Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 100

КОРПОРАТИВНЫЕ СИСТЕМЫ

«Дозор-Джет»: эффективность и безопасность использования электронной почты

Электронная почта на предприятии

Александр Таранов
Владимир Цишевский

СОДЕРЖАНИЕ

1. Введение. Электронная почта как корпоративный инструмент

Еще лет 10 назад электронная почта была довольно экзотичным средством связи. Использовали ее в основном для связи с зарубежными корреспондентами, а умение пользоваться ею представлялось непосвященным техническим волшебством среднего калибра.

Сегодня электронная почта стала обычным атрибутом офиса и используется всеми, от специалистов ИТ-подразделений до руководителей разных рангов.

Говоря об электронной почте, нельзя не упомянуть о том, что она является одним из главных коммуникационных средств, образующих инфраструктуру электронной коммерции. Именно электронная коммерция в значительной мере объясняет быстрый рост почтовых потоков и числа пользователей электронной почты. К сожалению, мы не обладаем статистикой использования электронной почты в России, и приведенные ниже данные относятся к США, однако, они все же дают некоторое представление о перспективах электронной почты в коммерческой жизни нашей страны.

Итак, по данным IDC число почтовых ящиков, обслуживающих бизнес, будет увеличиваться на 13.5% ежегодно и достигнет в 2003 г. 166 миллионов. В то же время число почтовых ящиков «потребителей» будет расти на 10% в год и в 2003 году достигнет 121 миллиона. При таких темпах роста почтовых ящиков в США скоро будет больше, чем телефонных номеров.

Одновременно с увеличением числа почтовых ящиков ожидается и рост количества пересылаемых писем, причем все большую долю среди них будут составлять «коммерческие» письма. Однако, было бы неправильно думать, что относительное увеличение доли таких писем означает уменьшение доли так называемого «спама», и не только потому, что предложения заработать 1 миллион долларов в неделю не прекратятся никогда, но и потому, что «полезность» информации решающим образом может зависеть от ее адресата. То, что одному представляется как раздражающий информационный шум, для другого может быть действительно важным.

У электронной почты есть все для того, чтобы обеспечить ей положение самого популярного средства коммуникации: дешевизна, удобство и простота использования, большая база пользователей (как, у вас нет адреса электронной почты!?). По ряду параметров она удобнее телефона и факса. По телефону мы можем не дозвониться, телефонный разговор не оставляет вещественных следов, «копию разговора» невозможно послать третьей стороне. Не все вопросы можно обсуждать вслух в людном офисе, в то время как писать можно и молча. Да и отправка, например, 10-страничного факса не в пример более хлопотное занятие, чем присоединение 40-килобайтного файла к электронному письму.

Электронная почта стала массовым средством общения. Однако, поскольку освоение этого нового средства коммуникации происходило стихийно, стихийно складывались и модели использования электронной почты в организациях.

1.1. Электронная почта

Если попытаться классифицировать все модели использования электронной почты по степени ее «заорганизованности», то на одном полюсе окажется *анархическая*, а на другом — *одномашинная* модель.

Анархическая модель открывает доступ к электронной почте всем желающим и в любых целях: деловых, личных, развлекательных, хулиганских. С одной стороны, она максимально стимулирует приобщение к технологии широких масс, с другой, предельно затрудняет организацию труда, при которой электронная переписка может трактоваться как деловая. Причин этого несколько:

Неформальный статус электронных писем. Отсутствие корпоративного стандарта на электронную цифровую подпись (ЭЦП) не позволяет трактовать электронное письмо как полноценный документ.

Отсутствие центра управления. Упомянутый неформальный статус писем не всегда необходим. Многие документы не могут иметь юридической силы просто по природе своей (черновики, предназначенные для согласования и доработки, служебные записки, распоряжения и т.п), но, тем не менее, должны циркулировать в соответствии с установленными в организации *правилами*, также должны быть обеспечены их учет, хранение, быстрый поиск и т.п.

Проблема конфиденциальности. Бесконтрольное использование электронной почты не только повышает вероятность нежелательной утечки информации, но и существенно затрудняет своевременное обнаружение утечки после того, как она произошла.

Компьютерные вирусы. Без сомнения, *анархическая* модель как нельзя больше подходит для их получения и распространения.

Неделовой трафик. Не секрет, что использование сотрудниками электронной почты организаций в неделовых целях — распространенное явление. Благодаря прогрессу компьютерных технологий в области multimedia в сотни раз возрос средний объем электронного письма. Если раньше оно

представляло собой небольшой текст, автором которого являлся сам его отправитель, то сегодня ничего не стоит получить по электронной почте и разослать друзьям небольшой видеофильм, объем которого может быть сопоставим с годовым объемом деловой переписки всей организации. Поэтому кроме очевидного отвлечения сотрудников от исполнения служебных обязанностей это явление может представлять серьезную угрозу доступности услуги электронной почты как таковой.

Другой крайний случай использования электронной почты — это *одномашинная* модель, когда почту можно отправлять с одной единственной машины, получать — тоже на нее. Весь процесс полностью контролируется выделенным сотрудником — оператором электронной почты. Как правило, имеется более или менее проработанный регламент, определяющий что, кому и как можно посылать (получать).

Исторические корни «одномашинной почты» лежат в скудости материальных ресурсов, она напоминает о времени, когда не у всех пользователей почты были компьютеры, не говоря уже о подключении к Интернет. Тем не менее, различные варианты *одномашинной* модели живы и по сей день, причем далеко не в самых бедных организациях. Причина этого в том, что такая модель (либо ее технически более развитые разновидности) позволяет обеспечить безопасное функционирование и эффективное использование электронной почты, поскольку предоставляет:

Формальный статус электронных писем. Отправленные и полученные письма могут регистрироваться и архивироваться.

Центр управления. Оператор электронной почты является единой точкой входа для всей электронной почты.

Контроль над распространением почтовых вирусов. Во-первых, в обязанности оператора может входить вирус-контроль почты, а, во-вторых, в худшем случае заражается только компьютер оператора.

Недопущение неделового трафика. Это, с одной стороны, есть следствие затрудненности пользования почтой, с другой — следствие наличия регистрации писем.

По-видимому, нет нужды говорить о том, что данная модель организации работы электронной почты обладает существенным недостатком: электронная почта перестает быть простым и доступным инструментом, а то, что сложно — мало используется.

Для эффективного использования электронной почты внутри организации необходима компромиссная модель, сочетающая положительные качества обеих описанных выше моделей.

1.2. Управление – ключ к эффективности

Утверждение, вынесенное в заголовок этого раздела, безусловно справедливо и в то же время тривиально. Чтобы наполнить этот тезис конкретным содержанием, сформулируем, чем именно мы собираемся управлять, применительно к электронной почте.

Управление на системо-техническом уровне. Это локальные сети, почтовые серверы, серверы каталогов и т.п. В рамках этой статьи мы не будем рассматривать соответствующие средства и методы управления, заметим только, что без этого вида управления говорить об эффективном использовании любого сервиса бессмысленно.

Управление пользователями. Электронная почта — это массовый сервис, она наиболее полезна, когда охватывает всех сотрудников организации. Отсюда необходимость «управления пользователями»: их регистрация, создание адресных книг, списков рассылки и т.п. Адекватные средства управления пользователями присутствуют в реализации большинства почтовых серверов, поэтому в этой статье не рассматриваются.

Борьба с компьютерными вирусами. Электронная почта является источником потенциальной опасности заражения вирусами[1].

Обеспечение конфиденциальности. Наряду с защитой от вирусов одной из наиболее важных задач является пресечение утечки из организации конфиденциальной информации. Заметим, что для решения этой задачи необходимо иметь техническую возможность анализировать структуру и содержимое электронных писем и гибко и оперативно реагировать на наличие «подозрительного» содержимого.

Управление информационными потоками. С точки зрения повышения эффективности использования корпоративной электронной почты, задачи управления включают ограничение неделового трафика, обеспечение доступности информации, а также контроль процессов, инициированных электронной перепиской.

Все это можно объединить под общим названием *информационное управление*. Такое управление позволяет, с одной стороны, существенно повысить безопасность использования информационного сервиса, с другой — увеличить его бизнес-эффективность.

[1] На рынке имеется ряд продуктов (почтовые сканеры), которые решают задачу обнаружения и последующей обработки подозрительных писем. Реальные функции продуктов этого класса несколько шире, чем просто обнаружение вирусов, и в ограниченных объемах почтовые сканеры позволяют реализовать корпоративную политику использования электронной почты, то есть управлять электронной почтой на информационном уровне, однако, в силу своей первоначальной направленности исключительно на борьбу с вирусами, возможности их в этой сфере обычно ограничены.

Необходимо отметить, что задача информационного управления электронной почтой не может быть решена только техническими средствами, которые играют здесь скорее вспомогательную роль. Другими словами, технические средства являются именно *средствами* реализации определенной *политики использования* электронной почты. Естественно, что технические средства управления и реализации политики необходимы, и, следовательно, они присутствуют на рынке. Сюда относятся антивирусные системы, системы фильтрации почты, направленные на отсечение нежелательной неделовой корреспонденции (так называемого «спама»), системы контекстного контроля содержимого писем и т.п. Подавляющее большинство этих систем нацелено на какие-то частные аспекты того, что выше было названо информационным управлением. Особенностью системы «Дозор-Джет» является комплексный подход к *реализации политики использования электронной почты.*

2. «Дозор-Джет»: средство реализации политики

2.1. Что это

В данном разделе мы попытаемся дать наиболее точное определение, что представляет собой «Дозор-Джет» с потребительской точки зрения. Принципы работы системы «Дозор-Джет» и ее устройство описываются далее в Разд. 2.2 и Разд. 2.3. Итак, прежде всего, «Дозор-Джет» это:

Средство реализации корпоративной политики использования электронной почты. Электронная почта является одним из наименее защищенных ресурсов корпоративной ИС. Неконтролируемость использования электронной почты сотрудниками предприятия влечет за собой утечку конфиденциальной информации, потерю рабочего времени из-за использования сотрудниками корпоративной почты в личных целях, перегрузку каналов передачи информации, распространение компьютерных вирусов и утрату информации. Для решения этих проблем необходимо использовать комплекс организационно-технических методов и средств. К организационным методам относится политика (свод *правил*) использования электронной почты. Технические методы включают контроль содержимого писем и ведения архива переписки по электронной почте.

