ДОЗОР™ джет

Система мониторинга и архивирования почтовых сообщений «Дозор-Джет» является программным средством, позволяющим реализовать корпоративную политику использования электронной почты. «Дозор-Джет» осуществляет контроль содержимого и структуры почтовых сообщений, а также их архивирование.

Система «Дозор-Джет» позволяет предотвратить утечку конфиденциальной информации из компании по каналам электронной почты, не допустить проникновения нежелательной информации в компанию, контролировать внутренние почтовые потоки, вести архив корпоративной электронной почты.

Мониторинг почтовых сообщений

Система «Дозор-Джет» осуществляет мониторинг всех входящих, исходящих и внутренних почтовых сообщений, передаваемых посредством протокола SMTP. При попадании почтового сообщения в систему производится его полный разбор (любого уровня вложенности) на составляющие компоненты и анализ структуры и содержимого как самого сообщения, так и присоединенных файлов. Анализ содержимого заключается в проверке текста сообщения и присоединенных файлов на наличие ключевых слов (например, запрещенных к использованию в почтовых сообщениях). Для повышения эффективности анализа содержимого применяется механизм регулярных выражений. «Дозор-Джет» обладает мощной системой фильтрации сообщений, основанной на правилах, каждое из которых состоит из набора условий и действий, выполняемых системой при соблюдении или не соблюдении определенных условий. Система имеет возможность создания сложных иерархических структур правил, позволяющих реализовать любую политику использования электронной почты.

Реагирование на нарушения политики

Система «Дозор-Джет» автоматически реагирует на нарушения политики использования электронной почты. При соблюдении (или не соблюдении) определенного условия система выполняет действие или последовательность действий, установленную соответствующим правилом политики. Основными действиями являются разрешение или запрет прохождения письма, а также посылка уведомления по назначению, например, администратору безопасности или на консоль администратора системы управления информационной инфраструктурой.

Архивирование почтовых сообщений

Система «Дозор-Джет» осуществляет как долговременное, так и краткосрочное хранение в архиве почтовых сообщений, удовлетворяющих определенным критериям. Задержанные письма хранятся в специальной области архива — карантине. Существует возможность быстрого поиска писем в архиве как по любым атрибутам письма, так и по содержанию (контекстный поиск) и создание запросов любой логической сложности.

Jet infosystems

Основные характеристики системы «Дозор–Джет»

Полный анализ сообщений

- Полный разбор почтовых сообщений любого уровня вложенности на составляющие компоненты;
- распознавание форматов присоединенных файлов всех популярных офисных приложений (включая вложенные в архивы файлы), раскрытие архивов всех распространенных типов и любого уровня вложенности;
- возможность обнаружения OLE-объектов в файлах приложений MS Office;
- анализ русскоязычных почтовых сообщений независимо от используемой кодировки кириллицы (Win-1251, DOS-866, ISO-8859.5, KOI-8, MAC).

Мощная подсистема фильтрации сообщений

- Мощная подсистема фильтрации сообщений, основанная на механизме правил и позволяющая реализовать политику использования электронной почты любой сложности;
- фильтрация по всем компонентам письма: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам;
- расширяемый набор проверок и действий, позволяющий администратору системы создавать собственные методы проверки сообщений и вложений, а также действия над ними;
- «мастер» создания типовых правил - средство построения типовых правил, позволяющее упростить процесс создания начальных правил фильтрации.

Гибкие механизмы реагирования

- Гибкие механизмы реагирования на выполнение условий фильтрации и возможность автоматического выполнения следующих действий: пропустить письмо, запретить прохождение письма, поместить письмо в архив, зарегистрировать письмо, добавить метку к письму, послать уведомление уполномоченным лицам;
- реинжиниринг почтовых сообщений, т.е. возможность модификации сообщений перед доставкой или пересылкой, включая удаление запрещенных вложений и добавление определенного текста (аннотирование) в зависимости от результатов анализа сообщения.

Мощная подсистема архивирования

Мощная подсистема архивирования, реализованная на основе реляционной СУБД Oracle. Архив системы снабжен как механизмом быстрого поиска писем по любым их атрибутам, так и механизмом индексирования, который позволяет осуществлять полнотекстовый поиск по архиву писем. Существует реализация этой подсистемы на основе СУБД PostgreSQL.

Внутренние механизмы защиты

Разграничение доступа ко всем объектам системы, в том числе к письмам, хранящимся в архиве, и правилам их обработки.

Использование открытых стандартов

Использование СУБД Oracle для хранения почтовых сообщений позволяет применять стандартные средства обработки, поиска и анализа накопленной информации, а также интегрировать базу почтовых сообщений в существующие в компании системы документооборота. В качестве пользовательского интерфейса администратора системы используется Web-навигатор.

Интеграция с другими системами

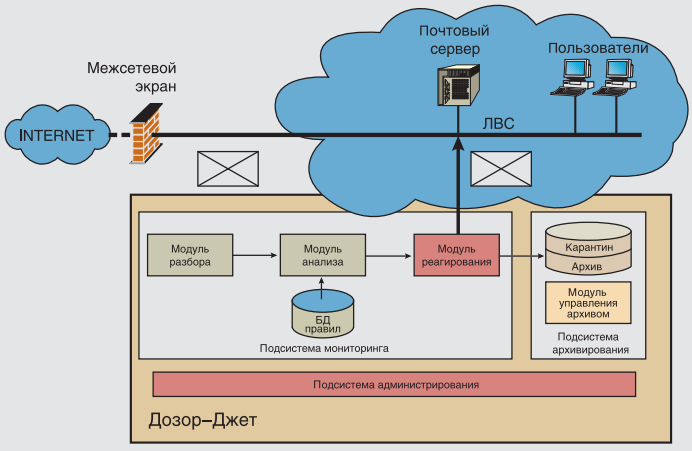
- Возможность интеграции с другими системами, такими как межсетевые экраны и антивирусные программы;
- возможность взаимодействия с системой управления HP OpenView, позволяющая контролировать работу компонентов «Дозор-Джет» и отображать информацию о нарушениях политики использования электронной почты на консоль администратора системы управления;
- возможность использования электронной цифровой подписи (ЭЦП), позволяющая автоматически подписывать почтовые сообщения и проверять подпись.

Надежная и производительная платформа

«Дозор-Джет» функционирует на UNIX-платформе под управлением ОС Sun Solaris, HP-UX и Linux. Система способна обрабатывать десятки мегабайт почтового трафика в час и практически не создает задержки прохождения писем.

Сертифицированное решение

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.



«Инфосистемы Джет»

Россия, 103006, Москва,
Краснопролетарская 6.
Тел.: (095) 972 11 82, (095) 972 13 32
Факс: (095) 972 07 91
www.jet.msk.su, dozor@jet.msk.su