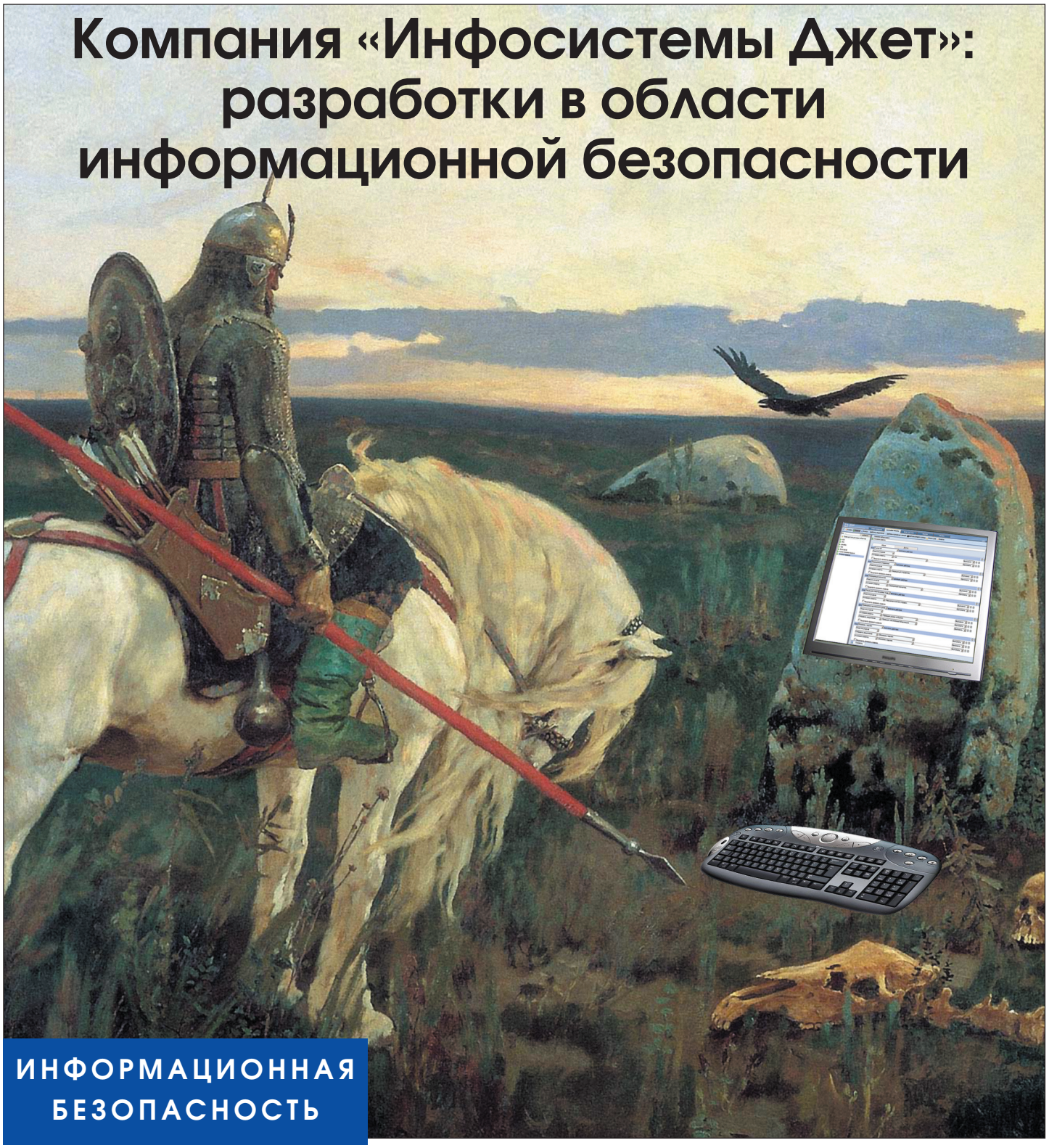
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 06 (169)/2007

Компания «Инфосистемы Джет»: разработки в области информационной безопасности



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Компания «Инфосистемы Джет»: разработки в области информационной безопасности

Александр Синельников,
менеджер по продвижению продуктов «Дозор»
Мария Беляева,
инженер-проектировщик

СОДЕРЖАНИЕ

Система мониторинга и архивирования почтовых сообщений «Дозор-Джет»

Роль электронной почты в информационном обмене

Роль электронной почты в информационном обмене и ее значимость для бизнес-процессов неоспоримы. К преимуществам этого способа передачи информации относятся: оперативность, доступность, универсальность передачи данных разных форматов, сравнительно невысокая стоимость сервиса, надежность, высокая скорость доставки информации.

Важнейшее значение в развитии этого вида сервиса играет тот факт, что во многих компаниях электронная почта служит основой для документооборота, поскольку эта система, обладая высокой степенью универсальности, позволяет без существенных затрат полностью интегрироваться с другими информационными процессами в компании.

Риски, связанные с использованием электронной почты

Первое, с чем мы сталкиваемся, когда говорим о рисках, связанных с использованием электронной почты, — **вирусы**, передаваемые в почтовых сообщениях. Действительно, в настоящее время это один из основных источников распространения вредоносного мобильного кода. Достаточно вспомнить хорошо известные почтовые черви I Love You, Kurnikova или вирус Chernobyl, нанесшие серьезный ущерб многим компаниям во всем мире. Их стремительность в распространении связана именно с популярностью электронной почты.

Второй значительной проблемой является **спам**. Статистика на сегодня неутешительная — около 80% почтовых сообщений являются спамом. Во-первых, он отвлекает от основных задач, которые мы выполняем на рабочем месте. Во-вторых, распространение, например, почтовых червей в некоторых случаях производится с использованием спамерских списков рассылки. Спамеры все чаще используют троянские программы, чтобы скрыть источник рассылки рекламы. Это делается следующим способом: на компьютер жертвы удаленно устанавливается (например, после посещения какого-либо сайта с сомнительным содержимым) программа, которая обеспечивает рассылку рекламы с его компьютера. При этом сам пользователь даже не догадывается об этом, только периодически задает себе вопрос, почему он тратит так много денег на обслуживание трафика, если не очень часто выходит в Интернет.

Помимо вирусов и спама существует множество других рисков для организаций, использующих систему электронной почты. При этом во многих организациях этим рискам порой не уделяется должного внимания, и не всегда руководство отдает себе отчет в серьезности связанных с ними проблем. К примеру, **использование электронной почты сотрудниками в личных целях** или **непродуктивное применение почтового сервиса**, по статистике, не считают серьезной проблемой около 45% руководителей, наивно полагая, что на частную переписку сотрудники тратят несущественно мало времени. Однако практика показала, что эти руководители резко меняют свое мнение после того, как получают анализ почтового трафика за определенный период времени. Согласно проведенным исследованиям, около 30% почтового трафика среднестатистической российской компании состоит из звуковых, видео- и графических файлов, которые, как правило, имеют большой объем и не относятся к работе.

Неконтролируемость системы электронной почты дает возможность использовать ее для организации скрытых каналов передачи информации, которая может представлять собой не только служебные данные (тексты договоров, сведения о планируемых сделках и т.п.), но и данные о внутренней сети (структура сети, пароли, системные данные, исходные коды программ и т.п.). Это, в конечном итоге, грозит **нарушением конфиденциальности** и может привести к серьезным для компании последствиям, причем не только финансовым.

Утечка конфиденциальной информации может произойти и по случайности, например, ошибочное направление письма не по тому адресу. Каждый пользователь может вспомнить

эпизод из своей практики, когда, случайно выбрав из списка пользователей ошибочный адрес, он нажимает на кнопку Send, и даже мгновенное осознание того, что письмо отправлено не по адресу, уже не остановит его отправку. Пользователь сразу обращается за помощью к администратору, но, к сожалению, администратор почтового сервера не в состоянии повлиять на ситуацию.

Еще один риск — **потеря информации**. Представьте себе, что вам необходимо найти письмо, полученное год назад. Хорошо, если вы периодически делаете backup всей своей информации в каком-то логическом виде. В данном случае длительные, упорные и кропотливые поиски могут привести к какому-нибудь результату. А если нет, то ваш почтовый архив представляет собой не больше чем файловую «помойку», в которой невозможно найти ничего, даже затратив на это уйму времени и средств.

Решение проблем, связанных с использованием электронной почты

К сожалению, список рисков велик, их описание может занять не одну страницу, а **причина этих рисков одна – бесконтрольность использования системы электронной почты**. Избежать большинства рисков можно лишь в том случае, если каждый руководитель, администратор сети и пользователь осознали, что **основа обеспечения безопасности системы электронной почты заключается в ее систематизации, организации и контроле**. Лучше всего, если в компании вводится политика использования электронной почты и организуется контроль за ее исполнением. Более простым вариантом может быть просто создание специального регламента по администрированию почтовой системы. Реализация контроля за исполнением политики использования электронной почты или каких-либо регламентов осуществляется при помощи специальных средств.

Для контроля использования электронной почты компанией «Инфосистемы Джет» разработана система мониторинга и архивирования почты — СМАП «Дозор-Джет», которая также является программным средством реализации политики использования электронной почты.

Благодаря своей высокой функциональности система «Дозор-Джет» позволяет предотвратить все описанные выше риски, а также решать множество других задач, помимо защиты почтовой системы.

Выгоды от внедрения СМАП «Дозор-Джет»:

- минимизация утечки конфиденциальной информации по электронной почте;
- использование СМАП «Дозор-Джет» в качестве дополнительного средства борьбы со спамом;
- защита почтового сервиса от остановки из-за внешних атак типа mail bombs;
- минимизация передачи потенциально опасных вложений, вирусов и вредоносных кодов посредством антивирусной проверки программами сторонних производителей;
- уменьшение затрат на содержание почтового сервиса посредством запрета или отложенной доставки писем с вложениями большого объема (музыка, видео, фото);
- выявление фактов рассылки резюме сотрудниками через корпоративную почту;
- повышение производительности труда сотрудников путем ограничения их личной переписки в рабочее время.

Компанией «Инфосистемы Джет» с 2001 г. осуществлено более 250 внедрений системы в компаниях с численностью от 50 до 15000 пользователей на всех вертикальных рынках.

Контроль над корпоративной электронной почтой предполагает выполнение как минимум трех основных задач:

1) создание условий для эффективного управления почтовым потоком;
2) обеспечение безопасности почтовой системы компании;
3) обеспечение надежного хранения почтовых сообщений.

Управление почтовым потоком

СМАП «Дозор-Джет» обеспечивает эффективное управление почтовым потоком. Это подразумевает внедрение политики использования электронной почты и контроль за ее исполнением всеми пользователями корпоративной почтовой системы.

