Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 6 (121)/2003

Безопасность систем электронной почты

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Безопасность систем электронной почты

Александр ТАРАНОВ
Олег СЛЕПОВ

СОДЕРЖАНИЕ

Роль электронной почты 2
Достоинства электронной почты
Риски, связанные с использованием электронной почты 3
Безопасность корпоративной системы электронной почты 7
Политика использования электронной почты
Средства реализации политики использования электронной почты
Требования к системам контроля содержимого электронной почты
Какую систему выбрать
Сравнительный анализ систем «Дозор-Джет» и MAILsweeper.
Выводы 20

Роль электронной почты

Электронная почта — один из наиболее широко используемых видов сервиса, как в корпоративных сетях, так и в Интернет. Она является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами в бизнесе. Роль электронной почты становится очевидной, если рассмотреть функции, которые выполняет почта:

- Обеспечивает внутренний и внешний информационный обмен;
- Является компонентом системы документооборота;
- Формирует транспортный протокол корпоративных приложений;
- Является средством образования инфраструктуры электронной коммерции.

Благодаря выполнению этих функций электронная почта решает одну из важнейших на настоящий момент задач — *формирует единое информационное пространство.* В первую очередь это касается создания общей коммуникационной инфраструктуры, которая упрощает обмен информацией между отдельными людьми, подразделениями одной компании и различными организациями.

Использование электронной почты для обмена информацией между людьми как внутри от-

дельно взятой организации, так и за ее пределами способно коренным образом изменить технологии и методы ведения дел. Переход к обмену документами в электронном виде открывает новые возможности для повышения эффективности труда и экономии средств и времени.

По мнению аналитиков компании IDC в ближайшие три года (2002-2005 г.г.) количество почтовых ящиков в Интернет достигнет 1,2 млрд, а в 2001 году насчитывалось всего 550 млн. почтовых ящиков. Таким образом рост составит 110%. Вместе с ростом количества пользователей будут расти и объёмы пересылаемой почты. Компания IDC прогнозирует, что количество электронных писем, проходящих по сети в течение одного дня, в 2005 году достигнет 36 млрд.

Достоинства электронной почты

Электронная почта обладает рядом преимуществ по сравнению с обычными способами передачи сообщений (традиционная почта или факсимильная связь). К ним относятся следующие:

- **Оперативность и легкость использования**
  Электронная почта — это глобальная система, позволяющая передавать письма в любую точку мира за считанные минуты, независимо от времени суток. Отправка и прием сообщений электронной почты не требуют глубоких знаний компьютерных технологий, благодаря чему этот сервис широко применяется не только в бизнесе, но и для личного общения. Кроме того современные условия требуют оперативного реагирования на процессы, происходящие в бизнесе. Электронная почта позволяет собирать информацию, принимать решения и доводить их до различных подразделений компании и партнеров по бизнесу.
- **Доступность практически в любом месте**
  Главное преимущество электронной почты — ее доступность. И хотя огромные пространства еще «не освоены» электроникой, стремительное развитие электронных коммуникаций, в конечном счете, приведет к тому, что «глобальная паутина» покроет весь земной шар.
- **Универсальность форматов писем и вложений**
  Удобство использования электронной почты состоит в том, что она способна "переносить" большие объемы информации различных форматов данных. В одном письме могут быть одновременно переданы графическая, видео, текстовая информация, файлы баз данных, приложений и т.п.
- **Дешевизна сервиса**
  Отправить электронное письмо стоит значительно дешевле, чем обычное или сделать междугородный или тем более международный телефонный звонок. Электронная почта позволяет рассылать письма сразу нескольким адресатам без дополнительных затрат.
- **Надежность и скорость инфраструктуры доставки**
  Так как электронная почта пересылается непосредственно с сервера отправителя на сервер получателя по каналам Интернет, этот процесс протекает быстро, даже если эти серверы расположены на противоположных сторонах земного шара. Фактически на передачу текстового сообщения, например, из России в Америку требуется не более 1-2 минут.
- **Использование для обработки электронной почты прикладного специального программного обеспечения**
  Электронный характер письма позволяет проводить его обработку при помощи дополнительного программного обеспечения. При этом виды обработки электронной почты зависят от характера деятельности организации. Это может быть: создание базы данных электронной почты, формирование различных отчетов, проведение анализа деятельности компании и т.п. Все это позволяет создать единую систему управления документооборотом, полностью интегрированную с остальными информационными процессами в компании.

Риски, связанные с использованием электронной почты

Электронная почта обладает многочисленными достоинствами, но именно из-за этих достоинств возникают основные риски, связанные с ее использованием. К примеру, доступность электронной почты превращается в недостаток, когда пользователи начинают применять почту для рассылки спама, легкость в использовании и бесконтрольность приводит к утечкам информации, возможность пересылки разных форматов документов — к распространению вирусов и т.д.

В конечном итоге любой из этих рисков может привести к серьезным последствиям для компании. Это и потеря эффективности работы, и снижение качества услуг информационных систем, и разглашение конфиденциальной информации. Недо-

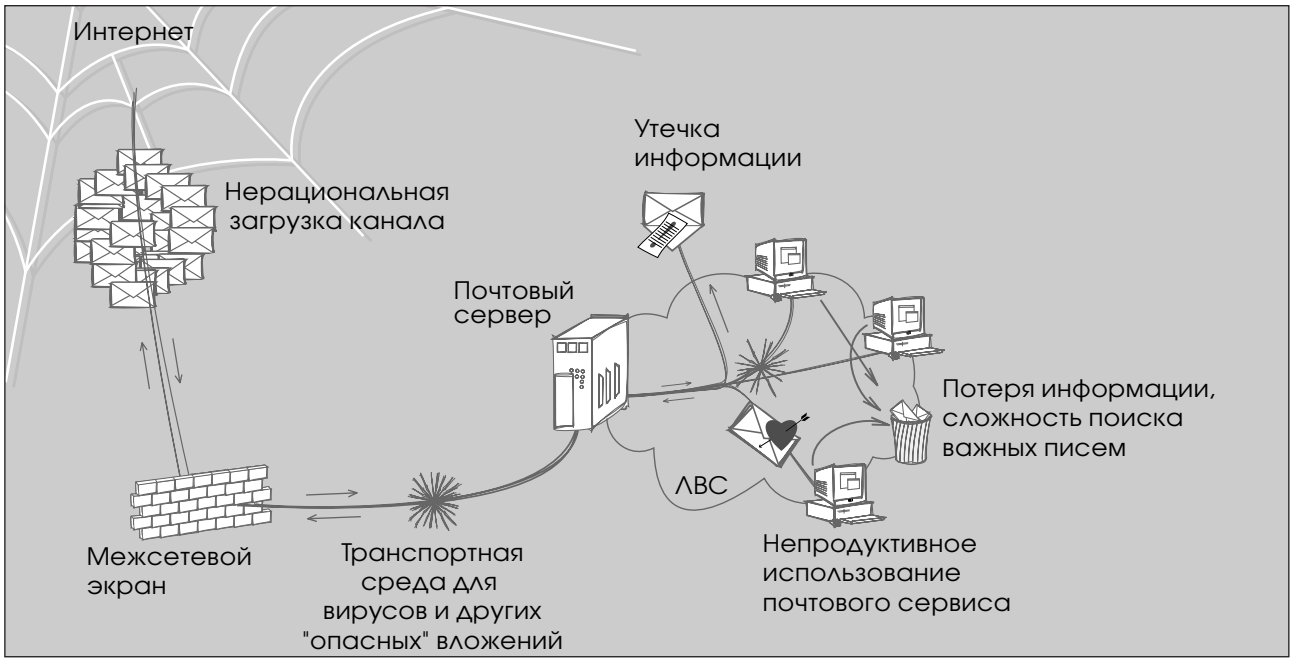

Рис. 1. Негативное воздействие различных факторов на незащищенную почтовую систему.

статочное внимание к данной проблеме грозит значительными потерями в бизнесе, а в некоторых случаях даже привлечением к юридической ответственности в связи с нарушением законодательства.

Компания подвергается данным рискам в силу ряда свойств электронной почты. Например, благодаря применению MIME-стандарта электронная почта может переносить большие объемы информации различных форматов данных в виде прикрепленных к сообщениям файлов. Такой возможностью сразу воспользовались злоумышленники. Достоинство электронной почты превратилось в угрозу, поскольку *электронная почта стала представлять собой практически идеальную среду для переноса различного рода «опасных» вложений, а именно компьютерных вирусов, вредоносных программ, «троянских» программ и т.п.* Если надлежащий контроль за использованием электронной почты не обеспечен, это может привести к чрезвычайно серьезным последствиям и даже нанести непоправимый ущерб. Избавиться от данного риска можно лишь путем блокировки писем с "опасными" вложениями, а также антивирусной проверки прикрепленных файлов. На практике же оптимальным средством может оказаться *блокировка определенных типов файлов*. Это, как правило, исполняемые файлы (exe, com, bat) и файлы, содержащие макросы и OLE-объекты (файлы, созданные в приложениях MS Office).

Серьезную опасность для корпоративной сети представляют различного рода *атаки с целью «засорения» почтовой системы*. Это, в первую очередь, пересылка в качестве вложений в сообщениях электронной почты файлов больших объемов или многократно заархивированных файлов. «Открытие» таких файлов или попытка «развернуть» архив может привести к «зависанию» системы. При этом одинаково опасны как умышленные атаки этого типа, например, «отказ в обслуживании» (Denial of Service) и «почтовые бомбы» (mail-bombs), так и «неумышленные», когда пользователи отправляют электронные письма с вложениями большого объема, просто не подумав о том, к каким последствиям может привести открытие подобного файла на компьютере адресата. Действенный способ избавиться от «засорения» почтовой системы и ее перегрузки — *фильтрация по объему передаваемых данных, по количеству вложений в сообщения электронной почты и глубине вложенности архивированных файлов*.