Средство мониторинга почтовых сообщений. Система «Дозор-Джет» осуществляет мониторинг всех входящих, исходящих и внутренних почтовых сообщений, передаваемых посредством протокола SMTP. При попадании почтового сообщения в систему производится полный разбор письма и анализ структуры и содержания как самого сообщения, так и присоединенных файлов. Анализ содержания заключается в проверке текста сообщения и присоединенных файлов на наличие слов, запрещенных к использованию в почтовых сообщениях. Для повышения эффективности анализа содержания применяется механизм регулярных выражений. «Дозор-Джет» обладает мощной системой фильтрации сообщений, основанной на *правилах*, каждое из которых состоит из набора *условий* и *действий*, выполняемых системой при соблюдении или не соблюдении этих *условий*.

Средство реагирования на нарушения политики. Система «Дозор-Джет» автоматически реагирует на нарушение политики использования электронной почты и обладает гибкими механизмами реагирования. При соблюдении (или не соблюдении) определенного *условия* система выполняет *действие* или последовательность *действий*, установленную соответствующим *правилом* политики. Основными *действиями* являются разрешение или запрет прохождения письма, а также посылка уведомления.

Архив почтовых сообщений. Система «Дозор-Джет» осуществляет как долговременное, так и краткосрочное хранение в архиве почтовых сообщений, удовлетворяющих определенным *условиям*. Обычно архив используется для хранения задержанных по каким-то причинам писем. Существует возможность быстрого поиска писем в архиве по любым атрибутам сообщений и создания запросов любой логической сложности.

Мы только что определили «Дозор-Джет» как средство реализации корпоративной политики использования электронной почты и далее расскажем, какие механизмы предоставляет администратору безопасности система «Дозор-Джет» для реализации этой политики.

2.2. Как это устроено

С точки зрения *системного администратора*, «Дозор-Джет» осуществляет мониторинг всех входящих, исходящих и внутренних почтовых сообщений, передаваемых посредством протокола SMTP.

Использование «Дозор-Джет» не устраняет необходимости использования обычного почтового сервера, однако, система предусматривает различные режимы его подключения, а именно: архивирующий и фильтрующий.

2.2.1. Архивирующий режим

Архивирующая модель может быть также названа «параллельной» и подразумевает, что весь почтовый поток организации должен быть каким-то образом продублирован (чаще всего это может быть сделано при помощи самого почтового сервера). Основной поток почты доставляется получателям как и прежде. Дополнительный поток направ-

ляется в «Дозор-Джет», где используется для анализа и архивирования.

Преимущество архивирующего режима заключается в том, что никакие сбои в работе «Дозор-Джет» не могут нарушить нормального хода доставки почты. Недостатки — в том, что возможности «Дозор-Джет» по реагированию на ситуации нарушения компьютерной безопасности оказываются весьма ограниченными. Нарушения компьютерной безопасности можно обнаружить, но нельзя предотвратить. Например, система может зафиксировать нарушение режима секретности и уведомить администратора безопасности, однако, она не может предотвратить саму утечку информации.

2.2.2. Фильтрующий режим

Фильтрующая модель подключения «Дозор-Джет» позволяет использовать весь спектр его возможностей. В этой модели «Дозор-Джет» и обычный почтовый сервер соединяются «последовательно». «Дозор-Джет» является единственным получателем корпоративной почты. На основании заданных администратором *правил* почта может быть доставлена или задержана, и если было принято решение о доставке почты, то она доставляется при помощи обычного почтового сервера. Одновременно с фильтрацией такой метод установки позволяет архивировать почтовый трафик.

Недостатком такого способа включения является то, что доставка почты адресатам зависит от надежности работы двух систем, а не одной, как в архивирующей модели.

2.3. Как это работает

С технической точки зрения политика выглядит как набор *правил*, определяющих, как следует действовать в зависимости от поступления (отправки) тех или иных писем. Ключевыми словами в этой фразе являются **`тех или иных`** и **`действовать`**. Таким образом, *правила* состоят из критериев выбора писем и возможных действий, инициированных выполнением этих критериев.

Ясно, что политика состоит из достаточно большого количества *правил* (и исключений из них). Поэтому важным моментом является возможность организации этих *правил* в ту или иную структуру. Кроме того, наличие исключений (которые по сути дела тоже являются правилами, однако, имеют более частный характер) заставляет задуматься о том, в каком порядке применяются правила и как выполнение одних *правил* может повлиять на выполнение других.

Далее в этом разделе будет рассказано о том, какие возможности предоставляет «Дозор-Джет» для построения *правил*, объединения их в удобные структуры и организации их взаимодействия.

2.3.1. Правило = условие + действие

Под корпоративной политикой мы понимаем определенный набор *правил*. *Правило* состоит из *условий* и *действий*. *Условия* определяют признаки возникновения определенной ситуации, а *действия* — ответную реакцию.

Непосредственно на основе использования *правил*, *условий* и *действий* основана работа «Дозор-Джет». Каждое попадающее в систему электронное письмо подвергается проверке на соответствие заданным *условиям*. В случае обнаружения соответствия какому-то *условию* выполняется соответствующее *действие*. Простейшими примерами *условий* могут быть определение направления письма (входящее, выходящее, внутреннее); обнаружение в тексте письма слова из списка слов, запрещенных к употреблению, или компьютерного вируса. В качестве примеров *действий* можно упомянуть доставку письма получателю, помещение письма в архив или отправление извещения.

Говоря о безопасности и эффективности электронной почты, надо заметить, что не все мыслимые правила могут контролироваться компьютерной системой автоматически, причем необходимость человеческого вмешательства может возникать достаточно часто, и тогда весьма полезными могут оказаться предоставляемые системой «Дозор-Джет» возможности архивирования писем и последующего анализа содержимого архива .

То же относится и к *действиям*. Некоторые из них могут быть выполнены автоматически (например, не пропускать внутрь почты заведомо рекламного характера), другие же требуют внимания администратора безопасности, и, при необходимости, принятия соответствующих мер нетехнического характера (например, при обнаружении писем, содержащих предположительно конфиденциальную информацию).

Поэтому помимо компьютеров и программ, корпоративной политике требуются методологическая основа и организационная поддержка. Именно человек разрабатывает политику, несет за нее ответственность и следит за ее соблюдением. Как и любой другой программный продукт, «Дозор-Джет» не заменяет человека, а является лишь инструментом в его руках.

Однако, завершим лирическое отступление и вернемся к программам. С технической точки зрения способность системы реализовывать политику безопасности в значительной мере зависит от:

- полноты системы *условий*;
- достаточности системы *действий*;
- возможностей комбинировать *условия* (и *действия*).

Условиям, *действиям* и их комбинациям посвящаются следующие разделы этой статьи.

2.3.2. Условия

Итак, какие *условия* нам нужны и как они реализованы в системе «Дозор-Джет».

Типичным примером правил, реализующих определенную политику, являются различного рода запрещения и исключения из них. Часто при этом требуется принять единственное решение: доставлять ли письмо адресату или не доставлять. А вот *условия* для принятия этого решения могут быть разнообразными, замысловатыми и представлять определенные трудности при реализации алгоритмов проверки.

Например, вполне разумным выглядит желание запретить работникам бухгалтерии получать в письмах вложения, являющиеся исполнимыми файлами. Или *правило*, запрещающее сотрудникам в текстах писем и вложенных файлах использовать определенные слова или их комбинации (в свое время автор этих строк был ознакомлен с приказом, запрещающим в междугородних телефонных разговорах пользоваться словами «имитатор цели»).

Даже на примере этих простых *правил* можно увидеть проблемы, которые возникают при их реализации. Во-первых, электронное письмо представляет собой довольно сложную структуру и мы должны обнаруживать нежелательные вложения, как бы глубоко они не были «спрятаны». Последнее слово взято в кавычки, поскольку часто речь идет не о сознательной попытке спрятать что-то в письме, а о тех довольно распространенных ситуациях, когда тот же самый исполнимый модуль сначала для экономии места сжат каким-либо архиватором, затем присоединен к письму, которое было, в свою очередь, несколько раз переадресовано разным людям. Во-вторых, слова и фразы из «черного списка» могут содержаться не только непосредственно в теле письма, но и в присоединенных файлах, которые могут иметь разные форматы, кодировки и т.д. В третьих, группы пользователей (в нашем примере сотрудники бухгалтерии) вовсе не обязательно могут быть оформлены как специальные групповые адреса.

Кроме того, такие простые *правила* в реальной жизни могут усложняться. Например, можно представить себе ситуацию, что один из контрагентов организации присылает информацию в виде саморазворачивающихся архивов, а это именно *исполнимые* файлы. Таким образом, наше *правило* нужно будет дополнить исключением, которое гласит, что допустимы исполняемые файлы, принимаемые с определенного адреса. Можно пойти дальше и ограничить число пользователей, в адрес которых допустимо посылать самороазворачивающиеся архивы.

Итак, чтобы в соответствии с нашим простейшим регламентом «правильные» письма доставлялись по назначению, а «неправильные» задерживались «до выяснения», необходимо иметь достаточное представление о структуре электронного письма. Тексты соответствующих стандартов ([1], [2], [3], [4], [5], [6]) занимают не одну сотню страниц, то, что относится непосредственно к работе «Дозор-Джет», кратко изложено в Приложениях С, здесь же отметим, что *условия* отбора писем должны по меньшей мере включать в себя следующее:

- *условия* на почтовые заголовки;
- *условия* на структуру письма (наличие, число и структура вложений);
- *условия* на типы вложений (MSOffice, исполнимые, архивы и т.п.);
- *условия* на содержимое (текст) писем и вложений;
- *условия* на результат обработки письма.

Условия, упомянутые в последнем пункте, не связаны напрямую со структурой почтового сообщения и требуют пояснений. Предположим, требуется анализировать содержимое вложений, содержащих файловые архивы. Предположим также, что среди таких вложений находится архив, который был зашифрован, ключ неизвестен и, следовательно, полный анализ такого письма невозможен. Таким образом, чтобы система *условий* была полной, необходимо иметь возможность анализировать также и результаты разбора почтовых сообщений.

