Система хранения сообщений электронной почты SecurityMailArchive

Системы хранения сообщений электронной почты

В современном мире электронная почта (ЭП) является важнейшим инструментом обмена информацией как внутри организаций, так и между ними. По мнению аналитиков Gartner Group, почти 97% организаций поддерживают взаимную деловую активность с помощью электронной почты. Объём почтового трафика увеличивается из года в год, несмотря на широкое распространение альтернативных коммуникационных сервисов (системы мгновенного обмена сообщениями, web-конференции, блоги и др.). В крупных организациях ежедневный объем электронной почты может достигать сотни гигабайт и более. Согласно исследованию компании Osterman Research "Archiving Email for Compliance and Competitive Advantage" 73% пользователей электронной почты почти непрерывно в рабочее время проверяют наличие новых сообщений, 16% – несколько раз в час.

Многие IT-руководители российских предприятий каждый год ставят перед собой вопрос (или не ставят, но задумываются): решать или не решать проблему хранения (архивирования) сообщений электронной почты. В совместном исследовании агентства Cnews Analytics и компании InfoWatch "Архивирование корпоративной корреспонденции в российских компаниях", опубликованном в конце 2006 г., отмечается, что "лишь 14% респондентов применяют специализированные решения архивирования почтового трафика, в то время как 86% компаний просто закрывают глаза на проблему". На дворе 2009 год, но верится с трудом, что за текущий период на российских просторах произошло серьезное продвижение в освоении систем обработки и хранения электронной почты.

Основные движущие силы

Существует несколько причин, которые могут сдвинуть компании в сторону выбора и внедрения систем обработки и хранения электронной почты. К таковым можно отнести: непреодолимое желание повысить эффективность использования почтового трафика и разрешить проблему управления его распухающими объемами, необходимость расследования инцидентов, связанных с утечкой информации через электронную почту, требование предоставить деловую переписку в судебные инстанции, необходимость соответствия законодательным и нормативным требованиям и др.

В развитых зарубежных странах ключевым фактором активности рынка корпоративных систем обработки и архивирования данных (в том числе и сообщений электронной почты) является необходимость соответствия регламентирующим документам (законам, постановлениям, стандартам, отраслевым правилам). Среди множества нормативных актов обычно выделяют следующие базовые документы, содержащие различного рода требования по хранению данных:

- Соглашение International Convergence of Capital Measurement and Capital Standards, Basel Committee on Banking Supervision (июнь 2004);
- Закон SOX (Sarbanes-Oxley Act of 2002);
- Директива Евросоюза о сохранении данных Data Retention Directive;
- Закон HIPAA (Health Insurance Portability and Accountability Act of 1996);
- Правило 17a-4 Комиссии по ценным бумагам США.

В настоящее время зарубежный рынок систем обработки и архивирования электронной почты широко представлен продуктами различных производителей, например, Symantec Enterprise Vault, IBM Tivoli Storage Manager for Mail, EMC EmailXtender, GFI MailArchiver и др. Аналитики IDC прогнозируют среднегодовой рост мирового рынка решений для архивирования электронной почты на уровне 23%. По их мнению, к 2011 году рынок достигнет 1,4 млрд долл.

Большинство российских предприятий подобного нормативного давления не ощущают, пожалуй, за исключением:

- государственных органов, органов местного самоуправления муниципального района и городского округа, которые в соответствии с Федеральным законом "Об архивном деле в Российской Федерации" обязаны "создавать архивы в целях хранения, комплектования, учета и использования образовавшихся в процессе их деятельности архивных документов";
- организаций банковской системы РФ, в которых "электронная почта должна архивироваться" согласно п. 8.2.6.4 стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения";
- предприятий, осуществляющих международную деятельность и попадающих под действие иностранных законов.

Место системы обработки и хранения ЭП в корпоративной сети

Задачи, решаемые системой обработки и хранения почтовых сообщений, структура системы и её место в корпоративной вычислительной сети определяются принятой в организации политикой применения электронной почты.

Обычно системы, обеспечивающие безопасность корпоративной ЭП, реализуют следующие основные функции:

- автоматический захват всех входящих, исходящих и внутренних сообщений;
- анализ компонентов сообщений – полей заголовка (почтовые адреса, даты отправления/получения, темы писем), типов и числа вложений, текстового содержимого тела письма и вложенных файлов, размеров сообщений и др.;
- проверка сообщений на соответствие принятой в организации политике и реализация соответствующих сценариев (разрешение на пересылку писем, блокировка сообщений, пересылка в карантин и др.);
- формирование архива сообщений;
- поиск сообщений в архиве;
- контроль использования почтовых ресурсов.

На рис. 1 представлен типовой вариант построения корпоративной вычислительной сети с внедрённой системой обработки и хранения ЭП.