Другой особенностью электронной почты является ее доступность и простота в использовании. Во многом результатом этого стало широкое и повсеместное применение этого вида сервиса Интернет. Стихийность развития и отсутствие единых правил функционирования почтового сервиса привели к неконтролируемому использованию электронной почты, а в связи с этим, и к возникновению целого ряда рисков, связанных с неуправляемой циркуляцией электронной почты в сети.

Отсутствие контроля над почтовым потоком, как правило, становится причиной того, что сотрудники компании *используют электронную почту в целях, не связанных с деятельностью компании* (например, для обмена видео-файлами и графикой, частной переписки, ведения собственного бизнеса с использованием почтовых ресурсов компании, рассылки резюме в различные организации и т.п.). Это

приводит к резкому падению производительности труда в целом по компании, поскольку результатом такой деятельности сотрудников является:

- Снижение производительности работы информационной системы (увеличение объема неделового трафика);
- Снижение производительности работы отдельного сотрудника (неоправданная потеря рабочего времени);
- «Засорение» ресурсов информационной системы (занятие дискового пространства под неделовую почту).

Кроме того, к такому же результату может привести *непродуктивное использование почтовых ресурсов* в трудовой деятельности сотрудников (например, чрезмерное увлечение почтовой перепиской в случаях, когда необходимости в такой переписке нет, использование электронной почты не по назначению и т.п.). Причиной этого, как правило, является отсутствие в компании правил, регламентирующих использование системы электронной почты. Последствиями непродуктивного использования почтового сервиса являются снижение производительности труда в компании, а также излишние финансовые затраты. Сэкономить средства в значительной степени поможет *проведение анализа эффективности использования системы электронной почты, который основывается на базе статистических данных о функционировании системы. Подобную статистику возможно получить лишь в случае ведения архива электронной почты.* Обработка информации, содержащейся в архиве, позволяет получать отчеты о различных параметрах электронной почты, ее объемах и структуре, представить наглядную картину использования почтового трафика сотрудниками компании, а это, в свою очередь, поможет предотвратить использование электронной почты, несвязанное с деятельностью компании, и повысить эффективность работы корпоративной почтовой системы.

Передача в электронных письмах графических, видео и звуковых файлов, которые, как правило, имеют *большой объем* даже если такая передача предусмотрена условиями ведения бизнеса, приводит к значительной перегрузке сети, соответственно к дополнительным финансовым затратам на ее обслуживание. Согласно проведенным исследованиям около 30% почтовых ресурсов среднестатистической компании ежедневно затрачивается на пересылку графических, видео и звуковых файлов. Избежать этого, а значит и добиться значительной экономии средств компании, поможет, так называемая, *отложенная доставка писем*, которая позволяет доставлять сообщения больших объемов в то время, когда загрузка сети не имеет критического значения (например, в ночное время, в выходные дни и т.п.).

К «засорению» трафика также ведет рассылка *спама*. Как правило, это письма, содержащие навязчивые предложения самых разнообразных услуг, товаров и т.п. Такого рода почта является «группой риска» с точки зрения переноса вирусов. Большое количество ненужной почты загружает каналы, «замусоривает» почтовые ящики, отнимает время на удаление ненужных писем и повышает вероятность случайного удаления нужных. Конечно рассылка, например, сообщений рекламного характера, напрямую не преследует цели «засорить» почтовую систему организации, однако косвенно приводит к негативным последствиям. Использование списков рассылки, в которую могут входить все пользователи одной корпоративной сети, и получение одновременно всеми этими пользователями сообщений рекламного характера грозит компании снижением производительности ее сетевых ресурсов. *Блокировка спама,* в первую очередь, связана с контекстным анализом сообщений, то есть проверкой электронной почты на наличие ключевых слов и выражений, которые обычно употребляются в сообщениях рекламного характера.

Переписка с внешними корреспондентами представляет наибольшую угрозу из-за особенностей электронной почты (невозможность контролировать маршрут передачи писем, а также их копирование и перенаправление, осуществлять аутентификацию отправителя/получателя, возвращать письма после их отправления). Кроме того невозможен либо затруднен контроль количества отправляемых копий письма. Содержимое сообщения может быть прочитано в процессе передачи его по Интернету, поскольку заголовки и содержимое электронных писем часто передаются в открытом виде.

Другой проблемой, связанной с особенностями электронной почты, является то, что электронная почта позволяет неконтролируемое накопление информации в архивах и практически неуничтожима. В противоположность бытующему мнению, удалить электронную почту непросто. Резервные копии сообщений могут оставаться на персональных компьютерах отправителя и получателя или в сети компаний, где они работают. Если электронное почтовое сообщение отправлено через коммерческую службу или через Интернет, то оно будет передаваться через несколько различных серверов. Каждый сервер в цепочке между отправителем и получателем может сохранить копию сообщения в своих архивах. Даже методичное выяснение местонахождения каждой копии электронного письма с последующим его удалением не дает никакой гарантии того, что сообщение не осталось

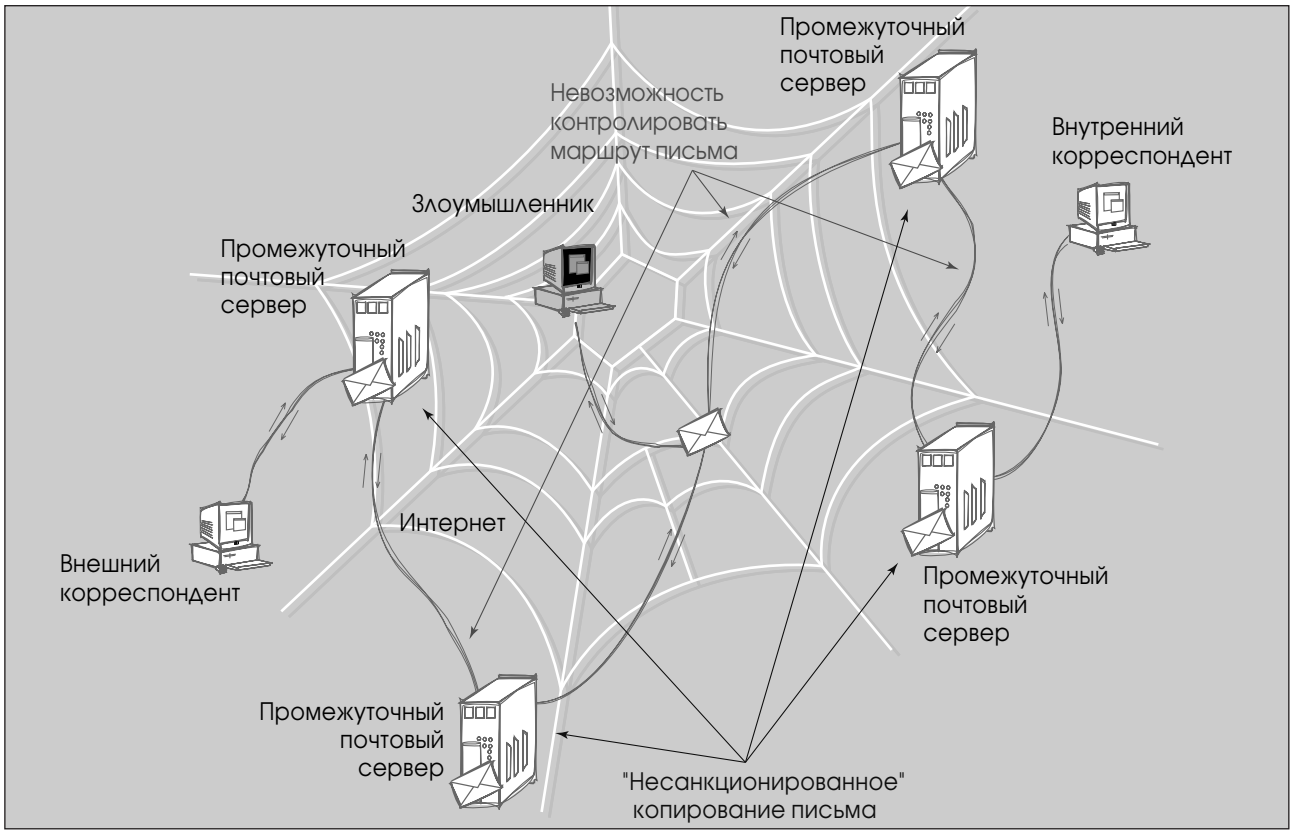

Рис. 2. Проблемы, возникающие при пересылке электронной почты через Интернет.

на жестком диске компьютера или сервера. С помощью широко доступного программного обеспечения даже рядовой пользователь сможет восстановить сообщение электронной почты после того, как его якобы удалили.

Все эти особенности, а также простота копирования электронного сообщения и невозможность проконтролировать данную операцию приводят к тому, что сотрудник может передать корпоративную информацию любому количеству людей как внутри, так и за пределами компании анонимно и без соответствующего разрешения, сразу или по истечении какого-либо времени. При этом, такая информация может представлять собой служебную информацию компании (тексты договоров, сведения о планируемых сделках и т.п.), пароли, системные данные, исходные коды программ или другую конфиденциальную информацию. Это, в конечном итоге, грозит серьезным нарушением конфиденциальности и может привести к неприятным для компании последствиям.

