Комплекс защиты от утечек информации «Дозор-Джет»

ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Комплекс защиты от утечек информации «Дозор-Джет» – одно из первых на российском рынке решений по контролю за утечками. Первая версия продукта появилась в 2000 году. Сегодня «Дозор-Джет» позволяет контролировать основные каналы утечки информации и обеспечивать соблюдение политик безопасности. «Дозор-Джет» стоит на защите более 300 компаний среднего и крупного бизнеса.

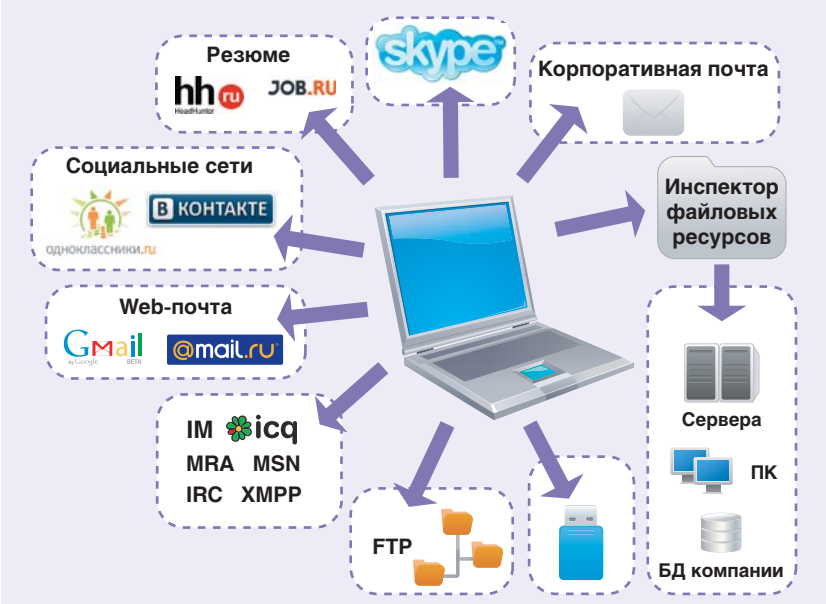
Комплекс защиты от утечек информации «Дозор-Джет» обеспечивает безопасность бизнес-процессов в части коммуникаций и позволяет легко реализовать корпоративную политику использования информационных ресурсов.

Востребованность подобных средств защиты обусловлена современными тенденциями и особенностями рынка, без учета которых развитие компании крайне затруднительно. В их числе:

- постоянно возрастающая ценность информации, потеря которой в результате действий инсайдеров приводит к имиджевым и финансовым потерям;
- необходимость соблюдения законодательных норм и исполнения требований регуляторов, нарушение которых приводит к штрафным санкциям;
- кадровый «голод» и растущая конкуренция на рынке требуют более внимательной работы с персоналом;
- рост нецелевого использования сотрудниками интернет-ресурсов организации для создания собственного микробизнеса, что отрицательно сказывается на эффективности деятельности компании.

В связи с этим компания нуждается в полноценной защите своих информационных ресурсов. Для этого ей необходим комплексный механизм, состоящий из организационных мер и разработанных регламентов, а также технических средств, позволяющих контролировать и обеспечивать их соблюдение.

Комплекс «Дозор-Джет» осуществляет мониторинг трафика, передаваемого по различным каналам коммуникации, проверяет сообщения, файлы и другие данные на соответствие положениям политики использования Интернет-ресурсов и внутренних информационных ресурсов компании, реагирует на нарушения этой политики согласно заданным сценариям, а также обеспечивает ведение архива сообщений.



В число возможностей программного продукта входят:

- Фильтрация, контроль и архивирование корпоративной электронной почты (SMTP);
- Контентная фильтрация Веб-трафика (HTTP, HTTPS, FTP over HTTP);
- Мониторинг коммуникаций, осуществляемых с помощью различных веб-сервисов (веб-почта, социальные сети и др.);
- Контроль сообщений, передаваемых через службы мгновенных сообщений;
- Контроль файловых хранилищ корпоративной сети;
- Контроль файлов и внешних устройств на рабочих станциях;
- Точное обнаружение конфиденциальных данных с помощью различных средств анализа (цифровые отпечатки, поиск идентификаторов и другие).

Комплекс состоит из систем, каждая из которых выполняет определенную задачу и может быть использована как самостоятельно, так и в составе единого решения. Ряд систем Комплекса может эффективно дополнять зарубежные DLP-системы для полного и удобного контроля российских интернет-ресурсов, ICQ и других служб мгновенных сообщений.

Комплекс «Дозор-Джет» сертифицирован ФСТЭК России.