Данная политика принимается в компаниях на административном уровне, устанавливаются правила использования электронной почты. Элементами политики являются:

- предметы контроля (прохождение каких категорий сообщений электронной почты должно быть разрешено или запрещено);
- объекты воздействия (группы пользователей, которым разрешено или запрещено

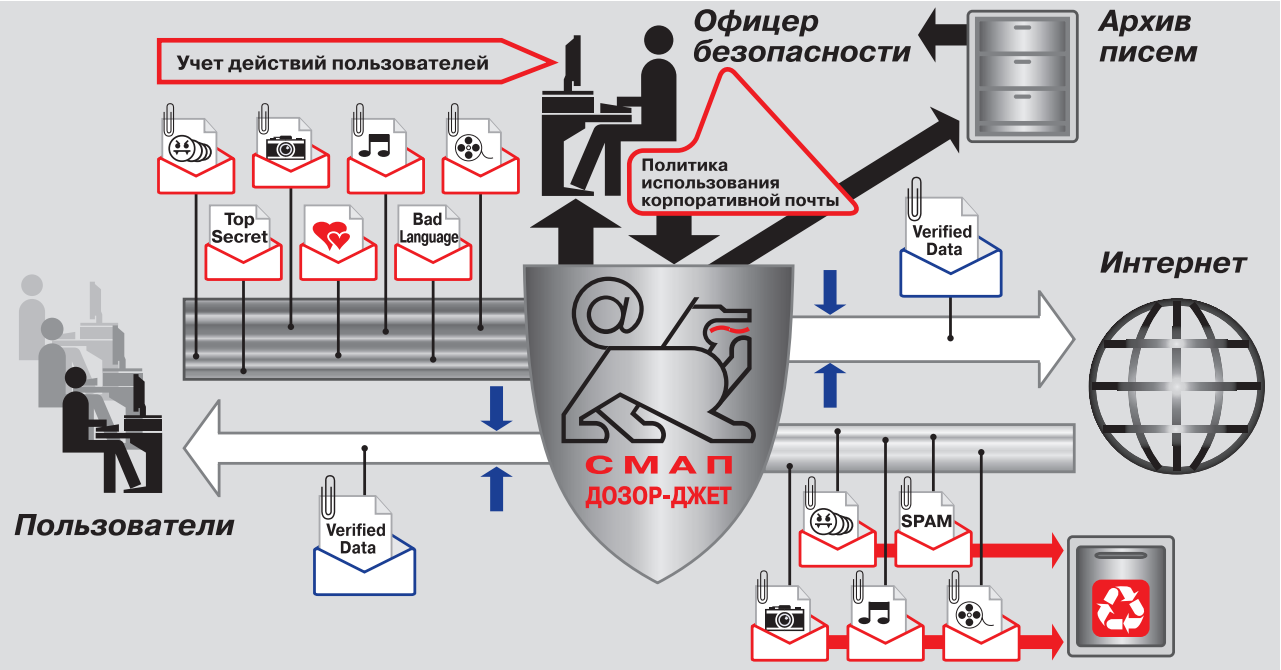


Рис. 1. Система мониторинга и архивирования почтовых сообщений СМАП «Дозор-Джет»

получать или отправлять почтовые сообщения определенной категории);
- реакция системы (действия программного комплекса в отношении почтовых сообщений, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты).

Безопасность почтовой системы

СМАП «Дозор-Джет» позволяет решить ряд проблем, связанных с неконтролируемым использованием электронной почты, таких как:
- утечка конфиденциальной коммерческой информации;
- передача потенциально опасных вложений, вирусов и вредоносных кодов;
- передача нежелательных вложений;
- несанкционированные почтовые рассылки (спам);
- атаки типа «mail bombs»;
- ошибочное направление писем;
- потери рабочего времени, ресурсов или блокирование почтового сервиса.

СМАП «Дозор-Джет» может осуществлять мониторинг и контроль всех входящих, исходящих и внутренних корпоративных почтовых сообщений. Мониторинг включает в себя анализ заголовков и структуры сообщений, а также *проверку на наличие в тексте сообщения или прикрепленных файлах слов или последовательностей слов*, разрешенных или запрещенных к использованию в электронной переписке.

СМАП «Дозор-Джет» — это гарантированный разбор объектов информационного обмена вне зависимости от их сложности.

СМАП «Дозор-Джет» осуществляет фильтрацию по тексту *в любой части электронного письма* (заголовках, теле сообщения, прикрепленных файлах и т.п.) вне зависимости от исходной кодировки текста письма или вложения, его сложной структуры (многоуровневая вложенность, OLE-объекты файлов MSOffice и т.п.) и упакованности (например, архивные файлы).

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

Результатом мониторинга может быть задержание или блокировка отправки подозрительных писем. СМАП «Дозор-Джет» дает возможность задавать корпоративные правила обработки входящей и исходящей почты в зависимости от предопределенных параметров, например:
- запрет пересылки файлов определенных форматов для заданных групп пользователей (рисунки формата gif могут пересылать только сотрудники рекламного отдела, ос-

тальным пользователям такая пересылка запрещена);
- ограничение на объем и количество присоединенных файлов, направляемых отдельным адресатам;
- запрет всех исходящих сообщений, не относящихся к внутрикорпоративным рассылкам, содержащим в тексте или вложенных файлах слово «безопасность»;
- автоматическое уведомление администратора системы и/или руководящего состава корпорации о письмах с определенными пометками или отвечающих поставленным условиям.

СМАП «Дозор-Джет» принимает решение о формате того или иного вложения на основании анализа типа передаваемых данных. Анализ текста производится как в тексте самого письма, так и во вложенных файлах следующих форматов: ps, pdf, rtf, doc, xls. Производится распаковка архивов форматов rar, zip, arj, lha, 7zip, bzip2, cab, cpio, gzip, tar.

Использование системы фильтрации сообщений позволяет реализовать гибкую схему прохождения электронной почты. Например, возможна отложенная доставка почтового сообщения, когда решение о направлении письма адресату принимается только после его дополнительного анализа администратором системы. Дополнительно могут применяться и другие системы обеспечения безопасности — антивирусное программное обеспечение, спам-фильтры и др.

Защита от утечек конфиденциальной информации

Основную проблему для фильтрации почтовых сообщений представляет анализ содержания в письмах конфиденциальной информации. После установки и настройки СМАП «Дозор-Джет» проверка происходит в автоматическом режиме.

После анализа заголовков и структуры сообщений может быть осуществлена *проверка на наличие в тексте сообщения или прикрепленных файлах слов или последовательностей слов*, разрешенных или запрещенных к использованию в электронной переписке.

Для осуществления настройки СМАП «Дозор-Джет» первоначально представляется разумным внести в список запрещенных слов следующее:

1) телефонные номера, не предназначенные для звонков клиентов или посторонних лиц;
2) номера мобильных телефонов сотрудников, предназначенные исключительно для внутреннего пользования;
3) номера телефонов и/или позывные радиостанций, установленных в автомобилях различных служб;
4) номера *внутренних* банковских счетов;
5) номера документов;
6) реквизиты налоговых и иных контролирующих органов;
7) номера пластиковых карт;
8) словосочетания, характеризующие секретные разработки организации.

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.

Антивирусная защита

Для защиты от вирусов, распространяемых с помощью почтовых сообщений, СМАП «Дозор-Джет» применяет как собственные средства (фильтрация писем по полям заголовка и по содержанию), так и антивирусные программы третьих производителей.

Проверка на наличие вируса может осуществляться на любом этапе обработки сообщения. Программный комплекс СМАП «Дозор-Джет» предоставляет унифицированный интерфейс для работы с антивирусными программами Symantec Antivirus (Symantec Corp.), Антивирус Касперского («Лаборатория Касперского») и Dr.Web («Диалог-Наука»). Также возможна работа с некоммерческим антивирусным программным обеспечением — ClamAV (http://clamav.org). Эти программы обеспечивают антивирусную проверку до начала обработки письма СМАП «Дозор-Джет». После окончания проверки, в зависимости от ее результатов, на письмо ставится соответствующая пометка, которая учитывается при дальнейшей обработке письма. Это позволяет автоматически посылать уведомления о зараженных письмах администратору системы, адресату и т.д. Затем письмо может быть помещено в архив, где оно хранится в первоначальном виде, то есть с вирусом и пометкой: «письмо содержит вирус». Хранение зараженных писем абсолютно безопасно. Кроме того,

администратор системы имеет возможность безопасного доступа к тексту письма без раскрытия вложенных файлов.

Также существует возможность выполнять проверку на наличие вирусов путем применения действия «вызов внешней программы». Таким образом, СМАП «Дозор-Джет» может быть интегрирована с другими антивирусными программами, что позволит, например, проверять на наличие вируса отдельные почтовые вложения.

Борьба со спамом

Фильтрация спама в системе «Дозор-Джет» происходит в несколько этапов. Часть спама отсекается уже на этапе получения почты с помощью следующих механизмов:

1) Проверка по RBL-спискам — сервис, обеспечивающий проверку адреса отправителя на принадлежность к определенным спискам: известных спамерских доменов и почтовых адресов, адресов открытых почтовых пересылок (openrelay), диапазонов адресов скомпрометированных сетей.
2) Anti-spoofing — проверка подлинности почтовых адресов путем поиска соответствующей записи в DNS (или проверки существования такого домена в DNS).
3) Anti-relay — запрет прохождения писем, адреса отправки и получения которых не принадлежат к заданным внутренним доменам.
4) Graylisting — блокировка нежелательных почтовых рассылок с помощью анализа реализации SMTP-протокола. Ключевым понятием метода graylisting является graylisting-триплет: комбинация из ip-адреса сервера отправителя письма, исходящего адреса SMTP-конверта и адреса получателя SMTP-конверта. Новое письмо, триплет которого ни разу не проходил в почтовом потоке сервера, отвергается с кодом временной ошибки (451). При следующей попытке доставки это письмо принимается, а его триплет заносится в базу данных SMTP-сервера. Последующие письма с таким же триплетом доставляются без задержек. Использование метода graylisting включается индивидуально для каждого списка доступа, благодаря чему можно выключать graylisting для локальных сетей и «дружественных» внешних почтовых серверов.

После завершения первого этапа проверки письмо передается на обработку подсистеме фильтрации, которая проводит декомпозицию почтового сообщения (разбор) и проверку его на соответствие условиям, заданным администратором системы (анализ и категоризация). По результатам анализа принимается решение о том, является ли почтовое сообщение спамом.