В отличие от бумажной корреспонденции, электронную почту очень легко неумышленно отправить по неверному адресу. Причиной этого может быть как неумелое использование адресных книг, так и ошибка в указании адреса получателя или, что еще хуже, случайный выбор опции, предусматривающей рассылку сообщения большой группе пользователей, в то время как сообщение является конфиденциальным.

Чтобы обеспечить *защиту от утечки конфиденциальной информации* из сети, необходимо осуществлять контроль адресатов, *фильтрацию* передаваемых данных на наличие в текстах сообщений или в прикрепленных к электронному письму файлах *слов и выражений, имеющих отношение к «закрытой» тематике*, осуществлять *разграничение доступа* различных категорий пользователей к архивам электронной почты и т.п.

Одно из основных отличий электронной почты состоит в формальном к ней отношении (по сравнению с другими видами коммерческих коммуникаций). Во-первых, большинство пользователей относятся к электронной почте как к чему-то временному, то есть поступают с ней по принципу «прочитал и выкинул». При таком отношении существует риск *случайного удаления значимой информации*. Кроме того, существует опасность *потери переписки с важным клиентом*. Все эти проблемы решаются путем *создания в организации архива электронной почты*. Во-вторых, такое отношение к электронной почте приводит к тому, что из-за кажущейся недолговечности электронных сообщений люди часто используют их для того, чтобы выразить чувства и мнения в выражениях, которые они никогда не позволили бы себе употребить в традиционных письмах. Публикация таких писем в сети может нанести серьезный ущерб ре-

путации компании или явиться причиной юридических исков к ней.

Еще одна область связана с возможностью привлечения к юридической ответственности компании и ее сотрудников — *за нарушение авторского права*. Защищенные этим правом материалы могут содержаться или в сообщении электронной почты, или в присоединенных файлах. К подобным материалам относятся графическая, аудио, видео и различная текстовая информация, т. е. любая информация, которая может быть представлена в электронном виде и передана по компьютерным сетям. Копирование или распространение этих материалов без предварительного согласия автора или владельца авторских прав является нарушением закона. Если компания допускает, чтобы материалы почты, защищенные авторским правом, использовались сотрудниками, не имеющими на это полномочий, то она может быть привлечена к ответственности за прямое или косвенное пособничество нарушению авторского права.

Безопасность корпоративной системы электронной почты

Учитывая описанные выше риски, связанные с использованием электронной почты, организациям необходимо принять соответствующие меры для защиты от них. *Подход к защите должен быть всесторонним и комплексным — необходимо сочетать организационные меры с использованием соответствующих технических средств.* К организационным мерам относятся разработка и внедрение в компании политики использования электронной почты. Технические средства должны обеспечить выполнение данной политики как за счет мониторинга почтового трафика, так и за счет адекватного реагирования на нарушения.

Для защиты компании от рисков, связанных с использованием электронной почты, необходимы:

Политика использования электронной почты + **Средство реализации политики**

Очень важно отметить, что политика использования электронной почты первична по отношению к средствам ее реализации, поскольку составляет основу для формирования комплекса мер по защите информационной системы от вышеперечисленных рисков. Сначала необходимо сформулировать политику, составить правила использования электронной почты, определить, как созданная система должна реагировать на определенные нарушения данной политики и только затем переводить правила на компьютерный язык того средства, которое используется для контроля выполнения положений политики использования электронной почты.

К таким техническим средствам относится специальное программное обеспечение, называемое *система контроля содержимого электронной почты* (content security software). В функции таких систем входит контроль почтового трафика и ведение архива переписки по электронной почте. К

Рис. 3. Решение проблем защиты почтовой системы.

данным системам предъявляются следующие требования:

- Проведение текстового анализа;
- Фильтрация передаваемых данных:
  - по размеру и объему данных;
  - по количеству вложений в сообщения электронной почты;
  - по типу файлов (вложенных в электронную почту);
  - по адресу электронной почты;
- Контроль использования почтовых ресурсов и разграничение доступа к ним различных категорий пользователей;
- Отложенную доставку сообщений электронной почты по расписанию;
- Ведение полнофункционального архива электронной почты.

Выполнение этих требований обеспечивается применением в средствах защиты определенных механизмов. К таким механизмам могут относиться:

- Рекурсивная декомпозиция (специальный алгоритм, применяемый для разбора сообщений электронной почты на составляющие компоненты с последующим анализом их содержимого);
- Эвристическое определение кодировок текстов;
- Определение типа файлов по сигнатуре;
- Полнотекстовый поиск по архиву электронной почты и т.п.

Политика использования электронной почты

Средство защиты — система контроля содержимого электронной почты, само по себе никаких задач по обеспечению безопасности не решает. Это всего лишь «машина», которая помогает человеку в решении данной проблемы. Поэтому задачу по обеспечению безопасности необходимо такой «машине» поставить. Это означает, что должен быть выработан специальный свод правил, который в дальнейшем будет переведен на язык машины. *Такой свод правил называется «политикой использования электронной почты».*

Во многих организациях такие правила существуют уже длительное время. Как и всякая ограничительная мера, они создают определенные неудобства пользователям системы, а если пользователю что-то неудобно, он либо перестает этим пользоваться, либо старается обойти препятствия. Поэтому такого рода политики, не подкрепленные техническими средствами контроля за их выполнением, постепенно теряют силу. Программные системы, ориентированные на фильтрацию почты, следует позиционировать именно как инструмент для внедрения и контроля исполнения этих правил.

Таким образом, *политика использования электронной почты — это закрепленные в письменном виде и доведенные до сотрудников инструкции и другие документы, которые регламентируют их деятельность и процессы, связанные с использованием системы электронной почты.* Данные документы и инструкции обладают юридическим статусом и, как правило, предоставляются для ознакомления сотрудникам организации.

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности и неотделима от нее.

Политика должна соответствовать следующим критериям:

- Быть лаконично изложенной и понятной всем сотрудникам компании, простота написания не должна привести к потере юридического статуса документа;
- Исходить из необходимости защиты информации в процессе экономической деятельности компании;
- Быть согласованной с другими организационными политиками компании (регламентирующими финансовую, экономическую, юридическую и другие сферы деятельности компании);
- Иметь законную силу, т.е. политика, как документ, должна быть одобрена и подписана всеми должностными лицами руководящего звена компании, а ее выполнение должно быть детально продумано;
- Не противоречить федеральным и местным законам;
- Определять меры воздействия на сотрудников, нарушивших положения данной политики;
- Соблюдать баланс между степенью защищенности информации и продуктивностью деятельности компании;
- Детально определять мероприятия по обеспечению политики использования электронной почты в компании.

Политика использования электронной почты, как правило, рассматривается с двух сторон — как официально оформленный юридический документ и как материал, который описывает технику реализации политики.

Как документ она должна включать:

1. Положение, что электронная почта является собственностью компании и может быть использована только в рабочих целях.

2. Указание на то, что применение корпоративной системы электронной почты не должно противоречить законодательству РФ и положениям политики безопасности.
3. Инструкции и рекомендации по использованию и хранению электронной почты.
4. Предупреждение о потенциальной ответственности сотрудников компании за злоупотребления при использовании электронной почты в личных целях и возможном использовании электронной почты в судебных и служебных разбирательствах.
5. Письменное подтверждение того, что сотрудники компании ознакомлены с политикой использования электронной почты и согласны с ее положениями.

С технической точки зрения политика устанавливает правила использования электронной почты, то есть определяет следующее:

Что контролируется	Прохождение *каких* сообщений входящей, исходящей или внутренней электронной почты должно быть разрешено или запрещено.
На кого распространяется	*Категории лиц*, которым разрешено или запрещено отправлять исходящие или получать входящие сообщения электронной почты.
Как реагирует система	*Что необходимо делать* с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты.

Средства реализации политики использования электронной почты

Внедрение политики использования электронной почты требует от руководства компании понимания, что наличие только документально оформленной политики не гарантирует ее выполнения. Необходимо создание в компании соответствующих условий реализации данной политики. При этом важнейшим условием является наличие в корпоративной сети программно-технических средств контроля выполнения положений и требований политики. К таким средствам относятся системы контроля содержимого электронной почты.

Системы контроля содержимого электронной почты — это программное обеспечение, способное анализировать содержание письма по различным компонентам и структуре в целях реализации политики использования электронной почты.

К особенностям данных продуктов относятся:

1. Применение при анализе содержания специально разработанной политики использования электронных писем.
2. Способность осуществлять «рекурсивную декомпозицию» электронных писем.
3. Возможность распознавания реальных форматов файлов вне зависимости от различных способов их маскировки (искажение расширения файлов, архивирование файлов и т.п.).
4. Анализ множества параметров сообщения электронной почты.
5. Ведение архива электронной почты
6. Анализ содержимого сообщения электронной почты и прикрепленных файлов на наличие запрещенных к использованию слов и выражений.

Требования к системам контроля содержимого электронной почты

Спектр возможностей всех категорий систем контроля содержимого электронной почты достаточно широк и существенно меняется в зависимости от производителя. Однако ко всем системам предъявляются наиболее общие требования, которые позволяют решать задачи, связанные с контролем почтового трафика.

Самыми первыми требованиями к таким системам должны быть полнота и адекватность.

Полнота — это способность систем контроля обеспечить наиболее глубокую проверку сообщений электронной почты. Это предполагает, что фильтрация должна производиться по всем компонентам письма. При этом ни один из объектов, входящих в структуру электронного сообщения, не должен быть «оставлен без внимания». Условия проверки писем должны учитывать все проблемы, риски и угрозы, которые могут существовать в организации, использующей систему электронной почты.

