заголовков с тем же именем никак не контролируется (**create**);
  - удалить все заголовки с указанным именем, если они были у сообщения (**delete**).

  Это действие позволяет приписать сообщению признаки, на основе которых клиентское ПО (например, Microsoft Outlook) сможет произвести фильтрацию или сортировку писем после их доставки в почтовый ящик пользователя.

  При указании нового значения заголовка может быть использован оператор **${CATEGORY}**, обозначающий список категорий спама, полученный при контентном анализе текста сообщения. Такой список может быть записан, например, в заголовок *Keywords*.

В общем профиле изменение заголовков производится для всех получателей сообщения, в персональном – для тех, для которых действует данный персональный профиль.

4.3.4. Порядок применения профилей и правил фильтрации

4.3.4.1. Порядок применения профилей

Как было сказано выше, профили фильтрации могут быть *общими* (их правила выполняются для всех адресатов любого письма) и *персональными* (их правила выполняются для конкретных адресатов).

Обработка письма осуществляется по следующей схеме:

1. для всего письма в целом выполняются правила одного общего профиля фильтрации[3]; если при этом сработало правило с *жестким действием*, выполнение которого означает прекращение дальнейшей обработки сообщения (см. п. 4.3.3 на стр. 31), никакие другие профили к данному сообщению не применяются;
2. если обработка письма не завершена и у письма несколько получателей, для каждого получателя создается виртуальная[4] копия письма;
3. для каждой копии письма выполняются правила одного персонального профиля фильтрации, либо просто выполняется действие **accept**;
4. на этом обработка письма заканчивается; перед отправлением писем получателям и/или отказов отправителям виртуальные копии, различающиеся только получателями, объединяются.

[3] В предустановленном комплекте профилей фильтрации срабатывают два общих профиля фильтрации, один из которых (выполняемый первым) – скрытый, то есть его редактирование через веб-конфигуратор не предусмотрено. Этот скрытый профиль, обеспечивающий распознавание подозрительных заголовков письма, автоматически обновляется через интернет вместе с Базой контентной фильтрации.

[4] Копия виртуальная, т. к. в реальности копии письма создаются только в тот момент, когда оказывается, что для разных получателей оно должно быть обработано по-разному.

Выбор **общего профиля**, срабатывающего на этапе 1, одинаков для всех обрабатываемых писем и осуществляется тривиальным способом. Программа веб-конфигуратор позволяет системному администратору создать несколько общих профилей фильтрации, однако "включить" (сделать активным) можно только один из них; правила остальных профилей не выполняются.

Выбор **персонального профиля**, срабатывающего на этапе 3, более сложен; он осуществляется отдельно для каждой виртуальной копии (точнее, для каждого адресата).

Программа веб-конфигуратор позволяет системному администратору создавать и подключать персональные профили в произвольном количестве и порядке. Администратор задает список получателей каждого персонального профиля; такой список может быть и пустым. Администратор имеет возможность выписать список получателей непосредственно или через ссылку на один из имеющихся списков адресов электронной почты (см. п. 5.2.2.1 на стр. 58).

Для каждой виртуальной копии письма выбирается и выполняется первый по порядку персональный профиль, в списке получателей которого есть адресат данной виртуальной копии. (Если получатель письма указан в списках нескольких профилей, для него всегда будет срабатывать только первый из них.)

Если такого профиля нет, т. е. адресата нет ни в одном из списков, выполняется первый по порядку профиль с пустым списком получателей. Таким образом, этот профиль применяется по умолчанию для писем всем адресатам, не упомянутым в других персональных профилях[5].

Наконец, если и такого профиля нет, для данной виртуальной копии по умолчанию выполняется действие **accept**, и на этом выполнение этапа 3 завершается.

Таким образом, к каждому сообщению всегда применяется один общий (активный) профиль, а затем, если обработка сообщения не завершена в общем профиле, для каждого из получателей применяется один из персональных профилей (или не применяется никакой, если для данного получателя не найдено "подходящего" персонального профиля).

[5] Другие частные профили с пустым списком пользователей не применяются никогда.

Если в результате применения общего профиля список получателей был изменен, то персональные профили применяются для измененного списка получателей; изменение же списка получателей в персональном профиле не оказывает влияния на применение персональных профилей – для вновь появившегося получателя другой персональный профиль применен не будет.

Внутри каждого профиля правила применяются в соответствии с их порядком, до тех пор, пока в текущем профиле не кончатся правила, либо пока в одном из правил не будет выполнено жесткое или полужесткое действие.

4.3.4.2. Модификация письма в процессе обработки

Существуют два типа действий, при выполнении которых письмо изменяется. **Change recipient** меняет список адресатов письма, а **change header** – какой-либо из его заголовков.

Оба действия нежесткие, и после их выполнения обработка письма продолжается. При этом последующие действия применяются уже к измененной версии письма[6].

Пусть, например, для почтового сообщения с адресатом x выполнено действие **change recipient**, меняющее x на y. Теперь для этого сообщения сработает правило, условием которого будет наличие у письма адресата y. А правило, требующее наличия адресата x, наоборот, не сработает.

Если в процессе применения общего профиля список адресатов изменился, то создание виртуальных копий и выбор персонального профиля для каждой из них пройдут уже в соответствии с обновленным списком.

При выполнении персонального профиля все действия производятся над одной виртуальной копией письма. Несмотря на то, что она "привязана" к конкретному адресату, действие **change recipient** вполне может к ней применяться, т. е. ее адресат может быть изменен.

[6] При этом первоначальные значения заголовков и т. п. сохраняются и при необходимости используются; так, вызов Библиотеки контентной фильтрации осуществляется с использованием исходного вида заголовка Subject.

Изменение адресата в процессе выполнения персонального профиля не означает, что к сообщению теперь должны применяться правила другого профиля (соответствующего новому адресу получателя). Продолжается выполнение правил текущего персонального профиля, который был выбран для первоначального адресата данной копии.

4.3.4.3. Результаты работы Фильтра

Результаты работы Фильтра для письма (или его виртуальной копии для конкретного адресата) в конечном счете определяются тем, какие действия были выполнены, и в каком порядке.

Наибольшее влияние на "судьбу" письма обычно оказывает действие, выполняемое последним. Поэтому сводка возможных результатов обработки письма (копии) ниже приводится в зависимости от последнего действия.

Выше уже говорилось, что если для письма (копии) не было выполнено одно из "жестких" действий – **reject**, **black hole** или **accept** – то в конце обработки **accept** выполняется по умолчанию. Таким образом, последним может быть только одно из трех указанных действий.

Действие **skip** в сводке не упоминается, поскольку это действие влияет только на порядок применения правил, но никаких операций непосредственно с письмом не предусматривает.

Последнее действие – **reject**

В случае срабатывания действия **reject** при выполнении общего профиля письмо отвергается на уровне SMTP-протокола; посылающему серверу возвращается код ошибки 550.

Действия, которые могли предшествовать **reject** – генерация уведомления (**bounce**), изменение заголовка или адресата (**change header**, **change recipient**) – фактически игнорируются.

При выполнении персонального профиля действие **reject** заменяется на **bounce + black hole**.

Последнее действие – **black hole**

Адресатам сообщение не доставляется.

Уведомление об отказе принять письмо отправителю не посылается (если только до выполнения **black hole** не было выполнено действие **bounce**).

Если до **black hole** было выполнено **bounce**, сообщение (копия) адресатам не доставляется, но отправителю посылается уведомление об отказе принять письмо.

Изменение заголовка или адресата (**change header**, **change recipient**), которые могли быть выполнены до **black hole**, фактически игнорируются.

В общем профиле блокируется доставка сообщения всем получателям, в персональном – тем, для которых действует данный персональный профиль.

Последнее действие – accept

Письмо доставляется адресатам.

При этом дополнительные нежесткие действия, которые могли быть выполнены до **accept**, оказывают на результат непосредственное влияние. (Это влияние может быть комплексным, если выполнено несколько дополнительных действий.)

Если выполнено действие **change recipient**, письмо доставляется по измененному списку адресов. Например, письмо может быть отправлено на специальный служебный адрес для архивации.

Если выполнено действие **change header**, письмо доставляется с измененными заголовками.

Если выполнено действие **bounce**, отправителю посылается уведомление об отказе принять письмо. (Это уведомление может не соответствовать действительности, поскольку на деле письмо может быть доставлено.)

4.4. Профили фильтрации, поставляемые с Фильтром

После установки Kaspersky Anti-Spam на компьютер на нем имеется комплект предустановленных профилей, которые позволяют сразу после инсталляции приступить к фильтрации спама.

По умолчанию устанавливается следующий режим фильтрации:

- при оценке признаков спама применяется средняя ("стандартная") степень строгости (действует общий профиль **Spam Detection Standard**);
- распознанные сообщения доставляются адресатам; при этом они маркируются метками в заголовке **Subject**.

Далее описаны состав предустановленного комплекта профилей фильтрации и логика выполняемых им операций, дано сравнение альтернативных профилей.

Администратор имеет возможность изменить заданные по умолчанию настройки, в том числе предусмотреть для разных пользователей свой режим обработки распознанных сообщений (реакцию на спам) (см. п. 4.4.2 на стр. 43).

Внимательно прочитайте также файл *readme-profiles*, в котором содержится наиболее свежая информация о предустановленных профилях, в том числе об изменениях, которые могли произойти со времени написания данного текста.

4.4.1. Этапы работы предустановленных профилей фильтрации

Обработка каждого письма включает три этапа:

1. выявление формальных признаков спама: анализ заголовков письма;
2. оценка письма; при необходимости – дополнительные проверки;
3. обработка писем, распознанных как спам, вероятный спам и др.

За каждый из этих этапов отвечает отдельный профиль. Для первого этапа предусмотрен один общий профиль; профили, которые будут работать на втором и третьем этапах, вы можете выбирать самостоятельно.

4.4.1.1. Выявление признаков спама: анализ заголовков письма

На первом этапе обработки почтовых сообщений выявляются формальные признаки спама – "подозрительные" заголовки и их комбинации. Для этого используется "скрытый" общий профиль **Analize Message Headers**, который хранится в файле *hidden/formal.xml*.

Например, если в конце заголовка **Subject** стоит значительное количество пробелов, а за ними бессмысленная последовательность букв вроде 'TVIWEGEQO', то это письмо, скорее всего, спам.

Почтовая программа *The Bat!* не проставляет заголовка **X-MSMail-Priority**, поэтому наличие в письме такого заголовка одновременно с **X-Mailer: The Bat!...** – признак спама.

Правила, позволяющие выявлять спамерские письма по их заголовкам, достаточно сложны и, главное, внесение в них даже незначительных изменений может привести к большому числу ложных срабатываний. Поэтому мы не предусмотрели редактирование профиля **Analize Message Headers** через программу веб-конфигуратор.

Мы не рекомендуем также редактировать этот профиль вручную. Если же вы все-таки решите сделать это, соблюдайте **МАКСИМАЛЬНУЮ** осторожность.

Кроме того, данный профиль может обновляться автоматически через интернет.

Если Вы решите поддерживать данный профиль самостоятельно и отказаться от автоматического получения его новых версий, вам необходимо удалить строку **ALLOW_UPDATES=yes** в начале файла *hidden/formal.xml*.

На выходе данного этапа в письмо добавляются следующие специальные заголовки:

- **X-SpamTest-Method** – заголовок, содержащий информацию о том, какие заголовки оценены как "подозрительные";
- **X-SpamTest-Info** – заголовок, содержащий информацию о том, какие именно "проблемы" выявлены.

4.4.1.2. Оценка письма

Выполнение данного этапа обуславливается следующими общими профилями:

- **Spam Detection Standard** (файл *detect-standard.xml*). Данный профиль активирован по умолчанию после установки Фильтра.
- **Spam Detection Standard (no RBL & DNS check)** (файл *detect-standard-no-rbl.xml*).
- **Spam Detection Soft** (файл *detect-soft.xml*).
- **Spam Detection Soft (no RBL & DNS check)** (файл *detect-soft-no-bl.xml*).
- **Spam Detection Hard** (файл *detect-hard.xml*).
- **Spam Detection Hard (no RBL & DNS check)** (файл *detect-hard-no-rbl.xml*).

Данные профили различаются:

- "строгостью" оценки признаков спама (профили **Soft** признают спамом меньше писем, а профили **Hard** – больше писем);
- использованием или неиспользованием проверок по RBL (а также на наличие посылающего сервера в DNS).

Подробнее о различиях между разными общими профилями, входящими в комплект, см. п. 4.4.2.3 на стр. 48.

На данном этапе письмо прежде всего проверяется по локальным "черным" и "белым" спискам e-mail и IP-адресов. Эти списки должны составляться и пополняться пользователем (администратором) при помощи программы веб-конфигуратор (см. п. 5.2.5 на стр. 80).

Далее оценивается, достаточно ли результатов выполненного ранее анализа заголовков письма для того, чтобы признать это письмо спамом.

Среди проверок, осуществляемых на первом этапе и учитываемых на данном, могут быть и проверки на нечитаемые "восточные" кодировки - например, китайскую.

Если кто-либо из пользователей получает письма в таких кодировках, соответствующие правила необходимо найти и удалить из применяемого вами общего профиля.

Если проведенных проверок недостаточно (письмо не получило статус "Спам"), последовательно осуществляются дополнительные проверки:

- проверки по трем различным спискам служб RBL (DNS-based real time black hole lists), начиная от наиболее надежного;
- проверка на наличие посылающего сервера в DNS;
- контентная фильтрация (проверка содержания письма).

После каждой из них письмо снова оценивается, и, в случае признания его спамом, проверки прекращаются. Контентная фильтрация – наиболее важная, но и наиболее ресурсоемкая проверка, поэтому она выполняется последней

На выходе данного этапа в письмо добавляется следующие специальные заголовки:

- **X-SpamTest-Categories** – заголовок, содержащий информацию о том, какие контентные категории были присвоены письму по результатам контентной фильтрации.
- **X-SpamTest-Status** – заголовок, указывающий на окончательный статус письма по результатам всех проверок: *SPAM*, *Probable Spam*, *Trusted* или *Not Detected*. Данный заголовок используется при последующей обработке письма персональными профилями. Он

может также использоваться для обработки письма почтовым клиентом получателя.

4.4.1.3. Реакция на спам

На данном этапе проверки почтового сообщения используются следующие персональные профили:

- **Marking Spam - Subject** (файл *do-mark-subject.xml*) Данный профиль активирован по умолчанию после установки Фильтра.
- **Marking Spam - Keywords** (файл *do-mark-keywords.xml*).
- **Archiving Spam** (файл *do-archive.xml*).
- **Archiving/Rejecting Spam** (файл *do-archive-or-reject.xml*).
- **root: No Filtering** (файл *rcpt-root.xml*).

Письмо обрабатывается в соответствии с результатами, полученными на предыдущих этапах. Различные действия над письмом выполняются в зависимости от следующих условий:

- какой окончательный статус (заголовок **X-SpamTest-Status**) оно получило;
- какие контентные категории (заголовок **X-SpamTest-Categories**) были ему присвоены;
  может учитываться, в частности, отнесено ли письмо к категориям *Obscene* (содержащее грубые выражения) или *Formal Messages* (сообщения почтовых роботов об отказе принять письмо из-за заражения вирусом, о невозможности доставить письмо адресату, о получении открытки и т. п.).
- какие методы были применены для распознания спама (заголовок **X-SpamTest-Method**).

Ниже описывается, как различные персональные профили реагируют на письма различных статусов. Профиль **root: No Filtering** в сводке не участвует, поскольку он всегда "пропускает" письмо получателю в неизменном виде.

Статус *SPAM*

- Профиль **Marking Spam - Subject**: доставляет письмо получателю, маркирует меткой **[!! SPAM]** в заголовке **Subject**.
- Профиль **Marking Spam - Keywords**: доставляет письмо получателю, маркирует заголовком **Keywords**, в котором

указываются статус письма и/или присвоенные контентные категории.

- Профиль **Archiving Spam**: пересылает письмо на адрес, указанный в правиле 1.
- Профиль **Archiving/Rejecting Spam**: в зависимости от методов, использованных для обнаружения спама, отвергает письмо (*reject*) или пересылает его на адрес, указанный в правиле 3.

Статус *Probable Spam*

- Профили **Marking Spam - Subject**, **Archiving Spam**, **Archiving/Rejecting Spam**: доставляют письмо получателю, добавляют метку **[?? Probable Spam]** в заголовке **Subject** (в зависимости от распознанной контентной категории метка может меняться; например, если распознана категория *Приглашения на семинары, конференции, выставки*, вместо этой метки используется метка **[?? Seminars etc.]**).
- Профиль **Marking Spam - Keywords**: доставляет письмо получателю, маркирует заголовком **Keywords**, в котором указываются статус письма и/или присвоенные контентные категории.

Статус *Trusted*

Все профили доставляют письмо получателю.

Статус *Not detected*

- Профили **Marking Spam - Subject**, **Archiving Spam**, **Archiving/Rejecting Spam**: доставляют письмо получателю; если письмо отнесено к категории *Obscene* или *Formal Messages*, оно может маркироваться соответствующей меткой в заголовке **Subject**.
- Профиль **Marking Spam - Keywords**: доставляет письмо получателю;
  если письму приписаны какие-либо контентные категории, маркирует заголовком **Keywords**, в котором они указываются.

4.4.2. Настройка предустановленных профилей фильтрации

Настройка профилей фильтрации осуществляется через програму веб-конфигуратор, работа с которой подробно описана в п. Глава 5 на стр. 52.

Предлагаемые профили реализуют лишь часть имеющихся возможностей Фильтра. Язык условий и действий, подробно описанный в п. 4.3 на стр. 27, предоставляет практически неограниченные возможности его настройки.

Мы рекомендуем начать с использования имеющихся профилей, а затем, в случае необходимости, видоизменять их или создавать новые профили, используя имеющиеся, как образцы.

Так, например, вы можете задать условия обработки почтовых сообщений, которые будут использоваться программой по умолчанию для всех пользователей (см. п. 4.4.2.1 на стр. 44), а также конкретизировать их для отдельных пользователей (см. п. 4.4.2.2 на стр. 46). Предусмотрена возможность регулирования степени строгости фильтрации почтового трафика (см. п. 4.4.2.3 на стр. 48).

Вы может вести собственные данные, помогающие распознанию спама:

- "черный" и "белый" списки адресов e-mail;
- "черный" и "белый" списки IP-адресов;
- базу образцов спамерских писем.

Кроме того, вы можете менять списки служб RBL, на которые ссылаются правила общих профилей (см. п. 4.4.1.2 на стр. 40).

Мы рекомендуем соблюдать максимальную осторожность при добавлении к спискам служб RBL новых служб, поскольку это может явиться причиной большого количества ложных срабатываний фильтра.

Подробнее о редактировании списков см. в п. 5.2.5 на стр. 80; о пополнении базы образцов спамерских писем см. в п. 5.2.6 на стр. 89.

4.4.2.1. Выбор реакции на спам "по умолчанию"

Предустановленный набор профилей предполагает несколько альтернативных схем обработки распознанных сообщений (см. п. 4.4 на стр. 38), таких как:

- маркирование в заголовке **Subject** (выполняется по умолчанию после установки Фильтра);
- маркирование в заголовке **Keywords**;
- архивирование спама;

- отказ в приеме некоторых типов спама и архивирование остального спама;
- отсутствие фильтрации.

За обработку писем, оцененных как спам (или вероятный спам), в предустановленном комплекте отвечают персональные профили фильтрации. Их выбор и настройка осуществляются на закладке **personal** программы веб-конфигуратор (см. п. 5.2.2 на стр. 57).

Для каждого обрабатываемого почтового сообщения сработает первый по порядку активный профиль, в котором:

- получатель, указанный в поле **Valid for Recipient(s)**, является лицензированным пользователем Kaspersky Anti-Spam;
- либо данный получатель входит в список, указанный в поле **Valid for Recipients List**;
- либо никакие получатели не указаны.

Таким образом, первый по порядку активный персональный профиль, в котором не указаны конкретные получатели, сработает по умолчанию для всех получателей, не учтенных в предшествующих активных профилях.

По умолчанию спамерские письма доставляются получателям и маркируются в заголовке **Subject**.

*Если вы хотите, чтобы по умолчанию спамерские письма маркировались в заголовке **Keywords** (который, например, показывается в Microsoft Outlook как поле **Categories**),*

- активируйте профиль **Marking Spam - Keywords**;
- отключите другие персональные профили, работающие для всех получателей.

Если вы хотите, чтобы по умолчанию письма, оцененные как спам, отправлялись в архив (пересылались в отдельный архивный почтовый ящик),

- активируйте профиль **Archiving Spam**;
- в правиле 1 этого профиля замените условный адрес **spam-archive@host.name** на имя реального почтового ящика, предназначенного для архивирования спама;
- отключите другие персональные профили, работающие для всех получателей.

Если вы хотите, чтобы по умолчанию письма, признанные спамом на основании ведущихся вами "черных списков" (см. ниже) или данных служб RBL, отвергались (reject), а остальные письма, оцененные как спам, отправлялись в архив,

- активируйте профиль **Archiving/Rejecting Spam**;
- в правиле 3 этого профиля замените условный адрес **spam-archive@host.name** на имя реального почтового ящика, предназначенного для архивирования спама
- отключите другие персональные профили, работающие для всех получателей.

Мы не рекомендуем использовать этот профиль, не говоря уже о возможных более жестких схемах фильтрации, поскольку в случае ложного распознавания спама восстановить не принятое сервером письмо будет невозможно.

Если вы хотите по умолчанию пропускать все письма всем лицензированным пользователям без ограничений и видимых изменений,

- убедитесь, что профиль **root: No Filtering** активирован и стоит первым в списке персональных профилей;
- примените данный профиль ко всем получателям:
  - откройте профиль для редактирования;
  - щелкните по кнопке **Properties**;
  - отметьте радиокнопку **Valid for Recipient(s)** и очистите соответствующее ей поле ввода.

При данной схеме фильтрации результаты распознавания спама маркируются только специальным заголовком **X-SpamTest-Status**.

Подробнее о работе предустановленных персональных профилей см. п. 4.4.1.3 на стр. 42.

