А. П. Р о с е н к о (Ставрополь, СГУ). **Имитационное моделирование процесса воздействия dнутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе.**

Проблема обеспечения безопасности конфиденциальной информации (КИ) относится к трудно формализуемым проблемам. В связи с этим, как показывает анализ, наиболее предпочтительным из подходов описания процесса воздействия на систему различных неблагоприятных факторов является имитационное моделирование.

Представим процесс воздействия на компьютерную систему (КС) конечного множества внутренних угроз. Пусть в момент времени t воздействует на КС i-я угроза (где $i = 1, 2, \ldots, n$) с целью несанкционированного доступа к КИ. В результате воздействия внутренних угроз на КС возможно возникновение особой ситуации, которая может привести к нарушению безопасности КИ.

Состояния КС в результате воздействия внутренних угроз представляется возможным описать следующими вероятностными характеристиками:

а) вероятностью $P_{\text{ву}}$ возникновения внутренней угрозы, которая характеризует возможности злоумышленника по применению методов и средств несанкционированного доступа к КИ;

б) вероятностью P_{ij} перехода АИС из состояния i в состояние j при воздействии на нее внутренних угроз, которая характеризует устойчивость системы к воздействию на нее i-й внутренней угрозы;

в) вероятностью обнаружения, локализации и парирования внутренних угроз; указанная вероятность характеризует возможности собственника КИ по применению имеющихся у него средств и методов ЗИ, представляющей коммерческую ценность.

Для указанного случая имитационную модель можно представить в виде отдельных взаимосвязанных блоков, в которых реализуются следующие переходы системы в различные состояния:

а) состояние проявления i-й внутренней угрозы, что соответствует переходу системы в следующее состояние с вероятностью P_1;

б) состояние возникновения особой ситуации, соответствующей переходу системы в следующее состояние с вероятностью P_2;

в) состояние нарушения безопасности КИ, что соответствует переходу системы в следующее состояние с вероятностью P_3;

г) состояние непарирования i-й внутренней угрозы и переходу системы в следующее состояние с вероятностью P_4.

Если последствия от реализации злоумышленником внутренних угроз имеются, то система переходит в следующее состояние оценки величины ущерба с вероятностью P_5.

Таким образом, имитационная модель представляет собой абстрактную модель, которая устанавливает причинно-следственные связи между различными элементами КС. Учет указанных концептуальных основ при имитационном моделировании будет способствовать повышению качества процесса моделирования реальных КС, реализации в полном объеме цели процесса моделирования, установлению степени опасности внутренних угроз и обоснованию практических рекомендаций по применению собственником КИ эффективных защитных механизмов.