Адекватность — это способность систем контроля содержимого как можно более полно воплощать словесно сформулированную политику использования электронной почты, иметь все необходимые средства реализации написанных людьми правил в понятные системе условия фильтрации.

К другим наиболее общим требованиям относятся:

- *Текстовый анализ электронной почты* (анализ ключевых слов и выражений с помощью встроенных словарей). Данная возможность позволяет обнаружить и своевременно предотвратить утечку конфиденциальной информации, установить наличие непристойного или запрещенного содержания, остановить рассылку спама, а также передачу других материалов, запрещенных политикой безопас-

ности. При этом качественный анализ текста должен предполагать морфологический анализ слов, то есть система должна иметь возможность генерировать и определять всевозможные грамматические конструкции слова. Эта функция приобретает большое значение в связи с особенностями русского языка, в котором слова имеют сложные грамматические конструкции.

- *Контроль отправителей и получателей сообщений электронной почты.* Данная возможность позволяет фильтровать почтовый трафик, тем самым реализуя некоторые функции межсетевого экрана в почтовой системе.
- *Разбор электронных писем на составляющие их компоненты* (MIME-заголовки, тело письма, прикрепленные файлы и т.п.), устранение «опасных» вложений и последующий сбор компонентов письма воедино, причем с возможностью добавлять к сообщению электронной почты необходимые для администраторов безопасности элементы (например, предупреждения о наличии вирусов или «запрещенного» текста в содержании письма).
- *Блокировка или задержка сообщений большого размера* до того момента, когда канал связи будет менее всего загружен (например, в нерабочее время). Циркуляция в почтовой сети компании таких сообщений может привести к перегрузке сети, а блокировка или отложенная доставка позволит этого избежать.
- *Распознавание графических, видео и звуковых файлов*. Как правило, такие файлы имеют большой размер, и их циркуляция может привести к потере производительности сетевых ресурсов. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы компании.
- *Обработка сжатых/архивных файлов*. Это дает возможность проверять сжатые файлы на содержание в них запрещенных материалов.
- *Распознавание исполняемых файлов*. Как правило, такие файлы имеют большой размер и редко имеют отношение к коммерческой деятельности компании. Кроме того, исполняемые файлы являются основным источником заражения вирусами, передаваемыми с электронной почтой. Поэтому способность распознавать и задерживать данные типы файлов позволяет предотвратить снижение эффективности работы компании и избежать заражения системы.
- *Контроль и блокирование спама*. Циркуляция спама приводит к перегрузке сети и потере рабочего времени сотрудников. Функция контроля и блокирования спама позволяет сберечь сетевые ресурсы и предотвратить снижение эффективности работы компании. Основными способами защиты от спама являются: проверка имен доменов и IP-адресов источников рассылки спама по спискам, запрос на указанный адрес отправителя (блокировка в случае отсутствия ответа), текстовый анализ спам-сообщения на наличие характерных слов и выражений в заголовках электронной почты (from/subject), проверка заголовков на соответствие спецификации RFC-822 и т.п.
- *Способность определять число вложений в сообщениях электронной почты*. Пересылка электронного письма с большим количеством вложений может привести к перегрузке сети, поэтому контроль за соблюдением определенных политикой информационной безопасности ограничений на количество вложений обеспечивает сохранение ресурсов корпоративной сети.
- *Контроль и блокирование программ-закладок* (cookies), вредоносного мобильного кода (Java, ActiveX, JavaScript, VBScript и т.д.), а также файлов, осуществляющих автоматическую рассылку (так называемые «Automatic Mailto»). Эти виды вложений являются крайне опасными и приводят к утечке информации из корпоративной сети.
- *Категоризация ресурсов почтовой системы компании* («административный», «отдел кадров», «финансы» и т.д.) и разграничение доступа сотрудников компании к различным категориям ресурсов сети (в т.ч. и в зависимости от времени суток).
- *Реализация различных вариантов реагирования*, в том числе: удаление или временная блокировка сообщения; задержка сообщения и помещение его в карантин для последующего анализа; «лечение» зараженного вирусом файла; уведомление администратора безопасности или любого другого адресата о нарушении политики безопасности и т.п.
- *Возможность модификации данных*, которая предусматривает, например, удаление неприемлемых вложений и замену их на тексты заданного содержания. Такая возможность позволит администратору удалять из писем прикрепленные файлы, тип которых запрещен политикой безопасности компании. К таким типам могут относиться исполняемые, видео и звуковые файлы, не имеющие отношения к деятельности компании. А это, в конечном итоге, позволит избежать заражения сети вирусами и добиться от сотрудников продуктивного использования почтового сервиса.

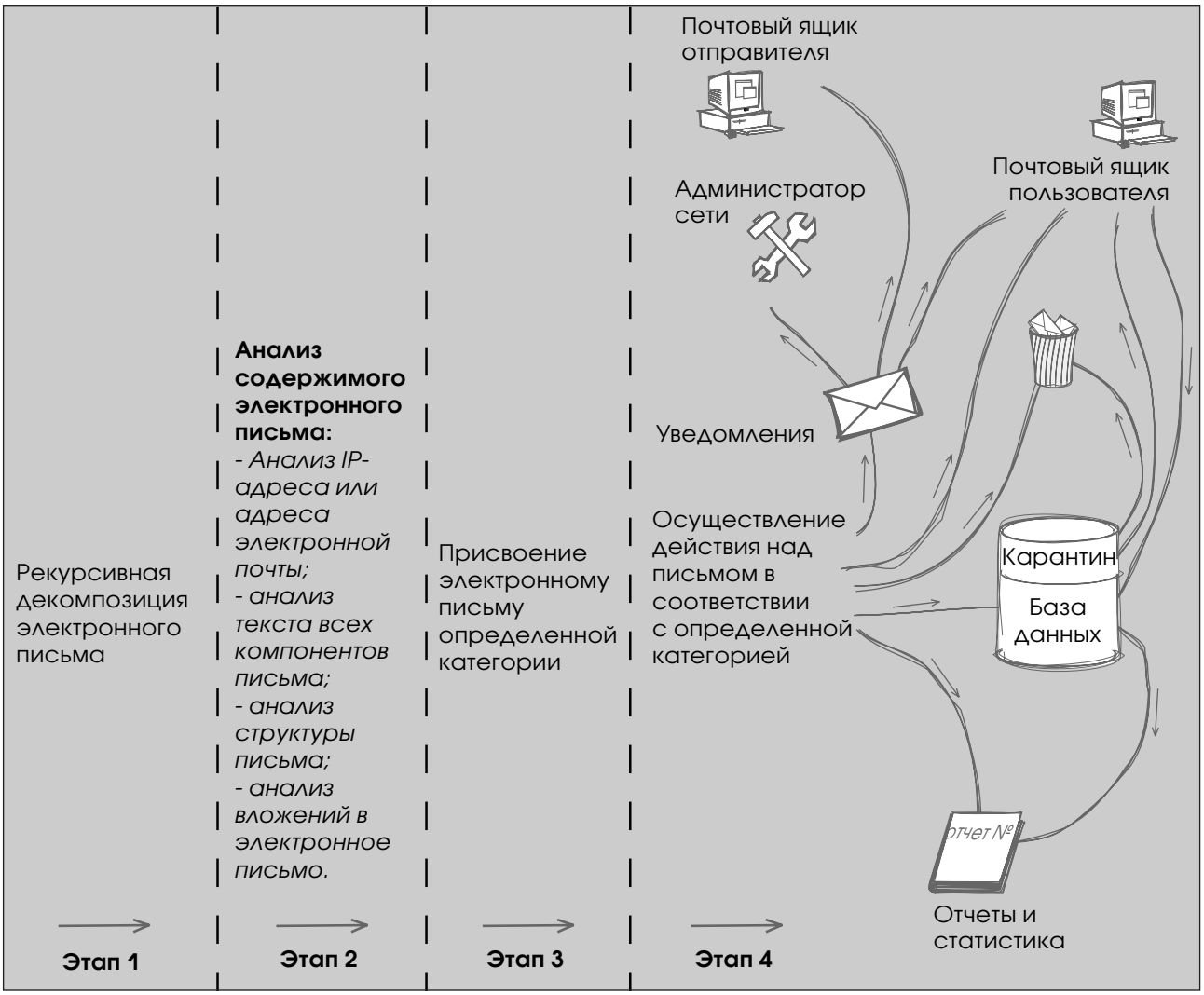

Рис. 4. Схема обработки сообщения системой контроля содержимого электронной почты.

- *Ведение полнофункционального архива электронной почты*, способного обеспечить хранение в режиме on-line большого количества электронной почты с высоким уровнем доступности данных. На основании хранящейся в архиве информации, возможно проводить дальнейший анализ почтового потока компании, корректировать работу системы, осуществлять анализ инцидентов, связанный с злоупотреблением сотрудниками компании почтовым сервисом и т.п.

На рис. 4 представлена последовательность работы типичной системы контроля содержимого электронной почты. Схема обработки сообщения, как правило, включает в себя следующие этапы: рекурсивная декомпозиция электронного письма; анализ содержимого электронного письма; «категоризация» электронного письма (отнесение к определенной категории); действие над письмом по результатам присвоения категории.

Какую систему выбрать?

Рынок систем контроля содержимого электронной почты сравнительно молодой, однако в настоящее время решения с применением технологии контекстного анализа стали пользоваться большой популярностью среди заказчиков. Наличие спроса привело к тому, что на рынке появилось большое количество подобных средств. Сходные задачи породили сходную функциональность, и если читать описания этих продуктов, то все они похожи друг на друга, как близнецы. Попробуем разобраться, что нужно для того, чтобы продукт, выбранный для реализации задач, перечисленных в предыдущем разделе, не обманул ваших ожиданий.