4.4.2.2. Выбор реакции на спам для конкретных пользователей

Для разных пользователей могут работать разные персональные профили, реализующие разные схемы фильтрации спама. Например, в поставляемом комплекте правил:

- для пользователя *root@host.name* предусмотрена "нулевая" схема фильтрации (все письма пропускаются без дополнительной разметки);
- для остальных пользователей предусмотрена разметка писем в заголовке **Subject**.

Чтобы для разных пользователей работали отдельные схемы фильтрации, необходимо, чтобы:

1. соответствующие им профили были активны;
2. в них были указаны нужные пользователи;
3. профили были расположены в правильном порядке.

Один из профилей целесообразно оставить работающим по умолчанию – для всех пользователей, не указанных в остальных профилях. В этом профиле список получателей почты, т. е. поле **Valid for recipient(s)**, необходимо оставить пустым.

Для каждого из остальных профилей необходимо указать, для каких пользователей он активен.

Чтобы указать, для каких пользователей действует персональный профиль,

- откройте профиль для редактирования, а затем нажмите на кнопку **Properties**;
- введите адрес пользователя (или адреса пользователей) в поле **Valid for recipient(s)**,

  или

  выберите список пользователей в поле **Valid for recipient list** предварительно создав его на закладке **e-mails**.

Порядок активных профилей очень важен, поскольку для каждого пользователя сработает только первый профиль, который для него действителен.

Профиль, работающий по умолчанию, должен быть последним активным профилем в списке. Он сработает для всех пользователей, не охваченных предыдущими профилями, и никакой профиль, идущий в списке после него, не будет применен.

Для профилей **Archiving Spam** (правило 1) и **Archiving/Rejecting Spam** (правило 3) необходимо заменить условный адрес *spam-archive@host.name* на имя реального почтового ящика, предназначенного для архивирования спама.

Адрес *spam-archive@host.name* – общий для всех получателей данного профиля; поэтому если вы хотите, чтобы для разных пользователей спам пересылался на разные адреса, необходимо создать несколько копий таких профилей.

Рекомендуем переименовывать профили, работающие для конкретных пользователей, таким образом, чтобы по названию было ясно, для каких пользователей профиль работает (пример: *root: No Filtering*).

4.4.2.3. Выбор степени строгости фильтрации

За определение статуса письма (его оценки как спама, вероятного спама и т. п.) отвечают общие профили. Их выбор осуществляются на закладке **common** программы веб-конфигуратор (см. п. 5.2.1 на стр. 54).

Выбранный общий профиль работает для всех лицензированных получателей почты. Мы рекомендуем использовать профиль **Spam Detection Standard**, выбранный по умолчанию.

Если вы боитесь ложных срабатываний Фильтра, вы можете выбрать профиль **Spam Detection Soft**, обеспечивающий более "мягкую" фильтрацию (меньшее число писем распознается как спам). В частности, для признания письма спамом в этом профиле используются данные только наиболее надежных служб RBL.

Если вы хотите, чтобы максимальное количество спамерских писем было распознано Фильтром, даже за счет увеличения вероятности ложных срабатываний, вы можете воспользоваться профилем **Spam Detection Hard**.

Наконец, если вы вообще не хотите использовать проверки по службам RBL (а также проверку на наличие посылающего сервера в DNS), воспользуйтесь одним из профилей **Spam Detection Standard/Soft/Hard (no RBL)**. Они отличаются от соответствующих профилей **Standard**, **Soft** и **Hard** только тем, что указанные проверки не выполняются.

Подробнее о работе общих профилей см. п. 4.4.1.2 на стр. 40.

4.4.3. Специальные заголовки, проставляемые Фильтром

В процессе работы Фильтр может проставлять или модифицировать следующие заголовки почтовых сообщений:

- **X-SpamTest-Status**;
- **X-SpamTest-Method**;

- **X-SpamTest-Info**;
- **X-SpamTest-Categories**;
- **Keywords**;
- **Subject** (только дописывание меток к заголовку).

Рассмотрим подробнее каждый из перечисленных заголовков.

X-SpamTest-Status – заголовок, который проставляется общими профилями в каждое обработанное письмо (по одному на письмо); содержит результат оценки письма. Может иметь следующие значения:

- *SPAM* – письмо признано спамом;
- *Probable Spam* – письмо с большой вероятностью представляет собой спам, однако обнаруженные признаки спама не дают утверждать это с достаточной уверенностью;
- *Trusted* – письмо пришло из известного источника (упомянутого в одном из "белых списков") и должно быть принято независимо от возможного наличия признаков спама;
- *Not Detected* – в письме не обнаружено признаков спама, достаточных для присвоения статуса *SPAM* или *Probable Spam*.

  Данный заголовок может быть использован при обработке писем в почтовом клиенте конечного получателя.

X-SpamTest-Method – заголовок, который проставляется скрытым общим профилем **Analize Message Headers** или другими общими профилями в письма, где обнаружены признаки спама. (При дальнейшей обработке письма эти признаки могут быть признаны недостаточными, и письмо может получить статус *Not Detected* или *Trusted*). Может иметь следующие значения:

- *Local Lists* – e-mail или ip-адрес отправителя письма встретился в одном из "черных" или "белых" списков;
- *Headers: ...* (например, *Headers: Suspicious To*) – заголовки письма содержат признаки спама; часть после двоеточия указывает на то, какой именно из заголовков вызывает подозрения (в данном случае заголовок **To**). Возможны следующие варианты:
  - *Suspicious From* – подозрительный заголовок **From**.
  - *Suspicious Reply-To* – заголовок **Reply-To**.
  - *Spamware Subject*, *Suspicious Subject* – последние два варианта относятся к заголовку **Subject**; в первом случае вероятность спама выше.

- *Spamware X-Mailer*, *Suspicious X-Mailer* – аналогично, для заголовка **X-Mailer**.
- *Incompatible Headers* – подозрительные сочетания заголовков.
- *Spamware Received* – "спамерский" заголовок **Received**.
- *Eastern Codepage* – письмо в одной из "восточных" кодировок (китайской, корейской, японской).
- и т. п.

- *RBL: 'premium' list*, *RBL: 'reliable' list*, *RBL: 'standard' list* – отправитель письма зарегистрирован в одной из служб RBL, входящих в соответствующие списки, начиная с наиболее надежного;
- *DNS: not in DNS* – сервер, с которого отправлено письмо, не зарегистрирован в системе DNS;
- *Content: Spam*, *Content: Probable Spam* – контентный анализ присвоил письму категорию *SPAM* или *Probable Spam*.

Заголовков **X-SpamTest-Method** в письме может быть несколько.

X-SpamTest-Info – заголовок, который имеет две различные функции:

- Во-первых, каждый профиль фильтрации, обрабатывающий письмо, проставляет в данном заголовке свою метку.
- Во-вторых, заголовки **X-SpamTest-Info** могут содержать более подробную информацию о признаках спама, обнаруженных в письме и зафиксированных в заголовках **X-SpamTest-Method**.

Заголовков **X-SpamTest-Info** в письме может быть несколько.

X-SpamTest-Categories – заголовок, который приписывается общими профилями; содержит список категорий, приписанных письму в результате контентного анализа (если такой анализ проводился, и если по его результатам письму приписаны какие-либо категории).

Заголовок **X-SpamTest-Categories** в письме может быть только один.

Keywords – заголовок, который приписывается персональным профилем **Marking Spam - Keywords**, если письмо распознано как спам или возможный спам, или если контентный анализ приписал письму какие-либо контентные категории.

Профиль **Marking Spam - Keywords** начинает свою работу со стирания старых заголовков **Keywords** (если они были); другие профили оставляют заголовки **Keywords** без изменения.

Subject – персональные профили **Marking Spam - Subject**, **Archiving Spam**, **Archiving/Rejecting Spam** могут дописывать в конец имеющегося заголовка **Subject** свои специальные метки, см. п. 4.4 на стр. 38.

ГЛАВА 5. НАСТРОЙКА ПАРАМЕТРОВ ФИЛЬТРАЦИИ

Kaspersky Anti-Spam предоставляет администратору почтового сервера мощный и удобный инструментарий для защиты пользователей от нежелательной корреспонденции (спама). Логика фильтрации не навязывается фильтром – администратор имеет возможность установить ее самостоятельно в соответствии с политикой своей компании и пожеланиями получателей почты.

Поскольку работа Kaspersky Anti-Spam полностью определяется настройками, выполняемыми администратором, мы рекомендуем отнестись к их осуществлению с максимальным вниманием. Неправильная настройка может привести:

- к неэффективности работы Фильтра (большинство нежелательных сообщений пропускается);
- к потере "нормальной" (желательной) почты.

Настройка всех параметров фильтрации осуществляется с помощью *программы* веб-конфигуратор, которая позволяет создавать, редактировать и удалять:

- профили (наборы правил) фильтрации – как общие, действующие для всех пользователей, так и персональные, действующие для отдельных пользователей или их групп;
- правила фильтрации (условия и соответствующие им действия), управлять порядком их применения;
- "черные" и "белые" списки IP-адресов и e-mail, на которые могут ссылаться правила фильтрации;
- списки DNS-based RBL.

Прежде, чем приступить к настройке Фильтра, ознакомьтесь с принципами его работы (см. п. 4.3 на стр. 27). Обратите особое внимание на описание действий, выполняемых Фильтром (см. п. 4.3.3 на стр. 31) и на порядок применения профилей и правил фильтрации (см. п. 4.3.4 на стр. 34). Изучите образцы профилей фильтрации, поставляемые с Фильтром.

Работа с программой веб-конфигуратор осуществляется удаленно посредством любого веб-браузера.

5.1. Запуск программы веб-конфигуратор

В состав Kaspersky Anti-Spam входит сервер *thttpd* (устанавливается под именем **kas-thhtpd**). Он запускается на порту 2880 и обеспечивает доступ к веб-конфигуратору по http.

Из соображений безопасности по умолчанию доступ к kas-thttpd разрешен только с того же компьютера, на которой он установлен.

При необходимости разрешить удаленное администрирование Kaspersky Anti-Spam, нужно:

- Изменить строчку `host=127.0.0.1` на `host=0.0.0.0` в файле */usr/local/ap-mailfilter/etc/kas-thttpd.conf*.
- Завести нового пользователя и задать пароль для доступа к веб-конфигуратору при помощи программы */usr/local/ap-mailfilter/bin/kas-htpasswd*.

Чтобы запустить программу веб-конфигуратор,

1. Запустите веб-браузер.
2. В поле вода URL-адреса введите адрес `http://localhost::2880`

5.2. Работа с программой веб-конфигуратор

С помощью программы веб-конфигуратор вы можете выполнять удаленную настройку параметров фильтрации:

- создавать и удалять общие профили фильтрации (см. п. 5.2.1 на стр. 54);
- создавать и удалять персональные профили фильтрации (см. п. 5.2.2 на стр. 57);

- редактировать профили фильтрации, создавать и удалять правила фильтрации (см. п. 5.2.3 на стр. 60);
- редактировать правила фильтрации (см. п. 5.2.4 на стр. 66);
- создавать, редактировать и удалять списки e-mail, IP-адресов и DNS-based RBL (см. п. 5.2.5 на стр. 80);
- добавлять, редактировать и удалять образцы спамерских писем (см. п. 5.2.6 на стр. 89);
- редактировать общие настройки Фильтра (см. п. 5.2.7 на стр. 91).

5.2.1. Работа с общими профилями. Закладка *common*

На закладке **common** представлен список существующих общих профилей (см. рис. 2) и ряд кнопок, позволяющих работать с ними:

- **new** – создать новый профиль (см. п. 5.2.1.1 на стр. 55);
- **activate** – активизировать выбранный профиль (см. п. 5.2.1.2 на стр. 56);
- **edit** – перейти к редактированию параметров выбранного профиля (см. п. 5.2.3 на стр. 60);
- **delete** – удалить выбранный профиль (см. п. 5.2.1.3 на стр. 57);
-  и  – передвинуть профиль на одну позицию, соответственно, вверх или вниз.

Список профилей может не помещаться целиком в видимом окне списка. В этом случае используйте полосу прокрутки справа от него.

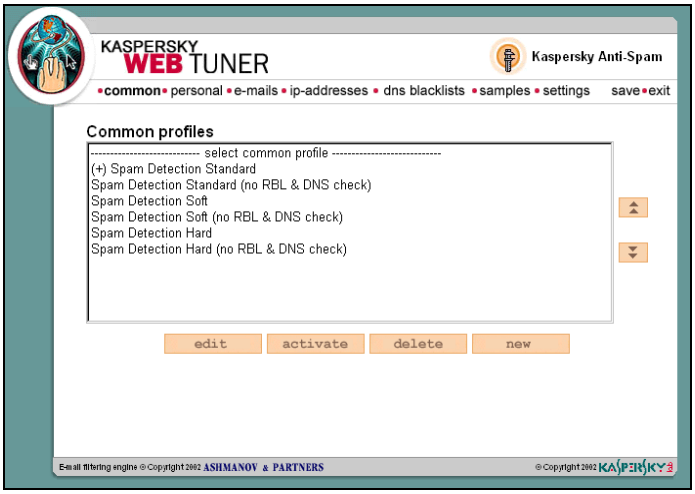

Рисунок 2. Закладка **common**

5.2.1.1. Создание общего профиля

Чтобы создать общий профиль фильтрации,

1. Нажмите на кнопку **new**.
2. В открывшемся окне **New common profile** (см. рис. 3) введите запрашиваемые параметры профиля:
   - **File** – имя файла профиля. В поле ввода вручную введите имя файла без расширения или с расширением *xml*);

     Обязательно задайте значение параметра **File**, иначе на экран будет выведено сообщение об ошибке, и профиль создан не будет!

   - **Name** – имя профиля. По умолчанию в качестве имени профиля используется имя файла без расширения. Вы можете ввести другое имя профиля в поле ввода параметра.
3. Нажмите на кнопку **create**.

Сразу же после создания профиля вам будет предложено перейти к редактированию его параметров (подробнее см. п. 5.2.3 на стр. 60).

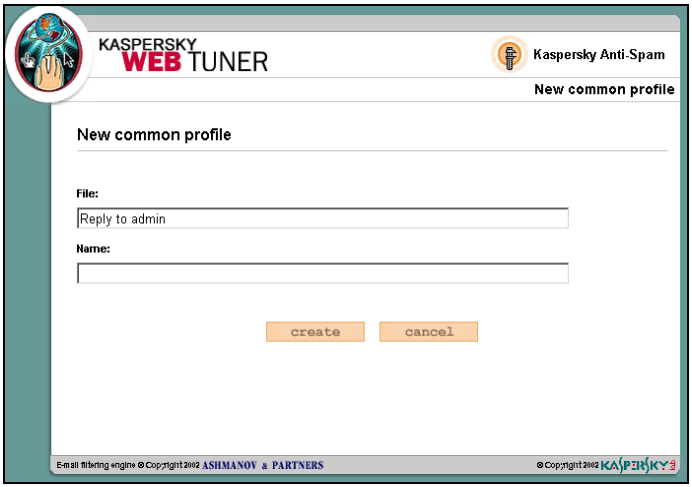

Рисунок 3. Окно создания общего профиля

При создании нового профиля он не вводится в действие автоматически. Профиль остается неактивным (не действующим, не участвующим в работе Фильтра) до тех пор, пока вы не сделаете его активным (подробнее об активации см. п. 5.2.1.2 на стр. 56).

5.2.1.2. Активизация общего профиля

Под *активизацией* профиля следует понимать подключение профиля к работе Фильтра. Вы можете подключить только один общий профиль.

Чтобы подключить общий профиль к работе Фильтра,

1. Выберите имя профиля из списка существующих общих профилей (см. рис. 2).
2. Нажмите на кнопку **activate**.

Выбранный вами профиль станет активным. При этом тот профиль, который был активным до этого, будет автоматически деактивизирован.

Активный профиль отмечен в списке профилей знаком **(+)**.

5.2.1.3. Удаление профиля

Чтобы удалить существующий профиль,

1. Выберите имя профиля, который вы хотите удалить, из списка существующих общих профилей (см. рис. 2).
2. Нажмите на кнопку **delete**.
3. В открывшемся окне подтверждения удаления (см. рис. 4) нажмите на кнопку **delete**.

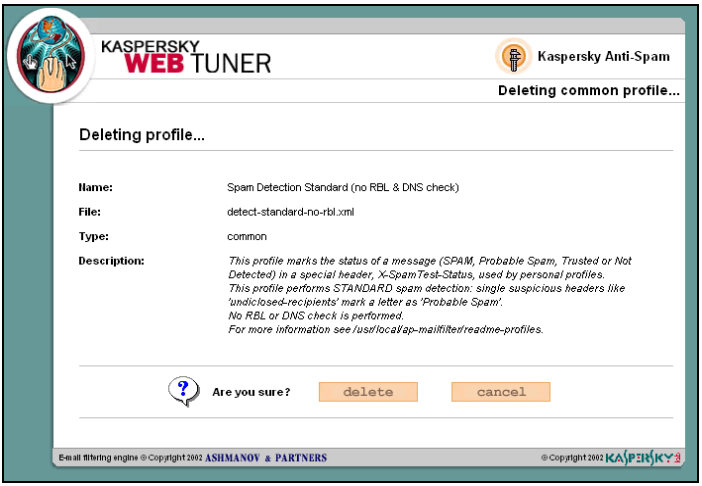

Рисунок 4. Окно удаления профиля фильтрации

5.2.2. Работа с персональными профилями. Закладка *personal*

Закладка **personal** включает список существующих *персональных профилей* (см. рис. 5) и ряд кнопок, позволяющих работать с ними:

- **new** – создать новый профиль (см. п. 5.2.2.1 на стр. 58);
- **on/off** – активизировать выбранный профиль (см. п. 5.2.2.2 на стр. 59);
- **edit** – перейти к редактированию параметров выбранного профиля (см. п. 5.2.3 на стр. 60);

- **delete** – удалить выбранный профиль (удаление персонального профиля аналогично удалению общего, см. п. 5.2.1.3 на стр. 57);
-  и  – прокрутить список профилей вверх или вниз, соответственно.

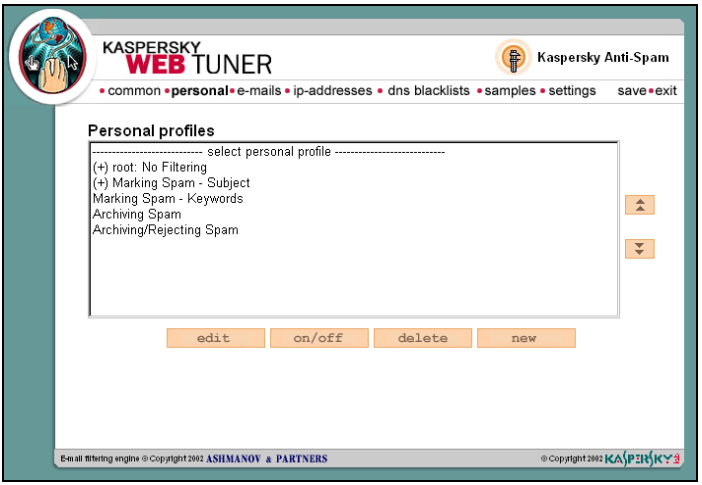

Рисунок 5. Закладка **personal**

5.2.2.1. Создание персонального профиля

При создании персонального профиля помимо имени файла и самого профиля (аналогично общему профилю, см. п. 5.2.1.1 на стр. 55) нужно указать *сферу применения профиля*, т. е. адрес или список адресов, для которых будет действовать данный профиль (см. рис. 6). Вы можете указать адреса вручную или выбрать список адресов из формируемых на закладке **e-mail** (см. п. 5.2.5 на стр. 80):

Valid for recipient(s) – сформировать адрес (список адресов), для которых будет действовать данный профиль, самостоятельно. В поле ввода параметра вручную укажите адрес или адреса e-mail через точку с запятой.

Адреса e-mail записываются в формате **user@domain** или **@domain**. Во втором случае подразумевается любой пользователь указанного домена.

Valid for recipient list – выбрать список адресов, для которых будет действовать профиль, из раскрывающегося списка.

Список получателей в персональном профиле может оставаться пустым (*default personal profile*), в таком случае данный персональный профиль может быть применен для всех получателей, к которым не применился никакой другой персональный профиль (см. п. 4.3.4.1 на стр. 34).

Рисунок 6. Окно создания персонального профиля

5.2.2.2. Активизация персонального профиля

Программа веб-конфигуратор позволяет подключать (активизировать) и отключать (деактивировать) созданные профили.

В работе Фильтра участвуют только активные профили. Остальные профили остаются в резерве. Они могут находиться в процессе редактирования, использоваться для быстрого переключения режимов работы Фильтра, и т. п.

Вновь созданный профиль остается неактивным до тех пор, пока вы его не активизируете.

Из персональных профилей активными может быть произвольное количество профилей. Активные профили отмечены в списке профилей знаком **(+)**.

Чтобы активизировать (деактивизировать) персональный профиль,

1. Выберите в списке профилей тот профиль, который вы хотите активизировать (деактивизировать).
2. Нажмите на кнопку **on/off**.

5.2.3. Редактирование профиля фильтрации

Внимание! Редактирование общего и персонального профилей фильтрации идентично, поэтому далее под *профилем фильтрации* подразумеваются оба типа профилей. Случаи различия в каких-либо настройках оговариваются отдельно!

Создание и редактирование правил фильтрации – наиболее важная часть настройки Kaspersky Anti-Spam. Редактируя правила, вы определяете, какие условия будут проверяться и какие действия – выполняться над письмами, удовлетворяющими этим условиям.

Редактирование профилей фильтрации, списков e-mail и IP-адресов и др. ведется на копиях конфигурационных файлов. Для того чтобы сделанные изменения вступили в силу, необходимо их сохранить (нажать на кнопку **save**, см. п. 5.2.3.6 на стр. 65).

Чтобы отредактировать профиль фильтрации,

1. Выберите в списке профилей тот профиль, который вы хотите редактировать.
2. Нажмите на кнопку **edit**.