СИСТЕМА АРХИВИРОВАНИЯ И АНАЛИЗА

Система архивирования и анализа «Дозор-Джет» является центральным компонентом Комплекса и в сочетании с другими системами позволяет реализовывать политику информационной безопасности в отношении электронной почты и других средств сетевого общения. В ее состав включена подсистема анализа, которая основана на механизме правил и позволяет реализовать политику использования средств коммуникации любой сложности.

Система архивирования и анализа «Дозор-Джет»:

- Обеспечивает оперативность реагирования на инциденты информационной безопасности. При этом гибкость в настройке правил и политик оптимизирует нагрузку сотрудников службы безопасности, обращая их внимание только на существенные события.
- Обеспечивает ведение оперативного и долгосрочного архива для ретроспективного анализа коммуникаций, ведения расследований и сбора «доказательной базы». Архив сообщений «Дозор-Джет» успешно применяется для реализации требований регулирующих органов (СТО БР ИББС, PCI DSS, ФЗ-152, SOX и других).
- Повышает эффективность расследований, благодаря возможности хранения информации, собранной из различных источников.

Возможности Системы архивирования и анализа могут быть расширены с помощью следующих дополнительных модулей, описанных ниже.

Модуль цифровых отпечатков DiFi

Модуль цифровых отпечатков DiFi «Дозор-Джет» позволяет обнаруживать утечку конфиденциальных документов в тех случаях, когда прямое сравнение текстов или ключевых слов неэффективно. Для работы с Модулем необходимо выбрать конфиденциальные документы, утечка которых недопустима, и загрузить их электронные копии в систему. Эталонами для сравнения могут выступать текстовые, графические и табличные документы.

Модуль цифровых отпечатков с высокой вероятностью устанавливает факт отправки конфиденциального документа за пределы компании. Даже если отправляется только его часть, Модуль все равно установит данный факт и сообщит, сколько процентов эталонного документа содержится в исходящем сообщении. Дальнейшие действия Системы зависят от величины совпадения в процентах и определяются политикой безопасности.

Цифровые отпечатки могут быть использованы как при фильтрации сообщений, так и при поиске в архиве.

Модуль идентификаторов IDID

Модуль идентификаторов IDID «Дозор-Джет» выделяет в текстовых сообщениях цифровые идентификаторы. Заложенный в его основу механизм позволяет избежать ложных срабатываний при поиске данных, содержащих цифровые последовательности.

Модуль позволяет находить и обрабатывать следующие идентификаторы из передаваемых данных:

финансовые	персональные данные	сетевые
• БИК • коды ОКАТО • Visa • MasterCard • Diners Club • Laser	• ИНН РФ • русские имена • номера российских паспортов • пенсионные карты (ПФ РФ СНИЛС)	• email • URL • samba shares • IP

Для каждого вида идентификаторов разработан набор алгоритмов, которые включают в себя проверку ключевых сумм, диапазонов значений, «окружающего» текста.

СИСТЕМА ПАССИВНОГО ПЕРЕХВАТА СООБЩЕНИЙ

Система пассивного перехвата сообщений «Дозор-Джет» легко встраивается в уже существующую ИТ-инфраструктуру и предоставляет возможность удобного контроля за основными каналами коммуникации:

- Корпоративная почта (SMTP, POP3);
- Веб-почта (Google mail, Yahoo mail, Mail.ru и аналогичные);
- Социальные сети (Одноклассники.ру, Вконтакте.ру, Facebook, различные форумы);
- Службы поиска работы и публикации резюме (HeadHunter, Job.ru, Zarplata.ru и аналогичные);
- Системы передачи мгновенных сообщений (ICQ, Mailru.Агент, MSN, Jabber).

Она может быть дополнена системами раскрытия HTTPS-трафика для перехвата сообщений, передаваемых через зашифрованные соединения. Для этого могут быть использованы как Система контроля веб-трафика «Дозор-Джет», так и разработки других производителей.

СИСТЕМА ИНСПЕКТИРОВАНИЯ ФАЙЛОВЫХ РЕСУРСОВ

Система инспектирования файловых ресурсов «Дозор-Джет» обеспечивает контроль данных в корпоративной сети на файловых хранилищах, на дисках рабочих станций, при копировании съемных носителей.

Данная система позволяет:

- контролировать распространение информации и данных в пределах компании;
- значительно снизить трудоемкость анализа данных, циркулирующих в корпоративной сети при помощи их автоматической классификации;
- обеспечивать политику компании в части хранения и обработки различных, в том числе категорированных данных;
- предотвращать возможные утечки информации через рабочие станции.