Архивация почтовых сообщений

Архив СМАП «Дозор-Джет» предназначен для хранения и поиска почтовых сообщений. В нем хранятся оригинал письма и метаданные (служебная информация о письме). Архив обеспечивает хранение большого количества корпоративной электронной почты с высоким уровнем доступности данных, при этом есть возможность экспорта данных на внешние носители, что повышает надежность и снимает ограничения по объему хранения данных.

Программный комплекс СМАП «Дозор-Джет» содержит механизм поиска писем в архиве. Формирование критериев поиска осуществляется с помощью веб-интерфейса.

Подсистема архивирования СМАП «Дозор-Джет» в настоящее время реализована на двух СУБД:

- Oracle;
- PostgreSQL.

Состав системы

СМАП «Дозор-Джет» представляет собой набор программных модулей, которые обеспечивают потоковый анализ SMTP-трафика.

СМАП «Дозор-Джет» состоит из следующих основных подсистем (рис. 2):

- мониторинг;
- архивирование;
- управление.

Все почтовые сообщения, поступающие из внешней среды или из локальной сети компании, обрабатываются СМАП «Дозор-Джет». В процессе обработки система архивирует сообщение, принимает решение о дальнейшей его отправке адресату или о его задержке, а также об уведомлении администратора системы о прохождении сообщения определенного типа. Вся почта, успешно прошедшая проверку на СМАП «Дозор-Джет», перенаправляется почтовому серверу для дальнейшей отправки по назначению.

СМАП «Дозор-Джет» функционирует под управлением следующих операционных систем:

- SunOS 5.10;

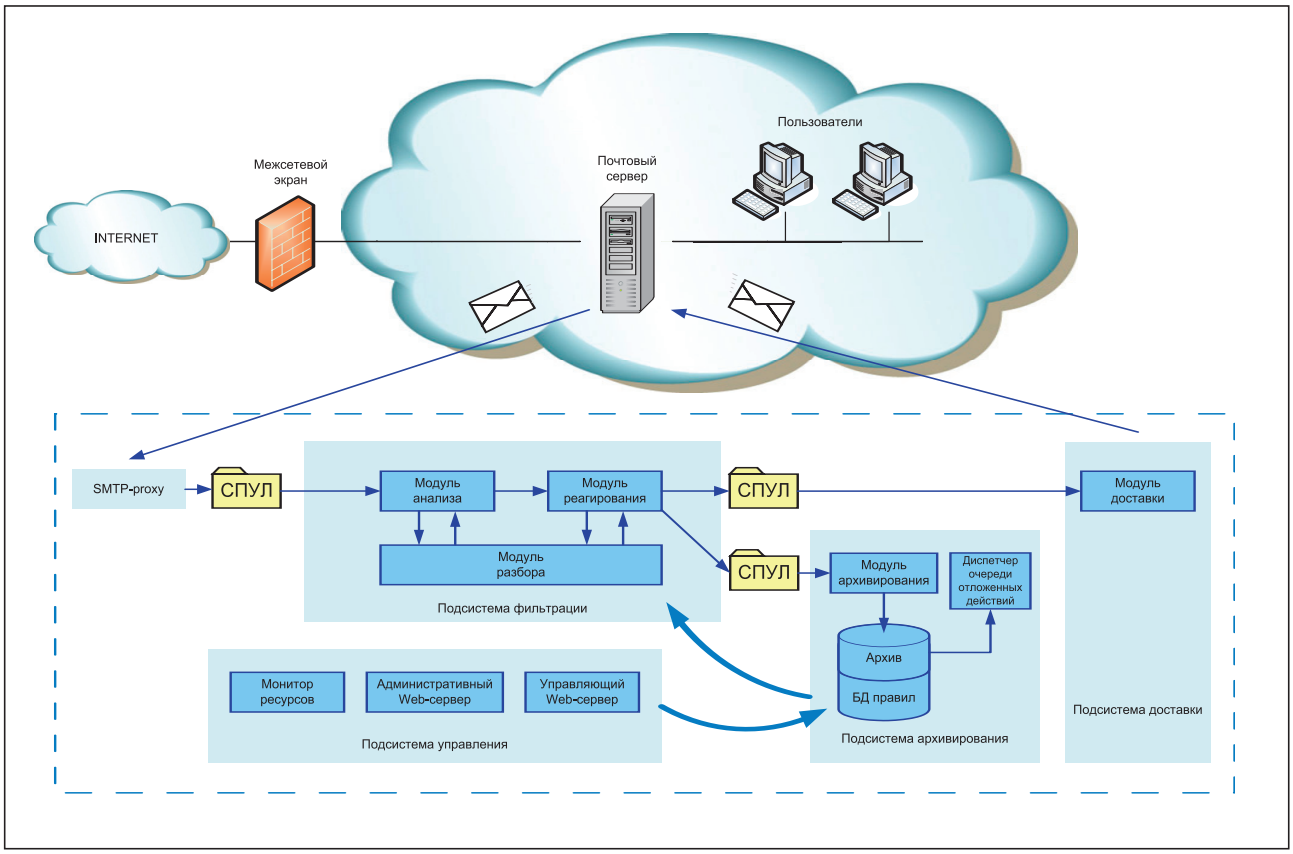


Рис. 2 Архитектура СМАП «Дозор-Джет»

- CentOs 4.3;
- RHEL 4.

Говоря о производительности, следует отметить положительный опыт обработки потока в 25 тысяч почтовых сообщений в час в режиме фильтрации.

Интеграция в почтовую систему

СМАП «Дозор-Джет» легко интегрируется в уже созданную почтовую систему. Она устанавливается на отдельный сервер, как правило, в демилитаризованной зоне корпоративной сети. Система представляет собой SMTP-proxy. Доставку электронной почты выполняет почтовый сервер.

СМАП «Дозор-Джет» может функционировать со следующими почтовыми серверами:

- Sendmail;
- Postfix;
- Netscape Messaging Server (SunOne messaging server);
- Exim;
- Qmail;
- Communigate PRO;
- MS Exchange 5.5, 2000.

Режимы функционирования системы

Режим функционирования СМАП «Дозор-Джет» выбирается в зависимости от задач политики использования корпоративной почты. При необходимости контролировать почтовый поток и влиять на прохождение писем (задерживать, перенаправлять, откладывать доставку) СМАП «Дозор-Джет» устанавливается в режиме фильтрации. Задача мониторинга почтового потока осуществляется в режиме архивирования.

Режим архивирования

В режиме архивирования СМАП «Дозор-Джет» устанавливается параллельно почтовому серверу (рис. 3). В СМАП «Дозор-Джет» направляются копии всех писем, проходящих через почтовый сервер. В СМАП «Дозор-Джет» почтовые сообщения анализируются и при необходимости заносятся в архив. Все события регистрируются в системном журнале. Информация, накапливаемая в архиве, может использоваться для выявления рисков использования электронной почты, для расследования инцидентов.

Режим фильтрации

В режиме фильтрации СМАП «Дозор-Джет» устанавливается «в разрыв» (рис. 4). Почтовый по-