В результате выполненных действий будет открыто окно (см. рис. 7), содержащее:

- набор кнопок:
  - **new** – создать новое правило (см. п. 5.2.3.1 на стр. 61);
  - **properties** – редактировать параметры (название, описание и сфера применения) профиля (см. п. 5.2.3.5 на стр. 64).
- таблицу **Filtration rules**, содержащую список правил профиля, а также кнопки для их редактирования:
  - – редактировать правило (см. п. 5.2.4 на стр. 66);

- ✕ – удалить правило (см. п. 5.2.3.3 на стр. 62);
- ⬆⬇ – поднять/опустить правило на один уровень в таблице правил (см. п. 5.2.3.4 на стр. 63).

- кнопки навигации по списку правил.

На странице редактирования профиля фильтрации одновременно показывается до 5 правил фильтрации; для перехода к последующим (предыдущим) правилам необходимо воспользоваться кнопками со стрелками под таблицей правил.

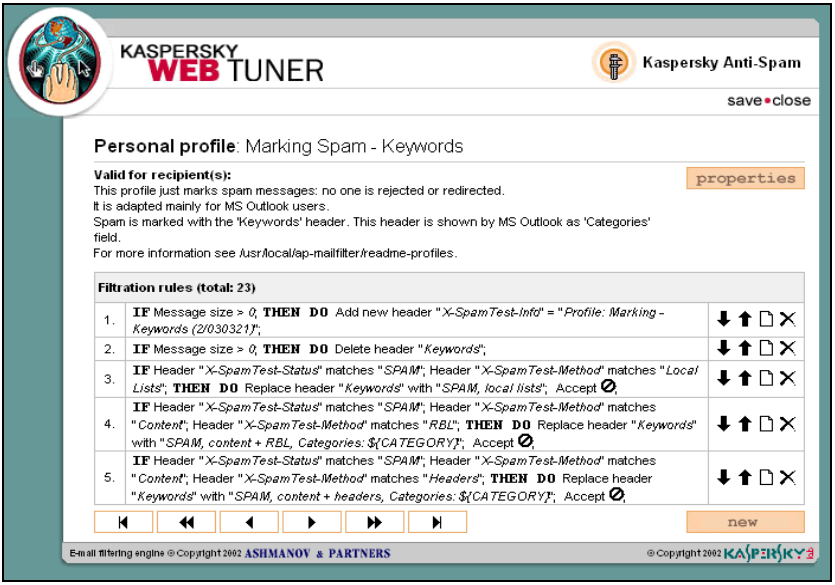

Рисунок 7. Создание/редактирование профиля фильтрации

5.2.3.1. Создание правила

Чтобы создать новое правило фильтрации,

1. Нажмите на кнопку **new**, расположенную под таблицей-списком существующих правил.
2. В открывшемся окне **Create new rule** (см. рис. 8) отредактируйте правило: введите условия и действия.
3. Сохраните созданное правило, нажав на кнопку **create**.

Редактирование правила фильтрации подробно описано в п. 5.2.4 на стр. 66.

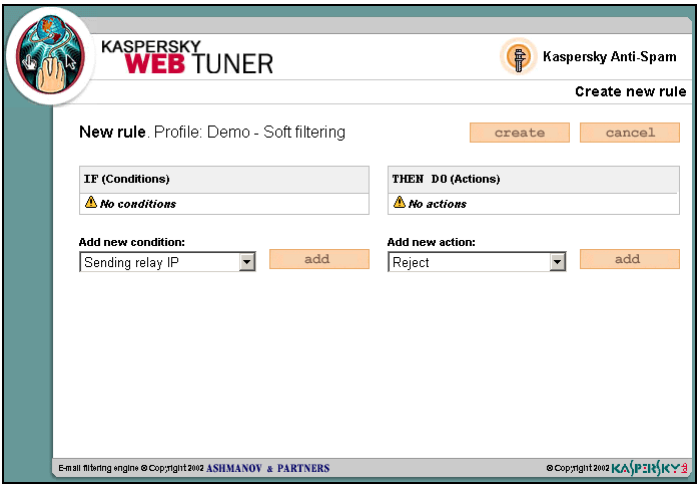

Рисунок 8. Окно создания нового правила фильтрации

5.2.3.2. Переход к редактированию существующего правила

Чтобы перейти к редактированию существующего правила фильтрации,

1. Выберите в таблице правило, которое вы хотите отредактировать.
2. Нажмите на кнопку справа от этого правила.

Редактирование правила фильтрации подробно описано в п. 5.2.4 на стр. 66.

5.2.3.3. Удаление существующего правила

Чтобы удалить существующее правило фильтрации,

1. Выберите в таблице правило, которое вы хотите удалить.
2. Нажмите на кнопку справа от этого правила.

5.2.3.4. Управление порядком применения правил

Правила, составляющие профиль фильтрации, выполняются в том порядке, в котором они перечислены в таблице (см. рис. 7).

Порядок применения правил имеет очень большое значение. Профили, отличающиеся только порядком правил, могут при обработке одного и того же письма давать совершенно разные результаты.

Пусть, например, некий профиль фильтрации состоит из двух правил, из которых правило А отвергает письма от серверов без DNS-имени (действие **reject**), а правило В принимает письма от серверов, входящих в белый список (действие **accept**). Тогда письмо, пришедшее с сервера без DNS-имени, входящего в этот белый список:

- будет отвергнуто, если первым выполняется правило А (после его выполнения обработка письма будет завершена, и правило В применено не будет);
- будет доставлено адресату, если первым выполняется правило В (после его выполнения обработка письма будет завершена, и правило А применено не будет).

Чтобы переместить существующее правило фильтрации на один уровень вверх,

1. Выберите в таблице правило, которое вы хотите переместить.
2. Нажмите на кнопку ⬆ справа от этого правила.

Чтобы переместить существующее правило фильтрации на один уровень вниз,

1. Выберите в таблице правило, которое вы хотите переместить.
2. Нажмите на кнопку ⬇ справа от этого правила.

5.2.3.5. Редактирование названия, описания и сферы применения профиля фильтрации

Параметры профиля фильтрации вы можете отредактировать в окне **Profile properties** (см. рис. 9), которое открывается по кнопке **properties** из списка правил профиля (см. рис. 7).

Для общего профиля вы можете корректировать вручную следующие параметры:

- **Name** – имя профиля.
- **Description** – описание профиля.

При создании профиля его описание остается пустым, и в окне редактирования профиля выводится ***(No description)***.

Тип общего профиля и имя файла, в котором хранится его описание, не могут быть изменены.

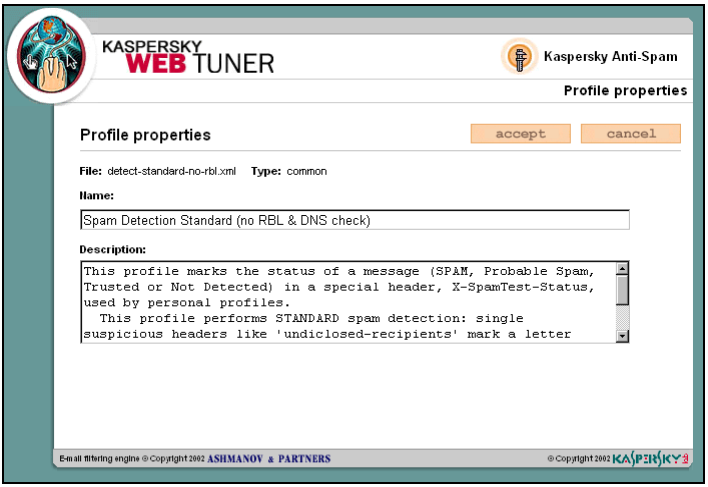

Рисунок 9. Редактирование параметров общего профиля

Для персонального профиля (см. рис. 10) дополнительно можно отредактировать сферу его применения посредством параметра **Valid for recipient(s)** или **Valid for recipient list** (подробнее об этих параметрах см. п. 5.2.2.1 на стр. 58).

Для сохранения выполненных настроек нажмите на кнопку **accept**.

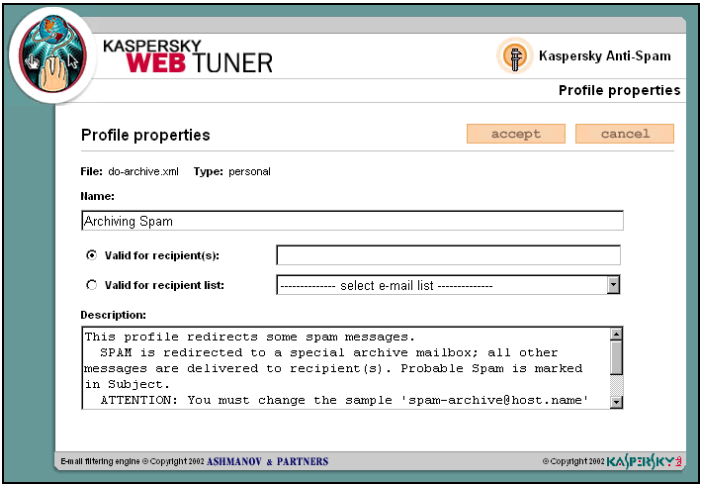

Рисунок 10. Редактирование параметров персонального профиля

5.2.3.6. Сохранение профиля

Редактирование профилей фильтрации (а также списков e-mail и IP-адресов и др.) ведется в копиях конфигурационных файлов, см. п. 5.2.8 на стр. 94. Изменения в эти файлы вносятся каждый раз после редактирования какого-либо правила фильтрации или параметров профиля фильтрации при нажатии на кнопку **accept**. Однако на работе фильтра это никак не сказывается – конфигурация Фильтра, сложившаяся в результате редактирования, не будет сохранена.

Чтобы сохранить и ввести в действие изменения, внесенные в описание профиля фильтрации и в другие конфигурационные файлы,

в окне редактирования профиля (см. рис. 7) нажмите на кнопку **save**.

Конфигурация Фильтра, полученная в результате редактирования, сохраняется целиком – все профили, списки e-mail и IP-адресов и т. п.

После сохранения конфигурационных файлов программа веб-configurator автоматически запускает Компилятор конфигурации, который создает из текстовых XML-файлов бинарные файлы, используемые при работе Фильтра.

5.2.4. Редактирование правила фильтрации

5.2.4.1. Страница редактирования правила фильтрации

Правило фильтрации представляет собой два списка: *условий*, которые должны быть выполнены, чтобы правило сработало, и *действий*, которые выполняются, если все условия выполнены.

В окне редактирования правила фильтрации **Rule properties** (см. рис. 11) вы можете добавлять, редактировать и удалять условия и действия.

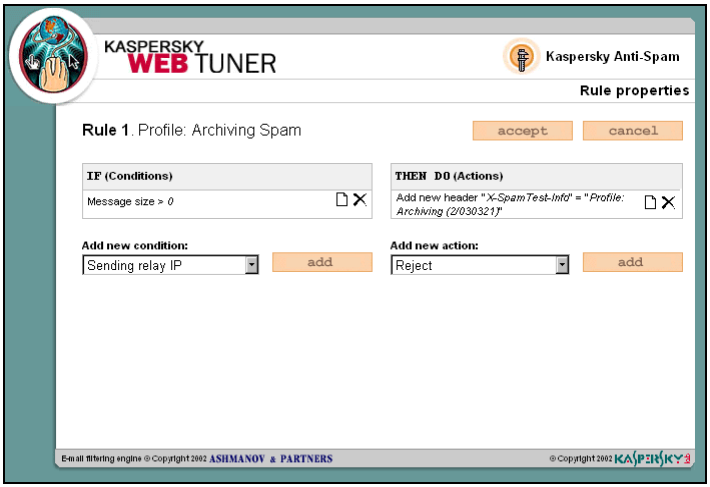

Рисунок 11. Редактирование правила фильтрации

Порядок условий значения не имеет, поскольку, чтобы правило сработало, они должны выполниться все одновременно. Действия выполняются в том порядке, в котором они выводятся в правой таблице (**THEN DO**) в окне редактирования правила фильтрации[7].

[7] Этот порядок определяется "совместимостью" действий между собой; например, первым в иерархии стоит действие **reject**, поскольку ни одно другое действие в сочетании с ним не имеет смысла; последним — действие **accept**, поскольку оно может быть выполнено вместе с любыми нежесткими действиями.

Знак ⊘ рядом с названием действия показывает, что оно является жестким или полужестким, и после его выполнения работа текущего правила (и профиля) прекращается. Таким образом, никакое действие, стоящее в таблице после него, выполнено не будет.

Знак ⚠ перед условием или действием показывает, что описание этого условия (действия) некорректно, либо условие (действие) бесполезно.

Например, этим знаком будут отмечены любые действия, заданные в правиле одновременно с действием **Reject** (см. рис. 12), поскольку это действие сработает первым, после чего обработка правила прекратится, и дополнительные действия никогда не будут выполнены. Этим знаком отмечаются также условия и действия, заданные без указания одного или нескольких необходимых параметров. Так, в приведенном ниже примере в первом условии не указан IP-адрес, с которым должен совпадать адрес отправляющего почтового сервера.

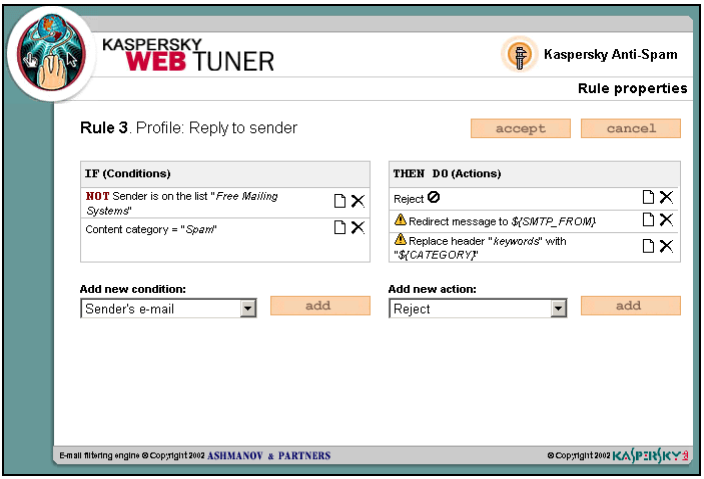

Рисунок 12. Некорректные условия и действия

5.2.4.2. Задание нового условия

Чтобы задать новое условие,

1. В окне редактирования правила фильтрации (см. рис. 11) выберите тип условия из раскрывающегося списка **Add new condition**.
2. Нажмите на кнопку **add** справа от него.

3. В открывшемся окне **Add new condition** (например, рис. 13):
   - выберите вариант условия (для каждого типа условия существуют несколько вариантов);
   - задайте параметры, относящиеся к выбранному варианту условия (подробнее о параметрах для каждого типа условий см. ниже).
4. Если это необходимо, установите флажок **negative (NOT)** в левом нижнем углу страницы. В этом случае будет действовать отрицание указанного вами условия.
5. Нажмите на кнопку **add**.

При необходимости вы можете изменить тип условия, выбрав его в списке **Condition applies to** на открывшейся странице и, если страница не обновилась сама, нажав на кнопку **select**.

5.2.4.2.1. Условия, относящиеся к IP-адресу посылающего почтового сервера

Предусмотрены следующие условия, связанные с IP-адресом посылающего почтового сервера (см. рис. 13):

matches the following mask – IP-адрес посылающего почтового relay'я совпадает (не совпадает) с указанным. В соответствующем поле ввода укажите маску, которой должен соответствовать адрес.

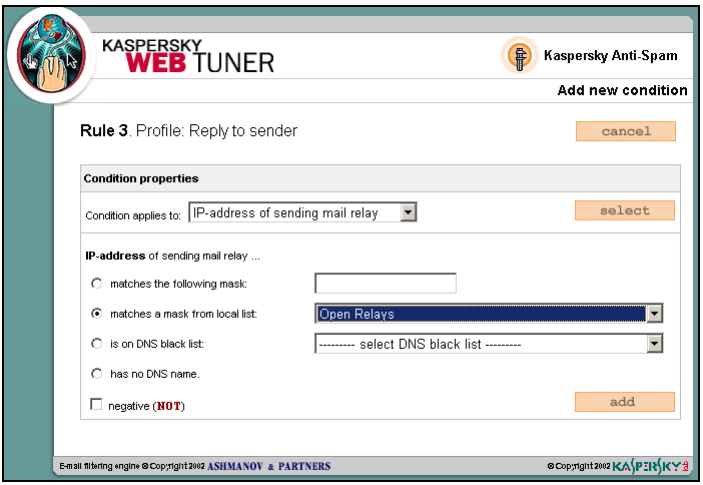

Рисунок 13. Условия, связанные с IP посылающего сервера

- **matches a mask from local list** – IP-адрес посылающего почтового сервера входит (не входит) в указанный список. Выберите имя списка IP-адресов (масок) из раскрывающегося списка.
- **is on DNS black list** – посылающий почтовый сервер зарегистрирован (не зарегистрирован) как "неблагонадежный" в системе DNS-based RBL на одном из специализированных серверов, входящих в указанный список. Из раскрывающегося списка выберите DNS-based RBL.
- **has no DNS name** – у посылающего почтового сервера отсутствует (имеется) DNS-имя.

5.2.4.2.2. Условия, относящиеся к e-mail отправителя

Предусмотрены следующие условия, связанные с адресом e-mail отправителя письма, указанным в SMTP-envelope (см. рис. 14):

- **is equal to** – e-mail отправителя совпадает (не совпадает) с указанным. В поле ввода параметра задайте e-mail.
- **is on local list** – e-mail отправителя входит (не входит) в указанный список. Из раскрывающегося списка выберите имя списка адресов e-mail.

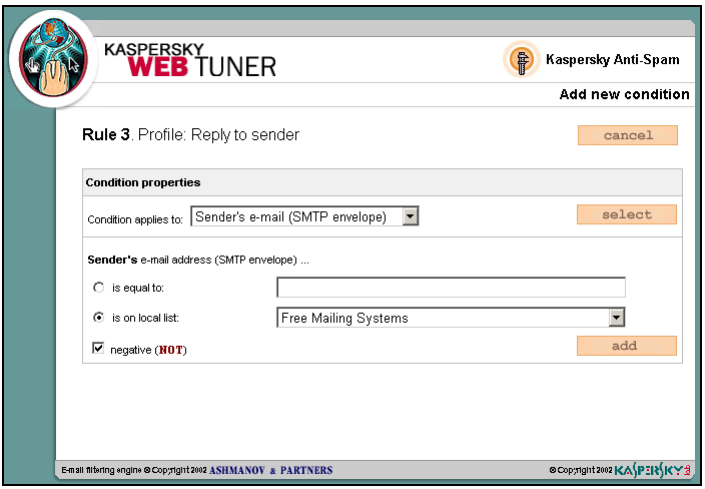

Рисунок 14. Условия, связанные с e-mail отправителя

5.2.4.2.3. Условия, относящиеся к e-mail получателя

Предусмотрены следующие условия, связанные с адресом e-mail получателя письма, указанным в SMTP-envelope (см. рис. 15):

- **is equal to** – e-mail получателя (одного из получателей, если их несколько) совпадает (не совпадает) с указанным в поле ввода адресом (маской адресов).
- **is on local list** – e-mail получателя (одного из получателей, если их несколько) входит (не входит) в указанный список. Из раскрывающегося списка выберите имя списка адресов e-mail.

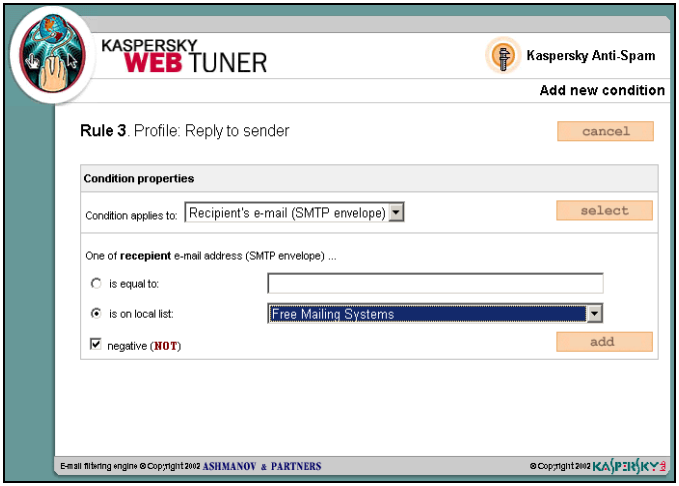

Рисунок 15. Условия, связанные с e-mail получателя

5.2.4.2.4. Условия, относящиеся к заголовкам сообщения

Предусмотрены следующие условия, связанные с заголовками сообщения (см. рис. 16):

Name – имя заголовка. В поле ввода параметра укажите имя заголовка.

- **matches regular expression** – сообщение имеет (не имеет) заголовок с именем, указанным в поле ввода **Name**, соответствующий шаблону, введенному в поле в поле ввода **matches regular expression**.

exists – сообщение имеет (не имеет) какой-либо заголовок с именем, указанным в поле ввода **Name**.

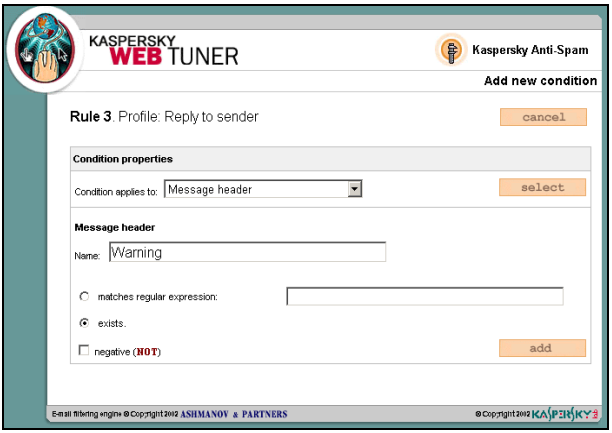

Рисунок 16. Условия, связанные с заголовками сообщения

5.2.4.2.5. Условие, относящееся к результатам контентной фильтрации

Предусмотрено следующее условие, связанное с результатами контентной фильтрации (см. рис. 17):

Incoming message falls into the following category – содержимое сообщения отнесено (не отнесено) к указанной контентной категории. В раскрывающемся списке выберите имя категории.