Отметим подробнее некоторые особенности реализации системы *условий* в «Дозор-Джет»:

- *Условия* могут быть составными, т.е. комбинироваться из простых с помощью логических связок И/ИЛИ.
- *Условия* на текстовые поля (и на содержимое письма) могут быть заданы не только с помощью стандартных строковых операторов («начинается с», «содержит», «оканчивается на»), но и с помощью так называемых «регулярных выражений».
- *Условия* на русский текст корректно проверяются независимо от того, в какой из пяти кодировок кириллицы этот текст написан (koi8, win-1251, ISO-8859-5, MAC, DOS). Причем, если кодировка текста не указана в письме явно, она определяется эмпирически.
- При работе с вложенными файлами возможен анализ имен файлов, их декларированных типов (`mime-type`) и их реальных типов, определяемых путем анализа содержимого файла. Последнее существенно, т.к. зачастую почтовые агенты, при помощи которых файл был прикреплен к письму, определяют его реальный формат весьма приблизительно.
- Имеется возможность определения наличия в письмах слов из заданного списка, причем автоматически осуществляется поиск всех словоформ (договор, договоры, договорной ...).

2.3.3. Действия

Вторая составляющая *правила* — это *действия*. В отличие от *условий*, которые могут быть самы-

ми разными и число которых неограниченно, набор возможных *действий* задан системой, а именно:

- доставить письмо адресату;
- пометить письмо;
- послать уведомление;
- зарегистрировать письмо;
- поместить письмо в архив;
- запустить другую цепочку *действий*.

Отметим, что *действия* не являются взаимоисключающими. Одно и то же письмо одновременно можно доставить адресату, пометить, поместить в архив, послать кому-то уведомление о том, что такое письмо имело место, и после всего этого, тем не менее, передать его на обработку в новую цепочку *правил*.

Рассмотрим *действия* каждого вида более подробно.

Доставка письма адресату. Это *действие* не нуждается в особых пояснениях. Отметим лишь, что технически «Дозор-Джет» не выполняет эту операцию сам, а использует какой-либо готовый почтовый сервер.

Установка меток. Письмо снабжается специальной меткой, характеризующейся типом, комментарием и временем постановки. Метка не изменяет письмо и адресат ее не увидит. Смысл метки в том, что, во-первых, наличие ее может повлиять на дальнейшую логику обработки письма, во-вторых, метка попадает вместе с письмом в архив и может быть использована при создании определенных выборок писем.

Посылка уведомления. Уведомления представляют собой электронные письма, сформированные на основании информации исходного письма. Уведомления создаются с помощью шаблонов и могут включать сведения об исходном письме. Среди этих сведений автор и адресат письма, тема письма и многое другое. Адресат уведомления может быть произвольным (в том числе им может быть и автор исходного письма). Имеется также возможность присоединить к уведомлению оригинал письма.

Регистрация письма. «Дозор-Джет» предоставляет возможность регистрации и архивации электронных писем. Регистрация означает сохранение в базе данных информации об определенных заголовках электронного письма (автор, адресат, размер и т.п.) и его **MIME** структуре (см. Прил. С).

Помещение письма в архив. Архивация письма означает, что помимо регистрации письмо помещается в базу данных.

Особенностью архивации писем в «Дозор-Джет» является то, что письмо помещается в базу в исходном состоянии, т.е. перед помещением в архив с письмом не производится никаких преобразований. Например, если письмо было подписано и зашифровано, оно помещается в архив до снятия подписи, несмотря на то, что без выполнения этой операции прочитать его невозможно. Такое решение позволяет при возникновении каких-либо спорных ситуации в любой момент предъявить оригинал письма.

Возникает вопрос, почему не архивировать все письма, которые необходимо. Ответов может быть несколько. Во-первых, некоторые письма могут содержать конфиденциальную информацию, и постоянное их хранение требует обеспечения повышенных требований к защите базы данных. Во-вторых, объем содержимого писем обычно многократно превышает объем регистрационной информации, и хранение писем целиком может потребовать существенного увеличения объема базы данных.

Запуск другой цепочки правил. В Разд. 2.3.5, посвященном технической реализации политики мы увидим, что все *правила* в «Дозор-Джет» группируются в цепочки. Возможность передать на обработку в другую цепочку *правил* при выполнении определенного *условия* позволяет сгруппировать *правила* по определенным признакам и тем самым снабжает их структурой.

2.3.4. Особенность реализации условий и действий

В системе «Дозор-Джет» существует два отдельных реестра: один для *условий*, другой для *действий*. Встроенный редактор позволяет как вести реестр *условий*, так и связывать *условия* из первого реестра с *действиями* из второго, образуя, таким образом, новые *правила*.

Такое раздельное существование *условий* и *действий* обеспечивает максимальную гибкость при составлении как *правил*, так и политики в целом. Библиотека типовых *условий* и *правил* (включающая, например, *правила*, отделяющие внутреннюю, входящую и исходящую почту) может быть заготовлена заранее и поставляться вместе с системой.

Кроме того, такая организация облегчает создание и отладку *правил*. Во-первых, можно сначала задаться вопросом: «Какие письма мы хотим выделять из общего потока?» и создать набор соответствующих *условий*. На следующем этапе мы можем сопоставить с этими *условиями* «безобидные», отладочные *действия* (например, постановку метки), чтобы убедиться в том, что *условия* выделяют именно то, что мы имели в виду. После этого можно привязать к *правилам* настоящие *действия*.

2.3.5. Политика = последовательность выполнения правил

Выше мы определили политику использования электронной почты как набор *правил*. При этом мы не упоминали о последовательности обработки этих *правил*.

Все *правила* в политике организованы в именованные цепочки. Одна цепочка является стартовой, а обработка письма начинается с первого *правила* этой цепочки.

По результатам проверки *условия* каждого *правила* могут быть выполнены три различных операции:

- завершение обработки письма;
- переход к выполнению следующего *правила* цепочки;
- передача управления другой *цепочке правил*.

2.3.5.1. Последовательное выполнение

Последовательное выполнение *цепочки правил* является наиболее естественным и простым способом обработки писем. Примером может быть политика, при которой доставлять можно лишь письма, удовлетворяющие одному из *условий*, а все остальные необходимо помещать в архив «до выяснения» или просто выбрасывать. Для реализации такой политики может быть использована цепочка, каждое *правило* в которой содержит *условие* доставки, а *действием* является сама доставка письма адресату. Проверки прекращаются при выполнении любого из *условий*. Письма, не удовлетворившие ни одному из *условий*, если необходимо, помещаются в архив *действием* последнего *правила*, *условие* которого выполняется всегда.

Такая простая последовательность может быть неудобна по нескольким причинам:

- Затрудняет реализацию сложной логики обработки.
- Чрезвычайно чувствительна к вносимым изменениям. Внося новое или изменяя существующее *правило*, мы скорее всего меняем всю логику работы, заданную правилами, стоящими «позже» измененного/внесенного.
- Неудобна в управлении, т.к. не поддается разделению на независимые сегменты.

2.3.5.2. Передача управления

В пределах одной цепочки *правил* проверка *условий* осуществляется последовательно. Обычно обработка кончается сразу, как только «сработает» любое *правило* цепочки. Однако, при формировании цепочки можно указать, что обработку следует продолжить независимо от того, сработало ли данное *правило*, позволяя таким образом выполниться более чем одному *правилу* для одного и того же письма.

Кроме этого, письмо может быть передано на обработку в другую цепочку *правил*. Таким образом, *цепочки правил* можно компоновать в иерархическую структуру. К примеру, типичной является ситуация, когда необходимо по-разному обрабатывать входящий, исходящий и внутренний потоки электронной корреспонденции. Наиболее просто это может быть реализовано следующей *цепочкой правил*:

Условие: Адресат письма вне организации

Действие: Передать письмо на обработку в *цепочку правил* «Исходящие», завершить работу

Условие: Автор письма вне организации

Действие: Передать письмо на обработку в *цепочку правил* «Входящие», завершить работу

Условие: Отсутствует (т.е. правило «срабатывает» всегда)

Действие: Передать письмо на обработку в *цепочку правил* «Внутренняя переписка»

В свою очередь, *цепочки правил*, определяющие обработку внутренней, исходящей и входящей почты, конструируются и отлаживаются отдельно, и, возможно, разными людьми.

2.3.5.3. Признак продолжения обработки

При образовании *правила* возможно указать, будет ли продолжена обработка письма после того, как это правило сработало. Обычно обработка прекращается, однако, при построении нетривиальной политики бывает удобно использовать *правила*, позволяющие продолжение обработки. Например, если мы хотим, чтобы письмо всегда помещалось в архив, мы можем сконструировать соответственное *безусловное правило*, поместить его в начало цепочки исполнения и установить признак продолжения выполнения. При этом сначала письмо будет помещено в архив независимо от хода всей дальнейшей обработки.

Интересно отметить, что, комбинируя признак завершения работы с возможностью исполнения других *цепочек правил*, возможно реализовать как «передачу управления», так и «вызов подпрограммы», когда после выполнения вызываемой цепочки управление возвращается в вызывающую цепочку.

2.3.5.4. Использование меток

Метки, поставляемые на письма, играют важную роль при работе с архивом. Однако, их можно использовать и при организации работы *правил*. Например, можно создать *цепочку правил*, в результате работы которой не будет произведено никаких *действий*, а будет проведена лишь предварительная классификация писем. Вот пример такой цепочки:

Условие: Письмо содержит исполнимый файл

Действие: Проставляем метку «Программа», переходим к следующему *правилу*

Условие: Письмо содержит видео-информацию

Действие: Проставляем метку «Видео», переходим к следующему *правилу*

Условие: Имя присоединенного файла содержит строку «doc.lnk»

Действие: проставляем метку «Вирус?»