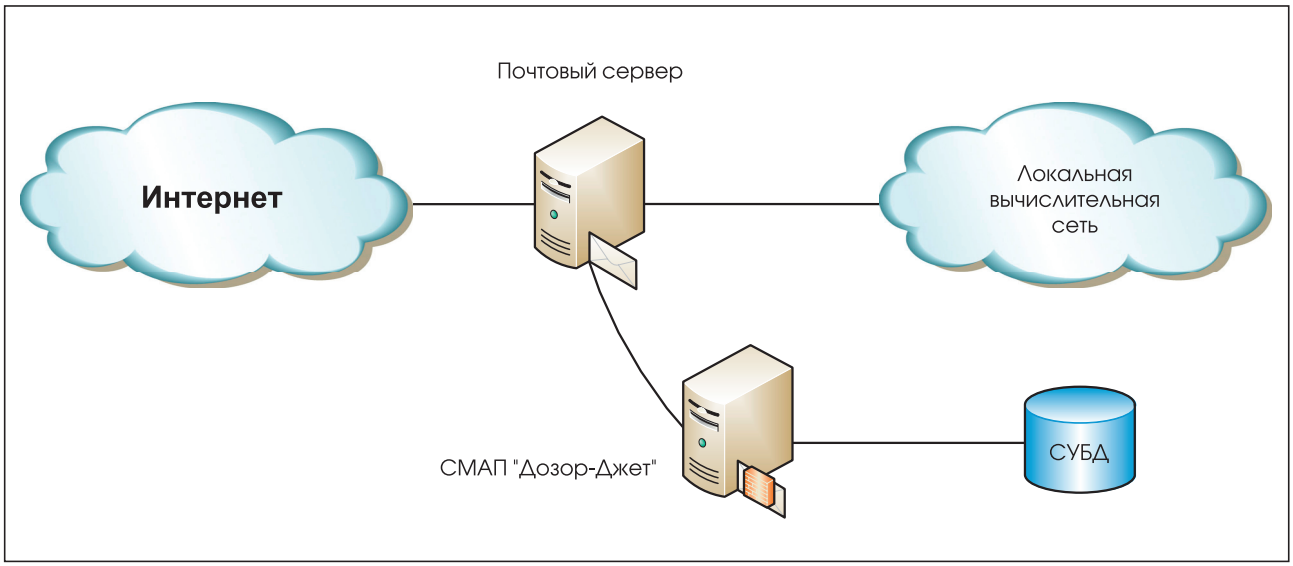


Рис. 3 Схема подключения СМАП «Дозор-Джет» в режиме архивирования

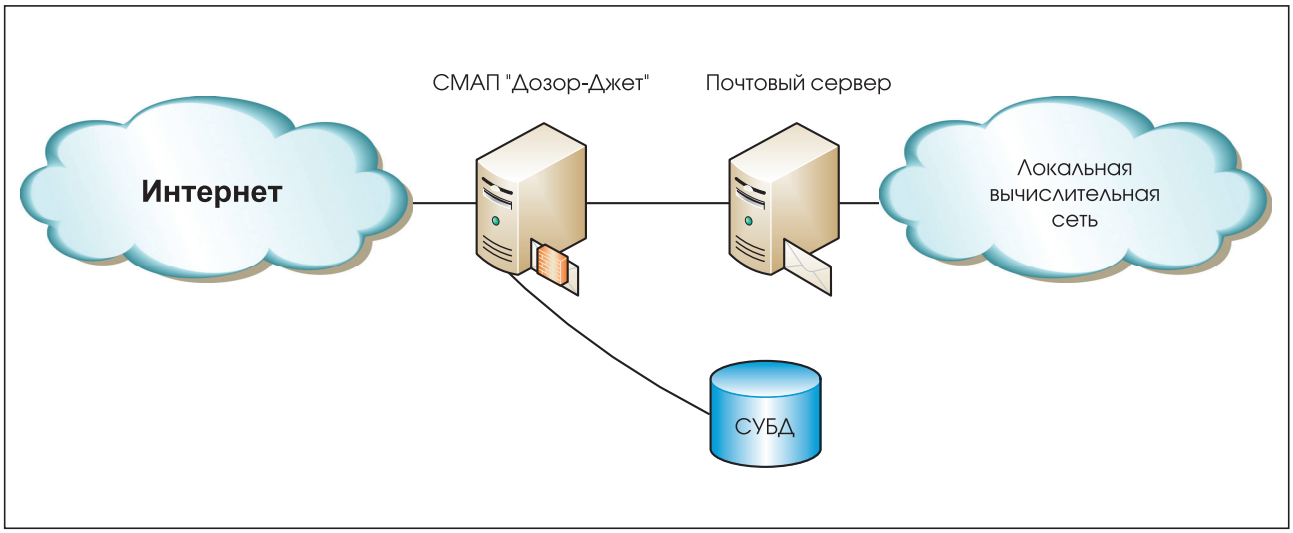


Рис. 4 Схема подключения СМАП «Дозор-Джет» в режиме фильтрации

ток перенаправляется на сервер, где установлена СМАП «Дозор-Джет». Каждое сообщение проверяется на соответствие политике. Письма, прошедшие проверку, передаются основной почтовой системе, которая доставляет их адресатам. В этом режиме функционирования одновременно с фильтрацией осуществляется архивирование почтовых сообщений.

Анализ содержимого почтовых сообщений

Все попадающие в СМАП «Дозор-Джет» почтовые сообщения проходят процесс декомпозиции. При этом происходит разбор как заголовков сообщения, так и всей его структуры, вне зависимости от количества уровней вложенности. Это позволяет анализировать сообщения, содержащие прикрепленные файлы, а также перенаправленные сообщения.

Анализ почтовых сообщений включает в себя:

- определение характеристик сообщения — отправитель, получатель, дата, размер, структура;
- определение характеристик вложений — имя, размер, тип, количество;
- распознавание форматов вложений;
- анализ текста в заголовках сообщения, теле письма и вложенных файлах.

Варианты реакции системы по результатам проверок

При обнаружении писем, отвечающих заданным критериям, СМАП «Дозор-Джет» может

wtf – what the file?

Главным этапом контентной фильтрации являются декомпозиция и анализ объекта. В связи со сложностью и комплексностью объектов информационного обмена невозможно обеспечить надежное распознавание формата (типа) файла, основываясь как на расширении (к примеру, файл формата exe легко может быть переименован и сохранен с расширением doc), так и на анализе mime-типа, указанного в служебных заголовках объекта. Mime-тип не всегда присваивается верно, что приводит к ошибкам при разборе. Использование существующих утилит (пример – программа file) также представляется нецелесообразным из-за невозможности контроля сигнатур для разных типов данных, отсутствия гибкого языка описания проверок типов данных.

Поэтому в линейке продуктов «Дозор-Джет» упор делается на надежное определение типов данных и гарантированное определение кодировки текстов. Это в итоге позволяет добиться высокой эффективности фильтрации.

В 2004 г. специалистами компании «Инфосистемы Джет» разработана технология wtf – what the file, предназначенная для гарантированного определения типов данных и кодировки текста. Любой объект информационного обмена по каналам Интернет изначально рассматривается как композитный. То есть в него могут входить различные компоненты: текст, файлы, закодированные бинарные данные, описания и комментарии. Предполагается, что каждый входящий в такой объект компонент, в отдельности также может быть сложным объектом. Все элементы, которые удалось выделить в ходе декомпозиции, анализируются.

Гарантированное определение кодировки в системе «Дозор-Джет» обеспечивается за счет эвристического анализа текстов, поэтому удается успешно проводить анализ текстов с неверно указанной кодировкой. Также важно, что «Дозор-Джет» позволяет определять кодировки в текстах внутри архивированных файлов.

Описанная выше функциональность «Дозор-Джет» стала возможной за счет:

- наличия специализированного языка описания проверок типов данных;
- возможности расширения языка проверок;
- возможности подключения модулей анализа;
- явного отображения сигнатур в mime-типы.

При уточнении типов данных и/или проведении глубокого анализа инфраструктура системы позволяет использовать модули расширения. В настоящее время реализованы следующие модули анализа данных:

- модуль определения текстов и методов их кодирования (ASCII, различные кодировки кириллицы); важность его определяется тем, что для текстовых файлов не существует сигнатур, по которым можно определять типы;
- модуль определения исполняемых файлов MS-DOS – .com-файлы; как и для текстовых, для таких файлов не существует стандартных сигнатур, поэтому необходимо проводить детальный анализ содержимого файлов;
- модуль определения главного типа OLE-контейнера – MS Visio, MS Project, MS Word, MS Excel, MS PowerPoint.

В настоящее время гарантированно распознаются несколько сотен форматов файлов, база сигнатур продолжает пополняться.

Полный список форматов, с которыми работает wtf, может быть предоставлен по дополнительному запросу.

осуществлять одно или несколько назначенных действий:

- отправка сообщения получателю;
- блокировка сообщения;
- задержка сообщения;
- архивирование сообщения;
- отправка письма на дополнительную обработку внешней программе;
- выставление пометок;
- отправка уведомления.

Кроме того, СМАП «Дозор-Джет» может выполнять реинжиниринг почтовых сообщений, то есть модификацию сообщений перед доставкой или пересылкой, включая удаление запрещенных вложений и добавление текста (аннотирование письма), в зависимости от результатов анализа сообщения.

При необходимости оригинал письма (до осуществления реконструкции почтового сообщения) может быть сохранен в архиве электронной почты с пометкой о модификации.

Все действия, производимые СМАП «Дозор-Джет», протоколируются.

Администрирование системы

Программный комплекс СМАП «Дозор-Джет» включает в себя систему централизованного управления через веб-интерфейс с использованием защищенного ssl-соединения. Также система позволяет настроить списки прав доступа для администраторов и операторов.

Дополнительные возможности

Программный комплекс СМАП «Дозор-Джет» имеет модульную архитектуру (см. рис. 2). Дополнительные модули, расширяющие функциональные возможности СМАП «Дозор-Джет», входят в стандартный комплект поставки, но возможность их использования определяется лицензионным файлом. К ним относятся:

- модуль S/MIME (подключения ЭЦП);
- модуль «Антиспам»;
- модуль «Антивирус»;
- модуль поддержки SNMP;
- модуль сегментирования;
- модуль контекстного поиска.

Модуль S/MIME

Модуль S/MIME предназначен для выполнения операций проверки ЭЦП на этапе фильтрации почтовых сообщений, шифрования и дешифрования сообщений, отправляемых и получаемых СМАП «Дозор-Джет». Модуль позволяет обеспечить конфиденциальность и контроль целостности информации, пересылаемой по электронной почте.

Проверка ЭЦП может проходить по следующим сценариям:

- проверка ЭЦП с использованием приложенного к письму сертификата;
- проверка ЭЦП с использованием внешнего хранилища сертификатов;
- проверка ЭЦП с проверкой совпадения адресов;
- проверка ЭЦП с проверкой подлинности сертификата подписавшего лица.

Модуль предоставляет базу данных и средства ее управления для сертификатов и ключей пользователей.

Модуль «Антиспам»

Модуль «Антиспам» решает задачу фильтрации нежелательных писем, писем с рекламной информацией; писем, содержащих запрещенную для рассылки информацию. Механизм настройки весов в модуле «Антиспам», основанный на подходе, предложенном Полом Грэхемом (Paul Graham), дает возможность на основе писем-образцов составить корректную таблицу весов с коэффициентами для проверки на наличие в письме спама или нежелательной информации.

Модуль «Антивирус»

Модуль «Антивирус» позволяет интегрировать внешние программы обнаружения и устранения вирусов, передаваемых с помощью электронной почты. В СМАП «Дозор-Джет» поддерживаются только антивирусы, работающие по протоколу ICAP. После настройки адреса антивируса все проходящие через фильтр письма будут направляться на проверку. По ее результатам может быть добавлена пометка с комментарием, описывающим произведенное действие (сообщение заражено, сообщение вылечено и др.)

Другие программы антивирусной защиты также могут использоваться с помощью действия «вызов внешней программы».

Модуль поддержки SNMP

Модуль предназначен для наблюдения за состоянием ресурсов СМАП «Дозор-Джет» средствами программного обеспечения, поддерживающего протокол SNMP. Встраиваемый модуль подключается к монитору ресурсов и служит для отправки SNMP-уведомлений при изменении состояния ресурсов до пороговых значе-

Особенности СМАП «Дозор-Джет»

- полный структурный анализ почтового сообщения с прикрепленными файлами любого уровня вложенности;
- распознавание форматов вложенных файлов в почтовых сообщениях;
- анализ почтовых сообщений вне зависимости от используемой кодировки;
- гибкая система фильтрации сообщений;
- наличие механизмов реагирования на выполнение условий фильтрации;
- модульная структура;
- система архивирования, позволяющая осуществлять полнотекстовый поиск по почтовым сообщениям;
- простота управления;
- наличие нескольких механизмов защиты от спама и вредоносных вложений;
- возможность интеграции с другими системами.

ний, определенных в мониторе ресурсов и предоставляет информацию по запросам.

Модуль сегментирования

Модуль сегментирования почтовых сообщений предназначен для повышения производительности и надежности работы с большими базами данных электронной почты. Сегментирование таблиц и индексов позволяет уменьшить время, требуемое на выполнение операций над данными. Наличие оперативного архива (сегмента) значительно упрощает оперативный поиск в текущих сообщениях.

Модуль контекстного поиска

Модуль предназначен для поиска определенного контекста в архиве сообщений СМАП «Дозор-Джет». При этом анализу подвергается не только текст почтового сообщения, но и текст прикрепленных файлов вне зависимости от уровня вложенности. Возможен поиск слов русского, английского, японского, немецкого и французского языков, вне зависимости от исходной кодировки текста. Поиск во вложенных файлах производится только в случае распознавания формата вложения и его распаковки в текстовое представление на этапе фильтрации.

Сертификация системы

СМАП «Дозор-Джет» версии III сертифицирована ФСТЭК РФ по 4 уровню контроля отсутствия недекларированных возможностей и имеет оценочный уровень доверия (ОУД) 3, о чем свидетельствует сертификат № 1037 от 5 июля 2005 г. (действителен до 5 июля 2008 г.). В настоящее время проводится сертификация СМАП «Дозор-Джет» версии IV.

