МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В.В. АКСЕНОВ, А.М. ПРУДНИК

Моделирование угроз безопасности информации предусматривает выявление угроз и их анализ с целью оценки возможного ущерба в случае их реализации. Определение значений показателей угроз информации представляет достаточно сложную задачу в силу следующих обстоятельств:

– добывание информации нелегальными путями не афишируется, и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные по видам угроз безопасности информации;

– оценка угроз информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;

– многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняет возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;

– априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Учитывая существенные различия процессов реализации угроз воздействия и утечки информации, моделирование угроз целесообразно разделить на:

– моделирование каналов несанкционированного доступа к защищаемой информации источников преднамеренных и случайных воздействий;

– моделирование технических каналов утечки информации.

Моделирование угроз безопасности информации завершается их ранжированием. На каждый потенциальный способ проникновения злоумышленника к источнику информации и канал утечки информации целесообразно завести карточку, в которую заносятся в табличной форме характеристики моделей канала.

Структурная, пространственная, функциональная и информационная модели являются приложениями к комплексной модели канала утечки. На этапе разработки способов и средств предотвращения проникновения злоумышленника и утечки информации по рассматриваемому каналу

к карточке добавляется приложение с перечнем мер по защите и оценками затрат на нее.

Более удобным вариантом является представление моделей на основе машинных баз данных, математическое обеспечение которых позволяет учесть связи между разными моделями, быстро корректировать данные в них и систематизировать каналы по различным признакам, например по виду, положению в пространстве, способам и средствам защиты, угрозам.