РФ и указов Президента РФ, дать количественную оценку соответствия ИС требованиям нормативных документов. В программном средстве представлен лист опроса, результаты которого показывают процент невыполненных требований используемой нормативной базы. Программа формирует отчет, содержащий рекомендации по устранению уязвимых мест ИС организации. В настоящее время информационное и соответствующее правовое пространство подвержено бурным изменениям. Программное средство для проведения аудита отдельных компонентов ИБ СФУ автоматически адаптируется к изменениям в нормативной базе.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000 Information technology. Code of practice for security management. М.: Стандартинформ, 2006.
2. ГОСТ Р ИСО/МЭК 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. ISO/IEC 27001:2005(E) Information technology. Security techniques. Information security management systems. Requirements — ИСО/МЭК 2005. Перевод на русский язык: ЗАО «Технорматив», 2006.

А. А. Колосов
Московский энергетический институт (технический университет)

ЗАЩИЩЕННАЯ СИСТЕМА ОБМЕНА ЭЛЕКТРОННОЙ ПОЧТОЙ НА ОСНОВЕ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ

Электронная почта является одним из самых распространенных способов общения пользователей компьютерных сетей в современном мире. В докладе рассматриваются основные существующие методы защиты почтовых систем от различных угроз с использованием средств асимметричной криптографии, а также определяется возможность их применения для построения защищенной системы электронного документооборота.

Основная особенность электронной почты заключается в том, что она является системой с промежуточным хранением, т. е. информация отправляется получателю не напрямую, а через промежуточное звено — электронный почтовый ящик, который представляет собой место на сервере, где сообщение хранится, пока его не запросит пользователь. Независимость от канала передачи данных и достаточно «мягкие» требования к промежуточным серверам являются источником основных опасностей электронных писем. Недостатки электронной почты напрямую вытекают из ее достоинств.

Все угрозы безопасности почтовых писем общеизвестны и не требуют детального рассмотрения. К ним относятся спам (нежелательная почта), перехват, олицетворение, искажение, отказ в обслуживании, внедрение вредоносных программ.

Учитывая, что электронная почта появилась уже достаточно давно, существует немало способов борьбы с известными атаками. Тем не менее построение по-настоящему универсального способа защиты является серьезной задачей, требующей тщательного анализа возможностей современных компьютерных систем и их пользователей с пониманием того, что каждый может выступать в роли злоумышленника, использования сложного математического аппарата,

изучения уже существующих средств защиты, совмещения их положительных черт и исключения неактуальных и неэффективных методов.

Существующими на сегодняшний день стандартами защищенного обмена электронной почтой являются S/MIME [1] и PGP [2].

S/MIME (Secure/Multipurpose Internet Mail Extension) – это усовершенствование с точки зрения защиты стандарта формата MIME электронной почты в Интернете, базирующееся на использовании технологии RSA Data Security [3]. Главной характеристикой S/MIME является иерархическая политика аутентификации, требующая для управления открытыми ключами развертывания инфраструктуры открытых ключей (PKI) [4]. В качестве документа, подтверждающего соответствие между открытым ключом и информацией, идентифицирующей владельца ключа, является сертификат (в формате PKIX на базе X.509v3 [5]).

Система PGP (Pretty Good Privacy – вполне надежная секретность) обеспечивает конфиденциальность и сервис аутентификации, которые можно использовать для электронной почты и приложений хранения файлов. Принципиальным отличием PGP является использование сетей доверия и распределенной аутентификации.

С точки зрения «качества» решения основных задач: аутентификации и обеспечения конфиденциальности – оба стандарта достаточно надежны, но имеют принципиальные отличия и не могут использоваться совместно. В первую очередь PGP ориентирована на физических лиц, в то время как S/MIME, требующая инфраструктуру открытых ключей, подходит для корпоративного использования.

Основной идеей развития в рассматриваемой области является объединение всех положительных сторон S/MIME и PGP в единую универсальную защищенную почтовую систему. Прежде всего, защита не должна ограничивать функционал защищаемой системы, но в то же время должна обеспечивать надежность. Кроме того, система должна быть гибкой по отношению к используемым средствам криптозащиты, которые приходится постоянно совершенствовать для обеспечения необходимого уровня безопасности и на которые накладываются жесткие ограничения, в том числе и законодательные.

Решение описанных задач позволяет перейти от защиты непосредственно электронных писем к созданию универсального защищенного транспорта, что откроет дорогу для разработки более глобальной защищенной системы электронного документооборота.

СПИСОК ЛИТЕРАТУРЫ:

1. RFC 3851. S/MIME Version 3.1 Message Specification. 2004.
2. *Zimmermann P.* The Official PGP User's Guide. MIT press, 1995.
3. RFC 3447. PKCS #1: RSA Cryptography Specifications Version 2.1, 2003.
4. *Nash A.* PKI: Implementing & Managing E-Security. 2001.
5. RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. 2008.