СМАП «Дозор-Джет» – от версии III к версии IV

- Расширены возможности фильтрации почтового трафика. Благодаря новому программному комплексу определения типов данных система осуществляет глубокий анализ комплексных объектов. Данная функциональность позволяет разбирать практически все объекты информационного обмена и избегать ошибок при их распаковке. Добавлен анализ комментариев архивов, тэгов mp3, exif-информации из jpeg и др.
- Переработан механизм работы с архивом писем и интерфейс построения запросов к базе данных, что позволило более чем в три раза увеличить скорость доступа к почтовым сообщениям в архиве вне зависимости от его объема. Добавлено сохранение результатов поисковых запросов и механизм кэширования результатов.
- Увеличение производительности системы за счет «ленивой» распаковки. Это означает, что из письма извлекаются только те данные, которые должны быть проанализированы. Например, если для группы писем фильтрация осуществляется только по заголовкам, то для них не будут извлекаться тела и вложенные файлы. Часть почты, определенная администратором системы как не подлежащая архивации, не анализируется и не распаковывается.
- При обработке данных в качестве внутренней кодировки используется UTF8, что позволяет работать с текстами в различных кодировках и языках. Добавлен механизм определения наличия кодированной информации во всех текстовых фрагментах, в том числе и в текстовых представлениях файлов. Например, в тексте файла формата MSOffice может быть информация, закодированная в base64, uue. Эти данные будут обнаружены, декодированы и проанализированы.
- Разработан новый интерфейс управления программным комплексом.

Дополнительные возможности

В настоящее время сотрудниками тестовой лаборатории компании «Инфосистемы Джет» разработаны дополнительные два модуля к СМАП «Дозор-Джет», находящиеся в опытной эксплуатации.

Модуль архивирования icq-сообщений.

ICQ сегодня это дешевый и удобный канал для оперативной связи с клиентами, партнерами и сотрудниками. Благодаря этим преимуществам данный канал связи разрешен во многих компаниях. Однако руководству важно знать, что данный канал используется во благо компании, а не во вред. Например, посредством ICQ можно пересылать конфиденциальную информацию, договориться о заключении сделки в ущерб компании, раскрыть информацию о готовящемся тендере, вести бесконечную личную переписку в ущерб рабочему времени и т.д.

Для возможности расследования инцидентов, связанных с такой перепиской, разработан модуль архивирования сообщений, предава-

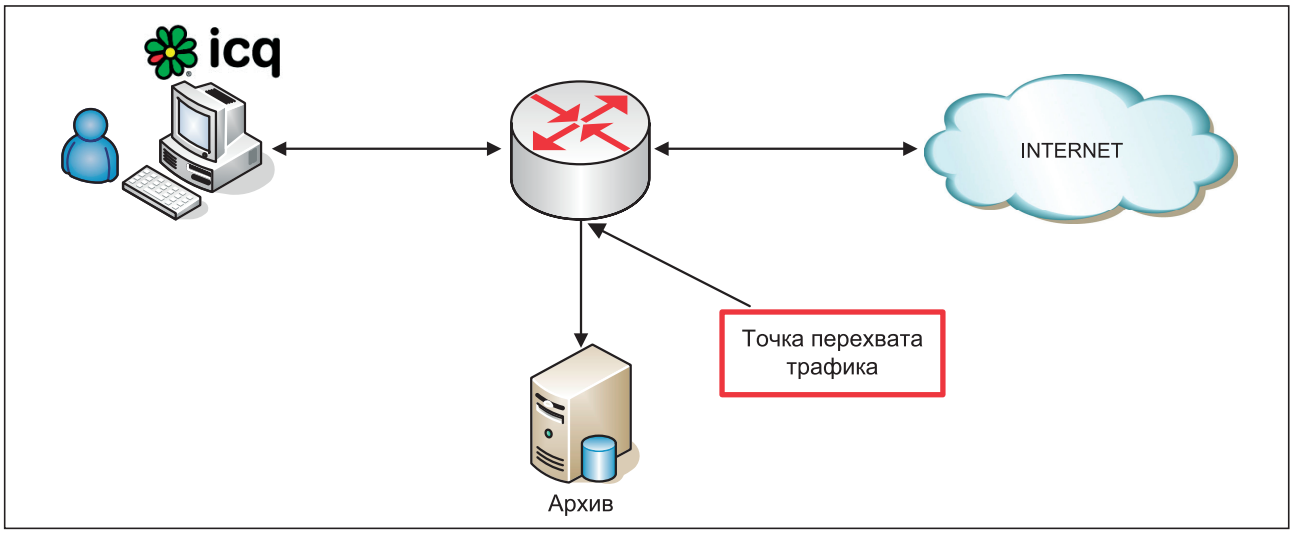


Рис. 5 Архивирование интернет-пейджера

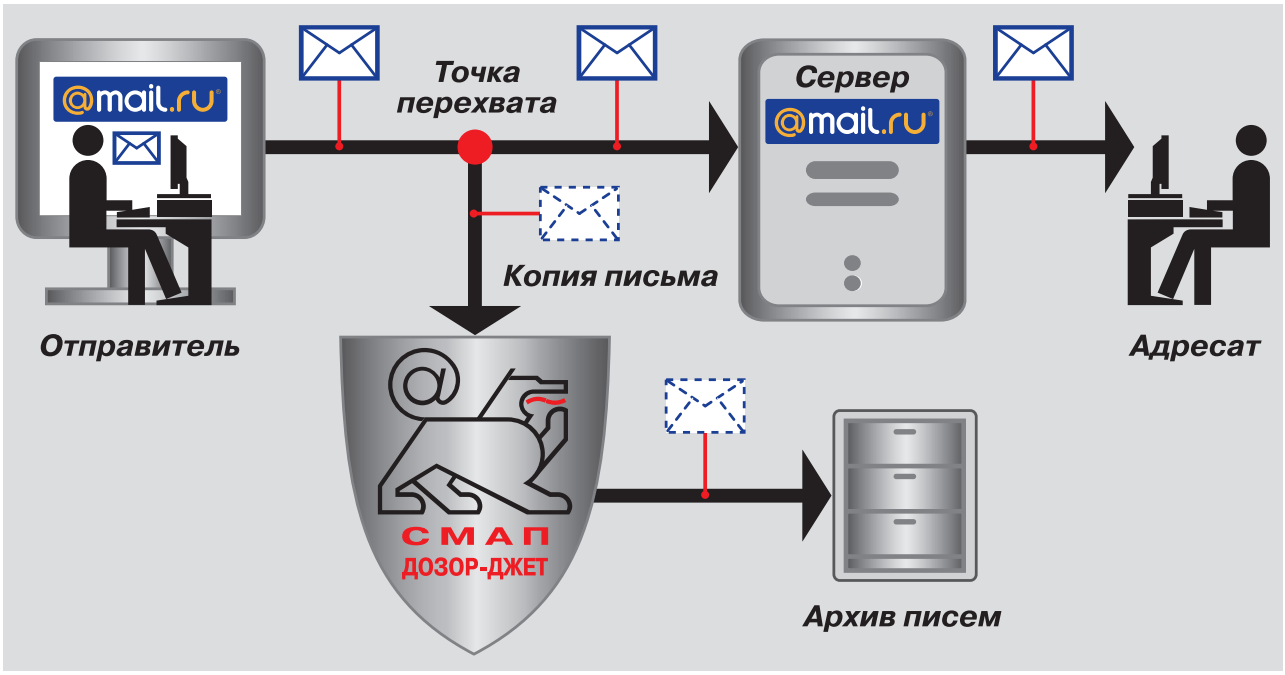


Рис. 6 Архивирование веб-почты

емых через интернет-пейджеры (ICQ, AOL, Jabber).

Модуль позволяет осуществить перехват icq-сессий с декодированием текста icq-сообщений.

Применение такого модуля обеспечит сохранность всей истории переписки сотрудников в архиве для возможности ее дальнейшего анализа.

Модуль архивирования веб-почты.

Модуль архивирования веб-почты является дополнительным модулем к СМАП «Дозор-Джет» и предназначен для своевременного выявления утечек конфиденциальной информации, распространения спама и личной переписки, отправляемой через популярные службы веб-почты. На сегодня поддерживается пять серверов веб-почты:

- mail.ru
- yandex.ru
- rambler.ru
- pochta.ru
- gmail.com

Принцип работы

В момент отправки письма с веб-почты его копия со всеми вложениями автоматически на-

правляется для анализа и архивирования в СМАП «Дозор-Джет».

Модуль готов к работе сразу после установки. Его подключение не требует внесения изменений в настройки серверов веб-почты и доступа Интернет.

Выгоды от внедрения модуля

1. **Отдел ИБ.** Расследование инцидентов, связанных с утечкой конфиденциальной информации через веб-почту.
   В случае отправки подозрительного письма через веб-почту СМАП «Дозор-Джет» автоматически отправит уведомление об этом сотруднику службы ИБ (что позволяет своевременно реагировать на инцидент) и положит это письмо в архив — для накопления «доказательной базы».
2. **Руководство компании.** Соответствие нормативным актам.
   Использование модуля предоставляет уникальную возможность архивировать веб-почту в дополнение к архивированию корпоративной почты, которое обеспечивается системой мониторинга и архивирования почтовых сообщений «Дозор-Джет». Это позволяет компании более полно соответствовать требованиям ряда российских и международных нормативных актов. Среди них ФЗ «О персональных данных», ФЗ «Об архивном деле в РФ», стандарт Банка России по ИТ-безопасности, соглашение Basel II, американские законы SOX, GLBA, HIPAA.
3. **Отдел HR.** Выявление неблагонадежных сотрудников.
   Модуль архивирования веб-почты позволяет своевременно уведомлять сотрудников отдела HR о фактах использования служб веб-почты для рассылки резюме, а также выявить сотрудников, занимающихся дополнительным заработком в рабочее время и за счет использования интернет-ресурсов компании. Методом обнаружения этого обстоятельства может служить регистрация факта рассылки результата выполненной второй работы или рассылка спама в рекламных целях с рабочего места.
4. **Отдел ИТ.** Снижение нагрузки на сеть.
   Уже одно использование сотрудниками сервисов веб-почты с большой вероятностью указывает на личную переписку.
   Архивирование веб-почты позволяет проанализировать занятость сотрудников личной перепиской и развлечениями — пересылкой не относящихся к работе файлов (фото, музыки, видео и т.д.) через сервисы веб-почты.
   Такой анализ позволяет снизить объем неделового трафика и, как следствие, снизить нагрузку на сеть, сократить затраты на оплату услуг доступа в Интернет и потерю рабочего времени сотрудников.

