СЕКЦИЯ 1. ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМНЫЙ АНАЛИЗ РИСКОВ. СУЩНОСТЬ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ

В.В. АНИЩЕНКО

Нормативная база в области обеспечения безопасности информационных технологий предусматривает анализ и оценку рисков при проведении любых работ. Однако для этого не в полной мере разработаны математический и методический аппараты. В связи с этим широко используются на практике базовый и экспертный методы анализа рисков. Первый из них не предусматривает оценку рисков, второй - использует качественную или количественную оценку рисков на основании экспертных данных. Основными недостатками данных методов являются субъективность оценки и невозможность сопровождения и использования полученных результатов в процессе эксплуатации объекта информационных технологий (ОИТ). Для устранения указанных недостатков разработан системный анализ рисков.

Системный анализ рисков основан на проведении комплексного анализа всех элементов безопасности и оценка рисков на его основе. Он разработан на основе базовой модели ОИТ, модели системы защиты и их комплексных показателей, характеризующих взаимодействие объекта оценки (00) с внешней средой и негативные последствия этого взаимодействия, а также изменение свойств и характеристик 00 и последствий нарушения информационной безопасности при изменении его структуры.

Основными направлениями использования системного анализа рисков являются:

– комплексная оценка элементов безопасности;

– разработка требований безопасности и требований к стойкости средств обеспечения безопасности (СОБ);

– обоснование и выбор варианта СОБ, проведение сравнительного анализа различных вариантов СОБ;

– оценка защищенности ОИТ на всех этапах жизненного цикла;

– оценка соответствия ОИТ заданным требованиям безопасности;

– принятие решения о доработке (модернизации) СБО и выработка рекомендаций по ее проведению.