Каждое попадающее в систему электронное письмо должно проверяться на соответствие заданным условиям. При этом, по меньшей мере, должны выполняться следующие условия отбора писем:

- Условия на почтовые заголовки;
- Условия на структуру письма (наличие, количество и структура вложений);

- Условия на типы вложений (MS Office, исполняемые, архивы и т.п.);
- Условия на содержимое (текст) писем и вложений;
- Условия на результат обработки письма.

Кроме того, система должна позволять анализировать почтовые сообщения по всем их составляющим: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам.

Вернемся опять к вопросу категоризации писем. Важно отметить, что гибкость при фильтрации почтовых сообщений особенно необходима, когда это касается такой проблемы, как спам. Одним из главных критериев выбора системы контроля содержимого электронной почты в настоящее время является как раз ее способность как можно более качественно справляться с данной проблемой. Существует четыре основные методики определения, какое письмо относится к спаму, а какое нет. Первая методика используется в антиспамных фильтрах, реализующих способ выявления спама по наличию в письме определенных признаков, таких как наличие ключевых слов или словосочетаний, характерное написание темы письма (например, все заглавные буквы и большое количество восклицательных знаков), а также специфическая адресная информация.

Вторая методика связана с определением адреса отправителя и его принадлежности к, так называемым, «черным спискам» почтовых серверов Open Relay Black List (ORBL). В эти списки заносятся те серверы, которые замечены в массовых рассылках спама и идея состоит в том, чтобы вообще не принимать и не транслировать почту, исходящую с этих серверов.

Третья методика включает обе перечисленные, но по продуктивности мало чем отличается от двух первых. Результаты тестирования хорошо настроенного фильтра с применением обеих методик показывают, что из 100% спам-сообщений обнаруживается только 79,7%. При этом был выявлен значительный процент ложных срабатываний, а это значит, что к спаму были отнесены обычные письма (1,2% от задержанных писем). В данном случае это грозит для компании потерей важной информации. Некачественное разделение спама и обычных писем обусловлено, в том числе и некоторой «однобокостью» стандартных фильтров. При отбраковке писем учитываются «плохие» признаки и не учитываются «хорошие», характерные для полезной переписки.

Этих недостатков лишена четвертая методика, предложенная американским программистом и предпринимателем Полом Грэмом. Она позволяет автоматически настроить фильтры согласно особенностям индивидуальной переписки, а при обработке учитывает признаки как «плохих», так и «хороших» фильтров.

Методика основывается на теории вероятностей и использует для фильтрации спама статистический алгоритм Байеса. По имеющимся оценкам, этот метод борьбы со спамом является весьма эффективным. Так, в процессе испытания через фильтр были пропущены 8000 писем, половина из которых являлась спамом. В результате система не смогла распознать лишь 0,5% спам-сообщений, а количество ошибочных срабатываний фильтра оказалось нулевым.

Таким образом, системы контроля содержимого электронной почты, которые в своем составе имеют модули фильтрации спама, основанные на методике Пола Грэма, являются в настоящее время наиболее эффективными и отвечающими современным требованиям по борьбе с рассылками рекламного характера. А это в конечном итоге и будет являться еще одним критерием при выборе системы контроля содержимого электронной почты.

Требование полного разбора письма следует дополнить требованием устойчивости. Во-первых, структура письма подчиняется определенным правилам. Разбор письма на составляющие основан на применении этих правил к конкретному письму. Вообще говоря, возможны случаи, когда почтовая программа автора письма формирует письмо с нарушением этих правил. В этом случае письмо не может быть корректно разобрано. Система должна быть устойчивой по отношению к обработке таких писем.

Во-вторых, система должна надежно определять типы файлов-вложений. Под «надежностью» имеется в виду определение, не основанное на имени файла, а также на информации, вписываемой в письмо почтовым клиентом при прикреплении файла (mime-type). Такая информация может быть недостоверна либо в результате сознательных попыток обмануть систему контроля, либо в результате неправильных настроек почтовой программы отправителя. Бессмысленно запрещать пересылку файлов типа JPEG, если файл picture.jpg после переименования в page.txt пройдет незамеченным.

В-третьих, большое значение для системы имеет полнота проводимых проверок, то есть количество и разнообразие критериев анализа электронной почты. При этом система должна осуществлять фильтрацию по любым атрибутам сообщений, по объему сообщений и вложенных файлов, по количеству и типу вложений, по глубине вложенности, а также уметь анализировать содержимое прикрепленных файлов вне зависимости от того, являются ли эти файлы сжатыми или архивными. Суще-

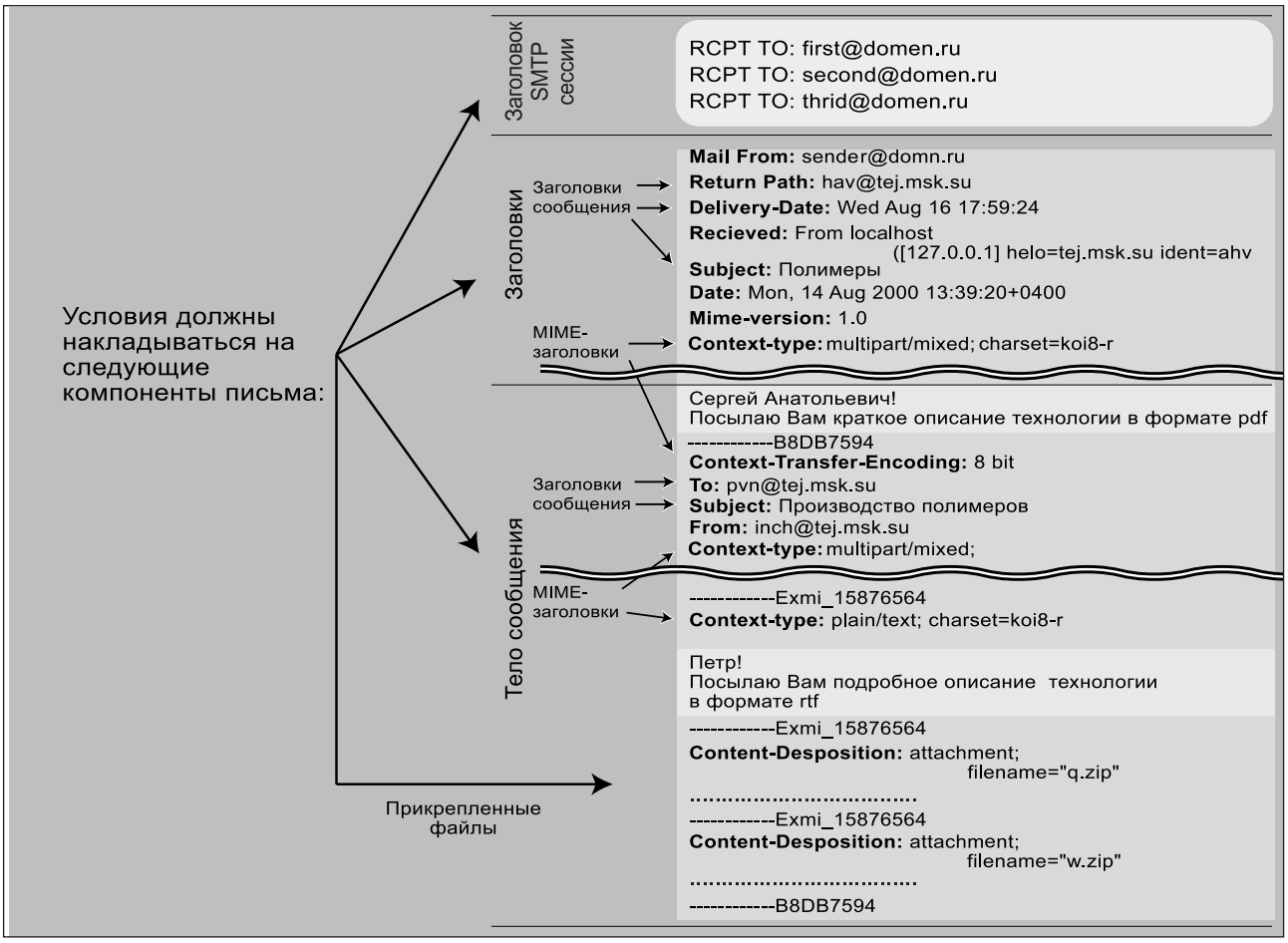

Рис. 5. Фильтрация по всем компонентам письма.

ственным преимуществом многих продуктов является возможность создания собственного сценария обработки сообщений электронной почты.

При анализе текста нужно иметь возможность работать с нормализованными словоформами и т.д.

Теперь поговорим немного не об отдельных правилах, а обо всем множестве правил, составляющих политику. Любая реалистичная политика состоит из целого множества правил, которые, естественно, объединяются в группы. Очевидно, что правила для исходящей почты отличаются от правил для входящей, правила для руководства компании — от правил для рядовых сотрудников и т.д. Более того, поскольку правила применяются к письму в определенной последовательности, хотелось бы, чтобы эта последовательность была логичной и могла зависеть от результатов анализа письма. Все это вместе приводит к требованию «прозрачности»: правила, заданные в системе, должны «читаться» как правила, написанные на естественном языке, понятном человеку.