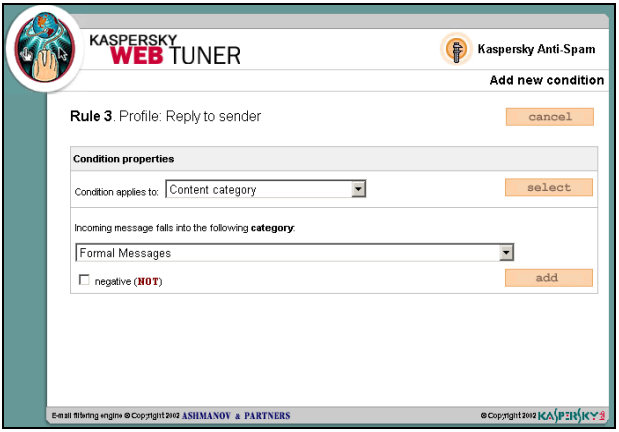

Рисунок 17. Условие, связанное с результатами контентной фильтрации

5.2.4.2.6. Условие, относящееся к размеру сообщения

Предусмотрено следующее условие, связанное с размером сообщения (см. рис. 18):

Incoming message is larger than ... bytes – общий размер сообщения превышает (не превышает) указанный предел. В поле ввода параметра укажите предельный размер письма в байтах.

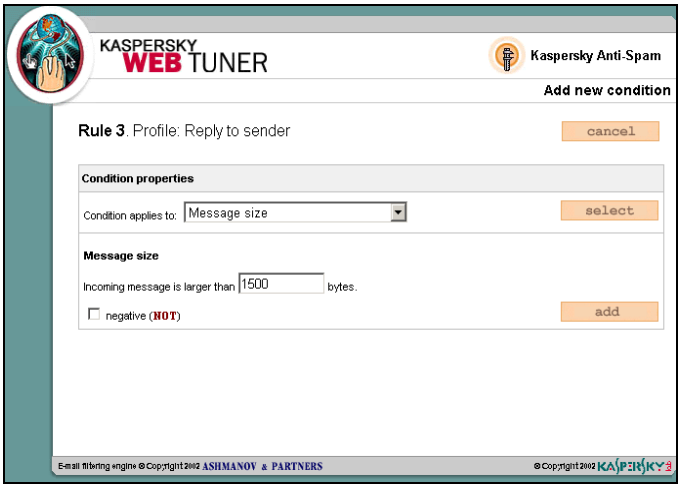

Рисунок 18. Условие, связанное с размером сообщения

5.2.4.3. Редактирование условия

Возможны два способа редактирования условия:

- изменить его параметры, не меняя типа условия;
- изменить тип условия.

Чтобы отредактировать условие,

1. В окне редактирования параметров правила **Rule properties** (см. рис. 11) в таблице **IF (Conditions)** выберите условие, параметры которого вы хотите изменить.
2. Нажмите на кнопку справа от этого условия.
3. В открывшемся окне **Condition properties** (см. рис. 19) при необходимости измените тип условия; для этого выберите нужный тип в списке **Condition applies to**. Если окно не обновится, нажмите на кнопку **select**.
4. Откорректируйте параметры, относящиеся к выбранному варианту условия (подробнее см. п. 5.2.4.2 на стр. 67).
5. Если это необходимо, установите флажок **negative (NOT)** в левом нижнем углу страницы (в этом случае будет действовать

отрицание указанного вами условия), или снимите такую отметку.

6. Нажмите на кнопку **accept**.

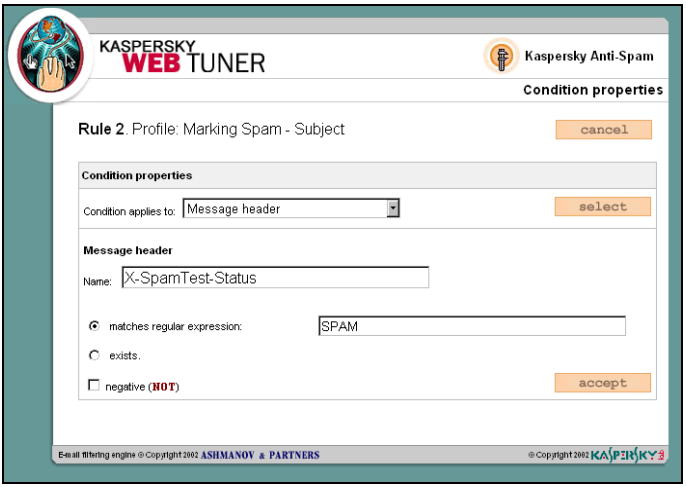

Рисунок 19. Редактирование условия (один из вариантов)

5.2.4.4. Удаление условия

Чтобы удалить существующее условие,

1. В окне редактирования параметров правила **Rule properties** (см. рис. 11) в таблице **IF (Conditions)** выберите условие, которое вы хотите удалить.
2. Нажмите на кнопку ✕ справа от этого условия.

5.2.4.5. Формирование нового действия

Возможные типы действий и их варианты описаны в п. 4.3.3 на стр. 31.

Создание нового действия для правила фильтрации осуществляется в окне редактирования параметров правила **Rule properties** (см. рис. 11) в таблице **THEN DO (Actions).**

Чтобы задать новое действие,

1. Выберите тип действия из раскрывающегося списка **Add new action**.
2. Нажмите на кнопку **add**.

   Для действий, не имеющих дополнительных параметров (**reject**, **black hole**, **bounce**, **skip, accept**) процедура на этом заканчивается. Дальнейшие шаги относятся только к действиям, имеющим варианты и дополнительные параметры.

3. В открывшемся окне **Add new action** (например, рис. 20) для действий **change recipient, change header** задайте параметры действия (подробнее о параметрах см. ниже).

   Здесь же вы можете изменить тип действия, выбрав его в раскрывающемся списке параметра **Action type**.

4. Нажмите на кнопку **add**.

5.2.4.5.1. Варианты и параметры действия *change recipient*

Для типа действия **change recipient** предусмотрены следующие параметры (см. рис. 20):

Recipient's e-mail – e-mail получателя сообщения. В поле ввода параметра укажите адрес или несколько адресов через точку с запятой.

Replace all – заменить адреса всех получателей на адрес (список адресов), указанный в поле ввода параметра **Recipient's e-mail**.

Delete – удалить указанный в поле ввода параметра **Recipient's e-mail** адрес (адреса) из списка получателей.

Add – добавить указанный в поле ввода параметра **Recipient's e-mail** адрес (адреса) к списку получателей.

Чтобы заменить один адрес получателя на другой (переадресовать письмо), необходимо последовательно выполнить два действия – **Delete** и **Add**. Либо, если нужна полная переадресация (замена всех получателей) – просто выполнить **Replace all**.

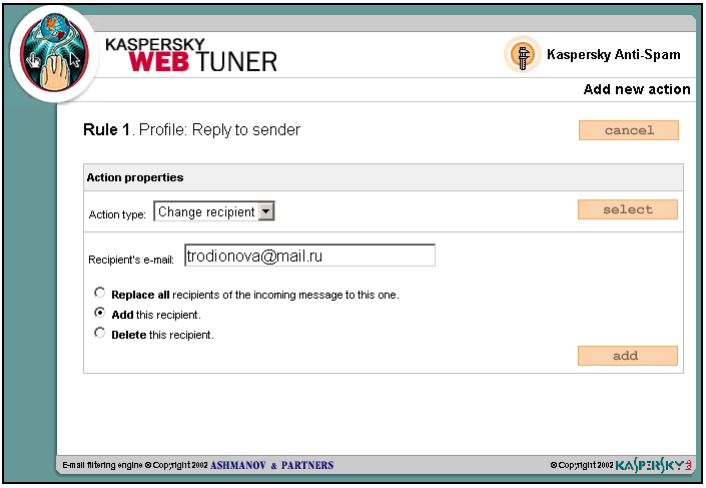

Рисунок 20. Добавление действия **change recipient**

5.2.4.5.2. Варианты и параметры действия *change header*

Для типа действия **change header** предусмотрены следующие параметры (см. рис. 21):

Header – имя заголовка, подвергающегося замене. В поле ввода параметра укажите, например, **Keywords** или **From**.

New value – новое значение заголовка.

При подстановке нового значения заголовка могут использоваться следующие макропеременные:

${CATEGORY} – список категорий спама, полученный при контентном анализе текста сообщения (например, этот список может быть записан в заголовок **Keywords**);

${SMTP_FROM} – адрес отправителя, указанный в SMTP-envelope.

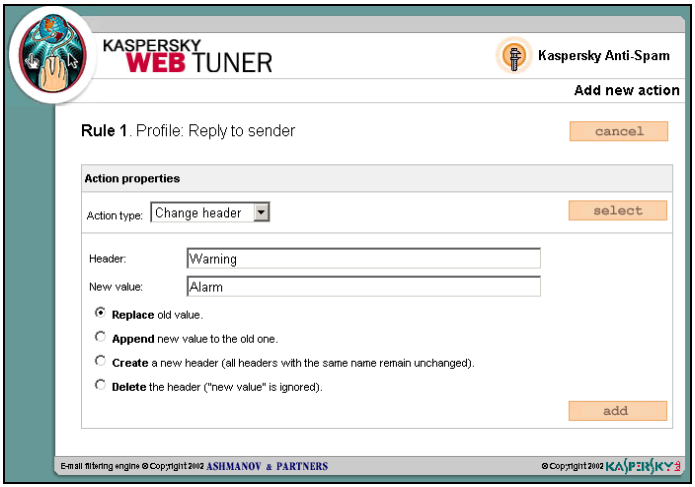

Рисунок 21. Добавление действия **change header**

Replace – заменить старый текст заголовка на указанный в поле ввода параметра **New value** новый текст.

При этом старые заголовки с указанным именем (**Header**), если они были, удаляются; создается новый заголовок с данным именем с указанным текстом (**New value**). Если заголовков с указанным именем ранее не было, у сообщения просто создается новый заголовок.

Append – добавить к старому тексту указанного заголовка (если он был) заданный в поле ввода параметра **New value** новый текст.

Новый текст (**New value**) дописывается в конец первого из существующих заголовков с указанным именем (**Header**). Если заголовков с указанным именем ранее не было, у сообщения просто создается новый заголовок.

Create – создать заголовок с именем, заданным в поле ввода параметра **Header** и текстом, заданным в поле ввода параметра **New value**, независимо от наличия у сообщения других заголовков с тем же именем.

Новый заголовок дописывается в начало списка заголовков.

Delete – удалить заголовок с указанным именем. Параметр **New value** в данном варианте действия игнорируется.

5.2.4.6. Редактирование действия

Редактирование действия правила фильтрации осуществляется в окне редактирования параметров правила **Rule properties** (см. рис. 11) в таблице **THEN DO (Actions)**.

Чтобы отредактировать (изменить) действие,

1. Выберите действие, которое вы хотите изменить.
2. Нажмите на кнопку справа от этого действия.
3. В открывшемся окне **Action properties** (см. рис. 22) при необходимости измените тип действия; для этого выберите нужный тип в списке **Action type**. Если окно не обновится, нажмите на кнопку **select**.
4. Если действие, которое вы хотите ввести вместо редактируемого, имеет варианты и параметры, введите их, как описано в п. 5.2.4.5 на стр. 74.
5. Нажмите на кнопку **accept**.

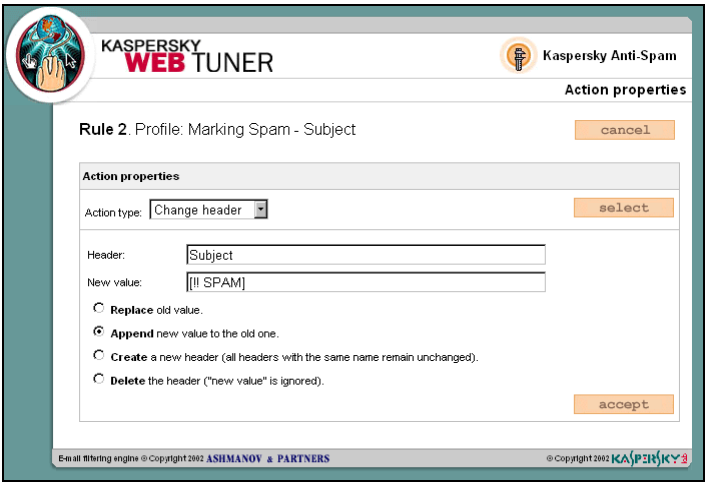

Рисунок 22. Редактирование действия (один из вариантов)

5.2.4.7. Удаление действия

Удаление действия правила фильтрации осуществляется в окне редактирования параметров правила **Rule properties** (см. рис. 11) в таблице **THEN DO (Actions)**.

Чтобы удалить существующее действие,

1. Выберите действие, которое вы хотите удалить.
2. Нажмите на кнопку ✕ справа от этого действия.

5.2.4.8. Сохранение правила

Изменения, вносимые при редактировании правила фильтрации (то есть при создании, редактировании и удалении условий и действий), должны быть сохранены (приняты) – иначе они будут проигнорированы. Это сделано для того, чтобы можно было при желании отказаться от внесенных изменений и вернуться к предшествующему виду правила (подробнее см. п. 5.2.3.6 на стр. 65 и п. 5.2.8 на стр. 94).

Чтобы сохранить (принять) изменения, внесенные в правило фильтрации,

в окне редактирования правила **Rule properties** (см. рис. 11) нажмите на кнопку **accept**.

Окно редактирования правила открывается каждый раз после завершения работы с условием или действием (по завершении их ввода или редактирования).

Чтобы отказаться от всех изменений, внесенных в правило фильтрации после того, как оно было открыто для редактирования,

1. В окне редактирования или добавления условия или действия нажмите кнопку **cancel**.
2. в окне редактирования правила (см. рис. 11) нажмите на кнопку **cancel**.

Задача: предположим, вы внесли изменения в условие одного из правил фильтрации. Что нужно сделать, чтобы эти изменения вступили в действие (учитывались при фильтрации писем)?

Решение: чтобы сохранить изменения и ввести их в действие, необходимо:

1. В окне редактирования условия **Condition properties** (см. рис. 19) нажать на кнопку **accept**, чтобы принять изменения в условии.
2. В открывшемся окне редактирования правила **Rule properties** (см. рис. 11) нажать на кнопку **accept**, чтобы принять изменения в правиле фильтрации.
3. В открывшемся окне профиля фильтрации (см. рис. 7) нажать на кнопку **save**.

В результате все изменения в конфигурации Фильтра будут сохранены, будет запущен Компилятор конфигурации, и изменения будут введены в действие.

5.2.5. Работа со списками. Закладки *e-mails*, *ip-addresses*, *dns blacklists*

Списки e-mail и IP-адресов и DNS-based RBL используются в правилах фильтрации (см. пп. 5.2.1–5.2.4 на стр. 54–66) для задания условий, относящихся не к одному отдельному адресу, а к целой группе адресов, которые должны обрабатываться одинаково. Иногда эта группа может быть очень большой; например, список e-mail отправителей спама, или почтовых серверов, с которых приходит спам, может включать сотни или даже тысячи единиц.

Работа с различными типами адресов при настройке Фильтра организована одинаково, с точностью до формата задания самих адресов, поэтому здесь они описаны вместе.

5.2.5.1. Просмотр списка

Каждый список e-mail, IP-адресов или DNS-based RBL хранится в отдельном xml-файле. Список таких файлов можно увидеть, открыв соответствующую закладку.

Работа со списками адресов e-mail ведется на закладке **e-mails** (см. рис. 23), со списками IP-адресов – на закладке **ip-addresses** (см. рис. 24), со списками DNS-based RBL – на закладке **dns blacklists** (см. рис. 25).

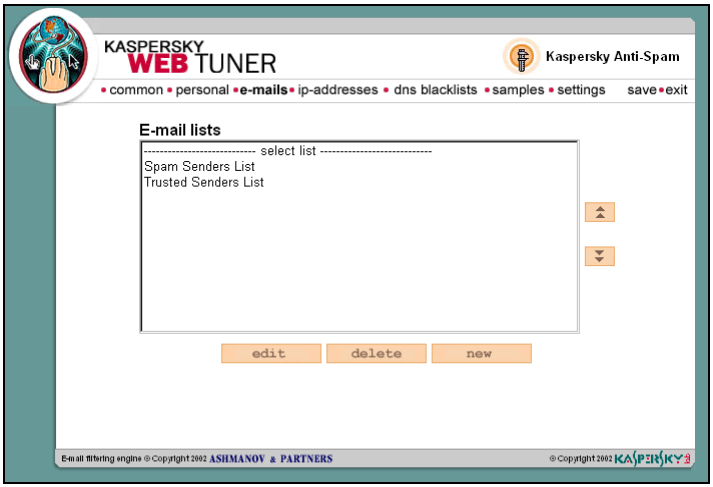

Рисунок 23. Закладка **e-mails**

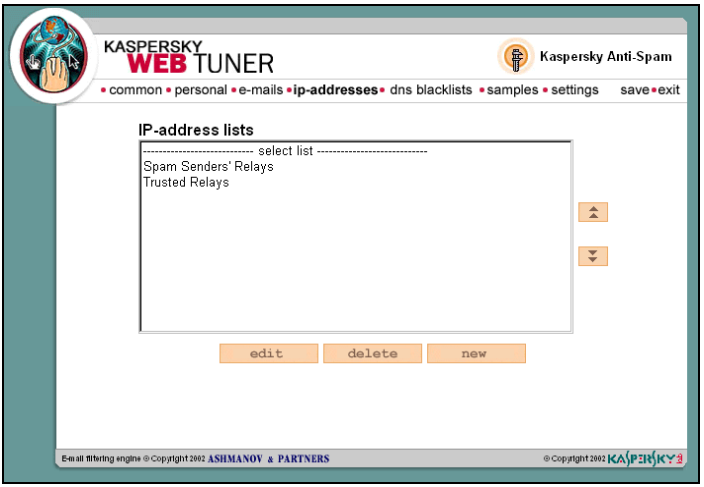

Рисунок 24. Закладка **ip-addresses**

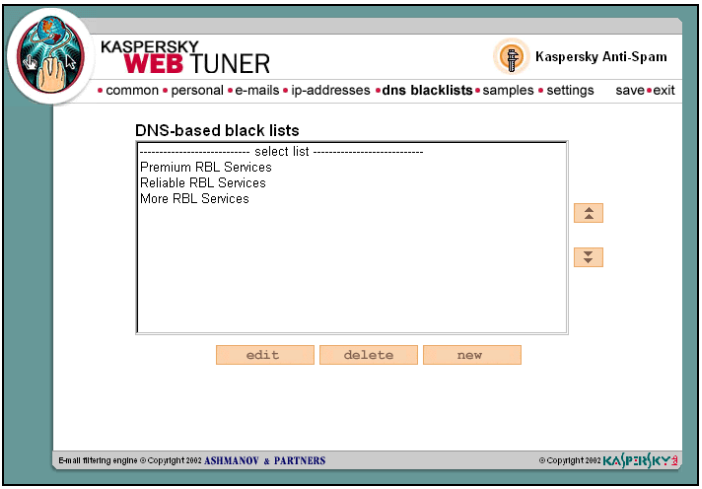

Рисунок 25. Закладка **dns blacklists**

Редактирование списков на каждой закладке осуществляется посредством следующих кнопок:

- **new** – добавить новый список (см. п. 5.2.5.2 на стр. 82);
- **edit** – отредактировать параметры выбранного списка (см. п. 5.2.5.3 на стр. 83);
- **delete** – удалить выбранный список (см. п. 5.2.5.4 на стр. 87).

Список может не помещаться целиком в окне. В этом случае используйте кнопки прокрутки справа от него.

5.2.5.2. Создание нового списка

Чтобы создать новый список e-mail, IP-адресов или DNS-based RBL,

1. Нажмите на кнопку **new** на соответствующей закладке (см. рис. 23 для закладки **e-mails**, рис. 24 для закладки **ip-addressed**, рис. 25 для закладки **dns blacklists**).
2. В открывшемся окне (см. рис. 26) введите следующие параметры списка:

- **File** – имя файла, в котором будет храниться формируемый список. В поле ввода параметра задайте имя файла без расширения или с расширением *xml*;
- **Name** – название списка.

3. Нажмите на кнопку **create**.

Имя файла обязательно для ввода; если оно не введено, выдается сообщение об ошибке. В качестве названия списка, если оно не введено, используется название файла без расширения.

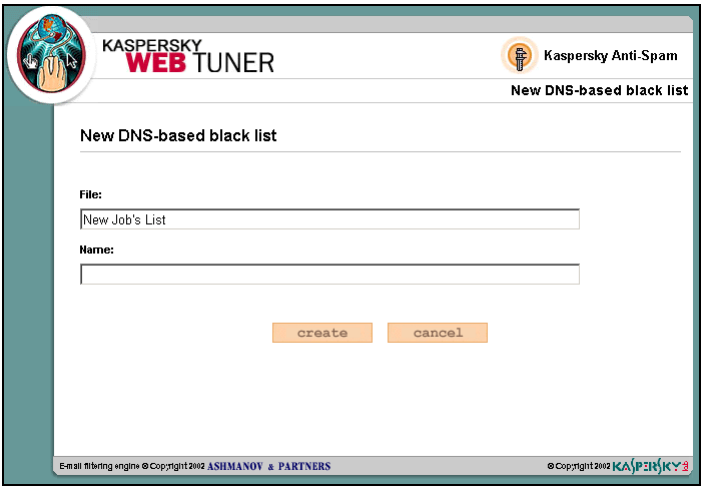

Рисунок 26. Создание нового списка (на примере списка DNS-based RBL)

5.2.5.3. Редактирование списка

Чтобы перейти к редактированию существующего списка e-mail, IP-адресов или DNS-based RBL,

1. Выберите на соответствующей закладке список, параметры которого вы хотите редактировать.
2. Нажмите на кнопку **edit**.

В результате будет открыто окно редактирования отдельного списка (см. рис. 27), где вы можете добавлять, редактировать и удалять отдельные элементы списка (адреса, black lists).

