Т. Н. Васильева, А. В. Львова

Применение оценок рисков в управлении информационной безопасностью[1]

В настоящее время все более актуальными становятся проблемы управления информационной безопасностью в корпоративных информационных системах. В статье предложен новый метод анализа и управления рисками в области информационной безопасности, базирующийся на стоимостных оценках.

В современных условиях развития компьютерных систем и телекоммуникаций, увеличения электронного документооборота, широкого распространения систем электронных платежей проблемы защиты информации от утраты, искажения и попадания в руки противника становятся все более серьезными и находят все более глубокое понимание среди руководителей и сотрудников различных организаций, использующих в своей деятельности информационные сети и системы.

С увеличением распространения информационных систем в бизнесе последствия нарушения информационной безопасности становятся все более дорогостоящими [4]. По данным исследований Института компьютерной безопасности США (Computer Security Institute) за 2005 г. 639 организаций оценили годовые потери только от одного типа инцидентов информационной безопасности — кражи конфиденциальной информации — в 31 млн долл., при этом потери, обусловленные всеми инцидентами безопасности, составили 130 млн долл. [2].

Наибольшее количество угроз информационной безопасности связано с передачей данных через глобальную сеть Интернет, а также хранением данных в базах данных информационной системы и на персональных компьютерах пользователей [4]. Источники угроз многочисленны. Для корпоративных систем это компьютерные вирусы, программы-шпионы, спам, злонамеренные действия противников, как внешних, так и внутренних, халатность сотрудников, износ оборудования, различные чрезвычайные происшествия и многое другое.

Для того чтобы в сегодняшних условиях защитить информационные ресурсы от всех этих угроз, недостаточно какого-либо разового мероприятия или даже создания системы защиты. Нужна постоянная и тщательная работа, которая бы позволяла адаптировать данную систему защиты к меняющимся условиям функционирования информационной системы. Такую работу и должна выполнять система управления информационной безопасностью.

Определение уровня безопасности

Принятие адекватных мер и проведение мероприятий по обеспечению информационной безопасности невозможно без определения текущего уровня безопасности, выявления наиболее уязвимых мест в существующей системе информационной безопасности, а также наиболее значимых угроз безопасности.

Для определения текущего уровня безопасности в развитых системах обязательно применяют различные количественные метрики и меры. Данные метрики используются на разных уровнях детализации: от наиболее низких и простых в оценке, таких как, например, количество инцидентов нарушения информационной безопасности за период времени или доля компьютеров, оснащенных сетевыми экранами и антивирусными программами, среди всех персональных машин корпоратиной сети, до наиболее сложных аг-

[1] Статья подготовлена по результатам Всероссийской научно-практической конференции Московской финансово-промышленной академии «Развитие конкуренции на рынке информационных технологий» (25–26 марта 2009 г.). — *Прим. ред.*