==========

Контроль над корпоративной электронной почтой: система «Дозор-Джет»

==========

С ростом популярности Интернета, электронная почта остается важнейшим средством коммуникаций. На ее долю приходится более половины всего сетевого трафика. Электронная почта имеет все необходимые качества для того, чтобы быть самым популярным средством связи: ***низкая стоимость, простота использования, большое количество пользователей***. Удобство обмена информацией с помощью электронной почты сделали это средство коммуникации ***самым распространенным видом связи*** для большинства организаций.

Однако, наряду с многочисленными преимуществами, существует ***ряд рисков***, связанных с использованием электронной почты, которые могут привести к ***значительному снижению эффективности работы организации, потере значимой информации***.

Система мониторинга и архивирования почтовых сообщений (СМАП) «Дозор-Джет» представляет собой специализированное программное средство, позволяющее реализовать ***корпоративную политику использования электронной почты*** и уменьшать риски неконтролируемой работы с электронной почтой в компании.

«Дозор-Джет» позволяет решить ряд проблем, таких как:

- **Утечка конфиденциальной информации;**
- **Передача сообщений неприемлемого содержания;**
- **Передача потенциально опасных вложений, вирусов и вредоносных кодов;**
- **Передача неприемлемых вложений – большого размера, нежелательного формата и т.д.;**
- **Несанкционированные почтовые рассылки («спам»);**
- **Ошибочное направление писем;**
- **Потери рабочего времени, ресурсов или блокирование почтового сервиса.**

Система «Дозор-Джет» осуществляет мониторинг и контроль всех входящих, исходящих и внутренних почтовых сообщений. Мониторинг включает в себя анализ заголовков и структуры сообщений и проверку на наличие в тексте сообщения или прикрепленных файлах разрешенных или запрещенных к использованию в почтовых сообщениях слов или последовательностей слов. Результатом мониторинга может стать, например, задержание подозрительных писем. «Дозор-Джет» позволяет задавать корпоративные правила обработки входящей и исходящей почты, в зависимости от тех или иных предопределенных событий, например:

- Запрет пересылки файлов формата EXE всем, кроме разработчиков программного обеспечения;
- Запрет пересылки картинок формата GIF и JPEG всем, кроме сотрудников рекламного отдела;
- Ограничение на объем и количество присоединенных файлов, направляемых отдельным адресатам;
- Автоматическое уведомление руководителя подразделения о письмах с определенными пометками или отвечающих поставленным условиям.

Использование гибкой системы фильтрации сообщений позволяет реализовать практически любую схему прохождения электронной почты. Например, возможна так называемая отложенная доставка почтового сообщения, когда решение о доставке конечному пользователю предпринимается только после дополнительного анализа Администратором безопасности и другими системами безопасности (проверка на наличие вирусов, контроль массовой рассылки сообщений рекламного характера, наличие неопознанных (закодированных) вложений и пр.).

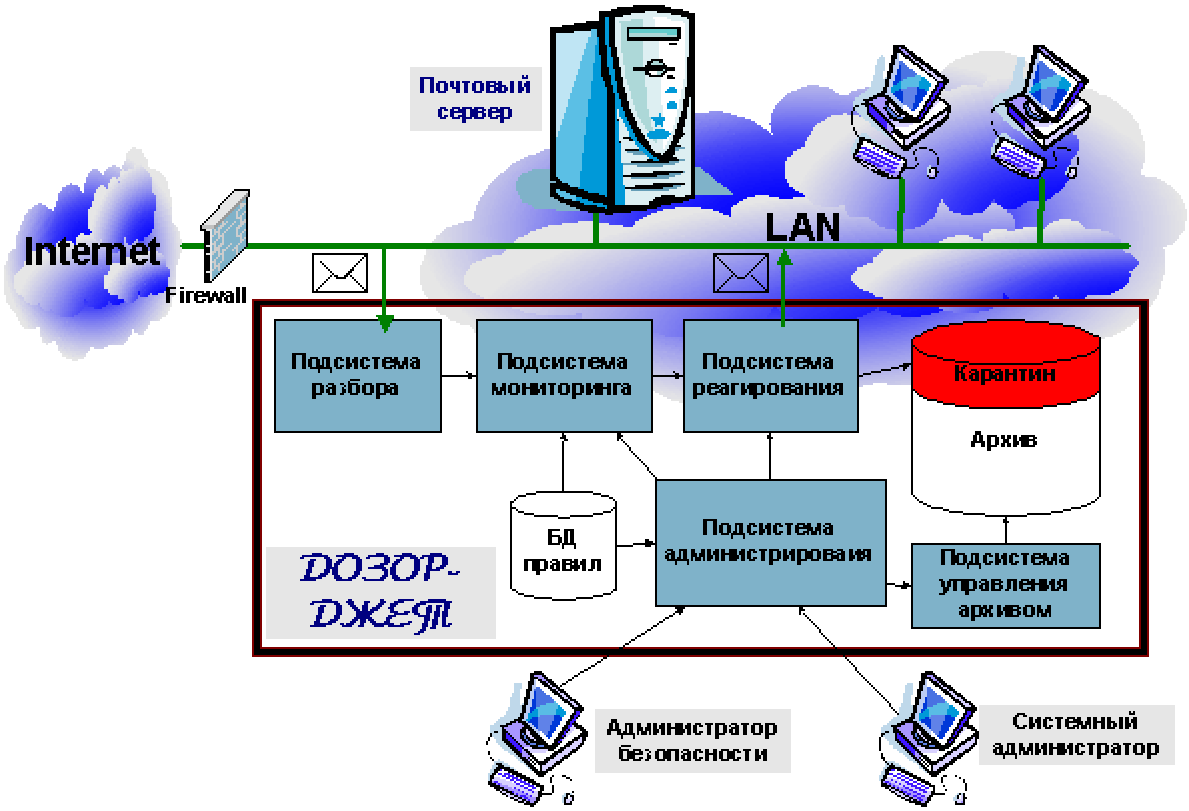
Состав системы «Дозор-Джет»