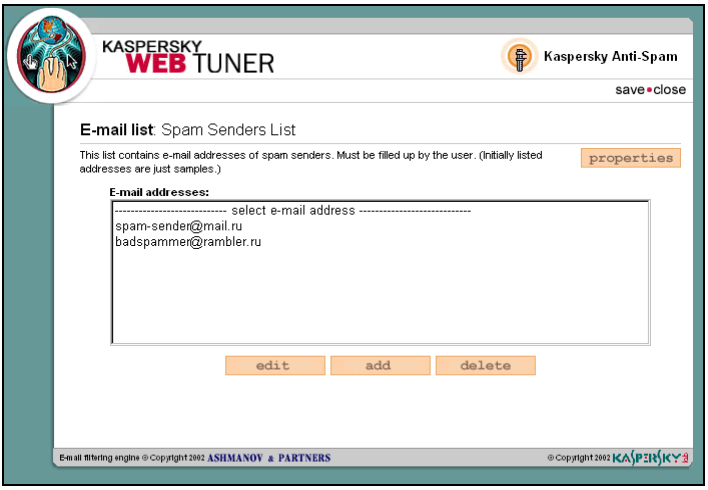

Рисунок 27. Редактирование отдельного списка
(на примере списка e-mail)

5.2.5.3.1. Создание нового элемента списка

Чтобы создать новый элемент списка e-mail, IP-адресов или DNS-based RBL,

1. В окне редактирования списка (см. рис. 27) нажмите на кнопку **add**.
2. В открывшемся окне (например, рис. 28) введите новый элемент списка: соответственно **E-mail**, **IP-address (network mask)** или **DNS-based black list**.
3. Нажмите на кнопку **add**.

Возможные форматы ввода адресов e-mail:

user@domain

@domain

Во втором случае подразумевается любой пользователь указанного домена.

Возможные форматы ввода IP-адресов (масок сетей):

aaa.bbb.ccc.ddd

aaa.bbb.ccc.ddd/nn

Запись **aaa.bbb.ccc.ddd** равносильна **aaa.bbb.ccc.ddd/32**.

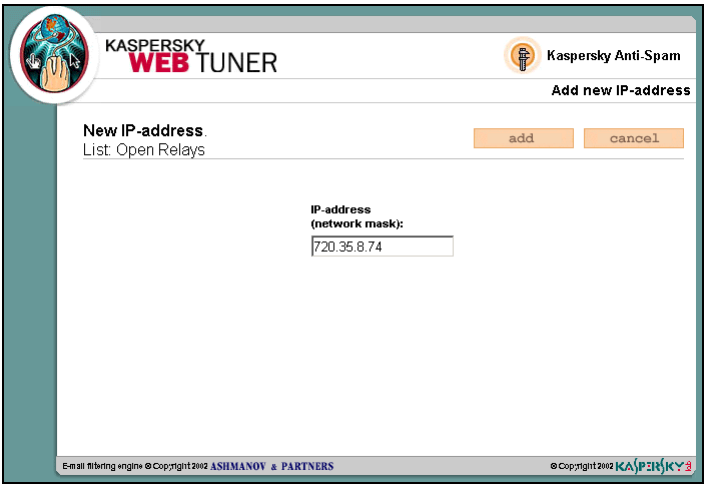

Рисунок 28. Ввод нового элемента списка (на примере IP-адресов)

5.2.5.3.2. Редактирование элемента списка

Чтобы отредактировать элемент списка e-mail, IP-адресов или DNS-based RBL,

1. В окне редактирования списка выберите (см. рис. 27) элемент, который вы хотите отредактировать.
2. Нажмите на кнопку **edit**.
3. В открывшемся окне (см. рис. 29) отредактируйте элемент списка: соответственно **E-mail**, **IP-address (network mask)** или **DNS-based black list**.
4. Нажмите на кнопку **accept**.

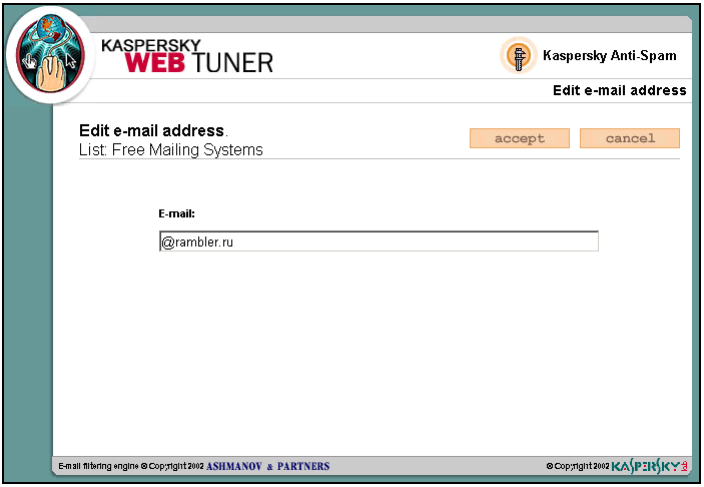

Рисунок 29. Редактирование элемента списка (на примере e-mail)

5.2.5.3.3. Удаление элемента списка

Чтобы удалить элемент списка e-mail, IP-адресов или DNS-based RBL,

1. В окне редактирования списка выберите (см. рис. 27) элемент, который вы хотите удалить.
2. Нажмите на кнопку **delete**.

5.2.5.3.4. Редактирование названия и описания списка

Название и описание списка e-mail, IP-адресов или DNS-based RBL редактируются в окне **E-mail properties**, **IP-address properties** или **DNS-based black list properties**, соответственно.

При создании списка его описание остается пустым, и на его странице редактирования выводится ***(No description)***. Имя файла, в котором хранится описание списка, не может быть изменено.

Чтобы отредактировать параметры списка,

1. В окне редактирования списка (см. рис. 27) нажмите на кнопку **properties**.

2. В открывшемся окне(см. рис. 30) отредактируйте:
   - **Name** – название списка. В поле ввода параметра отредактируйте название.
   - **Description** – описание списка. В поле ввода укажите необходимую информацию.

Имя файла не доступно для корректировки.

3. Нажмите на кнопку **accept**.

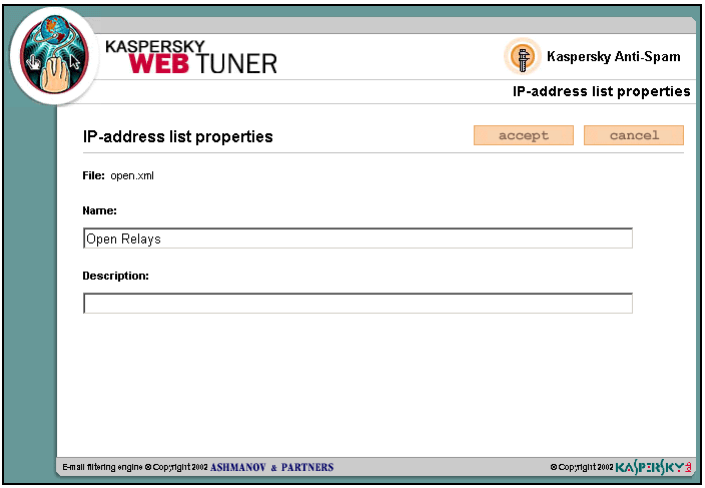

Рисунок 30. Редактирование параметров списка
(на примере списка IP-адресов)

5.2.5.4. Удаление списка

Чтобы удалить существующий список e-mail, IP-адресов или DNS-based RBL,

1. На соответствующей закладке выберите тот список, который вы хотите удалить.
2. Нажмите на кнопку **delete**.
3. В открывшемся окне подтверждения удаления (см. рис. 31) снова нажмите на кнопку **delete**.

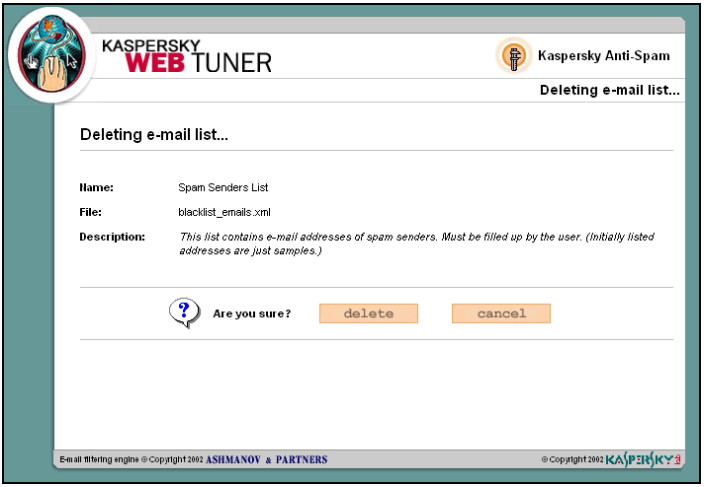

Рисунок 31. Удаление списка (на примере списка IP-адресов)

5.2.5.5. Сохранение списков

Редактирование списков e-mail, IP-адресов и DNS-based RBL, как и профилей фильтрации, ведется в копиях конфигурационных файлов. Изменения в эти файлы вносятся каждый раз после редактирования списка или профиля. Однако на работе фильтра это никак не сказывается – она ведется по старым конфигурационным файлам до тех пор, пока новая конфигурация Фильтра, сложившаяся в результате редактирования, не будет сохранена.

Чтобы сохранить и ввести в действие изменения, внесенные в конфигурационные файлы,

нажмите на кнопку **save**.

Конфигурация Фильтра, полученная в результате редактирования, сохраняется целиком – все профили, списки e-mail и IP-адресов и т. п.

После сохранения конфигурационных файлов программа веб-конфигуратор автоматически запускает Компилятор конфигурации, который собирает из текстовых xml-файлов конфигурации бинарные файлы, используемые в работе Фильтра.

5.2.6. Работа с образцами спамерских писем

Программа веб-конфигуратор позволяет добавлять в Базу контентной фильтрации образцы спамерских писем, во избежание повторного получения таких же или подобных писем, а также редактировать и удалять добавленные образцы.

Работа с образцами спамерских писем ведется на закладке **samples** (см. рис. 32).

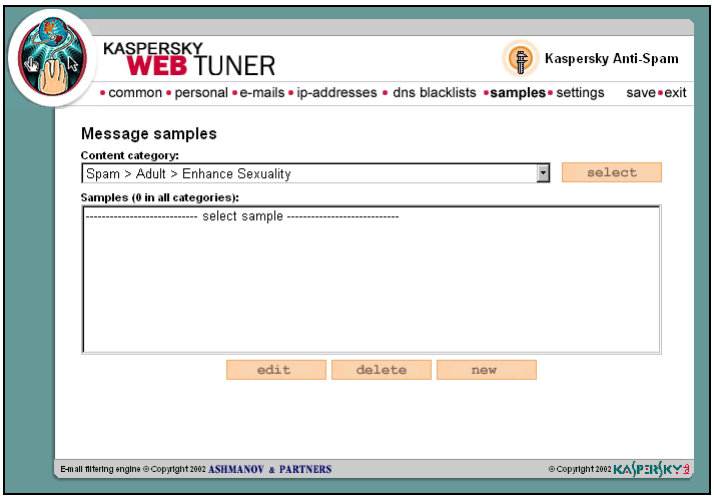

Рисунок 32. Закладка **samples**

5.2.6.1. Добавление письма-образца

При добавлении письма необходимо указать категорию нежелательной корреспонденции, к которой оно относится.

Чтобы добавить письмо-образец,

1. На закладке **samples** (см. рис. 32) нажмите на кнопку **new**.
2. В открывшемся окне **Create new message sample** (см. рис. 33) задайте следующие параметры письма-образца:

- **Category** – категория спама. Из раскрывающегося списка параметра выберите подходящую категорию.
- **Subject** – заголовок письма-образца. В поле ввода параметра введите заголовок письма-образца.
- **Body** – текст письма-образца. В поле ввода параметра введите текст письма-образца.

3. Нажмите на кнопку **create**.

Рисунок 33. Добавление письма-образца спама

5.2.6.2. Редактирование письма-образца

Чтобы отредактировать письмо-образец,

1. На закладке **samples** (см. рис. 32) выберите нужное письмо.

   Это можно сделать и при первоначальном состоянии закладки (**select content category**), однако, если писем-образцов много, лучше предварительно выбрать из списка категорию спама, к которой было отнесено письмо.

2. Нажмите на кнопку **edit**.
3. В открывшемся окне **Edit message sample** (см. рис. 34) вы можете:

- **Category** – выбрать из раскрывающегося списка категорию, к которой должно быть отнесено письмо, при этом письмо будет перенесено в новую категорию.
- **Subject** – отредактировать заголовок письма.
- **Body** – отредактировать текст письма.

4. Нажмите на кнопку **accept**.

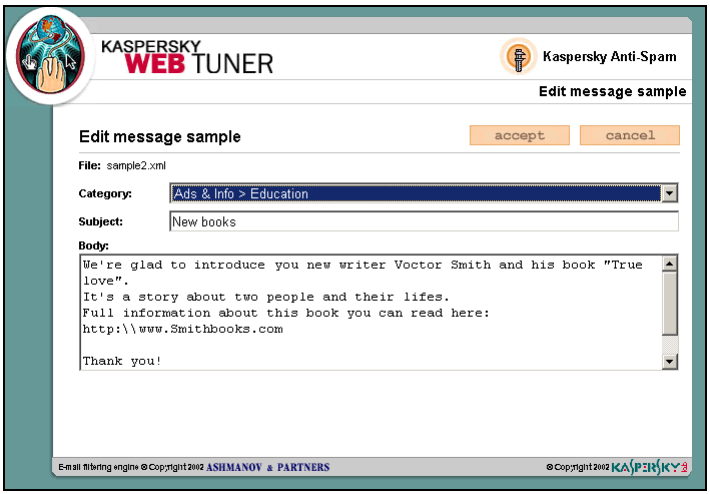

Рисунок 34. Редактирование письма-образца

5.2.6.3. Удаление письма-образца

Чтобы удалить письмо-образец,

1. На закладке **samples** (см. рис. 32) выберите нужное письмо.
2. Нажмите на кнопку **delete**.

5.2.7. Общие настройки Фильтра

К общим настройкам Фильтра относятся:

- уведомления отправителю об отказе принять посланное им письмо;

- список адресов лицензированных получателей, почта для которых обрабатывается на предмет спама.

Особенно важным является составление списка адресов лицензированных получателей, поскольку почтовые сообщения именно для этих пользователей будут анализироваться Фильтром. Следует помнить, что общее количество адресов не должно превышать оговоренное лицензией.

Все перечисленные выше настройки выполняются на закладке **settings** (см. рис. 35). Рассмотрим их подробнее.

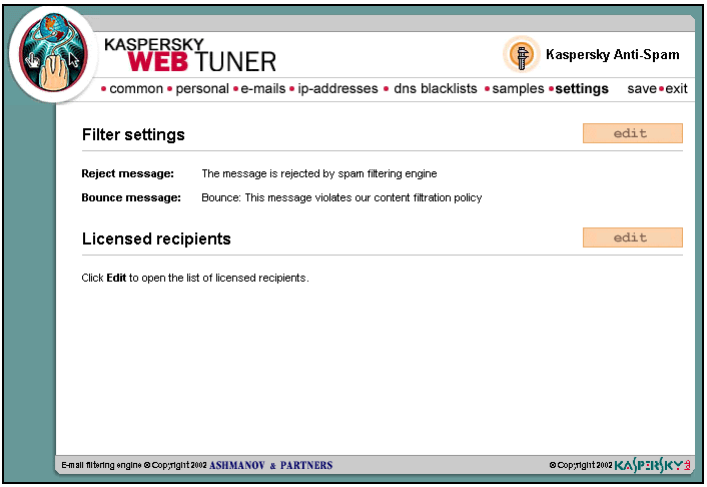

Рисунок 35. Закладка **settings**

5.2.7.1. Уведомления отправителю об отказе

Спам-фильтр генерирует уведомления отправителю об отказе принять письмо. Такие уведомления посылаются в двух случаях:

- когда выполняется действие **reject**;
- когда выполняется действие **bounce**.

Тексты уведомлений приведены на закладке **settings** в разделе **Filter settings**.

*Чтобы изменить текст уведомлений, высылаемых отправителю при осуществлении действий **reject** и **bounce**,*

1. В разделе **Filter settings** нажмите кнопку **edit**.

2. В открывшемся окне **Edit filter setting** (см. рис. 36) отредактируйте текст сообщений.

3. Нажмите на кнопку **accept**.

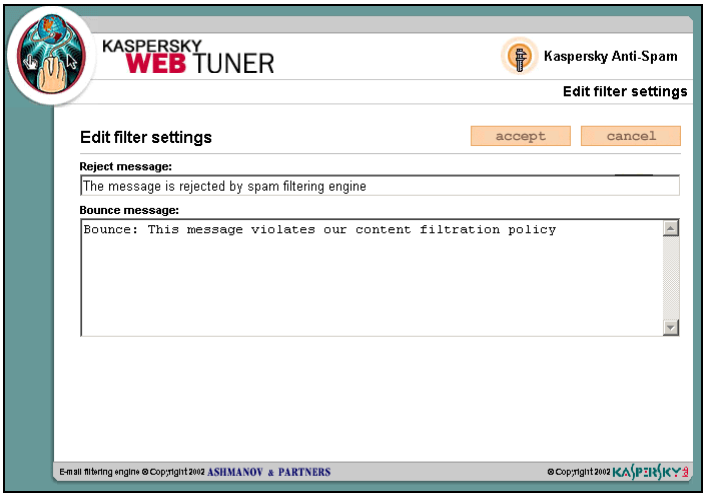

Рисунок 36. Окно редактирования уведомлений

5.2.7.2. Формирование списка лицензированных пользователей

Составление списка лицензированных пользователей имеет высокую важность при работе с Фильтром, поскольку почтовые сообщения именно для перечисленных в нем пользователей будут подвергаться фильтрации.

После инсталляции продукта данный список пуст. Вам необходимо перечислить в нем электронные адреса пользователей, почту для которых вы хотите обрабатывать.

Для просмотра и редактирования списка адресов лицензированных получателей Kaspersky Anti-Spam на закладке **settings** (см. рис. 36) в разделе **Licensed recipients** нажмите на кнопку **edit**.

В открывшемся окне (см. рис. 37) посредством кнопок **add** и **delete** вы можете отредактировать список.

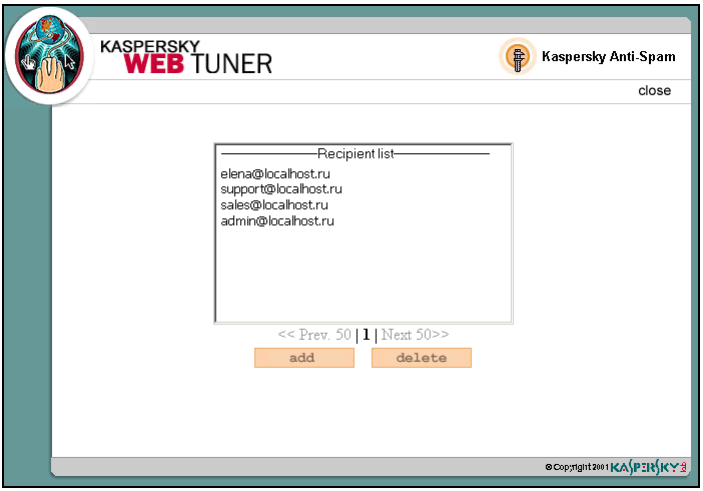

Рисунок 37. Список адресов лицензированных получателей

5.2.8. Сохранение конфигурации Фильтра

В процессе работы программы веб-конфигуратор создаются копии всех необходимых конфигурационных файлов, и изменения вносятся в эти копии. Сами конфигурационные файлы при этом остаются неизменными. Это дает возможность в любой момент (до того, как выполнено сохранение) отказаться от сделанных изменений; см. ниже.

Чтобы перенести сделанные изменения в рабочие конфигурационные файлы и ввести их в действие, необходимо *сохранить конфигурацию*.

Чтобы сохранить конфигурацию Фильтра,

на любой из закладок нажмите на кнопку **save**, расположенную в правом верхнем углу окна.

При сохранении конфигурации временные копии конфигурационных файлов сохраняются в качестве постоянных, и запускается *компиляция конфигурации*. Это необходимо для того, чтобы получить из текстовых XML-файлов, редактируемых программой веб-конфигуратор, бинарные файлы конфигурации, используемые Фильтром (для обеспечения необходимого быстродействия).

В случае успешного завершения компиляции производится обновление бинарного представления конфигурационных файлов, которым пользуется Фильтр, и Фильтру посылается сигнал о необходимости перечитать данные.

Если же копирование файлов или компиляция завершилась неудачно, вам будет предъявлен список обнаруженных ошибок. Бинарное представление конфигурационных файлов в этом случае не перезаписывается, и Фильтр продолжает работу со старыми данными.

Одна из возможных причин неудачи при сохранении и компиляции конфигурации – отсутствие необходимых прав на перезапись файлов.

Сохранение конфигурации делает отказ от внесенных изменений (возврат к предшествующей конфигурации) невозможным.

Чтобы отказаться от изменений, внесенных в конфигурацию Фильтра (до ее сохранения),

1. Откройте любую из закладок.
2. Нажмите на кнопку **exit**, расположенную в правом верхнем углу окна.

В результате будет запрошено подтверждение, и в случае его получения будет осуществлен выход из конфигурирования Спам-фильтра без сохранения временных копий конфигурационных файлов.

Крайне нежелательно прекращать работу по настройке Спам-фильтра простым закрытием окна веб-конфигуратора, без нажатия на кнопку **save** или **exit**. При таком выходе изменения, внесенные в конфигурацию, игнорируются. Измененные копии конфигурационных файлов остаются на компьютере, однако воспользоваться ими практически невозможно.

ГЛАВА 6. ОБНОВЛЕНИЕ БАЗЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Обновление Базы контентной фильтрации, используемой при анализе почтовых сообщений на предмет спама, осуществляется скриптом получения обновлений (*sfupdates*).

Обновление может производиться из перечисленных ниже источников (подробнее см. п. 6.1 на стр. 97):

- через интернет;
- из сетевого каталога.

Запуск обновления Базы контентной фильтрации может осуществляться одним из следующих способов (см. п. 6.2 на стр. 97):

- из командной строки;
- с помощью стандартной утилиты запуска программ по расписанию **cron**.