Все сказанное выше относилось к анализу письма. Однако сам по себе анализ ничего не дает. По его результатам письмо должно быть отнесено к какой-нибудь категории (безопасное, важное, неразрешенное и т.п.). Если такая категоризация проведена, то можно говорить о каких-либо действиях по отношению к проанализированному письму, например, доставить его адресату, заблокировать, и т.д. Другими словами, необходима возможность задавать системе правила, по которым она обрабатывает письма.

Любое правило можно представить себе как связку «условие + действие». Какие же действия нужны для того, чтобы обеспечить реализацию разумной политики?

Во-первых, само по себе отнесение письма к определенной категории уже может рассматриваться как неявное действие. На этом действии следует остановиться подробнее. Дело в том, что жесткая категоризация как основа для принятия решений по электронному письму оказывается весьма непрактичной. Действительно, пусть мы выделили категорию писем «письмо, отправленное на запрещенный адрес» для того, чтобы блокировать доставку. С другой стороны, у нас может быть категория «письма руководства компании», которые надо отправлять безусловно. Что делать с письмом президента, отправленным по «запрещенному» адресу? Здравый смысл подсказывает, что приоритет

должен быть отдан категории «письма руководства компании», что ,безусловно, и будет сделано в системе с жесткой категоризацией. Однако будет потеряна существенная информация о письме. Разумный выход из таких ситуаций заключается в возможности относить письма сразу к нескольким категориям. Такая "свободная категоризация" позволит системе гибко реагировать на самые различные комбинации данных, содержащихся в письмах.

Что касается последнего, то необходимо отметить, что мощность и гибкость реагирования системы по результатам анализа содержимого электронной почты является в настоящее время наиболее важным критерием оценки описываемых средств. Нет нужды говорить о том, что при оценке необходимо учитывать разнообразие вариантов действий, осуществляемых по результатам проверок. Системы контроля содержимого электронной почты должны иметь возможность блокировать (совсем или на время) доставку писем, помещать письма в карантинную зону для последующего их анализа, посылать уведомления администратору или другим адресатам о событиях, происходящих в системе и т.п. На рис. 6 показана схема действий, поддерживаемых правилами фильтрации почтовых сообщений типичной системы контроля содержимого электронной почты.

В последнее время большое значение для обеспечения безопасности информационных систем приобрело наличие в компании архива почтовых сообщений. Некоторые разработчики систем контекстного анализа предусматривают прикрепление к своим продуктам специальных модулей архивирования. Именно наличие архива электронной почты и определяет в настоящее время полнофункциональность продуктов этой категории. При этом ведение архива — это не просто автоматическая архивация почтовых сообщений в файл, а способность регистрации сообщений и учета необходимой информации на протяжении всего жизненного цикла сообщения, возможность получения любых выборок и статистики из архива по запросам, созданным с использованием любых критериев.

Кроме того долговременный архив предоставляет возможность ретроспективного анализа почтовых потоков и не только позволяет найти виновных в нарушении принятых в компании правил по прошествии определенного времени, но и дает материал для построения объективной и обоснованной политики использования электронной почты.

Отличительным признаком средств контекстного анализа является способность накопления статистики и генерации отчетов. Многие продукты имеют в своем арсенале только встроенные формы отчетов, другие способны осуществлять только просмотр статистики работы конкретного пользователя системы электронной почты. На наш взгляд, наиболее совершенными являются системы, которые способны обеспечить получение любых выборок и статистики из архива по создаваемым запросам, создание специфических запросов на SQL, генерацию любых видов отчетов для анализа эффективности использования почтового сервиса компании.

Одним из основных критериев оценки систем контекстного анализа для российского рынка является поддержка продуктом различных кодировок кириллицы (CP1251, CP866, ISO8859-5, KOI8-R, MAC), что дает возможность анализа русскоязычных текстов. Большинство продуктов иностранного производства не способны обеспечить поддержку кодировок кириллицы, а это в значительной степени снижает возможность их использования на территории РФ. Кроме того, проклятие множественных кодировок тяготеет и над российскими информационными системами. Все осложняется тем, что разные части письма, включая почтовые заголовки, могут быть написаны в разных кодировках. Вдобавок эти кодировки не всегда указаны или не всегда указаны верно.

Теперь рассмотрим вопрос, касающийся архитектуры систем контроля содержимого электронной почты. В подобных продуктах уникальной особенностью является открытая архитектура, которая позволяет разработчикам расширять функциональные возможности системы, интегрируя в нее дополнительные модули и не затрагивая ее ядра. Это дает возможность постоянно наращивать способности системы контроля содержимого по защите электронной почты и одновременно с этим экономить значительные средства, которые могут потребоваться на модернизацию всей системы. Кроме того возможность добавлять модули к базовой системе без внесения каких-либо структурных изменений позволяет оперативно решать постоянно возникающие проблемы, связанные с возникновением новых угроз безопасности систем электронной почты.

В настоящее время на рынке информационной безопасности существуют несколько систем контроля содержимого электронной почты с открытой архитектурой. В стандартный комплект поставки таких систем, как правило, входят несколько модулей, каждый из которых позволяет обеспечить защиту от определенного вида угроз или решает отдельную задачу безопасности функционирования системы электронной почты. Так, например, в состав системы может входить модуль электронно-цифровой подписи и шифрования, который обеспечивает конфиденциальность и кон-

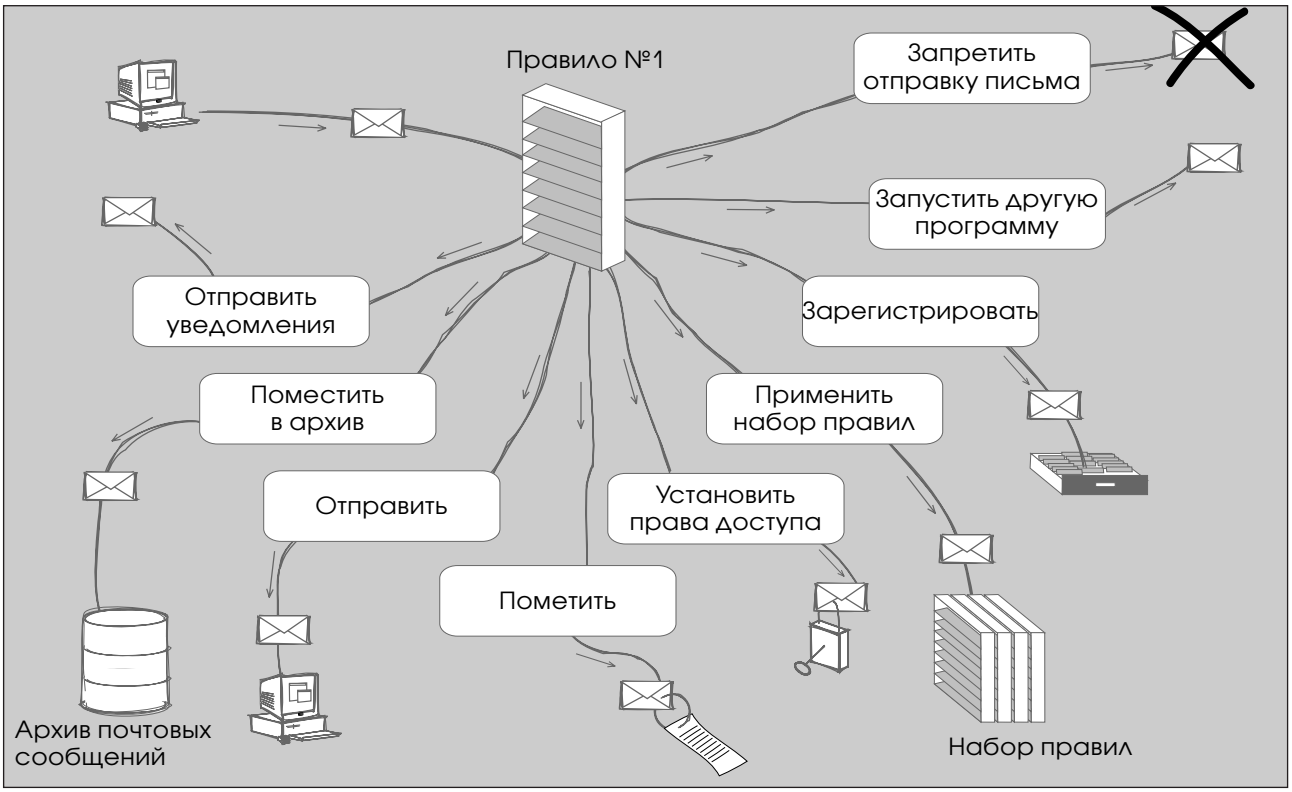

Рис. 6. Схема реагирования типичной системы контроля содержимого электронной почты.

троль целостности информации, пересылаемой по электронной почте.

Большое значение для систем контроля содержимого имеет удобство администрирования системы, что предполагает наличие русскоязычного интерфейса, возможность разделения функций управления и администрирования системы, то есть разграничения доступа различных категорий пользователей к средствам управления системой.

И наконец необходимо сказать о важности сертификации средств контроля содержимого электронной почты Гостехкомиссией РФ. Во-первых, потому что при проведении испытаний того или иного продукта Гостехкомиссия подтверждает его соответствие определенным техническим условиям, а это является подтверждением качества данного продукта. И во-вторых, сертификация позволяет использовать продукт в государственных структурах, где наличие сертификата является обязательным требованием.

Сравнительный анализ систем «Дозор-Джет» и MAILsweeper.

Анализ рынка программного обеспечения в области информационной безопасности и сравнение его функциональных возможностей показывает, что среди представленных в настоящее время на российском рынке продуктов наиболее полнофункциональными и отвечающими современным требованиям являются система мониторинга и архивирования электронной почты «Дозор-Джет», компании «Инфосистемы Джет» (Россия) и MAILsweeper, компании «ClearSwift» (Великобритания).