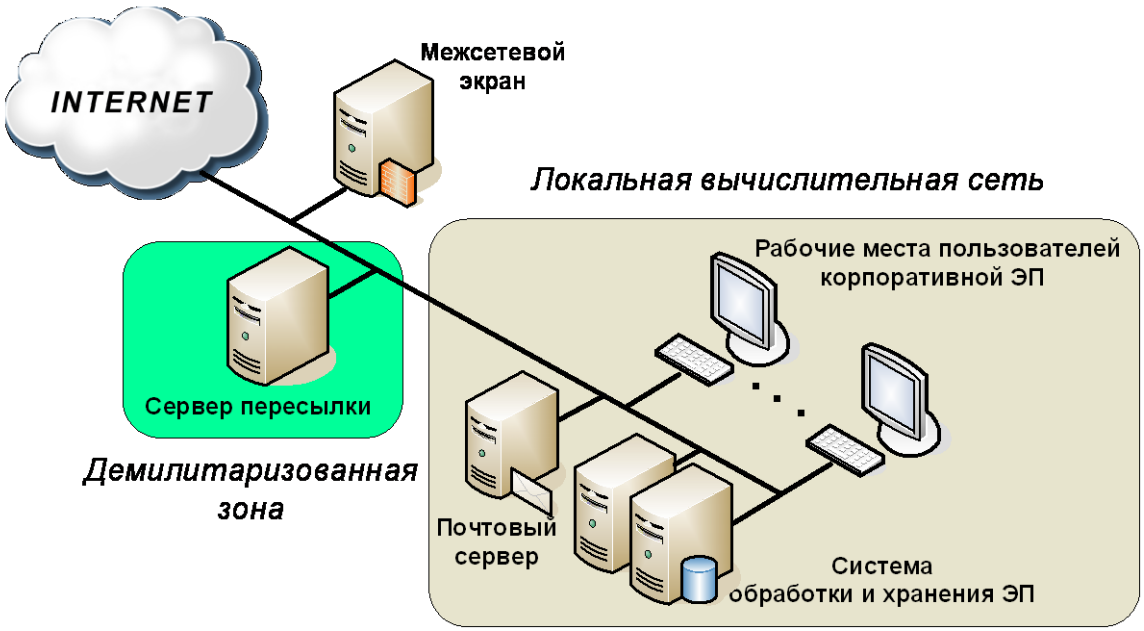
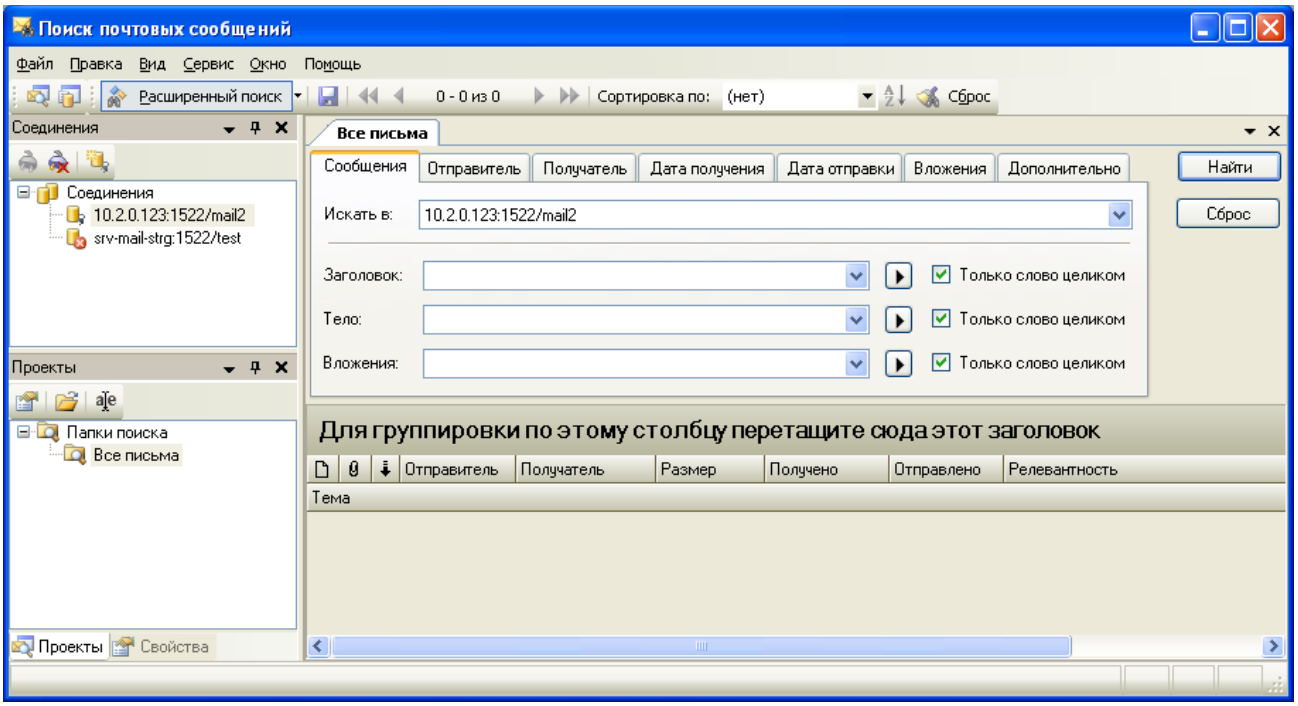