При дальнейшей обработке мы можем использовать эти метки либо совокупно (считая наличие одной из них признаком, по которому письмо отправляется на «личный досмотр»), либо раздель-

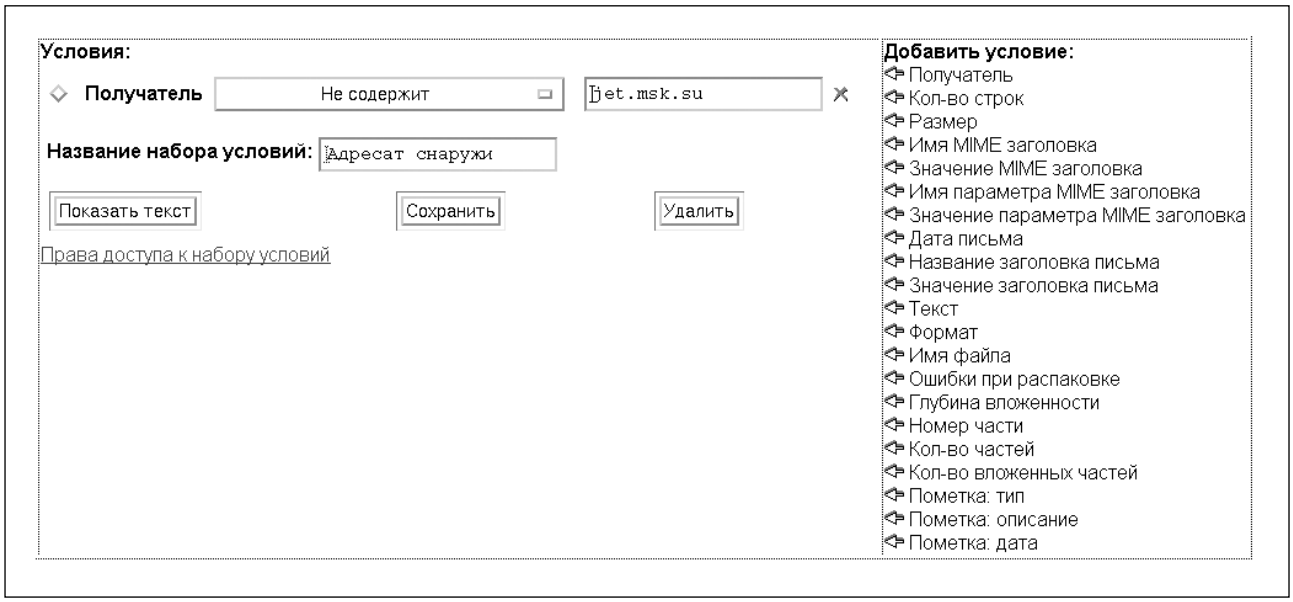

Рисунок 1. Экран редактирования *условия* `Адресат снаружи`

но, в зависимости от других атрибутов. Например, наличие видео-файла в корреспонденции, получаемой сотрудниками отдела рекламы, вполне естественно, в то время как письмо с исполнимым файлом может вызвать вопросы.

Обратите внимание на фразу «переходим к следующему *правилу*» в описании алгоритма. Она означает, что для данного *правила* установлен *признак продолжения обработки*, описанный в Разд. 2.3.5.3.

2.3.5.5. Отмена предыдущих действий

И наконец, несколько слов об отмене или «инвертировании» действий. Инвертирование *действия* означает, что мы решили отменить ранее назначенное для данного письма *действие*. Такая возможность часто бывает полезна в тех (очень распространенных) ситуациях, когда общие *правила* дополняются большим количеством разного рода исключений. Например, так может быть реализовано *правило*, согласно которому письма, направляемые президенту компании, не должны задерживаться ни при каких обстоятельствах. Или *правило*, по которому *ВСЯ* почта определенного «подозрительного» сотрудника должна помещаться в архив на период проверки. Возможность отмены ранее назначенного *действия* позволяет перечислять исключения не *до* формулировки общего *правила*, а *после*, что делает общий рисунок *правил* более логичным.

Отмена *действий* никак не сказывается на производительности работы системы, поскольку *правила* проходят предварительную обработку, при которой *действия* сортируются и «предвычисляются». При этом сохраняется последовательность операций назначения и отмены действий, т.е. можно отменить действие, назначенное лишь правилом, сработавшим *ДО правила*, отменяющего это действие. Поэтому отменяющие *правила* рекомендуется помещать в конец общего списка.

2.3.5.6. Мастер Построения Правил

Система правил представляет собой практически полнофункциональный язык программирования и позволяет создание модели обработки писем достаточной сложности. Однако, обратная сторона любой универсальности — определенные трудности при первоначальном освоении системы. Учитывая это, а также то, что большинство *правил* являются типовыми, в состав комплекса «Дозор-Джет» включен *Мастер Построения Правил*, позволяющий построить работоспособную модель в считанные минуты.

2.4. Как это выглядит

Управление системой «Дозор-Джет» осуществляется через WEB интерфейс. Памятуя о том, что лучше один раз увидеть, чем один раз услышать, в этом разделе статьи мы покажем утомленному теорией читателю некоторые примеры интерфейса, с которыми имеет дело пользователь системы, т.е. администратор безопасности.

Как следует из предыдущего материала, прежде всего, администратор безопасности должен определить *условия* фильтрации писем. Представленные ниже снимки с экрана отображают процесс создания *цепочки правил* для разделения почты на входящую, исходящую и внутреннюю (см. пример в Разд. 2.3.5.2).

Сначала (Рис. 1) мы создаем *условие*, называющееся *Адресат снаружи*, которое выделяет письма, адресованные в любой домен, кроме собственного (на рисунке это **`jet.msk.su`**). Это *условие* будет использовано при построении *правила* **`Исходящая почта`**.

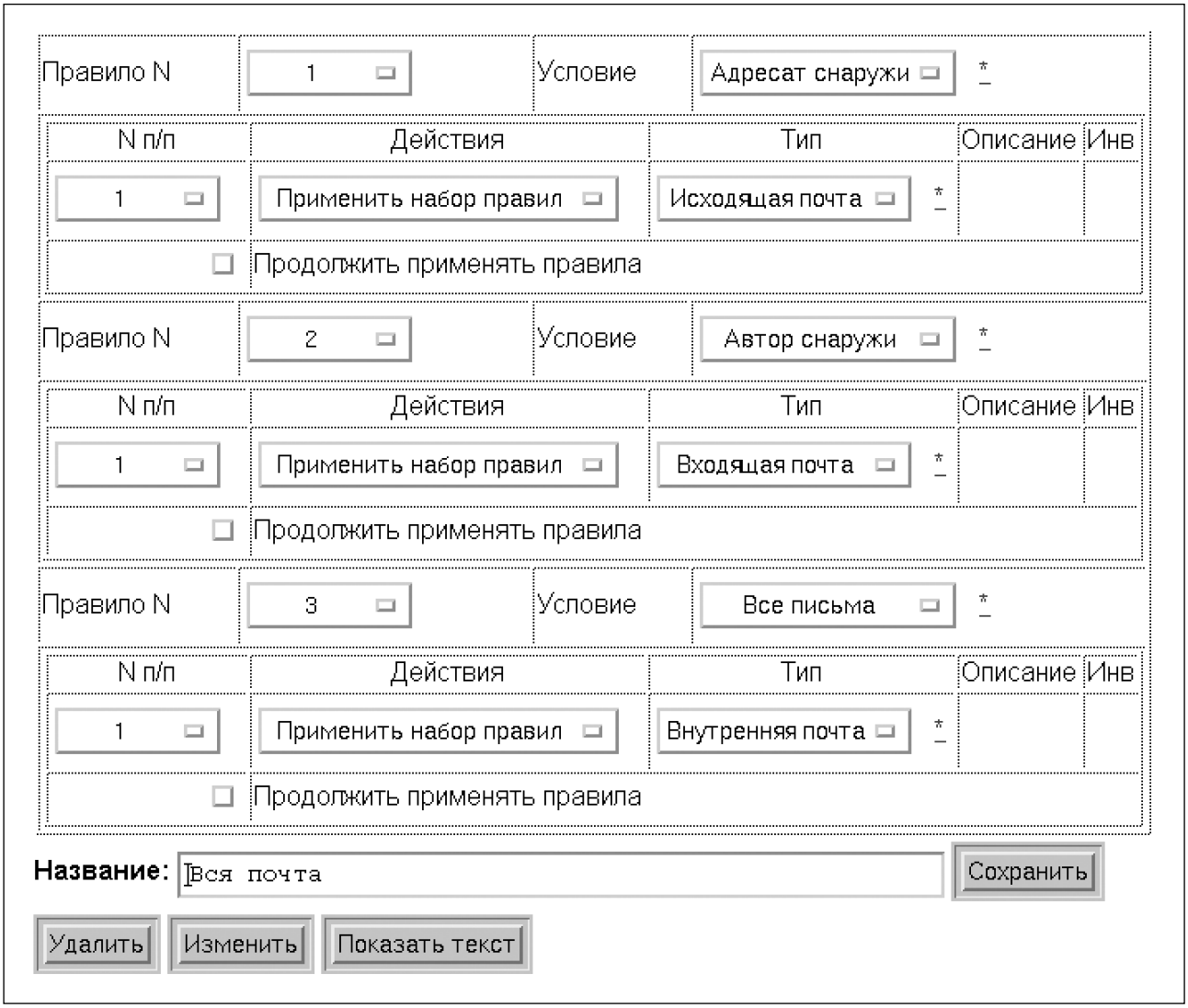

Рисунок 2. Экран редактирования цепочки *правил*

Аналогично определим *условие Автор снаружи* и перейдем к построению самой цепочки *правил* (Рис. 2).

Как видно из рисунка, цепочка состоит из трех *правил*. Условием первого является **Адресат снаружи**. Ему удовлетворяют письма, отправленные вовне, поэтому к ним применяется *цепочка правил* **Исходящая почта**. Обратим внимание, что признак **Продолжить применять** правила не установлен, поэтому применением этой цепочки обработка исходящей почты заканчивается.

Аналогично, действие второго *правила* с *условием* **Автор снаружи** состоит в вызове цепочки Входящая почта. Таким образом, последнее *правило* цепочки применяется лишь к письмам, не удовлетворившим ни одному из первых двух правил, т.е. к тем, отправитель и адресат которых находятся внутри организации и обрабатывать которые, следовательно, надо по алгоритму Внутренняя почта.

Таким образом, разделить почту на три потока удается всего тремя несложными правилами.

Предположим, что мы определили все необходимые *правила*, система поработала некоторое время, и в архиве накопилось определенное количество писем. Чтобы отыскать определенное письмо или письма, необходимо сформировать и выполнить соответствующий запрос. Пример такого запроса представлен на Рис. 3. Этот запрос предназначен для выделения писем, содержащих видеофрагменты.