«Дозор-Джет» и MAILsweeper являются программными продуктами, которые имеют общий набор функциональных возможностей, позволяющих отнести их к одному классу средств защиты информации. Такими возможностями являются:

1. Фильтрация электронных писем на основе анализа их содержимого.
2. Применение при анализе технологии рекурсивной декомпозиции, т.е. разбора электронных писем на составляющие его компоненты (заголовки письма, MIME-заголовки, тело письма, прикрепленные файлы и т.п.),
3. Применение специальных методов оценки при анализе содержимого.
4. Осуществление определенных действий над письмом по результатам такого анализа.

В качестве критериев сравнения систем выбраны следующие:

- гибкость в применении правил обработки писем, т.е. способность систем применять различные правила обработки к одному и тому же письму, присваивать ему различные категории, а также осуществлять различные действия по результатам обработки;
- глубина проводимого анализа сообщений, то есть количество и разнообразие критериев оценки, глубина проводимых проверок;

- способность системы адекватно реагировать на те или иные события, то есть применять разнообразные действия по результатам анализа содержимого электронной почты.

Применение вышеуказанных критериев позволило специалистам компании «Инфосистемы Джет» оценить системы «Дозор-Джет» и MAILsweeper и определить их соответствие требованиям, которые предъявляются в настоящее время к системам контроля содержимого электронной почты. Данное сравнение в дальнейшем поможет Заказчикам определиться в выборе продукта безопасности, который будет подходить для той или иной информационной системы (см. таблицу сравнения основных характеристик систем «Дозор-Джет» и Mailsweeper).

«Дозор-Джет» можно отнести к системам промышленного уровня за счет того, что продукт функционирует на UNIX-платформе и включает в свой состав подсистему архивирования, реализованную на основе СУБД Oracle. Система «Дозор-Джет» используется в организациях, объем почтового трафика которых достигает 5 гигабайт в день, а количество почтовых адресов превышает 5000. Это, в свою очередь, требует применения аппаратных средств, которые способны обеспечить высокую производительность и отказоустойчивость системы.

Система MAILsweeper устанавливается на серверы под управлением операционной системы MS Windows NT или Windows 2000. MAILsweeper не использует в своем составе подсистем хранения информации промышленного уровня.

«Дозор-Джет» имеет мощную систему фильтрации сообщений, которая позволяет реализовать политику использования электронной почты практически любого уровня сложности. При этом фильтрация осуществляется по всем компонентам письма: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам. Расширяемый набор проверок и действий позволяет администратору системы создавать собственные методы проверки сообщений и вложений и осуществлять различные действия над ними. Почта фильтруется на основании практически любых условий. Последовательность применения правил фильтрации в системе динамическая, что подразумевает применение любых наборов правил в заданной администратором безопасности последовательности.

В отличие от «Дозор-Джет», в MAILsweeper правила применяются в строго определенной последовательности в соответствии с их приоритетностью и иерархией проводимых проверок. Почта в MAILsweeper разделяется на потоки только на основании почтовых адресов. Кроме того, MAILsweeper не имеет возможности продолжить применение правила после выполнения текущего правила или применить другой набор правил.

В рассматриваемых системах различается подход к категоризации сообщений. Так «Дозор-Джет» имеет систему категоризации писем, которая позволяет относить одно сообщение электронной почты сразу к нескольким смысловым категориям. Работа категоризатора основана на простой, но весьма эффективной технологии Байесовских фильтров, одинаково хорошо работающей как с русским, так и с английским языком. Автоматическая корректировка категоризатора в значительной степени повышает эффективность подсистемы фильтрации и дает возможность избежать ложных срабатываний при блокировке «запрещенных» писем.

В MAILsweeper категоризация осуществляется только на основе лексического анализа (совпадения слов и выражений) и «веса» слова (частоты употребления в тексте), что не обеспечивает хорошую защиту от ложных срабатываний, а следовательно, может привести к потере нужной информации.

Работа с текстами писем в «Дозор-Джет» включает в себя морфологический анализ слов, что позволяет искать все словоформы для данного слова. В MAILsweeper такой анализ отсутствует. Эта функция приобретает еще большее значение в связи с особенностями русского языка, в котором слова имеют сложные грамматические конструкции.

В состав «Дозор-Джет» входит подсистема архивирования промышленного уровня, реализованная на основе СУБД Oracle. Архив обеспечивает хранение в режиме on-line большого количества корпоративной электронной почты с высоким уровнем доступности данных и долговременное хранение сообщений в течение десяти лет и более. Архив предоставляет широкий спектр возможностей по хранению и поиску писем. Следует отметить такие возможности как контекстный поиск по архиву, поиск по архиву с учетом морфологического строения русского языка, разделение архива на исторические области (Partitioning), экспорт электронной почты на внешние носители.

MAILsweeper не имеет в своем составе архива электронной почты. Система производит архивацию сообщений в виде файла. В архив письмо помещается целиком. «Дозор-Джет» предоставляет возможность регистрации электронных писем. Регистрация означает сохранение в базе данных только информации об определенных заголовках электронного письма (автор, адресат, размер и т.п.) и его MIME-структуре. Регистрация, в отличие от сохранения всего письма, дает возможность эконо-

мить пространство на дисковых массивах и ускорить поиск необходимой информации.

Говоря об архиве электронной почты, важно отметить, что в арсенале компании «ClearSwift» есть специально разработанный для MAILsweeper модуль, который называется Archivist. Данный модуль предназначен только для поиска необходимого почтового сообщения в архиве электронной почты по следующим атрибутам: адресат, получатель, тема письма, дата получения/отправки, наименование файлов-приложений.

Система «Дозор-Джет» имеет широкие возможности по генерации отчетов. Благодаря наличию архива, система способна получать выборки любой сложности по создаваемым запросам (создание специфических запросов на SQL, возможность генерации любых видов отчетов с помощью Oracle Report, Crystal Report). В архиве системы находится вся «учетная» информация о письмах (заголовки, типы вложений, их размеры и т.п.), что позволяет получать отчеты по самым разным параметрам почтового трафика. Дополнительный модуль «Статистика» содержит набор отчетов, представленных в формате MS Excel.

MAILsweeper осуществляет построение отчетов только при помощи Crystal Report. При этом для создания отчетов обязательно наличие Microsoft SQL server.

Благодаря технологии эвристического определения кодировки система «Дозор-Джет» способна осуществлять анализ русскоязычных почтовых сообщений независимо от используемой кодировки кириллицы (CP1251, CP866, ISO8859-5, KOI8-R, MAC), включая тексты, кодировка которых не указана (например, тестовые файлы в сжатых форматах) или декларирована неверно. Также определяется кодировка текстов, находящихся внутри архивированных файлов.

MAILsweeper не способен гарантированно осуществлять обработку текстов сообщений электронной почты, кодировка которых не декларирована (например, тестовые файлы в сжатых форматах) или декларирована неверно, поскольку кодировка определяется только по MIME-заголовкам.

«Дозор-Джет» имеет модульную структуру, которая позволяет добавлять в систему дополнительные функциональные возможности, не затрагивая его ядра. Это дает возможность подключать к системе внешние программы, которые предназначены для дополнительной обработки электронных писем, что расширяет функциональные возможности «Дозор-Джет». Таким образом, продукт способен интегрироваться с системами документооборота, различными подсистемами информационной безопасности (межсетевыми экранами, средствами создания виртуальных защищенных сетей, антивирусами, системами электронной цифровой подписи и т.д.) и системами управления корпоративными информационными ресурсами (HP OpenView). Всего в составе «Дозор-Джет» имеется девять различных модулей. Кроме того, в «Дозор-Джет» существует возможность вызова внешних программ (программ третьих производителей), что позволяет осуществлять дополнительную обработку электронных писем.

MAILsweeper имеет в своем составе только один модуль Archivist, предназначенный для работы с архивом электронной почты. Кроме того, система (так же как и в «Дозор-Джет») имеет возможность вызова внешних программ.

Продолжая тему модульности системы, отметим, что «Дозор-Джет» имеет в своем составе специальный модуль проверки и постановки ЭЦП, при активации которого система получает возможность обеспечивать контроль целостности, пересылаемой по электронной почте информации. Кроме того, «Дозор-Джет» имеет возможность автоматически шифровать исходящие сообщения в формате S/MIME.

В отличие от «Дозор-Джет», система MAILsweeper способна только определять наличие ЭЦП в письме, но не имеет возможности шифровать сообщения, а также проверять подлинность и ставить электронно-цифровую подпись.

«Дозор-Джет» является единственным сертифицированным продуктом на рынке систем контроля содержимого электронной почты. Гостехкомиссия России провела испытания системы «Дозор-Джет» и признала ее соответствие техническим условиям 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 № 465 от 14.06.2001. MAILsweeper является продуктом, применение которого на территории Российской Федерации не сертифицировано соответствующими органами.

И наконец, «Дозор-Джет» является отечественной разработкой. Компания «Инфосистемы Джет» предоставляет своим клиентам техническую поддержку любого уровня непосредственно от производителя. Это дает возможность оперативного решения любых проблем, связанных с функционированием системы. Компания «ClearSwift» предоставляет техническую поддержку только через сертифицированных партнеров на территории России (НИП «Информзащита»).

