Дополнительные модули системы «Дозор-Джет»

Дополнительные модули не входят в стандартный комплект поставки и предназначены для расширения функциональных возможностей системы «Дозор-Джет». К дополнительным модулям относятся:

- Модуль подключения ЭЦП;
- Модуль сегментирования архива почтовых сообщений;
- Модуль контекстного поиска в архиве почтовых сообщений;
- Модуль лексического контекстного поиска в архиве почтовых сообщений;
- Модуль статистики и отчетов;
- Модуль взаимодействия с HP OpenView;
- Модуль категоризации почтовых сообщений (анти-спам);
- Модуль доступа к архиву почтовых сообщений по протоколу IMAP4;
- Модуль реконструкции почтовых сообщений;
- Модуль подтверждения отправки почтовых сообщений.

Модуль подключения ЭЦП

Модуль подключения ЭЦП обеспечивает следующие дополнительные функциональные возможности:

- авторизацию и обеспечение юридической значимости электронных документов при обмене ими между пользователями;
- обеспечение конфиденциальности и контроля целостности информации, пересылаемой по электронной почте.

Данные возможности осуществляются посредством использования процедур формирования и проверки электронной цифровой подписи. Постановка ЭЦП и ее проверка осуществляется средствами третьих производителей, для подключения конкретной реализации ЭЦП к системе «Дозор-Джет» достаточно, чтобы был реализован простой интерфейс, являющийся подмножеством Microsoft CryptoAPI. Стоимость данного программного обеспечения определяется прайс-листами третьих производителей.

С включением модуля подключения ЭЦП в состав системы, появляются два новых действия: *подписать письмо* и *проверить подпись*. Оба этих действия возможны только при наличии базы данных, которая связывает авторов писем с соответствующими сертификатами. Такая база данных и средства для ее ведения входят в состав данного модуля.

Модуль сегментирования архива почтовых сообщений

Модуль сегментирования архива почтовых сообщений предназначен для повышения продуктивности и надежности работы с большими базами данных электронной почты. В модуле используется опция Partitioning СУБД Oracle (Enterprise Edition), которая позволяет строить секционированные таблицы и индексы. Секционированные таблицы и индексы применяются для разделения больших таблиц и индексов на части (секции), управлять которыми можно независимо друг от друга. При секционировании уменьшается время, которое требуется для выполнения большинства операций над данными. Объясняется это обработкой меньшего числа “единиц хранения” и увеличением производительности вследствие их параллельного выполнения.

Администраторы баз данных могут определять атрибуты хранения для каждой секции и планировать ее размещение на файловой системе сервера, увеличивая тем самым гибкость управления большой базой данных. Каждая из секций может быть переведена в автономное (offline) состояние или, наоборот, возвращена в оперативное (on-line) состояние. В автономном состоянии секция может храниться на внешних носителях, что обеспечивает практически неограниченные возможности по объемам хранения данных.

Модуль контекстного поиска в архиве почтовых сообщений

Модуль контекстного поиска позволяет осуществлять поиск в архиве электронной почты по тексту в теле сообщения и прикрепленных файлах. Поиск осуществляется по полному совпадению слова в тексте сообщения.

Поиск осуществляется вне зависимости от исходной кодировки текста. Если почтовое сообщение содержит архив (zip, rar, tar, arj, gzip), то поиск производится по содержимому архивированных файлов.

Данный модуль поставляются исключительно с "Дозор-Джет" Enterprise Edition. Интерфейс к функциям этого модуля обеспечивается через систему построения запросов к базе данных писем. Модуль реализован на основе Oracle Intermedia (в настоящее время данная опция СУБД Oracle называется Oracle Text).

Модуль лексического контекстного поиска в архиве почтовых сообщений

Модуль лексического контекстного поиска в архиве почтовых сообщений позволяет осуществлять поиск в архиве электронной почты по тексту в теле сообщения и прикрепленных файлах. В отличие от модуля контекстного поиска данный модуль позволяет находить в базе письма, содержащие любые грамматические производные от указанного слова.

Данный модуль поставляются исключительно с "Дозор-Джет" Enterprise Edition. Интерфейс к функциям этого модуля обеспечивается через систему построения запросов к базе данных писем. Модуль реализован на основе Oracle Text и Russian Context Optimizer. Система Russian Context Optimizer (RCO) поставляется третьими производителями. Поэтому стоимость системы RCO определяется прайс-листами третьих производителей.

Поиск осуществляется вне зависимости от исходной кодировки текста. Если почтовое сообщение содержит архив (zip, rar, tar, arj, gzip), то поиск производится по содержимому архивированных файлов.

Модуль статистики и отчетов

Модуль статистики и отчетов дополняет встроенную в «Дозор-Джет» систему отчетов. Он позволяет получать детальную информацию о почтовом трафике и преобразовывать ее в формат, пригодный для работы в MS Excel. С помощью этого модуля можно анализировать почтовый трафик организации как за относительно большие периоды времени, так и за сутки, что позволяет оперативно корректировать политику использования электронной почты. Если система «Дозор-Джет» поставляется с СУБД Oracle, то модуль статистики и отчетов включает в свой состав 7 стандартных отчетов для Oracle Reports.

