А. А. Микрюков, *канд. техн. наук, доцент Московского государственного университета экономики, статистики и информатики, AMikrukov@mesi.ru*

В. Н. Усцелемов, *аспирант Московского государственного университета экономики, статистики и информатики, s.uscelemov@mail.ru*

Гибридная модель оценки рисков в информационных системах

В статье рассмотрен один из подходов к построению адаптивной подсистемы защиты информационных систем на основе гибридной модели оценки уровня риска преодоления подсистемы защиты информационной системы нарушителем, включающей процедуры прецедентного и нейро-нечеткого выводов.

Ключевые слова: информационная безопасность, оценка информационных рисков, прецедент, система защиты, угроза, нейро-нечеткий вывод.

Введение

Уровень защищенности информационных ресурсов является одним из основных показателей эффективного функционирования предприятия. В настоящее время предприятия вынуждены тратить большие средства на построение систем защиты своих информационных ресурсов. Это обусловлено тем, что ежедневно по всему миру осуществляется огромное число атак на информационные системы с целью нанесения максимального ущерба их владельцам. Исследования, проведенные в области построения систем информационной безопасности, показали, что широкое применение нашли методики, основанные на концепции приемлемых рисков [1]. Это вызвано тем, что, во-первых, абсолютно непреодолимую систему защиты построить невозможно, а, во-вторых, многие руководители предприятий не имеют возможности тратить избыточные финансовые и вычислительные ресурсы на совершенствование систем защиты и готовы идти на приемлемые риски. Управление информационными рисками позволяет компаниям найти баланс между затратами на построение защиты информационной системы и получаемым эффектом.

В настоящее время в России при построении подсистем защиты на основе концепции приемлемых рисков руководствуются стандартами ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Практические правила управления информационной безопасностью» и ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Среди методик оценки информационных рисков широкое применение нашли такие методики, как CRAMM, FRAP, OCTAVE, Risk Watch, ГРИФ, методика *Microsoft* и др. [2, 3]. Проведенный анализ алгоритмов их применения выявил ряд значимых недостатков: отсутствие адаптивной реакции на возникающие угрозы, ограниченный набор шаблонов, существенная погрешность проводимых оценок и др.

Одним из возможных подходов, позволяющих устранить указанные недостатки, является построение гибридной модели подсистемы защиты информационной системы на основе оценки степени риска преодоления ее нарушителем.