СИСТЕМНЫЙ АНАЛИЗ РИСКОВ. ОПРЕДЕЛЕНИЕ ПОТЕНЦИАЛА АТАКИ

А.М. КРИШТОФИК

Выявление атак и других нарушений информационной безопасности, наряду с такими способами как уменьшение вероятности осуществления угроз безопасности, ликвидация уязвимостей или уменьшение их величины, уменьшение величины возможного ущерба, восстановление ресурсов, которым был нанесен ущерб, является одним из направлений снижения рисков нанесения ущерба. Данный способ реализуется путем разработки и использования систем обнаружения атак. Однако при их разработке возникает вопрос определения наиболее опасных атак, обнаружение которых является первоочередной задачей. Данная задача решается путем определения потенциалов атак и их ранжирования.

При использовании системного анализа рисков уточняется определение атаки по отношению к действующей нормативной базе в области безопасности информационных технологий. Потенциал атаки определяется как мера, характеризующая возможности по нанесению негативных последствий от реализации атаки, т.е. через риск нанесения ущерба владельцам активов. В качестве меры потенциала атаки используется частный Интегральный показатель защищенности. Численное значение потенциала атаки определяется на основании параметров и характеристик элементов безопасности с учетом вопросов коррелированности угроз безопасности и уязвимостей объекта оценки. Ранжирование атак проводится на основе коэффициентов их опасности.

Следовательно, при проектировании и разработке систем обнаружения атак с использованием системного подхода необходимо оценивать риски нанесения ущерба владельцам активов в целях определения потенциала атак и проведения их ранжирования