В процессе обновления выполняются следующие операции:

1. Скачивается архив Базы контентной фильтрации из указанной при запуске области (интернет, каталог) в следующий каталог: **/usr/local/ap-mailfilter/cfdata/received_updates**.
2. В случае если скачано кумулятивное (полное) обновление Базы, старые данные удаляются из папки хранения Базы контентной фильтрации **/usr/local/ap-mailfilter/cfdata/updates**, полученное обновление распаковывается и копируется в эту папку. Если получено частичное обновление, программа распаковывает и копирует его в папку хранения данных контентной фильтрации.
3. Полученные данные компилируются, Фильтр перезапускается, чтобы он использовал уже новые данные.

6.1. Выбор источника обновления Базы контентной фильтрации

Параметры обновления Базы контентной фильтрации хранятся в конфигурационном файле скрипта обновления – */usr/local/ap-mailfilter/conf/src/updater.ini* (подробнее см. п. А.5 на стр. 133). Посредством редактирования параметров вы можете изменять источник обновления Базы.

По умолчанию обновление скачивается через интернет с сайта "Лаборатории Касперского" (ftp://downloads1.kaspersky-labs.com/sfupdaters). Такой режим обновления обуславливается значением **download** параметра **METHOD**. Для изменения адреса обновления вам необходимо откорректировать значение параметра **URL**. Например:

METHOD=download

URL=ftp://user:password@localhost/dir/subdir

Если вам необходимо обновить Базу контентной фильтрации на нескольких компьютерах, удобнее вместо многократного обновления Базы через интернет получить ее один раз, записать в некоторый каталог, а затем обновлять Базу из этого каталога. Для выбота такого источника обновления необходимо параметру **METHOD** присвоить значение **copy** и указать полный путь к каталогу в качестве значения параметра **UPDATE_PATH**. Например:

METHOD=copy

UPDATE_PATH=/usr/local/share/updates/sfupdates

6.2. Запуск обновления

Существует два способа обновления Базы контентной фильтрации: автоматически по расписанию или вручную из командной строки.

Мы настоятельно рекомендуем настроить автоматическое обновление по расписанию, поскольку это позволяет постоянно использовать при фильтрации спама самые свежие данные, подготовленные лингвистической лабораторией компании "Ашманов и Партнеры", и обеспечивает наиболее эффективную фильтрацию спама.

6.2.1. Запуск по расписанию

В поставку любой операционной системы семейства Unix включена стандартная утилита запуска программ по расписанию **cron**, с помощью которой вы можете задать автоматическое обновление Базы контентной фильтрации через интернет.

Рекомендуется настроить обновление Базы таким образом, чтобы оно запускалось каждый час.

Выполнение скрипта обновления вы можете прописать в crontab к пользователю **root**, либо к пользователю **mailflt**, от имени которого работает Фильтр. Предварительно необходимо убедиться, что пользователь **mailflt** обладает правами на запись в следующие каталоги:

/usr/local/ap-mailfilter/cfdata – каталог с Базой контентной фильтрации;

/usr/local/ap-mailfilter/conf – каталог с конфигурацией Фильтра.

Например, файл с crontab может иметь следующий вид:

```
SHELL=/bin/sh
26 * * * * /usr/local/ap-mailfilter/bin/sfupdates
```

Для изменения параметров запуска, занесенных в cron, воспользуйтесь следующей командой:

- для пользователя **root**: `% crontab -e`
- для пользователя **mailflt**: `$ crontab –u mailflt –e`

6.2.2. Запуск из командной строки

Запуск обновления Базы контентной фильтрации из командной строки выглядит следующим образом:

./sfupdates [ключ]

где **[ключ]** – один из возможных ключей. Полный список ключей и их назначение приведен в п. А.6 на стр. 134.

При запуске скрипта обновления Базы контентной фильтрации без ключей командной строки новые обновления будут скачены через интернет, проверена их целостность, выполнится запуск компилятора обновлений, после чего Фильтр будет перезапущен на работу с новой Базой.

6.3. Просмотр результатов работы

По умолчанию результаты работы скрипта обновления Базы контентной фильтрации выводятся на консоль, а также фиксируются в системном журнале (syslog). Причем в журнал записываются только основные сообщения, касающиеся типа обновления, процесса обновления, его результатов.

При запуске скрипта обновления из командной строки вы можете выбирать режим информирования о процессе обновления Базы контентной фильтрации с помощью ключей командной строки.

Так, чтобы отказаться от вывода сообщений, запустите скрипт с ключем **–q**.

Если помимо справочной информации вы хотите получать и отладочную, при запуске скрипта укажите ключ **–v**.

ПРИЛОЖЕНИЕ А. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ О KASPERSKY ANTI-SPAM

А.1. Программа *ap-process-server* (мастер-процесс)

А.1.1. Запуск и остановка мастер-процесса

Программа *ap-process-server* (мастер-процесс) запускается при установке Kaspersky Anti-Spam и при перезагрузке сервера.

Для нормального функционирования Kaspersky Anti-Spam мастер-процесс должен работать постоянно.

Команда запуска мастер-процесса имеет вид:

```
/usr/local/ap-mailfilter/bin/ap-process-server
[<имя файла конфигурации>]
```

Имя файла конфигурации по-умолчанию: */usr/local/ap-mailfilter/etc/ap-process-server.conf*.

При запуске программа создает pid-файл, имя и путь к которому задается в конфигурационном файле, путь по умолчанию: */var/tmp/ap-process-server.pid*.

Мастер-процесс перечитывает конфигурационный файл при получении сигнала SIGHUP.

Остановка мастер-процесса производится при получении им сигнала SIGTERM. В процессе остановки мастер-процесс ожидает завершения дочерних процессов в течение 10 секунд, если за это время они не завершились, дочерним процессам отправляется сигнал SIGKILL.

A.1.2. Конфигурационный файл программы *ap-process-server*

Конфигурационный файл программы *ap-process-server* состоит из параметров конфигурации (ключевое слово и аргумент через пробел, по одному на строке) и комментариев. Комментарии начинаются с символов **#** или **;**

Пример конфигурационного файла:

```
FilterPath /usr/local/ap-mailfilter/bin/ap-mailfilter
FilterParam -a -V 1 -g mailflt:mailflt -K 1
StartFilters 0
MaxFilters 20
MinSpareFilters 0
PidFile /usr/local/ap-mailfilter/run/ap-process-server.pid
LogLevel 1
SysLogFacility Mail
Listen tcp:127.0.0.1:2255
```

Описание параметров конфигурации:

FilterPath – имя исполняемого файла процесса фильтрации. Значение по умолчанию: */usr/local/ap-mailfilter/libexec/ap-mailfilter*.

FilterParam – параметры командной строки, передаваемые процессу фильтрации; см. п. A.2 на стр. 103. Значение по умолчанию: **–V 1**.

StartFilters – количество фильтров, которые нужно запускать сразу после старта (prefork). Значение по умолчанию: **0**.

MaxFilters – максимальное количество процессов фильтрации, которое может быть запущено мастер-процессом. Значение по умолчанию: **50**.

Параметр **MaxFilters** должен быть установлен таким образом, чтобы в системе не начинался активный свопинг даже при максимуме загрузки. Типичное значение для сервера с 1ГБ памяти – **50**, если преимущественную часть трафика составляют очень короткие письма (и расход памяти процессами фильтрации мал), то это значение может быть увеличено.

MinSpareFilters – минимальное количество свободных процессов фильтрации. Если их оказывается меньше заданного количества, то мастер-процесс запускает дополнительные процессы. Значение по умолчанию: **0**.

Параметр **MinSpareFilters** может использоваться для сглаживания резких пиков нагрузки: при необходимости **MinSpareFilters** следует установить на уровне 10–20% от значения параметра **MaxFilters**.

PidFile – полный путь к pid-файлу. Значение по умолчанию: */var/tmp/ap-process-server.pid*.

LogLevel – числовое значение, определяющее уровень детализации записи в системный журнал (syslog); см. п. A.1.3 на стр. 102. Значение по умолчанию: **3**.

SysLogFacility – значение параметра facility, которое используется при записи в системный журнал. Значение по умолчанию: **mail**.

Listen – адрес сокета, через который устанавливаются соединения с клиентами. Параметр может быть задан в одном из следующих форматов:

tcp::port – сетевой сокет с привязкой к INADDR_ANY (принимаются соединения на любой из адресов сервера);

tcp:hostname:port – сетевой сокет с привязкой (в качестве *hostname* может быть указан IP-адрес или имя компьютера; если задано имя компьютера, обладающего несколькими адресами, то будет выдано сообщение об ошибке);

unix:/path/to/socket – локальный сокет. Значение по умолчанию: *unix:/var/tmp/ap-process-server-socket*.

A.1.3. Уровни детализации записи в системный журнал (syslog)

При записи в системный журнал (syslog) мастер-процесс использует следующие уровни детализации:

Уровень	Тип записываемых сообщений	Приоритет
0	Никаких сообщений в системный журнал не записывается.	–
1	Сообщения об ошибках: процесс фильтрации завершился с ошибкой или по сигналу, отличному от SIGHUP, невозможно запустить процесс фильтрации, процессы фильтрации слишком часто перезапускаются и т. п.	error

Уровень	Тип записываемых сообщений	Приоритет
2	Сообщения о достижении лимита количества запущенных процессов фильтрации.	info
3	Сообщения о запуске и завершении мастер-процесса, получении сигналов, перечитывании конфигурации.	info
4	Сообщения о запуске и завершении процессов фильтрации.	info
5	Информация об использовании ресурсов дочерними процессами.	info

A.2. Параметры командной строки программы *ap-mailfilter* (процесс фильтрации)

Программа *ap-mailfilter* (процесс фильтрации) запускается мастер-процессом. При запуске процесса фильтрации мастер-процесс передает ему параметры командной строки, заданные параметром **FilterParam** в конфигурационном файле мастер-процесса.

Программа *ap-mailfilter* поддерживает следующие ключи командной строки:

Общие параметры

- **–a** – работа в режиме клиент-сервер. Наличие данного ключа обязательно для работы со всеми клиентскими модулями Kaspersky Anti-Spam 2.0.
- **–b /path/to/ap-mailfilter/conf/data** – полный путь к каталогу с данными (база фильтрации, скомпилированные профили). Значение по умолчанию: */usr/local/ap-mailfilter/conf/data*.
- **–k /path/to/ap-mailfilter/run/kas-license** – полный путь к файлу сокета, через который работает лицензионный сервис *kas-licence*. Значение по умолчанию: */usr/local/ap-mailfilter/run/kas-license*.

Таймауты

–i <число_секунд> – максимальное время (в секундах), в течение которого свободный процесс фильтрации может оставаться в режиме ожидания (idle): если в течение указанного времени процесс не получает нового письма для фильтрации, его работа завершается. Значение по умолчанию: **300**.

–I <число_секунд> – максимальное время ожидания (в секундах) при получении данных от клиента в процессе обработки отдельного письма: если в течение указанного времени ни одного нового байта данных не получено, обработка текущего письма прекращается. Значение по умолчанию: **30**.

Работа с RBL

–r <число_секунд> – максимальное время выполнения отдельного правила фильтрации, связанного с обращением к DNS (проверка по списку служб RBL, проверка на наличие IP-адреса в DNS). Значение по умолчанию: **6**.

–k <число> – глубина разбора заголовков *Received* для извлечения IP-адресов (с дальнейшей проверкой их по RBL). При *K = 0* разбор не производится, при *K = n* IP-адреса извлекаются только из *n* верхних заголовков Received.

Безопасность

–r /path/to – режим работы с chroot в каталоге /path/to.

–g user:group, **–g userid:groupid** – пользователь и группа, от имени которых работает процесс фильтрации. Рекомендуется всегда использовать **-g mailflt:mailflt**.

Работа с системным журналом (syslog)

–V <число> – уровень детализации записи в системный журнал:

0 – минимальный уровень детализации, запись по действию DoSyslog не производится;

1 – вывод сообщений об ошибках и выполнение действия DoSyslog;

2 – вывод предупреждений (warnings);

3 и более – вывод отладочных сообщений.

–L /path/to/logfile – файл, в который перенаправляются сообщения при выполнении действия DoSyslog.

Управление загрузкой сервера

Описанные ниже параметры следует менять только в случае очень высоких нагрузок (сотни тысяч или миллионы писем в сутки на один сервер).

–m <число> – максимальное количество писем, которое обрабатывается одним процессом фильтрации. По достижении данного ограничения процесс фильтрации прекращает работу (при необходимости мастер-процесс запустит новые процессы фильтрации). Значение по умолчанию: **300**.

–M <число> – показатель рандомизации максимального количества писем, обрабатываемых одним процессом фильтрации. Значение по умолчанию: **30**.

Для каждого процесса фильтрации реальный лимит количества обрабатываемых писем устанавливается как *m + случайное число в диапазоне от 0 до M-1*; при значениях по умолчанию каждый процесс фильтрации будет обрабатывать от 300 до 329 писем. Использование рандомизации необходимо для того, чтобы избежать одновременного старта большого количества процессов фильтрации при высоких нагрузках на сервер.

–H <число_секунд> – показатель рандомизации времени завершения работы процесса фильтрации после получения им сигнала SIGHUP. Значение по умолчанию: **0**.

При ненулевом значении параметра **H** процесс фильтрации завершается по получении сигнала со случайной задержкой от **0** до **H-1** секунд. Данный параметр предназначен для того чтобы избежать возникновения пиковой нагрузки при одновременной перезагрузке всех фильтрующих процессов (например, после перекомпиляции конфигурации фильтра или обновлении базы фильтрации).

A.3. Клиентские модули для почтовых систем

Клиентские модули, входящие в состав Kaspersky Anti-Spam, предназначены для интеграции продукта в почтовые системы.

Для поддерживаемых почтовых систем используются следующие модули:

- *kas-milter* – для почтовой системы Sendmail.
- *kas-pipe* – для почтовой системы Postfix.
- *kas-pipe* (стандартная установка) – для почтовой системы Exim.

- *kas-exim* (альтернативная установка) – для почтовой системы Exim.
- *kas-qmail* – для почтовой системы Qmail.
- *kas-cgpro* – для почтовой системы Communigate Pro.

Необходимые действия по интеграции осуществляются при установке Kaspersky Anti-Spam при помощи скриптов конфигурирования почтовых систем.

В настоящем разделе более подробно описываются схемы работы клиентских модулей, их конфигурационные файлы и особенности настройки почтовых систем.

A.3.1. Схема взаимодействия клиентских модулей с фильтрующим сервисом

Взаимодействие всех клиентских модулей с фильтрующим сервисом осуществляется по единой схеме:

- клиент получает письмо от почтовой системы;
- клиент посылает запрос на соединение с процессом фильтрации;
- мастер-процесс осуществляет отслеживание запущенных процессов фильтрации (при необходимости запускает новые процессы) и устанавливает соединение между клиентом и свободным процессом фильтрации;
- по установленному соединению клиент передает письмо и получает от процесса фильтрации результат обработки письма;
- в соответствии с полученным результатом клиент производит модификацию письма и возвращает его почтовой системе.

Клиентский модуль взаимодействует с мастер-процессом и процессом фильтрации по внутреннему протоколу через TCP (сетевой) или unix (локальный) сокет.

При использовании TCP для связи клиента и фильтрующего сервиса существует возможность установить почтовую систему с интегрированным в нее клиентским модулем на одном сервере, а фильтрующий сервис (и остальные компоненты Kaspersky Anti-Spam) – на другом (выделенном) сервере. При этом если объем обрабатываемого почтового трафика позволяет, выделенный сервер может обслуживать несколько почтовых серверов. Данная конфигурация не поддерживается стандартным инсталлятором, но может быть реализована вручную.

Схемы взаимодействия клиентов с почтовыми системами описываются ниже в настоящем разделе.

A.3.2. *kas-milter* (клиентский модуль для Sendmail)

A.3.2.1. Схема работы *kas-milter*

Программа *kas-milter* предназначена для интеграции Kaspersky Anti-Spam с почтовой системой Sendmail.

Для связи с Sendmail используется библиотека *libmilter*.

Диаграмма взаимодействия модулей при работе Kaspersky Anti-Spam с Sendmail представлена на рисунке ниже.

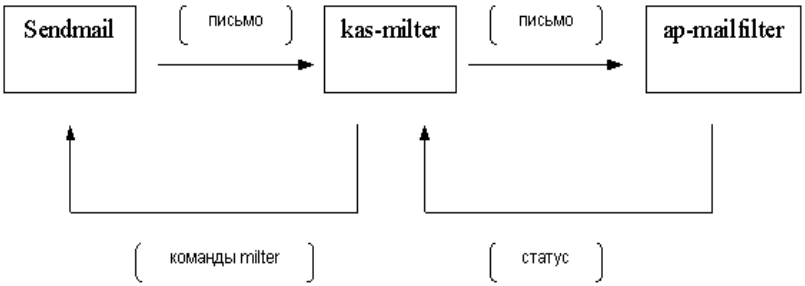

Рисунок 38. Схема работы *kas-milter*

A.3.2.2. Конфигурационный файл программы *kas-milter*

Параметры работы программы *kas-milter* задаются в конфигурационном файле */usr/local/ap-mailfilter/etc/kas-milter.conf*.

Пример конфигурационного файла:

```
SpamtestAddr tcp:127.0.0.1:2255
ConnectTimeout 10000
RWTimeout 30000
```

```
ClientAddr local:/usr/local/ap-mailfilter/run/kas-milter.sock
PidFile /usr/local/ap-mailfilter/run/kas-milter.pid
OnError ignore
FilteringSizeLimit 500
DefaultDomain localhost
LogFacility mail
LogLevel error
```

Описание параметров:

SpamtestAddr – адрес сокета, через который производится взаимодействие с процессом фильтрации. Формат: *tcp:host:port* или *unix:/path/to/socket*.

ConnectTimeout – максимальное время ожидания (в миллисекундах) при установке соединения с процессом фильтрации.

RWTimeout – максимальное время ожидания (в миллисекундах) при операциях обмена данными с процессом фильтрации.

ClientAddr – адрес сокета, через который осуществляется взаимодействие почтовой системы Sendmail и *kas-milter*.

PidFile – имя файла с pid процесса.

OnError – режим обработки ошибочной ситуации (невозможно установить соединение с процессом фильтрации, превышено время ожидания при обмене данными и т. п.). Возможные значения:

reject – выдать код 5xx (в Sendmail возвращается SMFIS_REJECT),

tempfail (по умолчанию) – выдать код 4xx (SMFIS_TEMPFAIL),

ignore – игнорировать ошибку (SMFIS_CONTINUE),

accept – принять письмо; все прочие фильтры игнорируются (SMFIS_ACCEPT).

FilteringSizeLimit – максимальный размер (в килобайтах) письма, которое может быть передано фильтрующему модулю. Письма большего размера пропускаются без фильтрации. При значении **0** данного параметра (значение по умолчанию) указанное ограничение снимается: все письма передаются на фильтрацию.

DefaultDomain – имя домена, используемое для получателей, адреса которых содержат только локальный элемент. Если данный параметр не задан, то подстановка имени домена не производится (значение по умолчанию отсутствует).

LogFacility – значение параметра facility, которое используется при записи в системный журнал. Возможные значения: **mail** (по умолчанию), **user**, **local0**-**local7**.

LogLevel – уровень детализации записи в системный журнал (syslog). Возможные значения: **error** (по умолчанию), **info**, **debug**.

A.3.2.3. Настройка Sendmail при работе с *kas-milter*

Для интеграции *kas-milter* в Sendmail в конфигурационном файле */etc/sendmail.cf* прописывается:

```
Xfilter1, S=local:/usr/local/ap-mailfilter/run/kas-milter.sock, F=R
O InputMailFilters=filter1
```

Подробное описание настройки фильтров в *sendmail.cf* приведено в документации по Sendmail.

A.3.3. *kas-pipe* (клиентский модуль для Postfix, Exim)

A.3.3.1. Схема работы *kas-pipe*

Программа *kas-pipe* является универсальным клиентским модулем Kaspersky Anti-Spam.

При стандартной установке *kas-pipe* используется для интеграции с почтовыми системами Postfix и Exim.

kas-pipe принимает почту на стандартный вход по протоколам SMTP/LMTP и отдает ее после фильтрации по SMTP/LMTP/pipe.

kas-pipe запускается внешним приложением (MTA или *inetd*), передача почты далее осуществляется через сетевой или локальный сокет, либо запуском принимающего приложения через *fork+exec*.

Диаграмма взаимодействия модулей при работе Kaspersky Anti-Spam с использованием *kas-pipe* представлена на рисунке ниже.

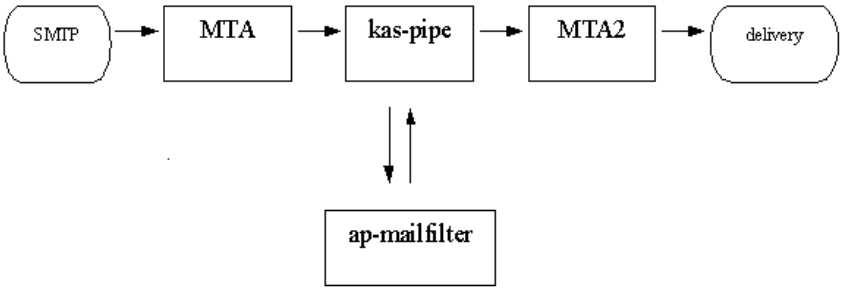

Рисунок 39. Схема работы *kas-pipe*

Данная схема работы может быть реализована с любым MTA, где поддерживается возможность запуска второй копии с другими настройками, либо доставка по LMTP (по TCP или pipe), либо доставка всей почты по SMTP на жестко заданный почтовый транспортный агент.

A.3.3.2. Конфигурационный файл программы *kas-pipe*

Параметры работы программы *kas-pipe* задаются в конфигурационном файле */usr/local/ap-mailfilter/etc/kas-pipe.conf*.