	«Дозор-Джет»	MAILsweeper для SMTP
Версия	2.6	4.3
Платформа	UNIX	Windows
Используемые процессоры	SPARC/PA-RISC/Intel	Семейство Intel
Операционная система	Sun Solaris, HP-UX, Linux	Windows 2000/NT
Интерфейс управления	Web-навигатор	Графический, с использованием Microsoft Management Console
Система обработки электронной почты	Последовательность применения правил определяется динамически Расширяемый набор проверок и действий Первое применяемое правило создается на основании любых условий К одному письму может применяться несколько правил	Правила применяются в строго определенной последовательности в соответствии с их приоритетностью и иерархией проводимых проверок Расширяемый набор действий Первое применяемое правило фильтрует сообщения на основании почтовых адресов Не имеет возможности продолжить применение правил после выполнения текущего правила или применить другой набор правил
Анализ текстов	Возможность поиска слов с учетом словообразования (как английского, так и русского) Полнофункциональные регулярные выражения	Совпадение слов и строк Ограниченное подмножество регулярных выражений
Категоризация сообщений	Адаптивная система категоризации, основанная на Байесовских фильтрах Автоматическая корректировка категоризатора	Категоризация на основе лексического анализа (совпадения слов и выражений) и «веса» слова (частотности употребления в тексте)
Действия по результатам обработки сообщения	Блокировать Отправить уведомление Зарегистрировать Поместить в архив Применить набор правил Доставить Установить права доступа Пометить Запустить внешнюю программу Переслать на определенный адрес	Блокировать Отправить уведомление Поместить в карантин Доставить Доставить в соответствии с расписанием Переслать на определенный адрес Копировать в архивный файл Запустить внешнюю программу
Модификация данных	Удаление вложения определенного типа Включение в тело письма определенного текста взамен удаленного вложения	Удаление вложения определенного типа Включение в тело письма определенного текста (bisclamer или legal bisclamer)
Проверка сообщений на вирусы	Средствами третьих производителей Наличие интерфейса для антивирусных программ Реализован унифицированный интерфейс к антивирусам: • Symantec Anti-Virus (Symantec) • AVP (Лаборатория Касперского) • Dr.Web (Диалог-Наука)	Средствами третьих производителей • Command Interceptor (Command Software Systems) • VetNT (Computer Associates • FPROT (Frisk==F-Secure Anti-Virus, компании F-Secure) • SAVAPI (H+BEDV) • Command line (McAfee) • Norman Virus Control (Norman) • TBA и Sophos Anti-Virus (Sophos) • Symantec Anti-Virus (Symantec)
Архив сообщений	Реализован на основе СУБД Oracle или PostgreSQL (для Lite-версии) Помещение писем в архив по любым критериям Помещение в архив всего письма или его регистрационной информации	Архивация в виде файлов Архивирование в директорию или на определенный адрес в сети Архивирование только всего письма
Контекстный поиск по архиву	Имеет модуль контекстного поиска в архиве электронной почты Также осуществляется по текстам вложенных файлов	Реализуется только дополнительно установленным модулем Archivist, который использует Indexing Service, входящий в состав Windows 2000/NT
Атрибутивный поиск по архиву	По любым атрибутам письма	• по адресату/получателю • теме письма • дате получения/отправки • наименованию файлов-приложений
Морфологический поиск по архиву	Имеет модуль поиска по архиву с учетом морфологического строения русского языка	Не имеет

Таблица сравнения основных характеристик систем «Дозор-Джет» и Mailsweeper

Возможность долговременного архива электронной почты	Имеет модуль разделения архива на исторические области (Partitioning)	Не имеет
Генерация отчетов	• 2 типа встроенных отчетов по любым атрибутным и текстовым запросам • фиксированные отчеты в MS Excel • возможность построения отчетов пользователем с помощью стандартных средств (Crystal Report, Oracle Report)	Для построения отчетов требуется наличие Microsoft SQL server Построение отчетов при помощи Crystal Report
Определение кодировки	Эвристическое определение кодировки Анализ русскоязычных почтовых сообщений независимо от используемой кодировки кириллицы (CP1251, CP866, ISO8859-5, KOI-8R, MAC), включая тексты, кодировка которых не декларирована или декларирована неверно Определение кодировки в текстах внутри архивированных файлов	Определение кодировки по MIME-заголовку Не гарантированная обработка текстов сообщений, кодировка которых не декларирована (например, тестовые файлы в сжатых форматах) или декларирована неверно
Удобство управления и администрирования	Русскоязычный интерфейс Русскоязычная документация	Отсутствие русскоязычного интерфейса Отсутствие русскоязычной документации
Удаленное администрирование	Удаленное администрирование по протоколу SSL	Не имеет
Разграничение доступа	Собственные средства разграничения доступа различных категорий пользователей к средствам управления и различным объектам системы	Средствами Windows 2000/NT Контролируется доступ к: • сервисам создания базы данных правил • средствам запуска/остановки сервисов
Возможность подключения и наличие дополнительных модулей	Имеет девять различных модулей: • Модуль подключения ЭЦП • Модуль разделения архива на исторические области (Partitioning) • Модуль хранения архива электронной почты на внешних носителях • Модуль контекстного поиска в архиве почтовых сообщений • Модуль поиска по архиву с учетом морфологического строения русского языка • Модуль статистики и отчетов • Модуль взаимодействия с HP Open View • Модуль категоризации почтовых сообщений (антиспам) • Модуль доступа к архиву почтовых сообщений по протоколу IMAP4	Имеет только один модуль - Archivist для работы с архивом электронной почты
Возможность проверки и постановки ЭЦП	Имеет модуль проверки и постановки ЭЦП.	Не имеет
Возможность шифрования отдельного письма	Возможность автоматического шифрования исходящего сообщения	Не имеет
Фильтрация спама	На основе модуля категоризации сообщений Автоматизированная корректировка фильтров Использование для блокировки сообщений списков ORBL	На основе лексического анализа (наличие определенных слов и фраз, а также частота их повторения в тексте письма) Не использует при блокировке сообщений списков ORBL
Защита от атак типа «mail-bombs»	Осуществляется за счет ограничения объема временного каталога, который создается специально для анализа каждого письма	Не имеет
Мониторинг ресурсов системы	Встроенными средствами Осуществляется мониторинг: • Свободное место в спуле (Мб) • Свободное место в директории логов (Мб) • Свободное место во временной директории (Мб) • Количество временных директорий фильтра • Доступность сервера баз данных • Свободное место, доступное для базы данных (Мб)	Встроенными средствами осуществляется предупреждение администратора о превышении лимита времени на обработку сообщения (по умолчанию всегда 30 минут) При помощи Windows 2000 Performance Monitor осуществляется мониторинг: • Количество запрещенных сообщений • Наличие и количество активных сессий • Количество сообщений в папке «Проверено» • Количество обработанных сообщений • Количество сообщений, находящихся на обработке

Таблица сравнения основных характеристик систем «Дозор-Джет» и Mailsweeper (продолжение)

	• Наличие сервисов • Количество сообщений в спуле • Количество сообщений, обработка которых завершилась с ошибкой • Самое старое сообщение находится в спуле (мин) • Количество блокированных сообщений до применения правил • Средняя загрузка (за 5 мин)	• Количество модифицированных сообщений • Количество сообщений в папке «Не проверено» • Количество сообщений, помеченных как «подозрительные» • Количество активных соединений • Общее количество соединений • Количество соединений после последней перезагрузки системы • Объем полученных и отправленных сообщений (байт) • Общее количество полученных и отправленных сообщений
Сертификация	Сертификат № 465 от 14.06.2001 «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»	Не имеет
Предоставление услуг и техническая поддержка	Компания-разработчик предоставляет полный комплекс услуг и техническую поддержку	Только через сертифицированных партнеров на территории России (НИП «Информзащита»)

Таблица сравнения основных характеристик систем «Дозор-Джет» и Mailsweeper (продолжение)

Выводы

В настоящее время деятельность компаний все больше зависит от электронной почты. Удобство и практичность электронной почты очевидны. Однако нельзя не учитывать проблемы, которые возникают в связи с ее неконтролируемым использованием. Последствия для компаний могут быть непредсказуемыми. Сейчас существуют средства реализации серьезных преимуществ электронной почты, которые помогают устранить угрозы надежности, конфиденциальности и продуктивности организации — это системы контроля содержимого электронной почты. Сегодня популярность таких средств растет в геометрической прогрессии. По прогнозу компании International Data Corp., к 2003 г. около 3,9 млн. различных организаций будут применять программы мониторинга электронной почты.

Системы контроля электронной почты помимо основной своей задачи мониторинга почтового трафика способны выполнять и другие функции. Практика показала, что в настоящее время такие системы используются в качестве:

1. Средств управления почтовым потоком.
2. Средств управления доступом.
3. Средств администрирования и хранения электронной почты.
4. Средств аудита контента (важнейшую функцию которого осуществляет архив электронной почты).
5. Основы системы документооборота.

И в заключение хотелось бы отметить, что необходимость систем контроля содержимого электронной почты подтверждается «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации», разработанными Гостехкомиссией при Президенте РФ в 2001 г. (СТР-К). В статье 6.3.11.5 этого документа говорится: «В целях контроля за правомерностью использования абонентских пунктов и выявления нарушения требований по защите информации осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в т.ч. на наличие вирусов. Копии исходящей электронной почты и отсылаемых в Сеть файлов следует направлять в адрес защищенного архива абонентских пунктов для последующего анализа со стороны администратора (службы безопасности)».

Таким образом, все перечисленные выше факты еще раз подтверждают необходимость применения в системах безопасности корпоративных сетей систем контроля содержимого электронной почты, которые способны не только обеспечить защиту системы электронной почты и стать эффективным элементом управления почтовым потоком, но и значительно повысить эффективность деятельности предприятия или организации.

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

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**