СИСТЕМА АКТИВНОГО КОНТРОЛЯ

Система активного контроля «Дозор-Джет» позволяет предотвратить утечку информации из корпоративной сети по различным каналам коммуникации.

Система автоматически реагирует на нарушения политики использования средств коммуникации по заранее заданному администратором безопасности сценарию. При соблюдении (или не соблюдении) определенного условия система выполняет последовательность действий, установленную соответствующим правилом политики.

Основными действиями являются:

- разрешение или запрет прохождения почтового сообщения;
- разрешение или запрет доступа к Интернет-ресурсу;
- удаление сообщения;
- запись сообщения в архив;
- регистрация сообщения;
- добавление меток к сообщению;
- отправка уведомления администратору безопасности или другому заранее заданному адресату;
- модификация содержимого сообщения перед доставкой или пересылкой, включая удаление запрещенных вложений и добавление определенного текста.

ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

О Центре информационной безопасности

Центр информационной безопасности компании «Инфосистемы Джет» на сегодняшний день самое крупное подразделение, занимающееся информационной безопасностью, среди всех российских системных интеграторов. В Центре работает более 130 высококвалифицированных специалистов.

Компания «Инфосистемы Джет» работает на рынке информационной безопасности с 1996 года и выполняет полный цикл работ по защите корпоративных систем любого масштаба и сложности – от обследования и анализа рисков до внедрения и сопровождения средств и систем информационной безопасности. За это время было выполнено более 2000 контрактов, в т.ч. более 200 крупных проектов федерального масштаба.

Благодаря наличию широкого спектра решений и услуг, сертифицированных специалистов и богатому опыту, а также четко организованной работе проектного офиса, Центру доверяют проекты крупные компании, в том числе и транснационального масштаба с численностью сотрудников в десятки тысяч человек.

Jet infosystems

Россия, 127015, Москва
ул. Б. Новодмитровская, д. 14, стр. 1,
офисный Центр «Новодмитровский»
Тел.: +7 (495) 411-7601
Факс: +7 (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su

МОДУЛИ СИСТЕМЫ АКТИВНОГО КОНТРОЛЯ

Система активного контроля «Дозор-Джет» состоит из двух основных модулей: Модуля фильтрации SMTP и Модуля контроля веб-трафика.

Модуль фильтрации SMTP

Модуль фильтрации SMTP «Дозор-Джет» позволяет реализовать корпоративную политику использования электронной почты, включая активную фильтрацию и оперативный контроль с участием офицеров безопасности (разрешение или карантинное хранение сообщения, регистрация или сохранение сообщения в архиве, отправка уведомлений и т.д.).

При фильтрации осуществляется полный разбор почтовых сообщений любого уровня вложенности на составляющие компоненты; распознаются форматы вложенных файлов офисных приложений (включая файлы в составе архивов); раскрываются архивы всех распространенных типов и любого уровня вложенности; распознаются форматы медиа-файлов (аудио, видео, изображения); обрабатываются OLE-объекты в файлах приложений MS Office; распознаются скрытые вложенные форматы.

Модуль фильтрации SMTP «Дозор-Джет» является дальнейшим развитием продукта СМАП «Дозор-Джет» в части активного контроля и фильтрации почты. Модуль сохранил все возможности СМАП, но при этом стал более гибок в интеграции с другими компонентами Комплекса.

Модуль контроля веб-трафика

Модуль контроля веб-трафика «Дозор-Джет» предназначен для защиты корпоративных локальных вычислительных сетей от рисков, связанных с использованием Интернет-ресурсов. Данная система позволяет контролировать доступ к Веб-ресурсам и осуществлять протоколирование действий пользователей. Модуль позволяет:

- предотвратить утечки конфиденциальной информации за счет фильтрации передаваемых данных и блокирования групп ресурсов потенциального риска;
- обеспечить безопасность использования Интернет-ресурсов (блокировка нежелательного и подозрительного содержания по адресам и форматам, протоколирование действий пользователей, оповещение о нарушениях политики безопасности);
- оптимизировать расходы предприятия на Интернет-трафик, повысить производительность сотрудников (блокирование ресурсов и файлов, не относящихся к работе; ограничения по объему трафика; возможность получения реальной картины использования Интернет-ресурсов).

Возможности контроля веб-трафика могут быть расширены следующими дополнительными модулями:

- Модуль категоризации – разграничение доступа к Интернет-ресурсам в соответствии с их категориями;
- Модуль раскрытия HTTPS – для контроля данных, зашифрованных с помощью прокола HTTPS.

Узнать больше:

О Комплексе защиты от утечек информации «Дозор-Джет»:
http://www.jetsoft.ru