Рис. 1. Место системы обработки и хранения ЭП в корпоративной сети

Для повышения безопасности внешней ЭП путь всех исходящих и входящих сообщений проходит через межсетевой экран и сервер пересылки, размещённый в демилитаризованной зоне. Помимо функции пересылки целесообразно на сервер возложить реализацию функций антивирусной и антиспамовой защиты.

Система SecurityMailArchive

Группа компаний "Информзащита" анонсировала программный продукт "Система хранения сообщений электронной почты SecurityMailArchive" (далее – система SMA) в 2007 году. Основное предназначение системы – организация хранения сообщений внешней и внутренней электронной почты, функционирующей на основе протокола SMTP.



Система SMA реализует:

- приём SMTP-трафика, поступающего от почтового сервера и сетевого IP-монитора;
- фильтрацию принятых сообщений электронной почты;
- формирование и рассылку уведомлений о приёме почтовых сообщений;
- хранение отфильтрованных сообщений в основной базе данных системы;
- формирование архивных файлов сообщений;
- распаковку архивных файлов сообщений и размещение извлеченных из них сообщений в архивной базе данных системы;
- поиск сообщений в основной и архивной базах данных системы;
- управление правами пользователей баз данных системы.

В состав системы SMA входят следующие компоненты (см. рис. 2):

- подсистема обработки сообщений;
- программа загрузки архивов;
- программа управления пользователями баз данных;
- программа поиска сообщений.