Отчет, полученный в результате выполнения подобного запроса представлен на Рис. 4.

По вертикали экран отчета разделен на две части: таблицу параметров найденных писем вверху и окно просмотра индивидуального письма внизу. Подробное описание всех возможностей, предоставляемых поисковой системой, можно найти в документации к системе, здесь же лишь перечислим некоторые из них:

- Просмотр тела письма и всех вложений в точном соответствии с их типом (например, HTML текст будет отображаться браузером как HTML текст, а изображения — как изображения).

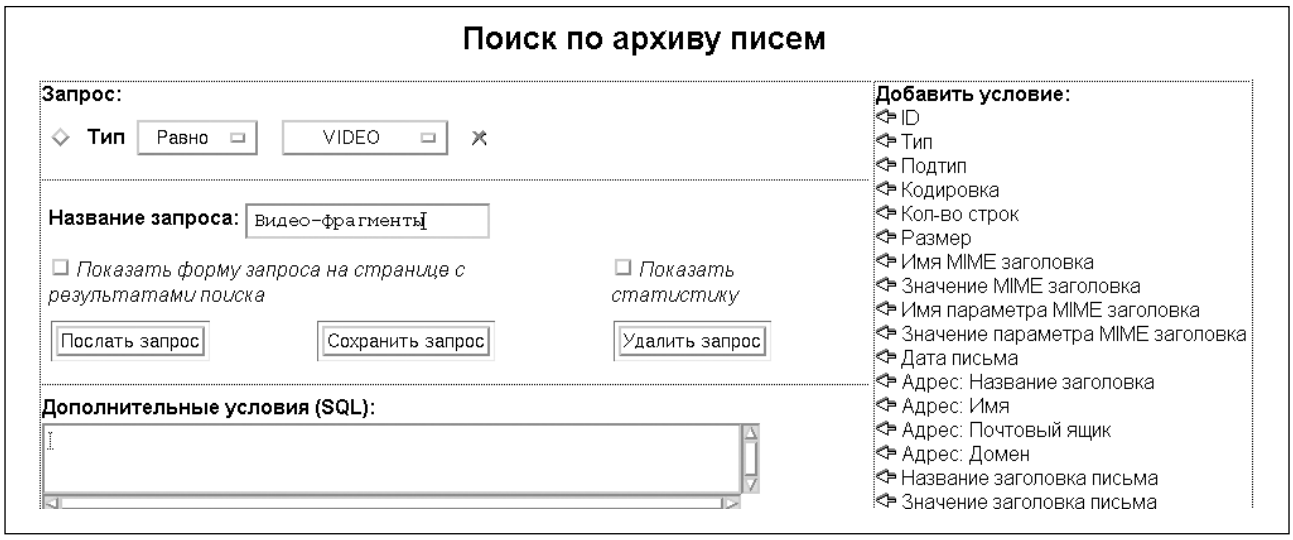

Рисунок 3. Экран запроса к каталогу архива

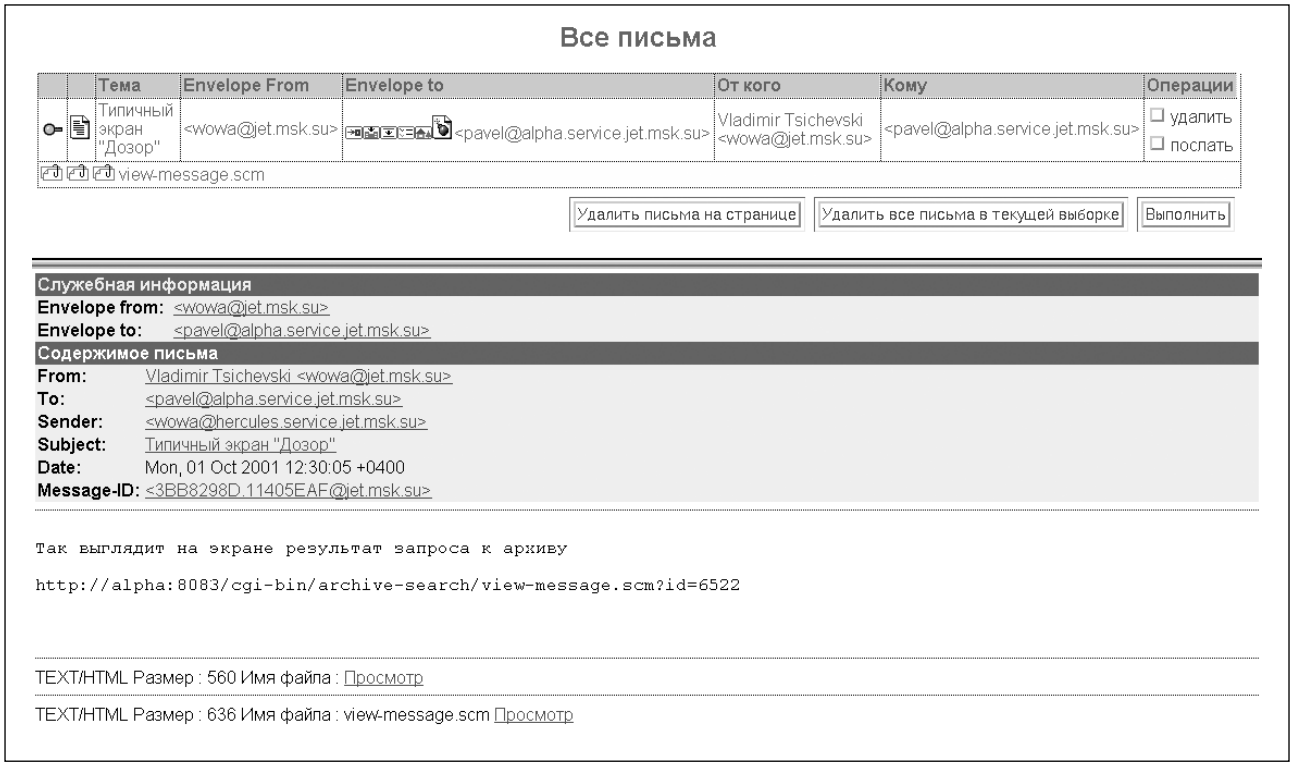

Рис. 4. Экран результатов запроса

- Просмотр оригинала письма *ДО* его анализа MIME-парсером. Это бывает полезно в тех случаях, когда структура письма по каким-то причинам нарушена (кстати, для выделения писем с нарушенной структурой в «Дозор-Джет» предусмотрено специальное *условие*).
- Выполнение запроса, сформированного автоматически на основании значения любого атрибута любого письма.
- Удаление всех удовлетворяющих запросу писем или некоторых из них.
- Просмотр списка присвоенных письму *меток*.
- Повторный запуск запроса с уточненными параметрами.

2.5. Дополнительные возможности

Проблема реализации политики использования электронной почты весьма сложна еще и потому, что, кроме некоторого набора «стандартных задач» , в политику входят правила, специфичные для каждой конкретной организации. Поэтому система управления электронной почтой обязательно должна быть расширяемой.

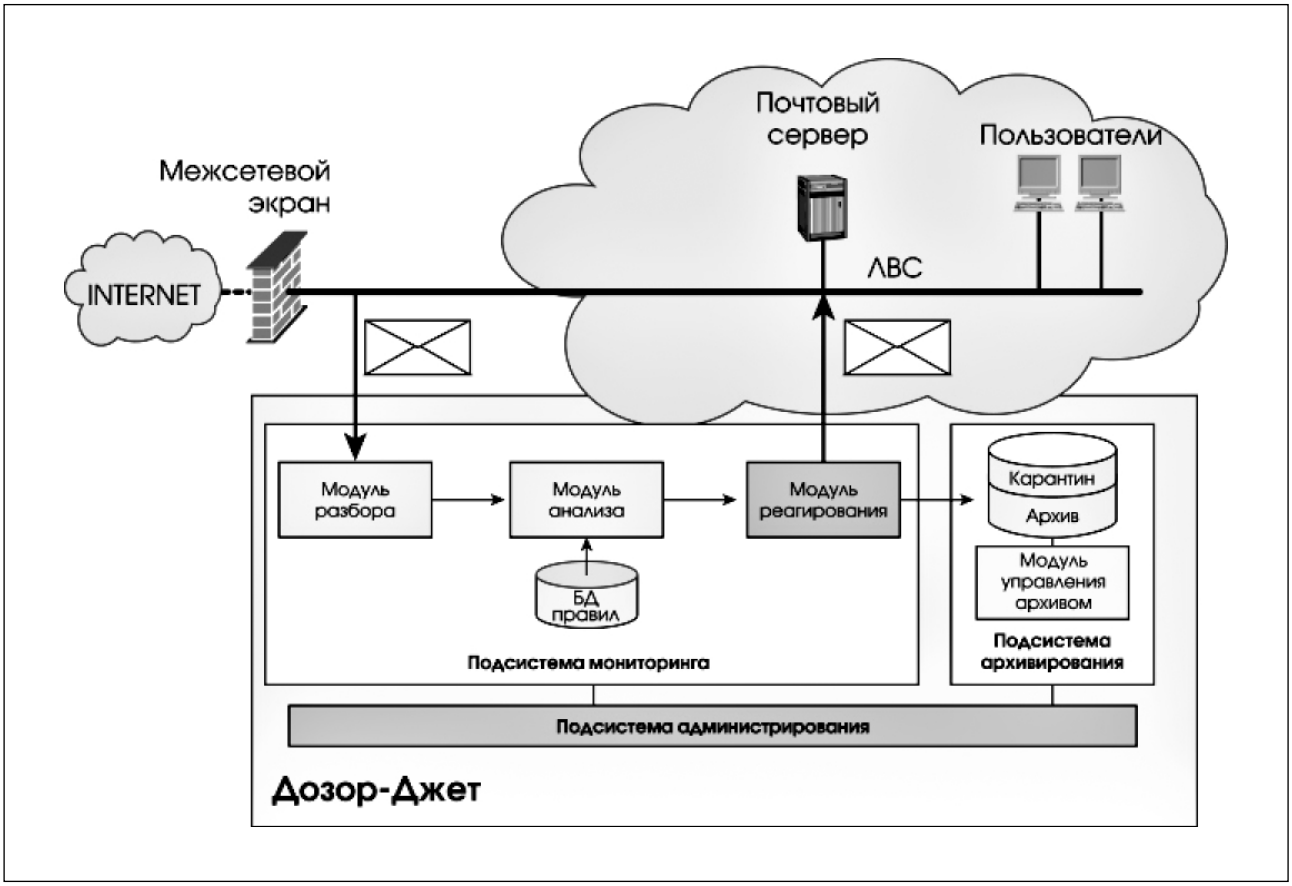

Рис. 5. Архитектура системы

Как программный комплекс, «Дозор-Джет» имеет модульную структуру (см. Рис. 5). Такая структура позволяет добавлять в систему дополнительные функциональные возможности, не затрагивая ее ядра, в которое входят *модуль разбора писем*, *модуль применения правил*, *модуль архивирования* и модули, реализующие *web-интерфейсы* к основным функциям.