Система «Дозор-Джет» представляет собой набор программных модулей, которые обеспечивают потоковый анализ SMTP-трафика почтовых сообщений как между локальной сетью компании и внешним миром, так и внутри локальной вычислительной сети компании, а также ведение архива почтовых сообщений.

"Дозор-Джет" состоит из следующих основных подсистем:

- подсистемы мониторинга, включающей в свой состав три модуля - модуль разбора сообщений, модуль анализа и модуль реагирования;
- подсистемы архивирования;
- подсистемы администрирования.

Рисунок 1: Состав системы «Дозор-Джет»



Все почтовые сообщения, поступающие из внешней среды (Интернет) или из локальной сети компании, обрабатываются системой «Дозор-Джет». В процессе обработки система принимает решение о дальнейшей отправке сообщения адресату или о его задержке, архивировании сообщения, а также уведомлении Администратора безопасности о прохождении сообщения определенного типа. Вся почта, успешно прошедшая проверку системы, перенаправляется почтовому серверу для дальнейшей отправки по назначению.

Анализ содержимого почтовых сообщений

Все попадающие в «Дозор-Джет» почтовые сообщения проходят процедуру разбора на составляющие компоненты. При этом происходит разбор как заголовков сообщения (отправитель, получатель, скрытая копия, тело сообщения и пр.), так и всей его структуры, вне зависимости от количества уровней вложенности. Это позволяет анализировать сообщения, содержащие прикрепленные файлы, а также сообщения, которые были несколько раз перенаправлены корреспондентами.

Анализ разобранных сообщений включает:

- Определение характеристик сообщения – отправитель, получатель, дата, размер, структура;
- Определение характеристик вложений – имя, размер, тип, количество;
- Распознавание форматов вложений –

сжатия/архивирования, документов,

исполнимых файлов, графических, аудио- и видеофайлов;

- Анализ текста в заголовках сообщения, теме, теле письма и вложенных файлах.

Варианты реагирования по результатам проверок

При обнаружении соответствия почтовых сообщений заданным в правилах фильтрации критериям, система осуществляет одно или несколько из заранее предписанных действий:

- Отправка сообщения получателю;
- Отказ в передаче (блокировка сообщения);
- Задержка сообщения для последующего анализа;
- Помещение в карантинную зону;
- Регистрация сообщения;
- Архивирование сообщения;
- Проставление пометок;
- Отправка уведомления (оповещение администратора системы и др.).

При этом обязательно осуществляется протоколирование всех производимых действий.

Архивирование сообщений и поиск по архиву

Архивирование почтовых сообщений позволяет хранить, учитывать и систематизировать сообщения и документы, передаваемые посредством корпоративной электронной почты. В архиве может осуществляться хранение либо регистрационной информации либо сообщения целиком.

Система «Дозор-Джет» предоставляет возможность как краткосрочного, так и долговременного хранения почтовых сообщений, удовлетворяющих определенным критериям. Кроме того, подотчетность и невозможность отказа от совершенных действий является немаловажным фактором повышения ответственности пользователей корпоративной почты за содержание передаваемой информации.

На каждое сообщение заводится учетная карточка, которая содержит всю идентификационную информацию сообщения и описание его структуры. В дальнейшем в учетную карточку попадает информация, связанная с жизненным циклом данного сообщения в системе (причина и сроки задержки, дальнейшие административные действия, время хранения в архиве и пр.). Для реализации модуля архивирования используется СУБД Oracle.

