возможно использование процессорной смарт-карты повышенной защищенности (например, интеллектуальной карты).

УДК 681.324.067

Н.М. Бобович, А.В. Шаповалов

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ МОНИТОРИНГА И АРХИВИРОВАНИЯ ПОЧТОВЫХ СООБЩЕНИЙ «ДОЗОР-ДЖЕТ» В СЭД «ДЕЛО»

Отличительной особенностью современного этапа совершенствования документационного обеспечения управления органами внутренних дел Республики Беларусь является внедрение системы электронного документооборота «Дело» и переход на электронный документооборот и технологии дистанционного межведомственного взаимодействия.

Система электронного документооборота (СЭД) «Дело» представляет собой автоматизированную многопользовательскую систему, сопровождающую процесс управления работой ОВД с целью обеспечения выполнения ими основных правоохранительных функций.

Работа с документами в электронной форме позволяет быстро и удобно хранить, обрабатывать и передавать их в рамках СЭД «Дело». Перечисленные функции, как правило, выполняет почтовая система, являющаяся неотъемлемой частью всякого электронного документооборота.

Благодаря таким качествам, как низкая стоимость, простота использования, большое количество пользователей, электронная почта стала одним из распространенных и популярных средств коммуникации.

Однако наряду с многочисленными преимуществами существуют риски, связанные с использованием электронной почты, которые могут привести к значительному снижению эффективности работы ОВД, потере значимой информации.

Основными проблемами, связанными с неконтролируемым использованием электронной почты, являются:

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.

В целях реализации корпоративной политики использования электронной почты в части обеспечения информационной безопасности СЭД «Дело» предлагается использовать специализированное программное средство –

систему мониторинга и архивирования почтовых сообщений «Дозор-Джет».

Система «Дозор-Джет» осуществляет мониторинг и контроль всех входящих, исходящих и внутренних почтовых сообщений. При этом анализируются заголовки и структура сообщений, проверяется 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 ведомственные правила обработки входящей и исходящей почты в зависимости от тех или иных предопределенных событий, например:

запрет пересылки файлов формата EXE всем, кроме администратора СЭД;

запрет пересылки картинок формата GIF и JPEG отдельным пользователям СЭД;

ограничение на объем и количество присоединенных файлов, направляемых отдельным адресатам;

автоматическое уведомление руководителя подразделения о письмах с определенными пометками или отвечающих поставленным условиям.

В системе реализована гибкая система фильтрации сообщений, что позволяет реализовать практически любую схему прохождения электронной почты.

Например, возможна так называемая отложенная доставка почтового сообщения, когда решение о доставке конечному пользователю принимается только после дополнительного анализа администратором СЭД и другими системами безопасности (проверка на наличие вирусов, контроль массовой рассылки сообщений рекламного характера, наличие неопознанных (закодированных) вложений и пр.).

При попадании в систему «Дозор-Джет» почтовые сообщения проходят процедуру разбора заголовков сообщения (отправитель, получатель, скрытая копия, тело сообщения и пр.) 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.

Процедура анализа разобранных сообщений включает:

определение характеристик сообщения – отправитель, получатель, дата, размер, структура;

определение характеристик вложений – имя, размер, тип, количество;

распознавание форматов вложений – сжатие (архивирование) документов, исполнимых файлов, графических, аудио- и видеофайлов;

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

По результатам анализа в случае обнаружения соответствия почтовых сообщений заданным в правилах фильтрации критериям система осуществляет одно или несколько из заранее предписанных действий:

отправление сообщения получателю;

отказ в передаче (блокировка сообщения);

задержка сообщения для последующего анализа;

помещение в карантинную зону;

регистрация сообщения;

архивирование сообщения;

проставление пометок;

отправление уведомления (оповещение администратора системы и др.).

При этом обязательно осуществляется протоколирование всех производимых действий.

В отличие от других традиционных анти-спам фильтров система «Дозор-Джет» позволяет одновременно использовать как статистические (вероятностные) методы фильтрации, так и фильтрацию спама на основе признаков электронного письма. В результате достигается более гибкая и глубокая контекстная фильтрация и повышается эффективность работы системы по борьбе со спамом.

УДК 343.5

П.Л. Боровик

СТРУКТУРНОЕ СОДЕРЖАНИЕ СПОСОБОВ ИЗГОТОВЛЕНИЯ И СБЫТА ДЕТСКОЙ ПОРНОГРАФИИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Структурным элементом механизма деяния и криминалистической характеристики оборота детской порнографии является способ преступления. Отмечая его значение для методики расследования, Г.Г. Зуйков подчеркивал, что способ указывает, какие именно действия произведены, выражает субъективные компоненты личности преступника, формы его вины, показывает мотив и цели совершения преступления, характер применяемых при этом орудий и средств, влияет на сокрытие следов [4, с. 10].

В научной литературе существуют различные подходы к делению способов преступления на виды в зависимости от их внутреннего строения. Наиболее уместное применительно к рассматриваемой проблеме предложил М.С. Уткин: полноструктурные способы (подготовка, совершение и сокрытие преступлений); усеченные первого типа (совершение и сокрытие преступлений); усеченные второго типа (подготовка и совершение преступлений); упрощенные, состоящие только из действий по совершению преступлений [3, с. 132].

Для оборота детской порнографии типичными являются полноструктурные способы, особенно в случае осуществления деяния организованной преступной группой, поскольку «подготовка к совершению преступлений есть элемент жизнедеятельности организованной и профессиональной преступности, а сокрытие преступной деятельности представляет систему обеспечения этой жизнедеятельности» [2, с. 199].

Анализ уголовных дел рассматриваемой категории за последние три года показывает, что *подготовка к изготовлению*:

– путем создания порнографической продукции с изображением несовершеннолетних (имела место в 35,7 % случаев создания) заключалась в следующих наиболее типичных действиях, осуществляемых заведомо в преступных целях:

приобретение фото- и видеоаппаратуры, осветительного оборудования, компьютерной техники, расходных материалов, цифровых носителей информации, а также иных приспособлений (60 % от общего числа случаев подготовки к созданию);

аренда квартир, домов, коттеджей под фотостудии, а также офисов для изготовления и обработки порнографической продукции (40 %);

разработка сюжета, сценария фильма, мультфильма или компьютерной игры порнографического содержания (20 %);

– путем копирования порнографической продукции с изображением несовершеннолетних (составила 80 % от числа случаев копирования детской порнографии) заключалась в следующих наиболее типичных действиях:

приобретение компьютерной техники, видеомагнитофонов, DVD-проигрывателей (20 %);

аренда web-сервера, на котором преступники размещают web-сайт и куда копируют порнографические изображения (26,7 %);

настройка работы web-сайта либо файлообменного сервиса (73,3 %);

– путем переделки продукции и придания ей характера порнографии имела место во всех случаях изготовления этим способом и заключалась в следующем:

в приобретении или изготовлении фотографий, видеофильмов, мультфильмов либо другой продукции, содержание которой подвергается изменению;

приобретении порнографических материалов (как правило, в сети Интернет), используемых в целях модификации;

установке и настройке специального программного обеспечения, предназначенного для фото- и видеомонтажа.

На стадии подготовки преступлений, связанных с изготовлением детской порнографии, в 55 % случаев из числа изученных нами уголовных дел злоумышленниками предпринимались меры по их сокрытию, направ-