В этом разделе мы кратко перечислим несколько дополнительных модулей, не входящих в состав стандартной поставки системы.

2.5.1. Модуль ЭЦП

Электронная цифровая подпись (ЭЦП) находит все большее применение в деловой переписке. Соответственно, в ряде случаев появляется потребность в автоматизации работы с ЭЦП.

В состав системы «Дозор-Джет» входит модуль, при активации которого в системе появляется два новых действия: *подписать письмо* и *проверить подпись*.

Оба этих действия возможны только при наличии базы данных, которая связывает авторов писем с соответствующими сертификатами. Такая база данных и средства для ее ведения входят в состав описываемого модуля.

Реализация постановки ЭЦП и ее проверки осуществляется средствами третьих производителей, для подключения конкретной реализации ЭЦП к системе «Дозор-Джет» достаточно, чтобы был реализован простой интерфейс, являющийся подмножеством Microsoft CryptoAPI.

2.5.2. Архив архива

Первоначально архив системы «Дозор-Джет» проектировался как некий «карантин» для подозрительных писем. Однако, первые же внедрения системы показали, что возможности, заложенные в архивную систему, позволяют использовать архив как часть системы документооборота предприятия.

Последнее означает, что, во-первых, в отличие от «карантина» архив выполняет функции долговременного хранения, и, во-вторых, что архив имеет тенденцию быстро расти.

Для того, чтобы управлять таким архивом нужна система, позволяющая переносить часть информации на другие носители, доступ к которым не столь оперативен, но которые обеспечивают долговременное хранение больших объемов информации.

В состав системы «Дозор-Джет» входит модуль, который позволяет выполнять экспорт из архива массива писем, отобранных в результате выполнения любого запроса к архиву. Отобранные письма помещаются в файл в формате стандартного почтового ящика, пригодный для работы любого

почтового клиента. Такие файлы могут быть помещены на носители для долговременного хранения. Впоследствии такие файлы могут быть вновь импортированы в систему «Дозор-Джет», причем импортированные письма могут быть снабжены специальными метками.

Данный модуль позволяет контролировать размер оперативного архива и в то же время хранить и использовать большие массивы данных, полученных с помощью системы «Дозор-Джет».

2.5.3. Контекстный поиск

Условия, которые накладываются на письма, обрабатываемые системой «Дозор-Джет», могут включать в себя *условия* на текст писем и вложений. Однако, в стандартной комплектации «Дозор-Джет» отсутствует возможность полнотекстового поиска по письмам, находящимся в архиве.

Дополнительный модуль контекстного поиска обеспечивает полнотекстовую индексацию архивируемых писем и последующий их поиск. Возможность искать слова вне зависимости от их грамматической формы обеспечивается специальным модулем, порождающим все допустимые словоформы.

Данный модуль реализован на основе Oracle Intermedia и Russian Context Optimizer.

2.5.4. Статистика и отчеты

Как уже говорилось выше, в архиве системы «Дозор-Джет» находится вся «учетная» информация о письмах (заголовки, типы вложений, их размеры и т.п.). Наличие такой информации позволяет получать отчеты по самым разным параметрам почтового трафика. «Дозор-Джет» обеспечивает стандартные отчетные формы по письмам, выделенным с помощью запроса к архиву.

Дополнительный модуль «Статистика» позволяет получать более полную информацию о почтовом трафике и преобразовывать ее в формат, пригодный для работы с помощью MSExcel. С помощью этого модуля можно анализировать почтовый трафик организации за относительно большие периоды времени, что позволяет оперативно корректировать политику использования электронной почты.

2.5.5. Взаимодействие с системами управления

Мы уже писали о том, что управление электронной почтой представляет собой комплексный процесс, который включает в себя различные аспекты, как программные, так и аппаратные. В ряде случаев чрезвычайно важно обеспечить взаимодействие системы «Дозор-Джет» и других систем управления.

Такое взаимодействие может иметь двоякую направленность. С одной стороны, «Дозор-Джет» является частью информационной системы и, как часть информационной системы, подлежит мониторингу и управлению. С другой стороны, определенная информация, полученная в результате анализа электронной почты, может быть нужна для оперативного реагирования со стороны системного администратора.

В составе системы «Дозор-Джет» может поставляться модуль, обеспечивающий «двустороннее» взаимодействие с системой HP Open View, которая позволяет контролировать работу компонентов «Дозор-Джет». Кроме того, инсталляция этого модуля добавляет в «Дозор-Джет» дополнительное действие: *сделать запись в журнал*. Это действие полностью аналогично действию *послать уведомление* (за исключением присоединения оригинала письма). Такая запись позволяет оперативно отображать на консоль управления HP Open View информацию об «опасных» письмах.

3. Заключение

Итак, сегодня, когда электронная почта по праву занимает ведущее место среди средств электронной коммуникации предприятия, все более актуальным становится комплекс проблем, решить которые можно, только внедряя *политику использования электронной почты*. Мы видели, что эта политика основывается на *правилах*, и поэтому ее реализация должна опираться на организационные меры, которые не может заменить никакая автоматизированная система.

В то же время без средств автоматизации контроль за выполнением *правил* может быть затруднен, а в ряде случаев (например, при больших потоках информации) практически неосуществим. Система «Дозор-Джет» является как раз тем средством, которое позволяет осуществлять эффективный контроль за выполнением *правил*, составляющих политику.

Предположим, наши доводы убедили читателя, и он решил, что пора, наконец, навести порядок в подведомственной ему электронной почте. С чего начинать?

Естественно, что начинать надо с *правил*, однако, чтобы сформировать работоспособные и содержательные *правила*, нужно как минимум хорошо представлять текущую ситуацию. И уже на этом самом первом этапе «Дозор-Джет» может оказать существенную пользу.

Установка «Дозор-Джет» в тестовую эксплуатацию на две недели даст возможность с помощью модуля статистики собрать полную информацию о почтовых потоках, классифицировать их и дать рекомендации о поэтапной выработке *правил*. Следует отметить, что в режиме сбора статистики можно ограничиться только регистрацией писем в архиве, что снимает все (или почти все) вопросы, связанные с конфиденциальностью переписки, попадающей в

тестовый вариант «Дозор-Джет». Кроме того, если для обработки статистической информации привлекаются сотрудники компании-производителя, то анонимными остаются и адреса корреспондентов.

Тестовая эксплуатация преследует и еще одну цель. «Дозор-Джет» является достаточно сложной системой, и решиться на ее внедрение, не опробовав в деле, довольно сложно. В процессе тестовой эксплуатации можно очень хорошо оценить технические характеристики требуемого аппаратного комплекса, а также провести обследование на предмет включения «Дозор-Джет» в сеть компании.

Подробную информацию о том как организовать тестовую эксплуатацию, можно получить, написав письмо по адресу <**dozor@jet.msk.su**> или <**sales@jet.msk.su**>. Свежую информацию о системе «Дозор-Джет» можно получить на сайте www.jet.msk.su.

Литература

[1] *Standart for the format of ARPA internet text messages*, CrockerDavid H., *August 13, 1982*.

[2] *Mapping between X.400(1988) / ISO 10021 and RFC 822*, Network Working Group S. Hardcastle-Kille, *May 1992*.

[3] *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples*, N. Freed и N. Borenstein, *November 1996*.

[4] *Communicating Presentation Information in Internet Messages: The Content-Disposition Header*, R. Troost и S. Dorner, *June 1995*.

[5] *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*, N. Freed и N. Borenstein, *November 1996*.

[6] *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*, N. Freed и N. Borenstein, *November 1996*.

A. «Дозор-Джет» Основные характеристики

Контроль всех почтовых сообщений. «Дозор-Джет» осуществляет мониторинг всех входящих, исходящих и внутренних почтовых сообщений, передаваемых посредством протокола SMTP.

Полный разбор почтовых сообщений. «Дозор-Джет» осуществляет полный разбор письма любого уровня вложенности.

Мощная система фильтрации. «Дозор-Джет» обладает мощной системой фильтрации сообщений, основанной на механизме *правил* и позволяющей реализовать практически любую политику использования электронной почты.

Фильтрация по всем компонентам письма. «Дозор-Джет» позволяет анализировать почтовые сообщения по всем его составляющим: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам.

Гибкие механизмы реагирования. «Дозор-Джет» позволяет автоматически реагировать на выполнение *условий* фильтрации выполнением следующих *действий*: пропустить письмо, запретить прохождение письма, поместить письмо в архив, зарегистрировать письмо, пометить письмо, послать уведомление уполномоченным лицам.

«Мастер» построения типовых правил. «Дозор-Джет» имеет средство построения типовых *правил* — «мастер», позволяющее упростить процесс создания начальных *правил* фильтрации.

Анализ русскоязычных сообщений. «Дозор-Джет» анализирует сообщения независимо от использованной в нем кодировки кириллицы (Win-1251, DOS-866, ISO-8859.5, KOI-8, MAC).

Распознавание форматов файлов. «Дозор-Джет» распознает реальные форматы присоединенных файлов всех популярных офисных приложений (включая вложенные в архивы файлы), раскрывает архивные вложения любого уровня.

Мощная подсистема архивирования. «Дозор-Джет» имеет мощную подсистему архивирования, реализованную на основе реляционной СУБД Oracle. Архив системы снабжен механизмом быстрого поиска писем по любым их атрибутам и, кроме того, может быть снабжен механизмом полнотекстового индексирования, который позволяет осуществлять полнотекстовый поиск по архиву писем.