Система архивирования позволяет осуществлять просмотр сообщений в архиве и поиск по любым критериям, (в т.ч. контекстный поиск), выполнять различные действия с хранимыми сообщениями, предоставляет возможность получения статистики использования почтового сервиса.

Получение статистики

Статистическая обработка накопленной в системе «Дозор-Джет» информации предоставляет возможность анализа эффективности использования почтового сервиса компании: насколько активно ведется переписка с партнерами и клиентами, как часто пользователи передают по почте файлы большого размера или определенного типа – графические, аудио- или видео-файлы. Также появляется возможность анализа эффективности и качества работы отдельных подразделений компании: средние сроки обработки запросов клиентов, количество обращений, поступающих в подразделения компании и многое другое.

Администрирование системы

Обслуживание системы «Дозор-Джет» осуществляется Администратором безопасности, в задачи которого входит обеспечение надежного функционирования системы, настройка фильтров, управление подсистемой архивирования. В обязанности Администратора безопасности могут быть включены, кроме этого, регулярный контроль и анализ задержанных писем, осуществление поисковых запросов и реагирование на сообщения системы.

Разграничение доступа к компонентам системы

Доступ к элементам системы «Дозор-Джет» определяется на основе использования списков прав доступа для каждой категории объектов. Например, имеются списки для работы с условиями, с поисковыми запросами, с шаблонами уведомлений.

Существуют также списки прав на выполнение определенных функций администрирования.

Особенности системы

Использование открытых стандартов

В системе «Дозор-Джет» для ведения архива электронных сообщений используется СУБД Oracle, что позволяет, во-первых, использовать стандартные средства обработки, поиска и анализа накопленной информации, а, во-вторых, достаточно легко интегрировать базу почтовых сообщений с уже существующими в компании системами с целью ее более широкого использования.

Применение в качестве пользовательского интерфейса Web-навигатора унифицирует рабочее место Администратора безопасности, что значительно упрощает как работу по настройке модулей системы, так и текущую работу Администратора безопасности.

Анализ русскоязычных текстов

В отличие от зарубежных аналогов «Дозор-Джет» осуществляет морфологический анализ русскоязычных текстов и поддерживает поиск последовательности символов (слов) как латиницы, так и кириллицы в кодировках Win-1251, DOS-866, ISO-8859.5, KOI-8, Mac.

Сертификация в Гостехкомиссии России

«Дозор-Джет» имеет сертификат Гостехкомиссии России № 465 от 14.06.01 на соответствие Техническим условиям и требованиям руководящего документа «Классификация средств защиты информации по уровню контроля недекларированных возможностей», что обеспечивает выполнение требований действующего законодательства в данной области.

Надежность и безопасность

Использование UNIX платформы (SPARC/ Solaris, HP-Unix, Linux) и современной промышленной СУБД (Oracle) для работы системы «Дозор-Джет» позволяет удовлетворить самым высоким требованиям по надежности, доступности и масштабируемости системы.

Размещение системы «Дозор-Джет»

Система «Дозор-Джет» размещается на выделенном сервере, располагаемом, как правило, в демилитаризованной зоне сети. Архив почтовых сообщений системы «Дозор-Джет» в случае большого количества почтовых адресов предпочтительно разместить на отдельном сервере.

Конкретная схема размещения и требования к аппаратной платформе для установки компонентов системы «Дозор-Джет» разрабатывается на основе результатов обследования почтовой системы и сбора информации о реализации почтового сервиса и почтового трафика.

Linux-версия «Дозор-Джет»

Linux-версия «Дозор-Джет» - Дозор/LX функционирует под управлением ОС Linux на процессорах с архитектурой Intel. Для хранения архива писем данная версия использует свободно распространяемую СУБД PostgreSQL, которая является стандартом “де-факто” для операционной системы Linux. Эта версия системы обладает той же функциональностью, что и полная версия (платформы SPARC-Solaris и HP-UX), за исключением функции полнотекстового поиска в архиве писем. Система прошла тестирование на дистрибутивах Red Hat Linux версий 7.1 и 7.2, а также на Mandrake Linux версии 8.1.

Дозор/LX обладает следующими достоинствами: простота установки системы, отсутствие необходимости в дорогостоящей СУБД, возможность установки на персональный компьютер. Однако Дозор/LX не используется для обработки больших архивов (более 30 000 писем) или больших потоков (более 1000 писем в час) и является «облегченная» версией для небольших компаний. «Облегченная» версия может быть модернизирована до полнофункциональной версии системы, работающей с СУБД Oracle с сохранением накопленного архива.

На основе версии Дозор/LX разработана демонстрационная версия Дозора, предназначенная для знакомства с рабочей системой.

========