МЕТОДОЛОГИЯ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ АНАЛИТИКО-ИЕРАРХИЧЕСКИМ МЕТОДОМ

А.А. ЗАМУЛА, Б.В. ВОЛОБУЕВ, В.И. ЧЕРНЫШ

В современном мире эффективное и комплексное решение задач защиты информации в организации является ключевым фактором развития бизнеса. Согласно общепринятой международной практике защиты информации ключевое значение в процессе обеспечения информационной безопасности (ИБ) занимает анализ информационных рисков. Нормативно-правовая база по ИБ, на данный момент, находится на этапе формирования, где есть определенный ряд руководящих актов, документов, стандартов, но вопросы анализа информационных рисков остаются нерегламентированными. Именно поэтому организации собственноручно должны выбирать средства анализа информационных рисков для комплексного обеспечения режима ИБ.

В докладе рассматривается технология анализа информационных рисков, которая учитывает ключевые требования к процессу анализа рисков в организациях. Проанализировав существующие средства анализа рисков можно выделить ряд этапов для технологии, которая предлагается. В первом этапе определяются эксперты, которые будут участвовать в процессе оценки и определении коэффициентов для обобщения данных нескольких экспертов. Второй этап — получение информации об инфраструктуре. Эксперт определяет компоненты инфраструктуры организации. Третий этап — экспертная оценка угроз. Необходимо определить вероятность и ущерб от реализации каждой из угроз для всех служб, ресурсов. С учетом задачи разработки данной технологии получение данных о возможностях будет происходить не прямым методом оценки вероятности, а будет использоваться аналитико-иерархический метод для определения утверждений эксперта о значении вероятности одной угрозы относительно другой. Четвертый этап — генерирование рекомендаций и отчетов. На данном этапе подсчитываются результаты оценки угроз и определяются необходимые меры защиты. После расчетов значений рисков для компонентов системы эксперт получает информацию, которая свидетельствует об общем риске для компонента, рисках отдельных угроз и градации компонентов по степени уязвимости согласно этому значению.

Поскольку вопросы анализа информационных рисков остаются нерегламентированными, предложенная методология может являться актуальным средством анализа информационных рисков для комплексного обеспечения режима ИБ на предприятии.