При запуске программы имя конфигурационного файла может быть переопределено:

```
kas-pipe -c /usr/local/ap-mailfilter/etc/kas-pipe-
postfix.conf
```

Пример конфигурационного файла:

```
SpamtestAddr tcp:127.0.0.1:2255
ConnectTimeout 10000
RWTimeout 30000
InProtocolLMTP No
OutProtocolLMTP No
OutgoingAddr exec:/usr/sbin/sendmail -bs
Domain antispam.localhost
OnError accept
MessageStoreMem 50
TempDir /var/tmp
FilteringSizeLimit 500
```

```
MultipleMessagesAllowed Yes
LogFacility MAIL
LogLevel silent
LogStderrToo No
```

Описание параметров:

SpamtestAddr – адрес сокета, через который производится взаимодействие с процессом фильтрации. Формат: *tcp:host:port* или *unix:/path/to/socket*.

ConnectTimeout – максимальное время ожидания (в миллисекундах) при установке соединения с процессом фильтрации.

RWTimeout – максимальное время ожидания (в миллисекундах) при операциях обмена данными с процессом фильтрации.

InProtocolLMTP – использование протокола LMTP на входе. Возможные значения: **Yes**, **No**.

OutProtocolLMTP – использование протокола LMTP на выходе. Возможные значения: **Yes**, **No**.

OutgoingAddr – адрес, куда передавать почту, в одном из форматов: *tcp:host:port*, *unix:/path/to/socket*, *exec:/path/to/program params*. Например:

```
exec:/usr/sbin/sendmail -bs -C /my/sendmail.cf
```

или

```
tcp:127.0.0.1:9025.
```

OnError – режим обработки ошибочной ситуации (невозможно установить соединение с процессом фильтрации, превышено время ожидания при обмене данными и т. п.). Возможные значения: **reject**, **tempfail**, **accept**.

Domain – имя домена в SMTP helo при приеме-передаче почты.

MessageStoreMem – размер письма в килобайтах, начиная с которого используется режим хранения промежуточных данных на диске. Такой режим позволяет контролировать объем занимаемой оперативной памяти. Если данный параметр равен **0** (значение по умолчанию), то все данные всегда хранятся в оперативной памяти.

TempDir – каталог для хранения промежуточных данных. Если данный параметр не задан, режим хранения промежуточных данных на диске не используется.

FilteringSizeLimit – максимальный размер (в килобайтах) письма, которое может быть передано фильтрующему модулю. Письма большего размера пропускаются без фильтрации. При значении **0** данного параметра (значение по умолчанию) указанное ограничение снимается: все письма передаются на фильтрацию.

MultipleMessagesAllowed – разрешение или запрещение режима создания копий письма в случае, когда результаты фильтрации различны для разных получателей. Возможные значения: **Yes** или **No**.

LogFacility – значение параметра facility, которое используется при записи в системный журнал. Возможные значения: **mail** (по умолчанию), **user**, l**ocal0**-l**ocal7**.

LogLevel – уровень детализации записи в системный журнал (syslog). Возможные значения: **vdebug**, **debug**, **verbose**, **silent**.

LogStderrToo – вывод информации об ошибках в stderr. Возможные значения: **Yes**, **No**.

A.3.3.3. Настройка Postfix при работе с *kas-pipe*

Ниже приводится пример конфигурации *kas-pipe* и почтовой системы Postfix, в котором реализуется следующая схема работы:

- *kas-pipe* работает как контентный фильтр (*content_filter*);
- *kas-pipe* принимает почту на localhost:9026 по SMTP;
- *kas-pipe* отдает почту на localhost:9025 по SMTP.

В конфигурационном файле */usr/local/ap-mailfilter/etc/kas-pipe-postfix.conf* указывается:

```
SpamtestAddr              tcp:127.0.0.1:2255
MultipleMessagesAllowed   Yes
InProtocolLMTP            No
OutProtocolLMTP           No
OutgoingAddr              tcp:127.0.0.1:9025
```

В конфигурации Postfix (*master.cf*) производятся следующие изменения:

```
smtp   inet   n      -      n       -       -       smtpd
  -o content_filter=smtp:127.0.0.1:9026
pickup fifo   n      -      n       60      1       pickup
  -o content_filter=smtp:127.0.0.1:9026


127.0.0.1:9026 inet n n    n       -       20      spawn
   user=mailflt argv=/usr/local/ap-mailfilter/bin/kas-pipe
   -c /usr/local/ap-mailfilter/etc/kas-pipe-postfix.conf
127.0.0.1:9025 inet n -    n       -       25      smtpd
  -o local_recipient_maps=
```

```
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o strict_rfc821_envelopes=no
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
```

Для Postfix версии 2.1 и выше вместо использования *kas-pipe* как контентного фильтра (*content_filter*) можно использовать его как прокси-фильтр (*smtpd_proxy_filter*), что ускоряет обработку писем, поскольку убирается излишнее прохождение через очередь:

```
smtp   inet   n       -       n       -       -       smtpd
  -o smtpd_proxy_filter=127.0.0.1:9026
```

A.3.3.4. Настройка Exim при работе с *kas-pipe*

Ниже приводится пример конфигурации *kas-pipe* и почтовой системы Exim, в котором реализуется следующая схема работы:

- на 25-м порту запускается Exim со специальным конфигурационным файлом */usr/local/etc/exim/exim.listen*;
- вся принятая программой Exim почта передается в *kas-pipe* по LMTP;
- *kas-pipe* передает дальше обработанные письма путем запуска */usr/local/sbin/exim -bs*.

В конфигурационном файле */usr/local/ap-mailfilter/etc/kas-pipe.conf* указывается:

```
InProtocolLMTP      Yes
OutgoingAddr        exec:/usr/local/sbin/exim -bs
```

В конфигурационном файле /usr/local/etc/exim/exim.listen:

1. В секции *routers* меняется для маршрутизаторов для секций *dnslookup* и *localuser* значение параметра *transport* на *kas_lmtp*:

```
dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = kas_lmtp
```

```
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
  no_more
localuser:
  driver = accept
  check_local_user
  transport = kas_lmtp
  cannot_route_message = Unknown user
```

2. В секции *transports* создается транспорт *kas_lmtp*:

```
kas_lmtp:
 driver = lmtp
 command = /usr/local/ap-mailfilter/bin/kas-pipe
```

Строка запуска Exim'a:

```
exim -bd -q3m -C /usr/local/etc/exim/exim.listen
```

В случае большой нагрузки может потребоваться явное управление очередью и разделение входной и выходной очередей.

A.3.4. *kas-exim* (клиентский модуль для Exim)

Модуль *kas-exim* предназначен для интеграции Kaspersky Anti-Spam с почтовой системой Exim 4.xx с использованием localscan API.

Работа через *kas-exim* является альтернативным решением: при стандартной установке интеграция с Exim осуществляется с использованием программы *kas-pipe*.

Применение localscan API требует перекомпиляции Exim, поэтому *kas-exim* поставляется в исходном коде на языке C.

A.3.4.1. Компиляция *kas-exim*

Для компиляции почтовой системы Exim с подключением модуля *kas-exim* необходимо:

1. поместить файл */usr/local/ap-mailfilter/src/kas-exim.c* в подкаталог *Local* дерева ресурсов Exim;
2. в файле *Local/Makefile* произвести следующие изменения:

```
CFLAGS= -I/usr/local/ap-mailfilter/include
EXTRALIBS_EXIM=-L/usr/local/ap-mailfilter/lib
-lspamtest
LOCAL_SCAN_SOURCE=Local/kas_exim.c
```

```
LOCAL_SCAN_HAS_OPTIONS=yes
```

3. скомпилировать Exim.

A.3.4.2. Параметры конфигурации *kas-exim*

Параметры работы *kas-exim* задаются в конфигурационном файле почтовой системы Exim, например:

```
begin local_scan
spamtest_address = tcp:193.124.130.9:2255
connect_timeout = 10000
rw_timeout = 30000
on_spamtest_error=tempfail
spamtest_filtering_size_limit=512
log_level=3
```

Описание параметров:

spamtest_address – адрес сокета, через который производится взаимодействие с процессом фильтрации. Формат: *tcp:host:port* или *unix:/path/to/socket*.

connect_timeout – максимальное время ожидания (в миллисекундах) при установке соединения с процессом фильтрации.

rw_timeout – максимальное время ожидания (в миллисекундах) при операциях обмена данными с процессом фильтрации.

on_spamtest_error – режим обработки ошибочной ситуации (невозможно установить соединение с процессом фильтрации, превышено время ожидания при обмене данными и т. п.). Возможные значения: **reject**, **tempfail**, **accept**.

spamtest_filtering_size_limit – максимальный размер (в килобайтах) письма, которое может быть передано фильтрующему модулю. Письма большего размера пропускаются без фильтрации. При значении **0** данного параметра (значение по умолчанию) указанное ограничение снимается: все письма передаются на фильтрацию.

log_level – числовое значение, определяющее уровень детализации записи в лог-файл. Запись ведется через debug-printf (т. е. осуществляется в отладочном режиме работы почтовой системы Exim).

A.3.5. *kas-qmail* (клиентский модуль для Qmail)

A.3.5.1. Схема работы *kas-qmail*

Программа *kas-qmail* предназначена для интеграции Kaspersky Anti-Spam с почтовой системой Qmail.

Для работы с *kas-qmail* используется следующая схема: *qmail-queue* подменяется на *kas-qmail*, после обработки письма передаются оригинальному *qmail-queue*.

Диаграмма взаимодействия модулей при работе Kaspersky Anti-Spam с использованием *kas-qmail* представлена на рисунке ниже.

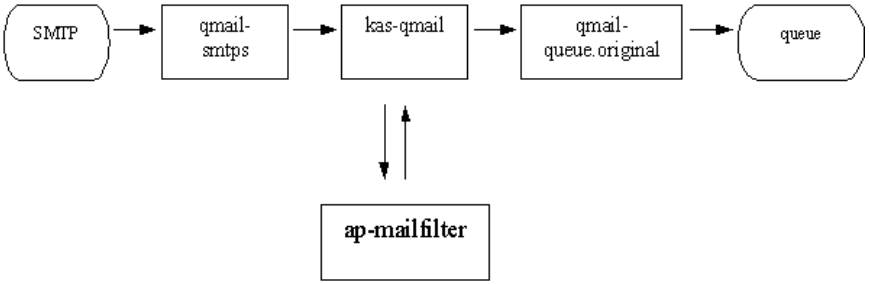

Рисунок 40. Схема работы *kas-qmail*

A.3.5.2. Конфигурационный файл программы *kas-qmail*

Параметры работы программы *kas-qmail* задаются в конфигурационном файле *control/kas-qmail*.

При запуске программы имя конфигурационного файла может быть переопределено через переменную окружения STPLUGINCONF.

Пример конфигурационного файла:

```
SpamtestAddr tcp:127.0.0.1:2255
ConnectTimeout 10000
RWTimeout 30000
OriginalQueue /var/qmail/bin/qmail-queue.kas
```

```
OnError ACCEPT
MessageStoreMem 50
TempDir /var/tmp
FilteringSizeLimit 500
DefaultDomain localhost
LogFacility MAIL
LogLevel ERROR
```

Описание параметров:

SpamtestAddr – адрес сокета, через который производится взаимодействие с процессом фильтрации. Формат: *tcp:host:port* или *unix:/path/to/socket*.

ConnectTimeout – максимальное время ожидания (в миллисекундах) при установке соединения с процессом фильтрации.

RWTimeout – максимальное время ожидания (в миллисекундах) при операциях обмена данными с процессом фильтрации.

OriginalQueue – полный путь до оригинального *qmail-queue*.

OnError – режим обработки ошибочной ситуации (невозможно установить соединение с процессом фильтрации, превышено время ожидания при обмене данными и т. п.). Возможные значения: REJECT, TEMPFAIL, ACCEPT.

MessageStoreMem – размер письма в килобайтах, начиная с которого используется режим хранения промежуточных данных на диске. Такой режим позволяет контролировать объем занимаемой оперативной памяти. Если данный параметр равен **0** (значение по умолчанию), то все данные всегда хранятся в оперативной памяти.

TempDir – каталог, для хранения промежуточных данных. Если данный параметр не задан, режим хранения промежуточных данных на диске не используется.

FilteringSizeLimit – максимальный размер (в килобайтах) письма, которое может быть передано фильтрующему модулю. Письма большего размера пропускаются без фильтрации. При значении **0** данного параметра (значение по умолчанию) указанное ограничение снимается: все письма передаются на фильтрацию.

DefaultDomain – имя домена, которое подставляется для получателей, адреса которых содержат только локальный элемент. Если данный параметр не задан, то подстановка имени домена не производится (значение по умолчанию отсутствует).

LogFacility – значение параметра facility, которое используется при записи в системный журнал. Возможные значения: **mail** (по умолчанию), **user**, **local0**-**local7**.

LogLevel – уровень детализации записи в системный журнал (syslog). Возможные значения: ERROR, INFO, DEBUG.

A.3.5.3. Настройка Qmail при работе с *kas-qmail*

При интеграции *kas-qmail* в Qmail:

- оригинальный *qmail-queue* сохраняется под другим именем:

```
mv /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue.kas
```

- устанавливается *kas-qmail* вместо *qmail-queue*:

```
cp /usr/local/ap-mailfilter/bin/kas-qmail /var/qmail/bin/qmail-queue
chown qmailq $destdir/bin/qmail-queue
chgrp qmail $destdir/bin/qmail-queue
chmod 04755 $destdir/bin/qmail-queue
```

- устанавливается конфигурационный файл:

```
cp /usr/local/ap-mailfilter/etc/kas-qmail.conf /var/qmail/control/kas-qmail
chmod 644 /var/qmail/control/kas-qmail
```

A.3.6. *kas-cgpro* (клиентский модуль для Communigate Pro)

A.3.6.1. Схема работы *kas-cgpro*

Программа *kas-cgpro* предназначена для интеграции Kaspersky Anti-Spam с почтовой системой Communigate Pro.

Для работы с *kas-cgpro* используется следующая схема:

- Communigate Pro передает всю принятую почту программе *kas-cgpro*;
- *kas-cgpro* обрабатывает письма, модифицирует их и помещает в каталог Submitted; при этом в Communigate Pro возвращается DISCARD;

- драйвер PIPE повторно передает письма из каталога Submitted в Communigate Pro, а та, в свою очередь, программе *kas-cgpro*;
- *kas-cgpro* повторно не обрабатывает письма, уже прошедшие фильтрацию: в Communigate Pro возвращается OK;

Чтобы избежать зацикливания используются два приема:

- *kas-cgpro* добавляет специальный заголовок в каждое обработанное письмо и проверяет его наличие;
- по умолчанию *kas-cgpro* обрабатывает только письма, пришедшие с SMTP (см. параметр конфигурации AllTransports).

A.3.6.2. Конфигурационный файл программы *kas-cgpro*

Параметры работы программы *kas-cgpro* задаются в конфигурационном файле */usr/local/ap-mailfilter/etc/kas-cgpro.conf*.

При запуске программы имя конфигурационного файла может быть переопределено:

```
kas-cgpro -C /path/to/conf/file
```

Пример конфигурационного файла:

```
SpamtestAddr tcp:127.0.0.1:2255
ConnectTimeout 10000
RWTimeout 30000
SubmitFolder Submitted
MaxThreads 50
LoopHeader X-Proceed_240578_by_spamtest
AllTransports No
FilteringSizeLimit 500
DefaultDomain localhost
LogFacility MAIL
LogLevel Error
```

Описание параметров:

SpamtestAddr – адрес сокета, через который производится взаимодействие с *ap-mailfilter*. Формат: *tcp:host:port* или *unix:/path/to/socket*.

ConnectTimeout – максимальное время ожидания (в миллисекундах) при установке соединения с процессом фильтрации.

RWTimeout – максимальное время ожидания (в миллисекундах) при операциях обмена данными с процессом фильтрации.

SubmitFolder – имя каталога, в который помещаются модифицированные письма.

MaxThreads – максимальное число одновременно обрабатываемых писем.

LoopHeader – заголовок, который добавляется в письма для предотвращения зацикливания.

AllTransports – разрешает/запрещает обработку почты, поступающей со всех транспортов. Возможные значения: **Yes** – обрабатывается вся почта, **No** (значение по умолчанию) – обрабатывается почта только с транспорта SMTP.

FilteringSizeLimit – максимальный размер (в килобайтах) письма, которое может быть передано фильтрующему модулю. Письма большего размера пропускаются без фильтрации. При значении **0** данного параметра (значение по умолчанию) указанное ограничение снимается: все письма передаются на фильтрацию.

DefaultDomain – имя домена, которое подставляется для получателей, адреса которых содержат только локальный элемент. Если данный параметр не задан, то подстановка имени домена не производится (значение по умолчанию отсутствует).

LogFacility – значение параметра facility, которое используется при записи в системный журнал. Возможные значения: **mail**, **user**, **local0**-**local7**.

LogLevel – уровень детализации записи в системный журнал (syslog). Возможные значения: **error**, **info**, **debug**.

A.3.6.3. Настройка Communigate Pro при работе с *kas-cgpro*

Настройка Communigate Pro производится через веб-интерфейс почтовой системы:

Settings->General->Helpers

Добавляется новый content-filter с параметрами:

```
Use Filter: kas-cgpro
Log: Problems
Path: /usr/local/ap-mailfilter/bin/kas-cgpro
Time-Out: 2 minutes
Auto-Restart: 15 seconds
```

Settings->Rules

Создается новое правило (проверять на спам сообщения менее 400 КБ):

```
Data: Message Size
Operation: less than
Parameter: 400000
Action: external filter
Parameters: kas-cgpro
```

A.4. Конфигурационные файлы

Конфигурационные xml-файлы – это текстовые файлы, содержащие описание данных на языке XML. Логически разделенные конфигурационные данные хранятся в отдельных файлах.

Конфигурационные файлы читаются и записываются программой веб-конфигуратор.

A.4.1. Состав конфигурационных файлов и их местонахождение в файловой системе

Конфигурационные файлы Kaspersky Anti-Spam находятся в каталоге **/usr/local/ap-mailfilter/conf/src** (далее **– CONFSRC**) и его подкаталогах.

Непосредственно в **CONFSRC** находятся файлы с фиксированными именами:

profiles.xml – список профилей фильтрации;

emails.xml – набор списков e-mail адресов;

iplists.xml – набор списков IP-адресов;

dnsblacklists.xml – набор списков служб DNS-based RBL;

samples.xml – список пользовательских образцов спамерских писем;

settings.xml – файл дополнительных настроек Фильтра.

В каталоге **CONFSRC** имеются следующие подкаталоги:

CONFSRC/profiles – каталог, содержащий файлы с описаниями профилей;

CONFSRC/emails – каталог, включающий файлы со списками адресов e-mail;

CONFSRC/iplists – каталог файлов со списками IP-адресов;

CONFSRC/dnsblacklists – каталог файлов со списками служб DNS-based RBL;

CONFSRC/samples – каталог, содержащий файлы с образцами спамерских писем.

Имена файлов, находящихся в подкаталогах, не фиксированы: имя каждого файла задается пользователем при его создании через программу веб-конфигуратор. Однако все эти файлы имеют расширение *.xml*.

A.4.2. Заголовки xml-файлов

Каждый конфигурационный файл начинается с декларации формата документа:

<?xml version="1.0" encoding="koi8-r"?>

Атрибут **encoding** задает кодировку данного файла.

Поддерживаются следующие кодировки:

- **windows-1251**;
- **koi8-r**;
- **iso-8859-5**;
- **x-mac-cyrillic**;
- **ibm866**.

Программа веб-конфигуратор сохраняет файлы в кодировке **koi8-r**.

A.4.3. Список профилей фильтрации (*profiles.xml*)

Список существующих профилей фильтрации – как общих, так и персональных – содержится в файле *profiles.xml*.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<Profiles>
      <Common>
            <ProfileRef file="rulset1.xml"
            name="Профиль 1" active="yes/no"/>
            <ProfileRef file="rulset2.xml"
            name="Профиль 2" active="yes/no"/>
            ...
```

```
        </Common>
        <Personal>
              <ProfileRef file="rulset3.xml"
              name="Профиль 3" active="yes/no"/>
              <ProfileRef file="rulset4.xml"
              name="Профиль 4" active="yes/no"/>
              ...
        </Personal>
</Profiles>
```

Тег **Common** содержит список общих профилей, **Personal** – персональных.

Тег **ProfileRef** задает ссылку на файл из каталога **CONFSRC/profiles**, содержащий описание профиля:

file – имя файла с описанием профиля (без пути);

name – имя профиля, которое показывается программой веб-конфигуратор в списке профилей; совпадает с именем, содержащимся внутри файла с описанием профиля;

active – атрибут, определяющий, является ли данный профиль активным, значениями **yes** или **no**.

A.4.4. Набор списков e-mail адресов (*emails.xml*)

Набор существующих списков адресов e-mail содержится в файле *emails.xml*.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<EMailLists>
      <EMailListRef file="emaillist1.xml"
      name="Список 1"/>
      <EMailListRef file="emaillist2.xml"
      name="Список 2"/>
      ...
</EMailLists>
```

Тег **EMailListRef** задает ссылку на файл из каталога **CONFSRC/emails**, содержащий список адресов e-mail:

file – имя файла со списком (без пути);

name – имя списка; совпадает с именем, содержащимся внутри файла с описанием списка.

A.4.5. Набор списков IP-адресов (*iplists.xml*)

Набор существующих списков IP-адресов содержится в файле *iplists.xml*.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<IPLists>
      <IPListRef file="iplist1.xml" name="Список
      1"/>
      <IPListRef file="iplist2.xml" name="Список
      2"/>
      ...
</IPLists>
```

Тег **IPListRef** задает ссылку на файл из каталога **CONFSRC/iplists**, содержащий список IP-адресов:

file – имя файла со списком (без пути);

name – имя списка; совпадает с именем, содержащимся внутри файла с описанием списка.

A.4.6. Набор списков служб DNS-based RBL (*dnsblacklists.xml*)

Набор существующих списков служб DNS-based RBL содержится в файле *dnsblacklists.xml*.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<DNSBlackLists>
      <DNSBlackListRef file="rbllist1.xml"
      name="Список 1"/>
      <DNSBlackListRef file="rbllist2.xml"
      name="Список 2"/>
      ...
</DNSBlackLists>
```

Тег **DNSBlackListRef** задает ссылку на файл из каталога **CONFSRC/dnsblacklists**, содержащий список служб DNS-based RBL:

file – имя файла со списком (без пути);

name – имя списка; совпадает с именем, содержащимся внутри файла с описанием списка.