Разграничение прав доступа. В «Дозор-Джет» реализовано детальное разграничение прав доступа ко всем объектам системы, в том числе к письмам, хранящимся в архиве и *правилам* их обработки.

Использование открытых стандартов. Использование системой «Дозор-Джет» для хранения сообщений СУБД Oracle позволяет, во-первых, применять стандартные средства обработки, поиска и анализа накопленной информации, во-вторых, достаточно легко интегрировать базу почтовых сообщений с уже существующими в компании системами с целью ее более широкого использования. Web-навигатор, применяемый в качестве пользовательского интерфейса, унифицирует рабочее место администратора системы, что значительно упрощает как работу по настройке модулей системы, так и текущую работу администратора.

Возможность интеграции с другими средствами защиты информации. «Дозор-Джет» имеет возможность интеграции с межсетевыми экранами, такими как «Застава-Джет», и антивирусными программами.

Надежная и производительная платформа. «Дозор-Джет» функционирует на UNIX-платформе под управлением ОС Sun Solaris и HP-UX.

Высокая производительность. «Дозор-Джет» способен обрабатывать десятки мегабайт почтового трафика в час и практически не создает задержки прохождения писем.

Сертифицированное решение. Гостехкомиссия России при Президенте РФ провела испытания системы «Дозор-Джет» и признала ее соответствие ТУ и руководящему документу «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», о чем свидетельствует сертификат No 465.

B. Рекомендации по настройке правил фильтрации электронной почты в системе «Дозор-Джет»

Настоящий документ содержит проект положения о политике безопасности в части фильтрации почтовых сообщений системой мониторинга и архивации почтовых сообщений «Дозор-Джет».

B.1. Общие положения

Политика безопасности при фильтрации почтовых сообщений есть набор *правил* фильтрации системы «Дозор-Джет», эксплуатирующейся в качестве почтового фильтра.

B.1.1. Условия применения системы фильтрации почтовых сообщений

Необходимым условием применения системы фильтрации почтовых сообщений является существование четко сформулированной политики безопасности, доведенной до сведения каждого пользователя электронной почты.

Составители должностных инструкций пользователя должны учитывать, что политика безопасности изначально не несет в себе карательных функций и лишь отражает точку зрения руководства предприятия на организацию делового процесса.

Возможным является доведение политики безопасности в части фильтрации почтовых сообщений до сведения сотрудников при приеме на работу одновременно с инструктажем по правилам техники безопасности.

B.1.2. Цели и задачи применения системы фильтрации почтовых сообщений

Для выработки набора *правил* необходимо, прежде всего, определить цели применения системы фильтрации почты.

Такими возможными целями могут быть:

- организация упорядоченной доставки писем, разделение почты на *входящую*, *исходящую* и *внутреннюю*;
- архивирование почтовых сообщений для обеспечения их сохранности;
- ограничение объема почтовых сообщений;
- блокировка массовых несанкционированных рассылок;
- блокировка доставки писем из нежелательных для организации списков рассылки;
- блокировка или ограничение доставки писем, содержащих исполняемые элементы (`javascript, ActiveX control`) и/или почтовые вирусы;
- защита от случайной посылки изнутри конфиденциальной информации;
- блокировка доставки писем, имеющих нежелательное для организации содержание.

B.2. Исходные данные для выработки *правил* фильтрации почтовых сообщений

Исходными данными для выработки *правил* фильтрации почтовых сообщений являются:

1. список пользователей электронной почты с указанием фамилии, имени, отчества пользователя, его почтового адреса и полного имени, предназначенного для указания в заголовке электронных писем;
2. почтовый домен организации, например, fbi.gov;
3. список ключевых слов, появление которых в тексте писем является нежелательным (список запрещенных слов);
4. список внешних почтовых адресов или почтовых доменов, сообщения из которых должны блокироваться или задерживаться для анализа;
5. список внутренних доверенных почтовых адресов, почтовые сообщения, пришедшие из которых или отправленных на которые, не подлежат контролю;
6. список недопустимых видов почтовых вложений или присоединенных файлов;
7. конфиденциальная информация, запрещенная для отправки на внешние почтовые сервера;
8. список внешних почтовых серверов, на которые запрещена отправка писем из организации.

Кроме сбора вышеперечисленных исходных данных следует сформировать неформальные груп-

пы пользователей электронной почтой, имеющих сходные функциональные обязанности в различных подразделениях. Такие объединения пользователей мы будем в дальнейшем называть *функциональными группами*, а объединения пользователей в группы согласно штатному расписанию — *административными группами*. Создание *административных групп* крупнее отдела представляется нецелесообразным в силу специфики задачи. Обычно в состав крупной административной единицы входят разнородные по выполняемым задачам подразделения.

Полезным может оказаться также создание группы, объединяющей всех пользователей электронной почты (то есть, всех пользователей, наделенных почтовыми адресами и имеющих право посылать почту во внешний мир). Группу, объединяющую всех пользователей электронной почты в дальнейшем будем называть *универсальной группой*.

Следует отметить, что все перечисленные списки не являются окончательными и должны дополняться и модифицироваться по мере необходимости.

B.3. Рекомендации по выработке *правил* фильтрации

B.3.1. Общие рекомендации

При определении нового набора *правил* целесообразно предусмотреть посылку уведомлений о задержании отправителям исходящих писем и получателям входящих. Уведомления должны также содержать указание на причину, по которой доставка письма не была произведена. Данная мера необходима для отладки вновь введенных *правил*, а также для того, чтобы пользователи знали о происходящих изменениях в политике безопасности предприятия.

Для разделения почтового потока на входящий, исходящий и внутренний (см. пример в Разд. 2.3.5.2) необходимо определить почтовый домен организации.

Для уменьшения общего потока писем целесообразно организовать службу централизованной подписки пользователей на списки рассылки, т.е. вести всю подписку от имени одного пользователя, а внутри предприятия организовывать внутреннюю рассылку. Это позволяет, во-первых, минимизировать и упорядочить почтовый трафик, во-вторых, заблокировать доставку нежелательных писем.

B.3.2. Правила формирования *списка запрещенных слов*

Основную проблему для фильтрации почтовых сообщений представляет анализ содержания в письмах конфиденциальной информации.

Первоначально представляется разумным внести в список запрещенных слов следующее:

1. телефонные номера:
   - не предназначенные для звонков клиентов или посторонних лиц;
   - внутренней АТС;
   - мобильных телефонов сотрудников, предназначенные исключительно для внутреннего пользования;
   - телефонов и/или позывные радиостанций, установленных в автомобилях различных служб или в спецмашинах;
2. номера *внутренних* банковских счетов, не отражаемые в балансовом отчете;
3. номера документов;
4. реквизиты налоговых и иных контролирующих органов;
5. номера пластиковых карт;
6. фамилии сотрудников организации;
7. устойчивые словосочетания типа *штатное расписание*, *докладная записка*, *служебная записка*, *распоряжение*, *регламент*, *должностная инструкция*, *маршрут движения*, *путевой лист*, *частотное расписание*.
8. словосочетания характеризующие секретные разработки организации типа *эпистемологические аспекты стратификации постмодернистски-легитимизированного общества*.

Поскольку система фильтрации «Дозор-Джет» позволяет использование регулярных выражений, то, например, правило поиска номеров выпущенных пластиковых карт VISA может быть записано в следующем виде: *четыре группы по четыре десятичные цифры, возможно, разделенные пробелом*.

Точно так же можно распознавать номера счетов или номера внутренних приказов и распоряжений, имеющие устойчивую структуру.

B.3.3. Защита от вирусов, распространяющихся в почтовых сообщениях

Основную опасность распространения вирусов несет в себе входящая почта. Хорошо организованная и поддерживаемая система анализа писем на содержание вирусов может сильно снизить вероятность распространения их внутри организации.

Для защиты от такого рода вирусов необходимо применять фильтрацию почтовых сообщений по полям заголовка, по содержанию и по форматам присоединенных файлов.

Для фильтрации по содержанию необходимо занести в *список запрещенных слов* фразы и слова, характерные для писем, содержащих тот или иной вирус. Например, наличие в письме фразы *VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURES*, указывает на наличие в нем также почтового вируса `VBS/Loveletter.as`.

Так как почтовые вирусы появляются регулярно, то *список запрещенных слов* необходимо по-

стоянно пополнять новыми *ключевыми словами*, следя за анонсами CERT и/или сообщениями фирм, занимающихся антивирусной защитой. Например, компания *Лаборатория Касперского* располагает большой и оперативно обновляемой базой вирусов, информация о которых доступна посетителям web-сайта компании.

Также, для выявления писем, содержащих вирусы, необходимо производить фильтрацию сообщений по полю *тема* (`Subject:`) в заголовке письма. Примером письма с определенным заголовком, содержащего вирус служит известный вирус *ILOVEYOU*. Вирус рассылался в письме, содержащем фразу *ILOVEYOU* в качестве заголовка.

Анализ других полей заголовка (например, поля `To:`) не является эффективным для фильтрации почтовых вирусов.

B.3.4. Правила построения фильтра полей заголовка почтового сообщения

B.3.4.1. Фильтрация по полю `From:`

Для исходящей почты почтовый адрес в поле *отправитель* должен входить в *универсальную группу*. Письма, отправленные с адреса, не содержащегося в *универсальной группе*, должны задерживаться до выяснения причин появления постороннего адреса.

Следующей проверкой поля *отправитель* должна стать проверка на попадание адреса отправителя в группу доверенных пользователей. Если выяснится, что отправитель письма является доверенным лицом, то дальнейшие проверки в отношении письма следует прекратить и переслать письмо адресату. То же *правило* действует и для входящей почты.

Поскольку изначально предполагается, что входящие письма могут иметь любой адрес отправителя, то создавать *правила* фильтрации входящей почты по адресу отправителя нецелесообразно. Исключением может стать ситуация систематической массовой рассылки рекламных писем с одного и того же адреса. В этом случае, письма с таким адресом отправителя должны блокироваться.

Возможно также создать *правило*, согласно которому будут задерживаться письма с неуказанным адресом отправителя. Такие письма, как правило, рассылаются массовым порядком и имеют явно рекламное содержание (spam). Обычно, организаторы несанкционированных коммерческих рассылок не указывают в письме ни адрес отправителя, ни адрес получателя и используют определенные особенности системы доставки почты.