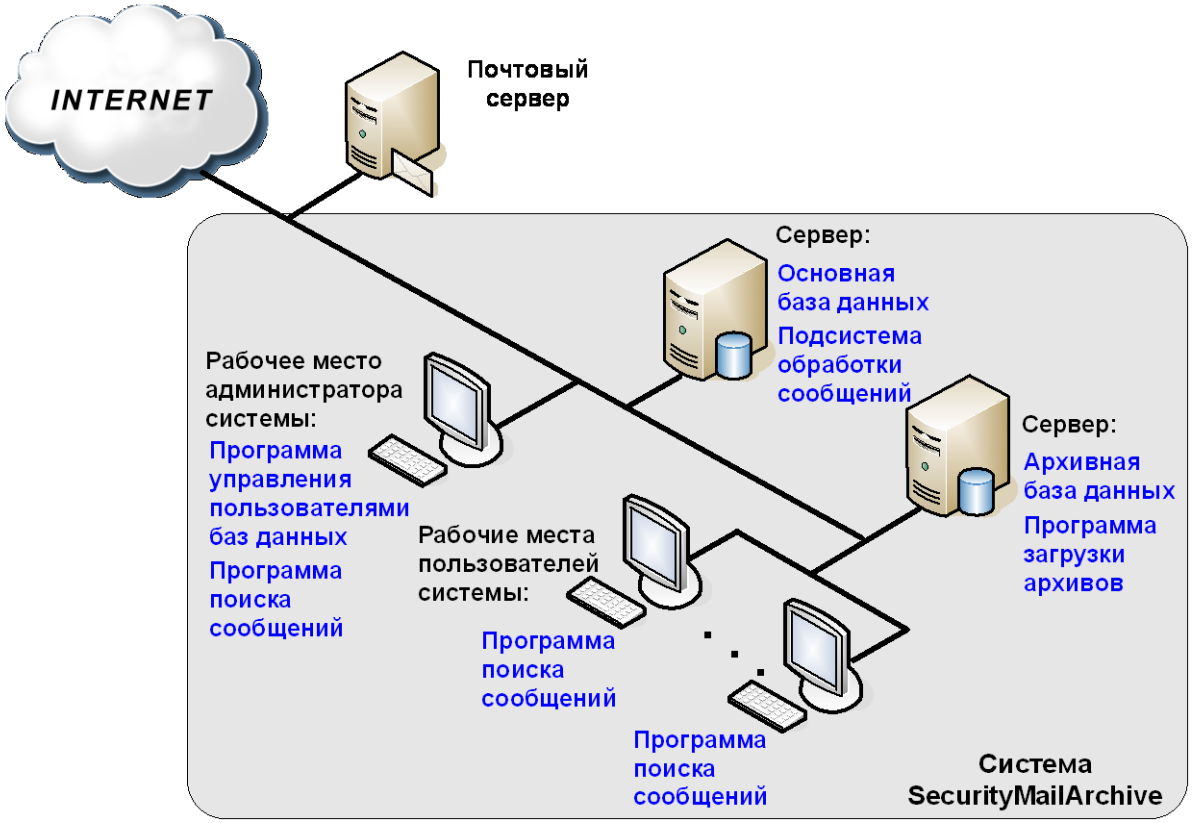


Рис. 2. Состав системы SMA

В системе в качестве основной и архивной баз данных (БД), используемых для хранения сообщений, может применяться любая из трёх редакций СУБД Oracle Database 10g Release 2: Standard Edition One / Standard Edition / Enterprise Edition.

Подсистема обработки сообщений обеспечивает приём и обработку SMTP-трафика, поступающего от почтового сервера и входящего в состав подсистемы монитора IP-трафика. Подсистема выполняет чтение обнаруженных файлов сообщений, их фильтрацию и разбор, распаковку присоединённых ZIP-, RAR-, GZIP-, 7z- и CAB-архивов, преобразование вложенных файлов и размещение поступивших сообщений в основной БД системы. Подсистема обеспечивает обработку входящих документов разнообразных форматов, например, текстовые документы в кодировках Windows-1251 и Unicode, документы Microsoft Word, Excel, PowerPoint, Help, документы OpenOffice и StarOffice, HTML, XML, PDF и др.

С целью эффективного использования ресурсов основной БД почтовые сообщения могут быть выгружены из основной БД и упакованы в архивные файлы. Для этого служит входящая в подсистему программа архивации, реализующая чтение сообщений из основной БД и их архивацию в файл с последующим сохранением архивного файла в заданном каталоге. После успешной архивации сообщения удаляются из основной БД.

Программа загрузки архивов обеспечивает распаковку архивных файлов и размещение извлеченных почтовых сообщений в архивной БД системы.

Программа управления пользователями БД обеспечивает создание и удаление учётных записей пользователей БД, назначение им ролей в системе, смену паролей.

Программа поиска сообщений реализует поиск необходимых сообщений в базах данных системы. Программа обеспечивает:

- стандартный и расширенный поиск электронных сообщений в БД системы;
- сортировку и группировку результатов поиска;
- просмотр сообщений;
- экспорт сообщений на компьютер пользователя.

Стандартный поиск позволяет осуществлять отбор сообщений в БД системы SMA по следующим параметрам:

- текст, содержащийся в заголовке, теле сообщения и его вложенных файлах;
- почтовые адреса отправителей и получателей сообщения;
- дата отправки и получения сообщения.

Дополнительно к стандартному расширенный поиск даёт возможность осуществлять отбор писем по имени домена и именам зарегистрированных в нём пользователей, размеру сообщений и типам вложенных файлов. Для повышения эффективности поиска сообщений по именам доменов и именам пользователей доменов в системе SMA используются регулярные выражения.

Важной особенностью системы SMA является реализация двух способов получения SMTP-сообщений: традиционный – посредством почтового сервера и дополнительный – путём прослушивания и анализа IP-трафика, перехвата электронных сообщений и формирования SMTP-сообщений.

Подробную информацию о продукте SecurityMailArchive смотрите на сайте:
http://www.securitycode.ru/products/security_mail_archive/

Заключение

С одной стороны, глобальный финансовый кризис, вызывающий сокращение расходов российских компаний на информационные технологии и информационную безопасность, никоим образом не может способствовать расширению рынка систем обработки и хранения ЭП. В связи с этим в ближайшей перспективе отечественный рынок, скорее всего, будет находиться в режиме ожидания, конкуренция разработчиков останется на прежнем уровне, выбор систем будет ограниченным.

С другой стороны, взаимную корпоративную деловую активность посредством электронной почты никто не отменит, объём почтового трафика будет возрастать, риски, связанные с использованием ЭП, не исчезнут. Если к тому же в нашей стране появятся серьёзные регламентирующие документы, то IT-руководителям предприятий всё-таки придется делать выбор.

Производитель

НИП «Информзащита» - ведущая российская компания, специализирующаяся на оказании услуг по обеспечению информационной безопасности автоматизированных систем различного назначения и уровня сложности.

127018, г.Москва, а/я 55, тел./факс (495) 980-23-45
www.infosec.ru; www.securitycode.ru

Дистрибьютор

Официальным дистрибьютором продуктов ГК «Информзащита» на территории России и стран СНГ является компания SafeLine.

partners@safe-line.ru
www.safe-line.ru