частотному диапазону, мощности и виду создаваемых помех, что позволило применять его в ходе испытаний радиолокационного обнародования и радиолокационных станций. Выполненное имитационное моделирование и проведенные натурные эксперименты позволили оценить эксплуатационную надежность малогабаритного тестового генератора радиопомех. Разработанный генератор радиопомех возможно использовать в качестве забрасываемого передатчика помех, который будет достаточно эффективным средством для усложнения работы радиолокационных средств противника, а также для тренировки работы операторов на радиолокационных станций, стоящих в настоящее время на вооружении.

Литература

1. Радиолокационная станция обнаружения маловысотных наземных объектов X-диапазона «Родник» [Электронный ресурс]. – URL: http://www.kbradar.by/products/radiolokatsiya/radiolokatsionnye-stantsii/519/ (дата обращения: 10.04.2018).

2. Охрименко А.Е. Основы радиолокации и радиоэлектронная борьба. Ч.1. Москва: Воениздат, 1983. 457 с.

КЛЮЧЕВЫЕ АСПЕКТЫ ПРОЦЕССА МОДЕЛИРОВАНИЯ РИСКОВ ДЛЯ ИНФОРМАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

А.В. Федорцов

Реализация эффективного управления информационной безопасностью (ИБ) в организации связана, в первую очередь, с формализацией координированных действий по руководству и управлению организацией в отношении рисков для материальных активов из состава информационной инфраструктуры. Менеджмент рисков [1], как правило, заключается (но не ограничивается) в последовательном выполнении следующих шагов: оценка рисков, обработка рисков, принятие рисков, обмен информацией о рисках. К ключевым аспектам процесса моделирования рисков для информационной сети организации следует относить вычисление значений вероятностей возникновения особого набора обстоятельств совершения атак на информационную инфраструктуру и ущерба (последствий) от таких событий ИБ для материальных активов [2], необходимых для выполнения количественной оценки рисков. Ввиду отсутствия универсального подхода к количественной оценке ущерба, позволяющего определить результат воздействия на программно-технические средства из состава информационной сети организации, решить задачу оценки последствий можно рассчитав прямой и косвенный ущерб соответствующим материальным активам. Прямой ущерб предлагается отражать как сумму отношений показателей функционирования программно-технических средств до и после совершения атаки либо отношений дополнительной стоимости затрат на восстановление оптимальных показателей функционирования к уже вложенным денежным средствам. Косвенный ущерб при этом будет характеризоваться суммой произведений определенных для организации весовых коэффициентов основных свойств обрабатываемой в информационной сети информации (конфиденциальность, целостность, сохранность и доступность) и количества атакованных материальных активов, обрабатывающих информацию.

Литература

1. СТБ ISO/IEC 27000-2012. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь.

2. Федорцов А.В., Кучинский П.В. Роль и место оценки ущерба от атак внутренних нарушителей в процессах управления информационной безопасностью организаций // Управление информационными ресурсами : материалы XIII Междунар. науч.-практ. конф. Минск, 9 декабря 2016 г. С. 205.