Система контроля веб-трафика СКВТ «Дозор-Джет» 2.0

Риски неконтролируемого использования Интернета

Неконтролируемое использование Интернета и отсутствие защиты сетевых ресурсов несет в себе множество угроз для бизнеса компании. Среди основных рисков, возникающих при использовании Интернета, можно выделить:

- вирусные атаки;
- снижение пропускной способности сети;
- резкое увеличение неделового трафика;
- утечку конфиденциальной информации;
- снижение производительности труда сотрудников.

Зачем создали российский продукт?

На необходимость создания системы контроля веб-трафика специалистам компании «Инфосистемы Джет» неоднократно указывали заказчики. На вопрос заказчикам: «Почему вы не покупаете готовый зарубежный продукт?» — многократно получали следующие ответы:

- эти продукты плохо работают с российскими интернет-сайтами;
- высокая стоимость;
- отсутствие русскоязычной технической поддержки, а также интерфейса программы и документации на русском языке.

Исходя из потребностей заказчиков и с учетом вышеописанных замечаний к зарубежным продуктам, компанией «Инфосистемы Джет» создана система контроля веб-трафика (СКВТ) «Дозор-Джет», вторая версия которой выпущена 26 сентября 2007г.

Назначение СКВТ «Дозор-Джет» 2.0

Система контроля веб-трафика СКВТ «Дозор-Джет» 2.0 предназначена для защиты корпоративных сетей от рисков, связанных с использованием интернет-ресурсов. Защита обеспечивается комплексом мер, включающим в себя фильтрацию содержимого информационного обмена, осуществляемого по протоколам http и ftp over http, авторизацию пользователей и протоколирование их действий.

СКВТ «Дозор-Джет» 2.0 осуществляет контроль проходящего веб-трафика с целью предотвращения доступа к запрещенным ресурсам и утечки важной информации. СКВТ «Дозор-Джет» 2.0 обеспечивает следующие функциональные возможности:

- анализ веб-трафика по различным критериям. Объектом анализа является информация, передаваемая в запросах и ответах протоколов HTTP и FTP over HTTP.
- Выполнение заранее определенных действий над передаваемой информацией, соответствующей заданным критериям. Примерами действий могут быть блокировка доступа, явное разрешение доступа и разрешение доступа после подтверждения пользователем.
- Автоматизированное помещение в архив данных о передаваемой информации, отвечающей заданным критериям.
- Формирование статистических профилей (отчетов) по различным критериям, таким как объем доставляемой информации или количество запросов по сайтам, типам данных и т.п.

При фильтрации данных применяются методики, позволяющие выполнить подробный анализ передаваемой информации, определить форматы передаваемых данных, определить язык и кодировку для текстовых данных. Применение этих методик делает СКВТ «Дозор-Джет» 2.0 максимально независимой от служебной информации, которая зачастую не соответствует действительности. Кроме того, служебная информация может быть подменена, что приведет к неправильной обработке данных.

Выгоды от внедрения СКВТ «Дозор-Джет»:

- минимизация риска утечки конфиденциальной информации при использовании сотрудниками интернет-ресурсов благодаря блокированию посещения нецелевых сайтов и фильтрации содержимого информации, исходящей из корпоративной сети вовне;
- минимизация передачи потенциально опасных вложений, вирусов и вредоносных кодов посредством антивирусной проверки программами сторонних производителей;
- уменьшение затрат на содержание интернет-сервиса посредством запрета или ограничения на скачивание файлов большого объема (музыка, видео, фото);
- выявление фактов поиска работы сотрудниками через специализированные сайты;
- повышение производительности труда сотрудников путем ограничения использования Интернета в личных целях в рабочее время.

Состав и архитектура

СКВТ «Дозор-Джет» 2.0 состоит из нескольких подсистем, обеспечивающих решение конкретных задач:

- подсистема фильтрации и аутентификации обеспечивает проверку прав доступа пользователя, определяет для него политику безопасности и на ее основании выполняет анализ данных, передаваемых в обоих направлениях;
- кэш-сервер служит для кэширования данных обмена с внешними серверами, для кэш-сервера используется ПО Squid (http://squid-cache.org);
- подсистема управления реализует управление политиками безопасности и пользователями Интернета;
- подсистема отчетности служит для формирования отчетов об использовании внешних ресурсов;
- база данных обеспечивает хранение политик безопасности для групп пользователей, а также журналов доступа пользователей к внешним ресурсам;
- подсистема реагирования получает сообщения от подсистемы фильтрации и аутентификации и выполняет заданный набор действий;

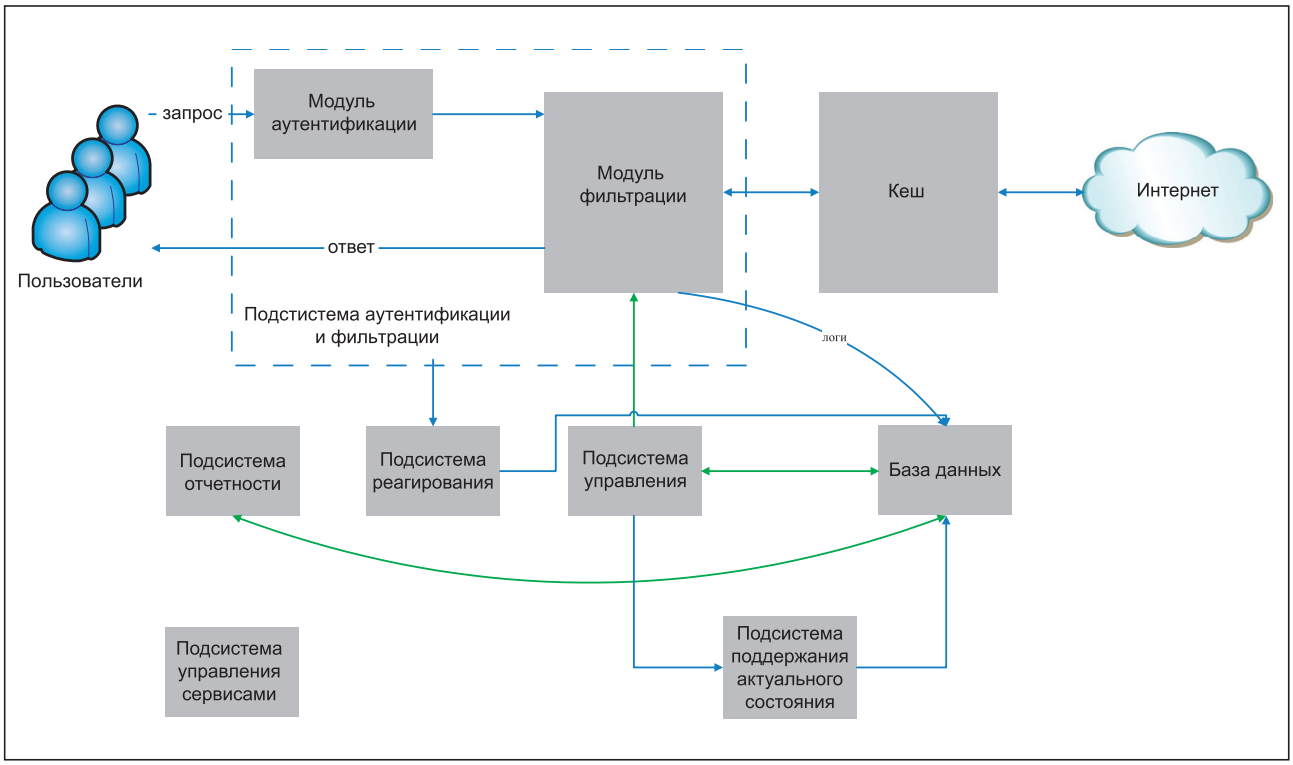


Рис. 7 Архитектура СКВТ «Дозор-Джет»

- подсистема управления сервисами следит за работой всех сервисов СКВТ «Дозор-Джет»;
- подсистема поддержания актуального состояния системы запускает действия по заданному расписанию.

Схема взаимодействия основных подсистем СКВТ «Дозор-Джет» представлена на рис. 7.

Программный комплекс СКВТ «Дозор-Джет» 2.0 включает в себя систему централизованного управления через веб-интерфейс с использованием защищенного ssl-соединения.

Системные требования и производительность

Программный комплекс СКВТ «Дозор-Джет» 2.0 функционирует на операционной системе CentOS 4.3. На данный момент существует два варианта реализации:

1 — в виде appliance;
2 — в виде распределенной системы (фермы) фильтрующих серверов.

Для обеспечения необходимой производительности и надежности фильтрации нагрузка распределяется на ферму из двух и более фильтрующих хостов с единой политикой. Система обеспечивает привязку пользователей к политике на основании исходящего адреса соединения или по имени пользователя и паролю (в СКВТ есть свой список пользователей, а также возможна авторизация на основании информации из имеющихся у клиента служб каталогов) и позволяет производить фильтрацию веб-трафика по ряду параметров, таким как содержимое URI, типы передаваемых данных, содержимое данных и некоторым другим. Комплекс обеспечивает автоматическую обработку запросов и принятие решения о доставке или запрете доступа к ресурсам. Решения принимаются на основании политики, общей для всех фильтрующих элементов. Комплекс предоставляет администратору управлять критериями политики (списками ресурсов и т.д.). Вариант подключения СКВТ «Дозор-Джет» 2.0 приведен на рис. 8.

Благодаря возможности масштабирования производительность программно-аппаратного комплекса СКВТ «Дозор-Джет» 2.0 лишена жестких ограничений по количеству подключенных пользователей и практически не создает задержек при информационном обмене.