A.4.7. Профиль фильтрации

Файлы профилей фильтрации расположены в каталоге **CONFSRC/profiles**.

Файл *profiles.xml* содержит список таких файлов.

Профиль – это упорядоченный список правил фильтрации (Rule); порядок правил существен и задается пользователем при помощи программы веб-конфигуратор.

Каждое правило состоит из списка условий и списка действий; порядок условий внутри правила несущественен; порядок действий – фиксирован.

Список условий содержит не менее одного описания условия; условия описываются специальными тегами, которые могут повторяться по несколько раз. У каждого тега свой набор параметров.

Список действий содержит не менее одного описания действия; действия описываются специальными тегами, которые могут повторяться по несколько раз. У каждого тега свой набор параметров.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<Profile name = "имя профиля" type="common">
```

или

```
<Profile name = "имя профиля" type="personal"
rcpt="email">
```

или

```
<Profile name = "имя профиля" type="personal"
rcptlist="filename.xml">
      <Comment>
            текст комментария или описания,
            может быть многострочным
      </Comment>
      <Rule>
            <Conditions>
                  Описание условия 1
```

```
                    Описание условия 2
                    ...
                </Conditions>
                <Actions>
                    Описание действия 1
                    Описание действия 2
                    ...
                </Actions>
            </Rule>
            <Rule>
                ...
            </Rule>
            ...
        </Profile>
```

Тег **Profile** задает свойства профиля:

name – имя профиля;

type – атрибут, определяющий, является ли данный профиль общим или персональным, со значениями **common** или **personal**;

rcpt (возможен только в персональном профиле) – список получателей, для которых действует данный профиль; может быть задан в двух форматах:

user1@domain[, user2@domain[, user3@otherdomain] ...]

или

@domain (подразумевается любой пользователь указанного почтового домена)

rcptlist (возможен только в персональном профиле) – имя списка адресов e-mail (без пути); не может встречаться вместе с **rcpt**.

Тег **Comment** содержит многострочный произвольный комментарий; может быть пустым или отсутствовать; не может повторяться.

Тег **Rule** задает описание правила фильтрации; состоит из двух тегов: **Conditions** и **Actions**, каждый из которых не может повторяться.

Теги **Conditions** и **Actions** содержат произвольное количество описаний условий/действий, каждое из которых описывается одним из тегов, приведенных ниже.

В конфигурационном файле могут быть использованы следующие условия:

- IP-адрес, с которого пришло сообщение, равен указанному или входит в указанную подсеть:

```
<IPFrom mask="aaa.bbb.ccc.ddd" />
```

или

```
<IPFrom mask="aaa.bbb.ccc.ddd/nn" />
```

- IP-адрес, с которого пришло сообщение, входит в указанный список:

```
<IPFromList list="filename" />
  filename – имя файла (без пути) из каталога
  CONFSRC/iplists.
```

- IP-адрес, с которого пришло сообщение, занесен в черные списки типа DNS-based RBL; проверка осуществляется по указанному списку служб:

```
<IPFromDNSBlack list="filename" />
  filename – имя файла (без пути) из каталога
  CONFSRC/dnsblacklists.
```

- IP-адрес, с которого пришло сообщение, отсутствует в DNS:

```
<IPFromNotInDNS />
```

- E-mail отправителя равен указанному:

```
<SMTPFrom email="address" />
  address указывается в формате user@domain или @domain
```

- E-mail отправителя входит в указанный список:

```
<SMTPFromList list="filename" />
  filename – имя файла (без пути) из каталога
  CONFSRC/emails.
```

- E-mail получателя (одного из получателей, если их несколько) равен указанному:

```
<SMTPTo email="address" />
  address указывается в формате user@domain или @domain
```

- E-mail получателя (одного из получателей, если их несколько) входит в указанный список:

```
<SMTPToList list="filename" />
  filename – имя файла (без пути) из каталога
  CONFSRC/emails.
```

- Сообщение имеет указанный заголовок (например, *From*, *To* или *Keywords*):

```
<HasHeader header="name" />
```

- Указанный заголовок сообщения (например, *From*, *To* или *Keywords*) соответствует указанному шаблону (regular expression):

```
<HeaderMatch header="name" regexp = "reg_exp"/>
```

- Сообщение отнесено к указанной контентной категории:

```
<CategoryMatch category="name" />
```

category – полный путь к категории в рубрикаторе Базы контентной фильтрации (через */*)

- Общий размер письма (в байтах) превышает указанный предел:

```
<MsgSize limit="n" />
```

Любой из перечисленных выше тегов может иметь атрибут **negative="yes"**, который означает, что к данному условию надо применить логический оператор **NOT**.

Любой из перечисленных выше тегов может иметь атрибут **invalid="yes"**, который означает, что данное условие некорректно (обычно из-за нехватки параметров).

В конфигурационном файле могут быть использованы следующие действия:

1. **accept** – переслать сообщение адресату (адресатам) без изменения:

```
<DoAccept />
```

2. **reject** – "отказаться" принимать данное сообщение на уровне SMTP-chat:

```
<DoReject />
```

3. **black hole** – уничтожить сообщение (не пересылать дальше), не генерируя никаких уведомлений отправителю:

```
<DoBlackHole />
```

4. **skip** – прекратить выполнение всех правил текущего профиля фильтрации и перейти к выполнению следующего профиля:

```
<DoSkip />
```

5. **bounce** – послать уведомление отправителю об отказе принять данное письмо:

```
<DoBounce />
```

6. **change recipient** – изменить список получателей сообщения:

- удалить указанный адрес получателя (*delete*):

```
<DoRcptDelete email="e@mail" />
```

- добавить к списку получателей адрес (список адресов), указанный в правиле (*add*):

```
<DoRcptAdd new="e@mail;e@mail2" />
```

- заменить адреса всех получателей на адрес (список адресов), указанный в правиле (*replace all*):

```
<DoRcptReplaceAll new="e@mail;e@mail2"/>
```

При указании нового адреса может быть использована макропеременная **${SMTP_FROM}** – адрес отправителя, указанный в SMTP-envelope.

7. **change header** – дописать (изменить) указанный в правиле заголовок сообщения:

- удалить все заголовки с указанным именем, если они были у сообщения (*delete*):

```
<DoHeaderDelete header="name"/>
```

- удалить старое значение (если у сообщения уже был указанный заголовок), дописать новое, указанное в правиле (*replace*):

```
<DoHeaderReplace header="name" value = "новое
значение"/>
```

- оставить без изменения старое значение, дописав к нему новое значение, указанное в правиле (*add*):

```
<DoHeaderAdd header="name" value = "новое
значение"/>
```

- добавить новый заголовок с указанным именем и значением (*create*):

```
<DoHeaderNew header="name" value = "новое
значение"/>
```

При указании нового значения заголовка может быть использована макропеременная **${CATEGORY}** – список категорий спама, полученный при контентном анализе текста сообщения (например, этот список может быть записан в заголовок *Keywords*).

A.4.8. Список адресов e-mail

Файлы адресов e-mail расположены в каталоге **CONFSRC/emails**.

Файл *emails.xml* содержит список таких файлов.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<EMailList name = "имя списка" description = "краткое
описание">
       <EMail address = "..."/>
       <EMail address = "..."/>
       ...
<EMailList/>
```

Тег **EMailList** задает свойства списка:

name – имя списка;

description – произвольный комментарий (может отсутствовать или быть пустым).

Тег **EMail** задает адрес e-mail. Значение атрибута **address** может быть указано в двух форматах: **user@domain** или **@domain** (подразумевается любой пользователь указанного почтового домена).

A.4.9. Список IP-адресов

Файлы IP-адресов находятся в каталоге **CONFSRC/iplists**.

Файл *iplists.xml* содержит список таких файлов.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<IPList name = "имя списка" description = "краткое
описание">
       <IP mask="aaa.bbb.ccc.ddd/nn"/>
       <IP mask="aaa.bbb.ccc.ddd"/>
       ...
</IPList>
```

Тег **IPList** задает свойства списка:

name – имя списка;

description – произвольный комментарий (может отсутствовать или быть пустым).

Тег **IP** задает IP-адрес. Значение атрибута **mask** может быть указано в двух форматах: **aaa.bbb.ccc.ddd/nn** или **aaa.bbb.ccc.ddd** (равнозначно **aaa.bbb.ccc.ddd/32**).

A.4.10. Список служб DNS-based RBL

Файлы служб DNS-based RBL находятся в каталоге **CONFSRC/dnsblacklists**.

Файл *dnsblacklists.xml* содержит список таких файлов.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<DNSBlackList name = "имя списка" description =
"краткое описание">
      <Service zone = "..." description = "..."/>
      <Service zone = "..." description = "..."/>
      ...
<DNSBlackList/>
```

Тег **DNSBlackList** задает свойства списка:

name – имя списка;

description – произвольный комментарий (может отсутствовать или быть пустым).

Тег **Service** задает описание службы:

zone – название зоны;

description – произвольный комментарий (может отсутствовать или быть пустым).

A.4.11. Список пользовательских образцов спамерских писем (*samples.xml*)

Файл *samples.xml* содержит список пользовательских образцов спамерских писем и имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<Samples>
      <Sample file="filename.xml" catID="..."
      name="..." />
```

```
        ...
</Samples>
```

Атрибуты тега **Sample**:

file – имя файла с образцом (без пути), генерируется автоматически программой веб-конфигуратор при заведении нового образца;

catID – идентификатор категории (текстовая строка, состоящая из латинских букв, цифр, знаков "_" и "/"); должен соответствовать списку, имеющемуся в catlist.xml.

name – название образца; формируется автоматически программой веб-конфигуратор.

A.4.12. Пользовательский образец спамерского письма

Файлы такого типа находятся в каталоге **CONFSRC/samples**.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<Sample xmlns="http://www.ashmanov.com/cf/1.0/">
      <Subject>...</Subject>
      <Body>
      ...
      </Body>
</Sample>
```

A.4.13. Файл дополнительных настроек Фильтра (*settings.xml*)

Файл *settings.xml* содержит тексты сообщений, используемые Фильтром при выполнении действий **bounce** и **reject**.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<Settings>
      <BounceMessage>
      ....
      </BounceMessage>
      <RejectMessage text="текст сообщения"/>
</Settings>
```

А.4.14. Список предопределенных категорий (*catlist.xml*)

Конфигурационный файл *catlist.xml* находится в каталоге **/usr/local/ap-mailfilter/cfdata/mainset**. Он читается программой веб-конфигуратор, но не модифицируется.

Файл порождается специальной утилитой при изменении базового набора данных (поступления обновлений). При вводе образца письма пользователь выбирает категории из этого списка.

Конфигурационный файл имеет следующую структуру:

```
<?xml version="1.0" encoding="koi8-r"?>
<Categories>
      <Category ID = "CatLevel1/CatLevel2" title =
      "название категории" />
      <Category ID = "CatLevel1/CatLevel2/CatLevel3"
      title = "название категории" />
      ...
</Categories>
```

Атрибуты тега **Category**:

ID – идентификатор категории (текстовая строка, состоящая из латинских букв, цифр, знаков "**_**" и "**/**");

title – название категории.

А.5. Конфигурационный файл скрипта обновления

Параметры функционирования скрипта обновления Базы контентной фильтрации содержатся в конфигурационном файле */usr/local/ap-mailfilter/conf/src/updater.ini*. Файл содержит следующие параметры:

METHOD – источник обновления Базы контентной фильтрации. По умолчанию обновление осуществляется через интернет, что соответствует значению параметра **download**. Для обновления Базы из сетевого каталога присвойте параметру значение **copy**.

URL – адрес, с которого выполняется обновление Базы контентной фильтрации через интернет. По умолчанию **URL=ftp://downloads1.kaspersky-labs.com/sfupdates**. Значение

данного параметра используется только если **METHOD=download**. Иначе значение параметра ингорируется.

UPDATE_PATH – полный путь к сетевому каталогу, из которого выполняется обновление Базы контентной фильтрации, если **METHOD=copy**. По умолчанию данному параметру не присвоено значение, поскольку обновление Базы выполняется через интернет.

KAVUPDATER – полный путь к файлу *kavupdater*.

A.6. Ключи командной строки скрипта обновления

Запуск скрипта обновления из командной строки может быть выполнен следующей строкой:

./sfupdates [ключ]

где:

[ключ] – один из возможных ключей.

Вы можете использовать следующие ключи:

–q – не выводить на консоль никаких сообщений.

–v – вывести на консоль отладочные сообщения.

–V – не блокировать сообщения от kavupdater.

–f – запустить компилятор обновлений даже в случае отсутствия новых обновлений (если перекомпиляция не требуется, скрипт возвращает код ошибки).

ПРИЛОЖЕНИЕ В. ЗАО "ЛАБОРАТОРИЯ КАСПЕРСКОГО"

ЗАО "Лаборатория Касперского" была основана в 1997 г. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

"Лаборатория Касперского" – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

"Лаборатория Касперского" сегодня – это более двухсот пятидесяти высококвалифицированных специалистов, девять из которых имеют дипломы MBA, пятнадцать – степени кандидатов наук и двое являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг "Лаборатории Касперского". Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. "Лаборатория Касперского" первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского®, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, межсетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие западные разработчики используют в своих продуктах программное ядро Антивируса Касперского®, например, такие как: Nokia ICG (США), F-Secure (Финляндия), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты "Лаборатории Касперского" обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наша антивирусная база обновляется каждые три часа. Мы обеспечиваем наших пользователей круглосуточной технической поддержкой на нескольких языках.

B.1. Другие разработки "Лаборатории Касперского"

Антивирус Касперского® Personal

Антивирус Касперского® Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное ПО. Программа осуществляет постоянный контроль всех источников проникновения вирусов – электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

- **Постоянная защита компьютера** – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
- **Проверка компьютера по требованию** – проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

Антивирус Касперского® Personal теперь не проверяет повторно те объекты, которые были проанализированы во время предыдущей проверки и с тех пор не изменились, не только при постоянной защите, но и при проверке по требованию. Такая организация работы **заметно повышает скорость работы программы**.

Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского® Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах.

Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их

содержимого, а также удаление вредоносного кода из архивных файлов формата **ZIP**, **CAB**, **RAR**, **AFJ**.

Простота настройки программы осуществляется за счет возможности выбора одного из трех предопределенных уровней: **Максимальная защита**, **Рекомендуемая защита** и **Максимальная скорость**.

Обновления антивирусных баз осуществляется каждые три часа, при этом обеспечивается их гарантированная доставка при разрыве или смене соединений с интернетом.

Антивирус Касперского® Personal Pro

Пакет разработан специально для полномасштабной антивирусной защиты домашних компьютеров, работающих под управлением операционных систем Windows 98/ME, Windows 2000/NT, Windows XP с бизнес-приложениями из состава MS Office 2000. Антивирус Касперского® Personal Pro включает программу загрузки ежедневных обновлений антивирусной базы и программных модулей. Уникальная система эвристического анализа данных второго поколения эффективно нейтрализует неизвестные вирусы. Простой и удобный пользовательский интерфейс позволяет быстро менять настройки и делает работу с программой максимально комфортной.

Антивирус Касперского® Personal Pro обеспечивает:

- **антивирусную проверку по требованию пользователя** локальных дисков;
- **автоматическую проверку в масштабе реального времени** на присутствие вирусов всех используемых файлов;
- **почтовый фильтр**, осуществляющий проверку входящих и исходящих почтовых сообщений в фоновом режиме.
- **поведенческий блокиратор**, гарантирующий стопроцентную защиту от макро-вирусов.

Kaspersky® Anti-Hacker

Программа Kaspersky® Anti-Hacker представляет собой персональный межсетевой экран, обеспечивающий полномасштабную защиту компьютера, работающего под управлением операционной системы Windows, от несанкционированного доступа к данным, а также от сетевых хакерских атак из локальной сети и интернета.

Kaspersky® Anti-Hacker отслеживает сетевую активность по протоколу TCP/IP для всех приложений на вашем компьютере. При обнаружении подозрительных действий какого-либо приложения программа информирует вас об этом, и, при необходимости, блокирует сетевой доступ этому приложению. В результате обеспечивается конфиденциальность информации, находящейся на вашем компьютере.

Благодаря технологии SmartStealth™ значительно затрудняется обнаружение компьютера извне: режим невидимости вашего компьютера обеспечивает защиту от хакерских атак, не оказывая никакого негативного влияния на вашу работу в интернете. Программа обеспечивает стандартную прозрачность и доступность информации.

Kaspersky® Anti-Hacker также блокирует наиболее распространенные сетевые хакерские атаки, отслеживает попытки сканирования портов.

Программа поддерживает упрощенное администрирование по пяти режимам безопасности. По умолчанию используется режим самообучения, который позволяет настроить систему безопасности в зависимости от вашей реакции на различные события. Данный режим позволяет сконфигурировать межсетевой экран под конкретного пользователя и конкретный компьютер.

Kaspersky® Security для PDA

Kaspersky® Security для PDA обеспечивает надежную антивирусную защиту данных, хранимых на КПК, работающих под управлением Palm OS или Windows CE, а также информации, переносимой с PC или любой карты расширения, ROM файлы и базы данных, В состав программы входит оптимальный набор средств антивирусной защиты:

- **антивирусный сканер**, обеспечивающий проверку информации (хранимой как на PDA, так и на картах расширения любого типа) по требованию пользователя;
- **антивирусный монитор**, осуществляющий перехват вирусных программ, передаваемых в процессе синхронизации с использованием технологии HotSync™ или с другими КПК.

Программа также обеспечивает защиту данных, хранящихся на карманном компьютере, от несанкционированного доступа путем шифрования доступа к самому устройству и ко всей информации, хранящейся на портативном компьютере и картах расширения.

Антивирус Касперского® Business Optimal

Программный комплекс представляет собой уникальное конфигурируемое решение антивирусной защиты для предприятий малого и среднего бизнеса.

Антивирус Касперского® Business Optimal обеспечивает полномасштабную антивирусную защиту[8]:

[8] В зависимости от типа поставки

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD и OpenBSD, Linux.
- *почтовых систем* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; MS ISA Server.

Антивирус Касперского® Business Optimal также включает систему централизованной установки и управления – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

Kaspersky® Corporate Suite

Kaspersky® Corporate Suite – это интегрированная система, обеспечивающая информационную безопасность вашей корпоративной сети независимо от ее сложности и размера. Программные компоненты, входящие в состав комплекса, предназначены для защиты всех узлов сети компании. Они совместимы с большинством используемых сегодня операционных систем и программных приложений, объединены системой централизованного управления и обладают единым пользовательским интерфейсом. Программный комплекс обеспечивает создание системы защиты, полностью совместимой с системными требованиями вашей сети.

Kaspersky® Corporate Suite обеспечивает полномасштабную антивирусную защиту:

- *рабочих станций* под управлением Windows 98/Me, Windows 2000/NT/XP Workstation и Linux.
- *файловых серверов* под управлением Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD и Linux.
- *почтовых систем* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim и Qmail.
- *интернет-шлюзов*: CheckPoint Firewall –1; MS ISA Server.
- *карманных компьютеров*, работающих под управлением Windows CE и Palm OS.

Kaspersky® Corporate Suite также включает *систему централизованной установки и управления* – Kaspersky® Administration Kit.

Вы можете самостоятельно выбрать антивирусные программы в соответствии с используемыми операционными системами и приложениями.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal предназначен для защиты пользователей почтовых клиентов Microsoft Outlook и Microsoft Outlook Express от нежелательных писем (спама).

Программный пакет Kaspersky Anti-Spam Personal представляет собой мощный инструмент для обнаружения спама в потоке входящей электронной почты, поступающей по протоколам POP3 и IMAP4 (только для Microsoft Outlook).

Во время фильтрации проверяются все возможные атрибуты письма: адреса отправителя и получателя, его заголовки. Также используется *контентная фильтрация*, то есть анализируется содержание самого письма (включая заголовок *Subject*) и файлов вложений. Применяются уникальные лингвистические и эвристические алгоритмы.

Высокая эффективность работы программы достигается благодаря ежедневному автоматическому обновлению базы контентной фильтрации образцами, предоставляемыми специалистами лингвистической лаборатории.

B.2. Наши координаты

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО "Лаборатория Касперского". Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Адрес:	Россия, 125363, Москва, ул. Героев Панфиловцев, 10	
Факс:	+7 (095) 797-8700	
Экстренная круглосуточная помощь	+7 (095) 797-8707 support@kaspersky.com	
Поддержка пользователей Business Optimal	+7 (095) 363-4205 (с 10 до 19 часов)	smb-support@kaspersky.com

Поддержка пользователей Corporate Suite	Телефоны и электронный адрес предоставляются при покупке Corporate Suite.	
Антивирусная лаборатория	newvirus@kaspersky.com (только для отправки новых вирусов в архивированном виде)	
Департамент продаж	+7 (095) 797-8700	sales@kaspersky.com
Департамент маркетинговых коммуникаций	+7 (095) 797-8700	info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.com	

ПРИЛОЖЕНИЕ С. ЗАО "АШМАНОВ И ПАРТНЕРЫ "

Технология фильтрации почтовых сообщений, лежащая в основе Спам-фильтра, разработана компанией "Ашманов и Партнеры".

ЗАО "Ашманов и Партнеры" – один из ведущих российских разработчиков систем семантического анализа и автоматического рубрицирования текстов, других технологий искусственного интеллекта.

Среди других направлений деятельности компании "Ашманов и Партнеры" – разработка полнотекстовых поисковых систем, лингвистических и информационных систем. Компания ведет также заказные разработки программного обеспечения, технически сложных интернет-проектов.

Подробнее о компании "Ашманов и Партнеры", направлениях ее деятельности и оказываемых услугах можно узнать на сайте компании: www.ashmanov.com

Компания "Ашманов и Партнеры" будет благодарна всем, кто сможет пересылать нам образцы нежелательной электронной корреспонденции – особенно те, которые Фильтр по той или иной причине "пропускает". Вместе мы сможем сделать защиту от спама еще более эффективной.

E-mail для посылки образцов спамерской корреспонденции: newspam@ashmanov.com

E-mail для отзывов и пожеланий, писем по вопросам сотрудничества: info@ashmanov.com

ПРИЛОЖЕНИЕ D. УКАЗАТЕЛЬ