И. Н. Кирико, О. А. Колычева
Институт космических и информационных технологий Сибирского федерального университета, Красноярск

НАУЧНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ НА ПРИМЕРЕ СФУ

Формулируются задачи, решаемые в процессе проведения аудита информационной безопасности высшего образовательного учреждения, представлено программное средство для проведения аудита отдельных компонентов информационной безопасности Сибирского федерального университета (СФУ).

Адекватная защита административного, профессорско-преподавательского и студенческого состава, интеллектуальной собственности, имущества и информации образовательного учреждения от всего спектра угроз предполагает решение следующих задач: разработка концепции безопасности образовательного учреждения, выявление объектов, наиболее вероятно подверженных атаке, определение уязвимостей и угроз, установление уровней опасности по территориальному и структурному принципам, рациональное планирование расхода финансовых, людских и материальных ресурсов на обеспечение безопасности, сокращение затрат на обеспечение безопасности путем мобильного применения имеющихся сил и средств защиты, разработка модели системы безопасности. Для решения этих задач необходим аудит информационной безопасности (ИБ). Аудит ИБ — это системный процесс, позволяющий оценить текущее состояние информационной системы (ИС) организации, а также разработать рекомендации по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и других ресурсов ИС от угроз ИБ.

Аудит ИБ включает в себя:

• оценку информационных активов и ресурсов ИС;

• анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;

• оценку текущего уровня защищенности ИС;

• оценку соответствия ИС существующим стандартам в области ИБ;

• разработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

В связи с тем, что Сибирский федеральный университет создан на основе объединения четырех государственных вузов города Красноярска: классического университета, архитектурно-строительной академии, технического университета, университета цветных металлов и золота — имеются сложности в осуществлении организации аудита ИБ в распределенной разнородной системе. Кроме того, территориально административные корпуса объединенных вузов расположены на нескольких площадках, что требует определения периметра безопасности СФУ в целом. Объединение вузов — процесс длительный, требующий рассмотрения множества вопросов, но уже на ранней стадии IT-планирования необходимо пересмотреть и/или определить ключевые стандарты в области информационной безопасности, а также рассмотреть актуальность существующей нормативной базы.

Для автоматизации процесса проведения аудита информационной безопасности разработано программное средство, позволяющее на основе анализа ответов на вопросы, составленные по требованиям международных стандартов в области информационной безопасности [1, 2], руководящих документов Гостехкомиссии России в области защиты информации, а также законов

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,