Антивирусная проверка

Возможность интеграции СКВТ «Дозор-Джет»2.0 со средствами третьих производителей позволяет адаптировать политику использова-

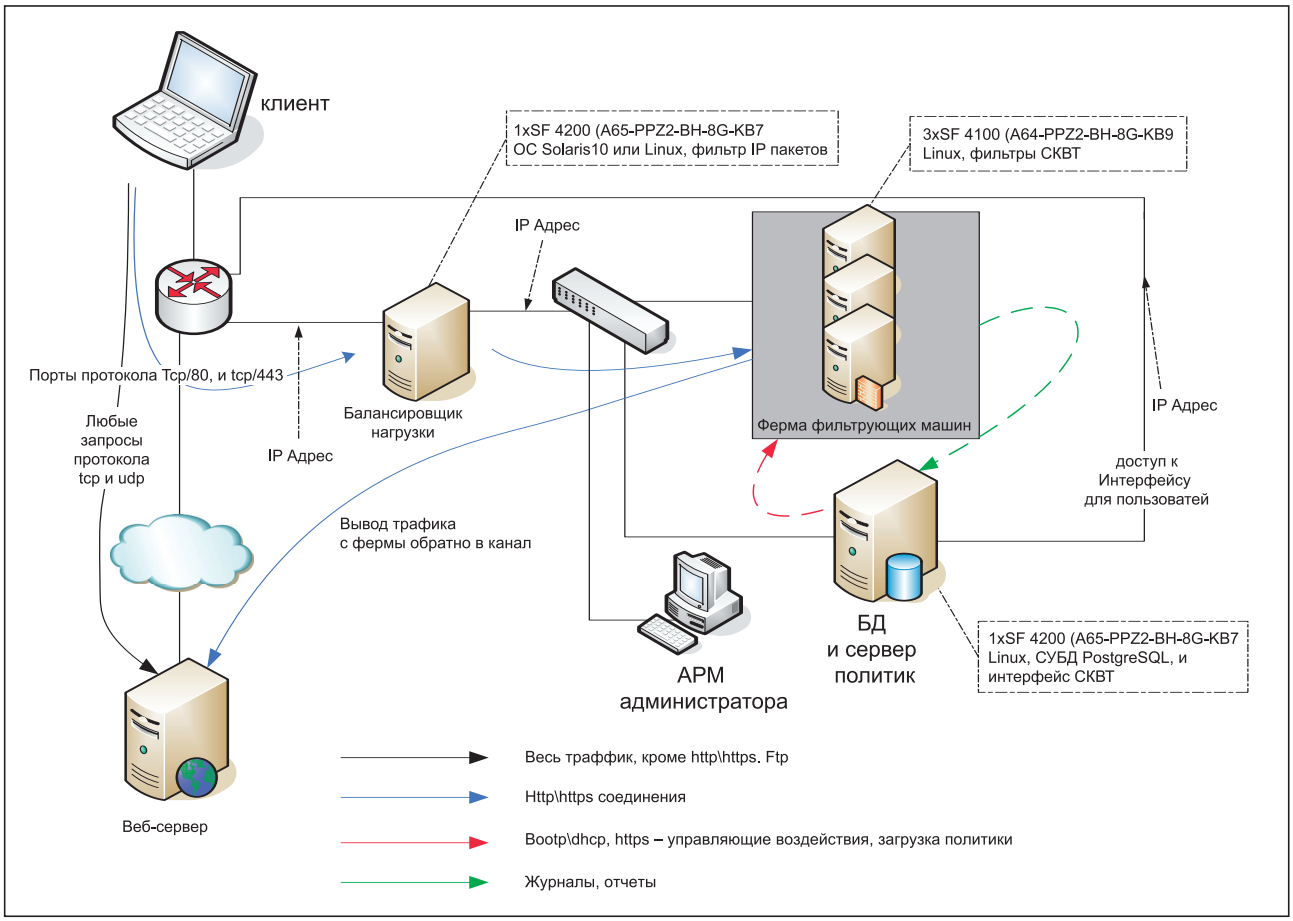


Рис. 8 Вариант подключения СКВТ «Дозор-Джет» 2.0 в виде распределенной системы

Балансировщик нагрузки	Распределение нагрузки по ферме. Распределение трафика. Вывод трафика с фермы обратно в канал. NAT. Может быть реализовано на активном оборудовании.
Ферма фильтрующих машин	Обработка запросов. Журналирование.
БД	Хранение журналов. Построение отчетов.
Сервер политик	Администрирование, контроль функционирования комплекса. Сервер сетевой загрузки. Сервер пользовательских интерфейсов.

Таблица 1. Пояснения к рис. 8

ния интернет-ресурсов компании и избегать, например, загрузки данных с тех сайтов, откуда ранее был получен вредоносный мобильный код.

Контроль ресурсов

В соответствии с политикой использования интернет-ресурсов для каждой группы пользователей устанавливается связь с набором политик, которые обеспечивают фильтрацию по следующим параметрам:

- расширение файлов;
- тип данных;
- ресурсы (URL);
- ключевые слова;
- расписание;
- категории (используется база категорий компании Netstar Inc).

Фильтрация по расширению файлов

Данный метод фильтрации обеспечивает проверку имен передаваемых/ получаемых файлов на наличие определенных расширений, что позволяет, например, блокировать передачу мультимедийных файлов в рабочее время. Этот метод обеспечивает быструю проверку.

Фильтрация по типам данных

Фильтрация по данному методу обеспечивает высокую степень надежности определения формата передаваемых данных. Тип данных в этом случае определяется не по расширению файла, а распознается с помощью специального программного обеспечения. (См. врезку Wtf — what the file?)

Фильтрация по ресурсам (URL)

Данный метод фильтрации позволяет ограничить доступ на уровне запроса ресурсов. С помощью регулярных выражений возможно запрещение доступа как к целым сайтам, так и к их отдельным веб-страницам.

Фильтрация по ключевым словам (контентная фильтрация)

Данный метод фильтрации обеспечивает проверку получаемой информации на наличие в ней определенного текста (допустимо использование регулярных выражений). При обнаружении заданных слов передача данных либо блокируется сразу, либо продолжается поиск других слов до тех пор, пока не будет превышен определенный порог, заданный администратором системы. Механизм реализации основан на присвоении словам весовых коэффициентов и их последующего суммирования. Например, данный метод может быть очень удобен для блокировки передачи данных через веб-почту, серверы которой еще не попали в список запрещенных сайтов.

Фильтрация по расписанию

СКВТ «Дозор-Джет» 2.0 позволяет разграничить доступ к Интернет-ресурсам в зависимости от времени суток и дней недели.

Фильтрация по категориям

Модуль фильтрации основан на базе решения компании NetSTAR Inc. (http://www.netstar-inc.com/eng/products_01.html). Для категоризации ресурса используется внешняя база ресурсов, доступная при наличии лицензии.

Действия по результатам проверки

В зависимости от результатов конкретной проверки СКВТ «Дозор-Джет» 2.0 может реагировать различным образом — блокировать передачу данных, разрешать передачу, разрешать передачу с подтверждением пользователя, отправлять уведомительное сообщение администратору.

Все производимые СКВТ «Дозор-Джет» 2.0 действия пользователей протоколируются, что позволяет анализировать использование интернет-ресурсов и корректировать политику доступа.

Отчеты

СКВТ «Дозор-Джет» 2.0 раскрывает полную и реальную картину использования интернет-ресурсов сотрудниками. Это осуществляется за счет встроенного модуля построения отчетов, который дает возможность получать:

- сводную информацию об использовании интернет-ресурсов всеми пользователями;
- информацию о нарушениях политики безопасности (отчеты практически по любым параметрам веб-трафика).

Совместное использование СМАП «Дозор-Джет» и EMC EmailXtender

Центр информационной безопасности компании «Инфосистемы Джет» предоставляет не только конечные продукты собственной разработки (СМАП и СКВТ «Дозор-Джет»), но и создает решения специфических задач клиентов «под ключ» на основе возможности интеграции собственных продуктов с продуктами других разработчиков.

Одним из успешных примеров разработки нестандартного решения является построение системы корпоративной электронной почты в части подсистемы долговременного (до 3-х лет) хранения почтовых сообщений с обеспечением их юридической значимости и целостности.

Разработанное решение было основано на совместном использовании СМАП «Дозор-Джет» и EMC EmailXtender. При этом СМАП «Дозор-Джет» использовался в качестве фильтра почтовых сообщений и создания оперативного архива, а EMC EmailXtender — в качестве долговременного архива писем.

Разработка решения началась с определения целей и задач, которые должна решать система, а также основных требований к ней.

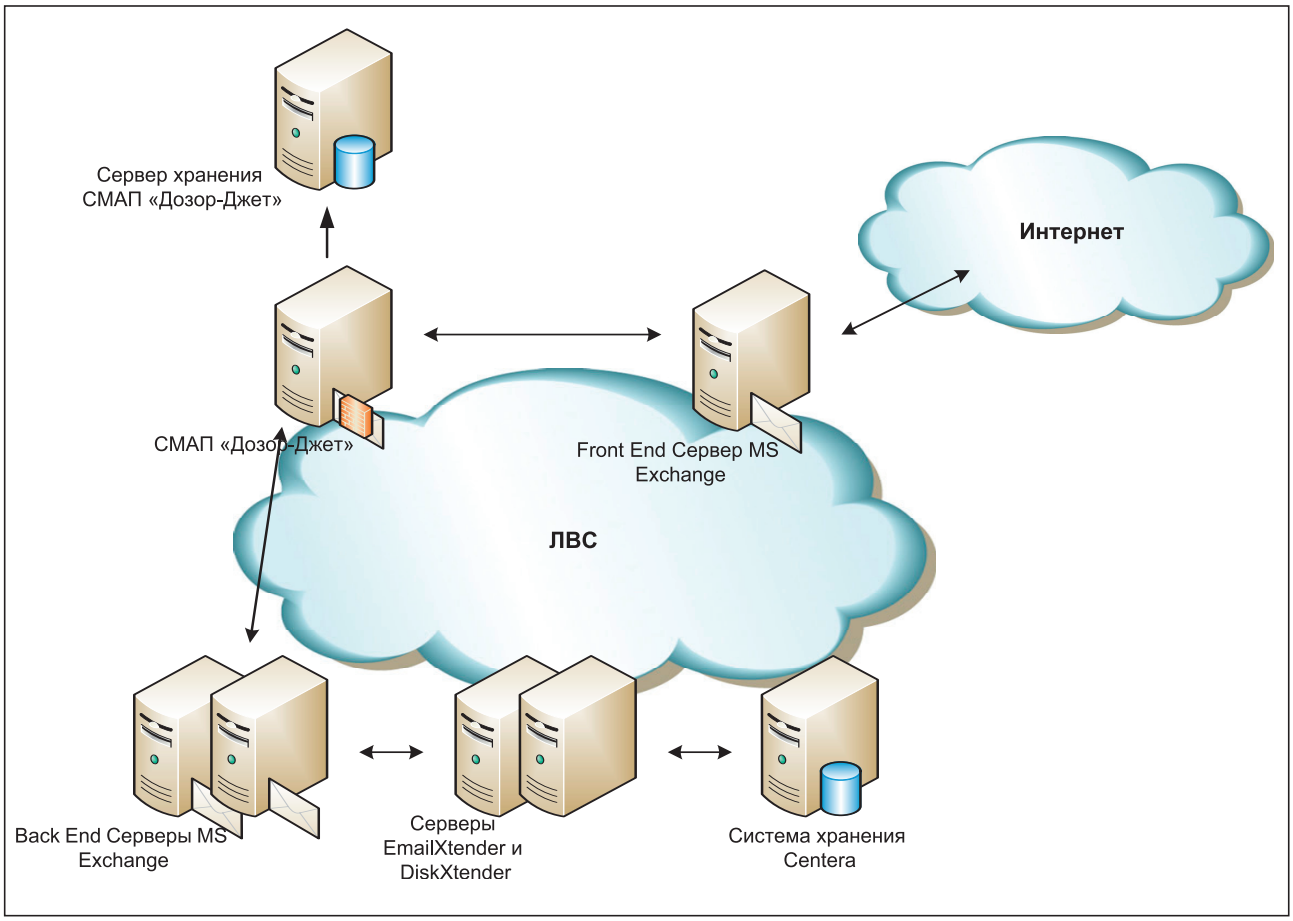


Рис. 9 Принципиальная схема подключения оборудования

Основные цели и задачи

Подсистема контроля и архивного хранения предназначена для архивного хранения всех входящих и исходящих сообщений электронной почты, а также для осуществления мониторинга и фильтрации почтовых сообщений. Она должна обеспечивать:

- анализ входящих, исходящих и внутренних почтовых сообщений, передаваемых посредством протокола SMTP, на предмет соответствия определенным критериям;
- фильтрацию почтовых сообщений с последующим выполнением в отношении них определенных действий в соответствии с заданными администраторами правилами;
- блокирование подозрительных сообщений;
- ведение оперативного архива, доступного службе безопасности;
- ведение долговременного архива, доступного всем пользователям системы.

В части архивного хранения подсистема должна обеспечивать:

- невозможность внесения изменений в почтовые сообщения, помещенные в архив;
- невозможность удаления почтовых сообщений, помещенных в архив;
- невозможность фальсификации почтовых сообщений;
- возможность онлайнового доступа и поиска в архиве почтовых сообщений;
- возможность сохранения поисковых запросов;
- возможность разграничения доступа пользователей к архиву почтовых сообщений;
- гарантированное хранение всех входящих и исходящих почтовых сообщений;
- возможность просмотра почтовых сообщений, их структуры, заголовков и пометок;
- возможность просмотра статистических данных.

Описание решения

Предлагаемое решение состоит из следующих компонентов:

- система мониторинга и архивирования почтовых сообщений «Дозор-Джет»;
- программное решение EMC EmailXtender/DiskXtender;
- система архивного хранения EMC Centera.

Принципиальная схема подключения оборудования в существующую инфраструктуру приведена на рис. 9.

Система мониторинга и архивирования почтовых сообщений «Дозор-Джет» представляет собой программный комплекс, предназначенный для сбора и анализа проходящих через него сообщений электронной почты, передаваемых посредством протокола SMTP, для идентификации событий, которые могут свидетельствовать о нарушении правил информационного обмена, а также для создания оперативного почтового архива в интересах службы безопасности компании.

СМАП «Дозор-Джет» является инструментом реализации политики использования электронной почты в компании и позволяет контролировать ключевые аспекты информационной безопасности организации, связанные с использованием электронной почты.

Обеспечение безопасного функционирования системы электронной почты

Основой обработки сообщений электронной почты в СМАП «Дозор-Джет» является фильтр — набор данных, который определяет алгоритм обработки почтовых сообщений и описывает способы воздействия на письма, соответствующие тем или иным условиям. Если в результате фильтрации устанавливается, что почтовое сообщение должно быть доставлено, оно передается подсистеме доставки.

Основу почтового фильтра составляют правила, выполняемые последовательно в процессе применения фильтра к сообщению. Каждое правило состоит из условия и набора действий. Условия реализуют проверку сообщений на соответствие определенным критериям. Действия выполняются, если письмо удовлетворяет условию правила.

Условия фильтрации могут накладываться как на общие свойства сообщения (размер письма, количество вложений и т. п.), так и на служебные поля письма и ключевые слова, встречающиеся в тексте письма. Анализу подвергается не только текст сообщения и его вложенных частей, но и текст, выделяемый из присоединенных файлов. Для всех вложенных и выделяемых частей производится анализ форматов, и по его результатам выполняется дальнейшая обработка.

Если в почтовом сообщении содержится вложенный архив (файл с расширением zip, tar, rar, arj, gzip и пр.), то он распаковывается и его содержимое анализируется аналогичным образом.

Правила группируются в наборы, что позволяет осуществлять сложные алгоритмы проверок. Фильтрация начинается с головного набора правил. Правила выполняются в заданном порядке. Если сообщение удовлетворяет условию правила, то выполняются определенные действия, после чего применяется следующее правило.

В процессе обработки СМАП «Дозор-Джет» над сообщением выполняются следующие действия:

- прием сообщения и помещение его в очереди ожидания фильтрации (при этом СМАП «Дозор-Джет» получает письмо от почтового сервера через предопределенный порт и размещает в специальном каталоге на файловой системе);
- перемещение сообщения из очереди писем, ожидающих обработки, во временный каталог (при этом из очереди выбирается письмо в соответствии с полученным от почтового сервера порядком и приоритетом);
- применение к почтовому сообщению фильтра, ассоциирующего с письмом набор действий (в ходе чего при необходимости происходит распаковка и выделение текстовых частей сообщения, необходимых для проверки выполнения условий и правил фильтрации, заложенных в политике);
- выполнение всех указанных действий над письмом в соответствии с политикой (под действиями понимается доставка письма, архивирование, установление пометки и т.д.).

В качестве основных действий, выполняемых по результатам фильтрации сообщения, могут выступать:

- сохранение или регистрация почтового сообщения в архиве;
- отправка уведомления реципиенту (администратору безопасности СМАП «Дозор-Джет» и/или отправителю/получателю и т.п.);
- доставка почтового сообщения одному или нескольким адресатам с учетом приоритета (доставить вне очереди или отправить в заданное время);
- отказ в передаче;

- установка пометки;
- выполнение другого набора правил;
- установка специальных прав доступа и др.

Возможность помещения в архив сообщений, отвечающих определенным условиям, позволяет администраторам безопасности СМАП «Дозор-Джет» анализировать подозрительную корреспонденцию и принимать решения о доставке письма адресатам, удалении письма, отправки письма на указанный почтовый адрес, установке или снятию пометки.

Почтовый архив предоставляет администратору безопасности возможность удобного анализа задержанной почты.

Система EMC EmailXtender/DiskXtender предназначена для создания долговременного почтового архива и решения двух основных проблем, с которыми сталкиваются пользователи корпоративных почтовых систем: управление хранением (storage management) и обеспечение соответствия нормативным требованиям (compliance).

Обеспечение соответствия нормативным требованиям

На практике обеспечение соответствия нормативным требованиям по хранению электронной почты, будь то формальные требования законодательства, отраслевые нормативы или принятая в конкретной организации политика, означает необходимость обеспечения:

1. Гарантированного захвата всех почтовых сообщений, проходящих через почтовую систему, до их доставки пользователю и помещение их в архив в оригинальном формате.
2. Классификации сообщений и их долговременного (в течение нескольких лет) хранения в зависимости от присвоенного класса.
3. Предоставления гарантии того, что сообщения, хранящиеся в почтовом архиве, не могут быть искажены и не могут быть удалены до окончания назначенного срока хранения.
4. Быстрого поиска сообщений в архиве по различным критериям с гарантией полноты и аккуратности результатов поиска.

Для обеспечения требуемой функциональности EmailXtender совместно со службами Exchange в реальном времени перемещают копии входящих и исходящих сообщений в служебный почтовый ящик, тем самым гарантируя невозможность изменения и/или удаления сообщений пользователями до помещения их в архив. Затем EmailXtender периодически перемещает сообщения из служебного почтового ящика на архивный сервер, где они дедублицируются, классифицируются, индексируются и помещаются на долговременное хранение в EMC Centera.

Таким образом, в ходе процесса архивирования создается хранилище почтовых сообщений, отобранных в соответствии с установленными политиками и защищенных от изменения и удаления в течение установленных сроков хранения на аппаратном уровне.

Для гарантированного долговременного хранения данных используется специализированная платформа архивного хранения EMC Centera, обеспечивающая постоянную доступность содержимого и простой доступ к любому его элементу, а также гарантированную достоверность и защиту содержимого от искажений, неограниченную масштабируемость и минимизацию затрат на администрирование и обслуживание.

Управление хранением

Под управлением хранением данных подразумевается весь комплекс мер, направленных на минимизацию стоимости хранения почтовых сообщений, повышение эксплуатационной эффективности и повышение производительности пользователей при работе с почтовой системой. Основными заказчиками решения по управлению хранением являются сотрудники департамента ИТ, для которых важна минимизация усилий по управлению почтовым хранилищем и надежность работы архивной подсистемы, а также обычные пользователи системы, требующие обеспечить возможность хранения почтовых сообщений без каких-либо ограничений по объему и прозрачный доступ к своим данным.

EmailXtender дает возможность заменить редко используемые пользователями сообщения (или вложения) ссылками. При этом на основе определенных администратором критериев (например, для всех писем объемом более 100 Кбайт, полученных более 6 месяцев назад) производится замена сообщений, хранящихся на почтовом сервере, указателями на соответствующие сообщения, хранящиеся в архиве. Как правило, такая замена позволяет достичь 50-60% сокращения объема почтового хранилища.

При этом пользователям по-прежнему предоставляется прозрачный доступ к содержимому почтовых ящиков. Работа с сообщениями, замененными на ссылки, практически ничем не отличается от обычной практики. Основное раз-

личие — во времени реакции системы. При использовании EMC Centera, типичная дополнительная задержка при открытии письма составляет не более 5-10 секунд.

Таким образом, можно рекомендовать совместное использование СМАП «Дозор-Джет» и EMC EmailXtender. Комплекс «Дозор-Джет» будет обеспечивать мониторинг потока почтовых сообщений, их анализ и фильтрацию. Также решение «Дозор-Джет» будет использоваться для создания оперативного архива, используемого службой безопасности и/или юридическим отделом заказчика для анализа недавно отправленных сообщений. В свою очередь EMC EmailXtender предлагается использовать для построения долговременного масштабируемого почтового архива, обеспечивающего соответствие нормативным требованиям и управление хранением данных почтовых хранилищ Microsoft Exchange.

Схема подключения оборудования, приведенная на рис. 9, свидетельствует о том, что оба продукта могут функционировать совместно в рамках системы корпоративной электронной почты и будут дополнять друг друга, решая каждый свою задачу.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555