Модуль взаимодействия с HP OpenView

В составе системы «Дозор-Джет» поставляется модуль, обеспечивающий взаимодействие с системой HP OpenView. Это позволяет обеспечивать контроль работа различных

компонентов «Дозор-Джет». Установка этого модуля добавляет в «Дозор-Джет» дополнительное действие: *сделать запись в журнал*. Это действие полностью аналогично действию *послать уведомление* (за исключением присоединения оригинала письма) и позволяет оперативно отображать на консоль управления HP OpenView информацию об «опасных» письмах.

Кроме того, данный модуль позволяет проводить мониторинг различных параметров СУБД Oracle, которая входит в систему «Дозор-Джет», а также контролировать критичные ресурсы системы (мониторинг работы почтовых утилит, http-сервера Apache; контроль размеров каталогов, системных журналов и log-файлов) и передавать полученные результаты администратору. Это значительно повышает надежность работы системы «Дозор-Джет».

Модуль категоризации почтовых сообщений

Модуль категоризации почтовых сообщений предназначен для фильтрации электронных писем определенной категории. Письма автоматически относятся к той или иной категории на основании ранее выполненного анализа выбранной администратором базы образцов писем. При этом категоризация писем осуществляется на основе теории вероятности с использованием статистических алгоритмов. Данная технология позволяет автоматически корректировать работу категоризатора, что значительно облегчает задачу администратора системы по ее контролю и настройке и сокращает время на обслуживание системы.

Особенностью данного модуля является возможность индивидуальной настройки фильтра в соответствии с требованиями конкретного заказчика. В частности, по желанию заказчика, модуль может быть настроен на фильтрацию сообщений рекламного характера (spam).

Модуль доступа к архиву электронной почты по протоколу IMAP4

Модуль доступа к архиву электронной почты по протоколу IMAP4 предоставляет администраторам и пользователям системы «Дозор-Джет» возможность доступа к почтовому архиву по стандартному протоколу с помощью распространенных пользовательских почтовых клиентов. При этом такими почтовыми клиентами могут быть любые широко используемые в настоящее время программы, например, MS Outlook, Netscape Messenger, The Bat и т.п.

Использование модуля предоставляет администраторам и пользователям системы «Дозор-Джет» единый интерфейс доступа как к своей электронной почте, так и к почтовому архиву. Они получают возможность экспортировать письма из архива в свой почтовый ящик путем простого «перетаскивания» писем и соответственно осуществлять необходимую обработку почты. При этом необходимо отметить, что такую возможность пользователи получают в соответствии с правами доступа, установленными администратором системы.

Модуль реконструкции почтовых сообщений

Модуль реконструкции почтовых сообщений позволяет вносить изменения в электронное письмо перед отправкой получателю и заменять определенные части письма на текстовые сообщения.

При включении данного модуля в состав системы появляется возможность осуществлять следующие действия над письмом:

- заменять определенные части письма на заданный текст;
- удалять, перезаписывать или добавлять заголовки;

- добавлять дисклеймер (disclaimer) - предупреждение об ограничении ответственности).

Решение о замене части письма на заданный текст принимается на основе ее типа (content-type). Для замены части письма администратором задаются ряд текстовых шаблонов. Каждому типу соответствует определенный шаблон.

Модуль реконструкции почтовых сообщений позволяет удалять «ненужную» информацию (поля) из писем, вставлять в заголовки специальные метки, которые могут быть использованы для дальнейшей обработки почты, уведомлять пользователей о проведенных проверках (на вирус, спам) и т.п.

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

Модуль подтверждения отправки почтовых сообщений

Данный модуль предназначен для подтверждения автором необходимости отправки почтового сообщения, которое в соответствии с политикой безопасности было задержано системой «Дозор-Джет».

В случае, если система «Дозор-Джет» определила, что в письме есть текст «запрещенного» содержания, то в соответствии с принятой в компании политикой безопасности данное письмо задерживается. Модуль подтверждения отправки почтовых сообщений добавляет функциональность, при которой «запрещенное» письмо может быть временно помещено в архив, а его автору отправлено уведомление о том, что письмо было задержано. При этом, в случае необходимости, указывается причина задержки. Автору письма передается право решать, подтвердить отправку письма или отменить ее.

При получении такого уведомления, пользователю выдается приглашение к авторизации. На основе полученных данных система производит аутентификацию и авторизацию, проверяя совпадение имени пользователя с именем почтового ящика (mailfrom), с которого было отправлено письмо. В случае успешной авторизации пользователю выдается сообщение о возможности отправить письмо или отменить его отправку. В противном случае пользователь получает сообщение о том, что он не имеет доступа к данному письму.

В зависимости от выбора пользователя на письмо устанавливается соответствующая пометка: «отправка подтверждена» или «отправка отменена». Пользователю выдается сообщение о произведенных действиях: «Ваше сообщение отправлено» или «Отправка сообщения отменена». Все действия пользователя регистрируются в системном журнале. Кроме того, регистрируются попытки неавторизованного доступа к письмам.

Функциональность модуля не зависит от механизма аутентификации пользователя, так как применяется PAM-модуль на Web-сервере, что позволяет подключать различные схемы аутентификации, не модифицируя систему.