B.3.5. Фильтрация по полю `To:`

Для исходящей почты фильтрация почтовых сообщений по адресу получателя представляется целесообразной в очень немногих случаях. Например, если организация выбирает из нескольких поставщиков одного и работу с этими поставщиками ведут разные менеджеры организации, то можно составить список почтовых адресов, на которые менеджеру запрещено отсылать почту (для предотвращения случайной отправки писем). Для входящей почты должно действовать *правило доверенных лиц*, т.е. доверенным лицам почта должна доставляться безусловно, без проверок.

В Разд. B.3.4.1 указывалось на возможность задержки писем с неуказанным адресом отправителя. То же правило действует и в отношении адреса получателя для входящих писем.

Аналогично, организаторы списков рассылки обычно указывают в поле *To:* посторонний адрес (обычно свой внутренний, например, *null@subscribe.ru*), а адреса получателей (подписчиков списка рассылки) перечисляют в поле *BCC:*, чтобы получатель письма не мог узнать из заголовка письма, кто еще подписан на список рассылки. Для блокировки доставки писем из нежелательных списков рассылки следует создать *правило*, блокирующее доставку писем, имеющих в качестве адресов получателя служебные адреса почтовых роботов.

B.3.6. Фильтрация по полю `Subject:`

Правило фильтрации по *Subject:* письма необходимо как для входящей, так и для исходящей почты. В Разд. B.3.3 уже говорилось о пользе такой фильтрации для выявления вирусов.

Желательно также организовать фильтрацию писем по теме на предмет задержки писем из несанкционированных массовых рассылок.

B.4. Групповые ограничения

Мы уже упоминали о групповом ограничении для пользователей, входящих в **универсальную группу** и в группу доверенных пользователей. Необходимо также создать **функциональную группу** технических специалистов и разрешить только членам этой группы получать почту с вложенными исполняемыми файлами (тип вложения — **application/octet-stream**). Возможно, что для технических специалистов не должно действовать правило, ограничивающее размер принимаемых почтовых сообщений.

Если организация производит официальную рассылку писем от имени предприятия, то целесообразно создать группу пользователей, имеющих право отсылать официальные письма. Обычно в заголовке или теле официального письма содержится какая-либо ключевая фраза, по которой данные письма могут быть однозначно идентифицированы. Официальные письма, отправленные с адреса, не входящего в указанную группу, следует задерживать до выяснения обстоятельств отправки.

Если в организацию приходят письма из оплачиваемых списков рассылки или из списков рас-

сылки ограниченного распространения, то следует определить группу пользователей, имеющих право на получение писем из указанных списков рассылки и определить отличительные формальные признаки подобных писем. Следует создать *правило*, разрешающее доставку писем с ограниченным распространением только членам указанной группы.

C. Структура почтовых сообщений

В данном разделе кратко изложены сведения о структуре почтового сообщения и о тех его частях, на которых основана фильтрация. Более подробно формат электронной почты рассмотрен в [1], [2], [3], [4], [5], [6].

Почтовое сообщение состоит из трех частей:

1. *Содержательная часть.* Она создается отправителем и содержит те сведения, которые автор отправляет своему корреспонденту. В дальнейшем эта часть будет называться **телом сообщения** (**mail body**).
2. *Данные, относящиеся к способу пересылки.* Чаще всего эта часть называется конвертом (**envelope**). В процессе передачи сообщения по каналам связи информация, относящаяся к конверту, может быть изменена.
3. Служебной части, однотипной для всех почтовых сообщений и содержащей служебные поля. В дальнейшем эта часть будет называться **заголовком сообщения** (**mail header**).

C.1. Тело сообщения

Тело сообщения может иметь простую или комплексную структуру.

Элементами простой структуры могут быть:

- Текстовые данные.
- Графические изображения.
- Аудио-записи.
- Видеозаписи.
- Приложения.[1]

Каждый из этих элементов имеет несколько подтипов представления информации. Более подробные сведения о структуре элементов почтового сообщения и соответствующих значениях **Content-Type** приведены в [6].

Тело сообщения с комплексной структурой может объединять несколько частей или включать в себя другое почтовое сообщение. При этом допускается вложенность: составные части почтового сообщения могут быть образованы как из отдельных элементов, так и из их объединений, а инкапсулированное сообщение может содержать другие инкапсулированные сообщения.

[1] Таким способом передаются все остальные типы данных, они никак не интерпретируются почтовой программой.

Два указанных типа обозначаются как **multipart** и **message**. Каждый из них допускает использование следующих подтипов:

multipart

Почтовое сообщение данного типа может объединять текстовые части, изображение, аудио и видео. Для него допускается использование подтипа **mixed** для сообщения, состоящего из нескольких вложенных частей, подтипа **alternative** для представления одних и тех же данных в различных форматах, подтипа **parallel** для частей, которые должны просматриваться одновременно и подтипа **digest** для сообщений, в которых каждая из частей представляет собой вложенное сообщение.

message

Сообщение данного типа состоит из вложенных почтовых сообщений. Рекурсия в данном случае не ограничивается и составные части также могут состоять из вложенных сообщений. Возможны следующие подтипы: **rfc822** для вложенного письма, **partial** для его части, **external-body** для тех случаев, когда объем данных велик и целесообразно определить их через ссылку на внешний источник.

Детальное описание комплексной структуры почтовых сообщений приведено в [6].

C.2. Конверт сообщения

Конверт сообщения представляет собой данные, относящиеся к способу пересылки. Эта информация служебная, поэтому она обычно не отображается в почтовых клиентах.

Система «Дозор-Джет» поддерживает работу с двумя полями, которые включаются в конверт:

Адрес отправителя

Фактический адрес пользователя, отправившего почтовое сообщение (т.е. поле **MAIL FROM** конверта сообщения, передаваемого по протоколу SMTP). В некоторых случаях этот адрес может не совпадать со значением поля **From**:.

Адрес получателя

Фактический адрес пользователя, которому предназначено почтовое сообщение (т.е. поле **RCPT TO** конверта сообщения, передаваемого по протоколу SMTP). . Кроме того, доступ к данному полю можно получить так же, как и ко всем другим полям заголовка сообщения. Если в конверте сообщения присутствуют несколько полей **RCPT TO**, то система «Дозор-Джет» «пропускает» такое письмо через фильтр соответствующее число раз. Использование условия «Получатель» позволяет в этом случае осуществлять различные проверки в зависимости от указанного адреса получателя.

С.3. Заголовок сообщения

Заголовок сообщения состоит из нескольких полей, а поле, соответственно, образуется из имени поля, его значения и, иногда, имен и значений дополнительных параметров. Значение поля отделяется от имени двоеточием и пробелом. Пар имя=значение параметра в одном поле может быть несколько. Заголовок отделяется от тела сообщения пустой строкой.

Поля, присутствующие в заголовке, подразделяются на две группы:

- Поля, в которых используются почтовые расширения для мультимедиа (**MIME**).
- Все остальные поля.

В дальнейшем первая группа будет называться **MIME**-заголовками, а вторая — заголовками почтового сообщения (письма). Следует иметь в виду, что при визуальном просмотре писем эти две части не разделены и различаются только по ключевому слову **Content,** которое предшествует **MIME**-заголовку.

Система «Дозор-Джет» позволяет производить фильтрацию сообщений по обоим группам, и, кроме того, по параметрам **MIME**-заголовков *условиями* фильтрации могут являться:

Имя **MIME**-заголовка:

Название поля в заголовке письма, начинающееся со слова **Content**, например, **Content-Type, Content-Description, Content-Transfer-Encoding**. Обязательно должно начинаться с самого первого символа в строке. Полный список поддерживаемых системой «Дозор-Джет» имен **MIME**-заголовков хранится в базе данных.

Значение **MIME**-заголовка:

Строка символов, являющаяся значением какого-либо поля в **MIME**-заголовке и отделенная от имени поля двоеточием и пробелом. Для описания типа передаваемых данных применяется двойной параметр, например, **image/gif** или **multipart/mixed**. В остальных случаях используется одиночное слово, например, **8bit**, **inline** или строку символов, например, **message body text**.

Имя параметра **MIME**-заголовка:

Параметр несет дополнительную информацию, уточняющую интерпретацию полей в MIME-заголовке. Параметром является любая строка символов, отделенная от значения MIME-заголовка точкой с запятой и пробелом, например, **charset** или **boundary**. Значение параметра указывается за ним, после знака = и заключается в кавычки, например: **charset="koi8-r"**.

Значение параметра **MIME-заголовка**:

Строка символов, следующая за именем параметра после знака =. Значение должно быть заключено в кавычки, например: boundary="FCSECouY5/" filename="cross.gif".

Название заголовка письма:

Имя любого поля в заголовке почтового сообщения, например, **From, To, Subject, Date, Received**. Обязательно должно начинаться с самого первого символа в строке. Перечень всех поддерживаемых системой «Дозор-Джет» имен заголовков почтовых сообщений хранится в отдельной таблице метаданных.

Значение заголовка письма:

Строка символов, являющаяся значением какого-либо поля в заголовке сообщения. Может представлять собой строку символов, как, например, для поля **Subject** или адрес электронной почты, например, для поля **From**.

Наиболее рациональным является группирование *условий* типа **Имя** и **Значение** в пары, т.е. построение конструкций вида: **ИМЯ = XXX** и **ЗНАЧЕНИЕ = УУУ** Например: **Имя MIME-заголовка = Content-Type** и **Значение MIME-заголовка = text/plain** Это означает, что данное условие описывает все почтовые сообщения, где используется **Content-Type: text/plain**.

Но подобный подход не является обязательным. Вполне допустимо использование и одиночных *условий* вида: **ИМЯ = XXX** Таким способом, например, выделять все письма, где в заголовке есть хотя бы одно поле **X-Mn-Key**.

Кроме того, дата и время задержания почтового сообщения системой «Дозор-Джет» также могут являться *условием* фильтрации. Таким способом можно, например, использовать разные фильтры в дневное и ночное время.[1]

[1] Необходимо отметить, что система «Дозор-Джет» позволяет использовать поле «Дата» заголовка сообщения двумя способами: во-первых, как строку символов и во-вторых, как собственно дату, если удалось произвести ее синтаксический разбор.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. (vlad@jet.msk.su)
Технический редактор: Антонов А.Н. (silver@jet.msk.su)
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555