УДК 004.056

Разработка методики оценки рисков информационной безопасности

Павлов К.А.
Белорусский национальный технический университет

Информационные технологии являются одним из самых динамично развивающихся направлений в Республике Беларусь и в мире. Ключевым аспектом в IT-сфере является обмен информацией в качестве продукции или услуги. Поэтому защита информации становится необходимой составляющей современного бизнеса в сфере информационных услуг, а также надежным инструментом защиты персональных данных, сбережений, интеллектуальной собственности. Все эти особенности защиты информации заложены в систему менеджмента информационной безопасности (далее – СМИБ), положения которой регламентированы международными стандартами ISO/IEC серии 27000.

Одним из главных положений при разработке и внедрении СМИБ в организации является выявление и оценка рисков информационной безопасности (далее – ИБ). Процедура оценивания рисков ИБ поэтапно изложена в ISO/IEC 27005. Согласно ISO/IEC 27005 алгоритм оценки рисков ИБ состоит из следующих этапов: инвентаризация активов; идентификация уязвимостей активов; идентификация угроз (источники потенциальных рисков); оценка последствий и описание средствами управления (механизмы снижения влияния угроз на активы организации через их уязвимости). Фактически данный алгоритм и определяет методику оценки рисков ИБ, которую внедряют организации в рамках функционирования СМИБ.

Однако практика применения данной методики показывает, что в ней, наряду с ее доступностью и итоговой информативностью, имеется существенный недостаток – этап инвентаризации активов. По сути, на этом этапе необходимо выявить все имеющие значимость (ценность) для деятельности организации объекты. И часто, специалисты для достижения этой цели руководствуются рекомендациями ISO 31010 – используют метод мозгового штурма. Данный метод также имеет ряд уязвимостей, связанных с корректным формированием экспертной группы (состав, согласованность эксперта и экспертов в группе и т. д.).

Поэтому для разработки результативной методики оценки рисков ИБ на стадии идентификации активов предлагается использовать функциональную модель бизнес-процессов, т.к. она, при корректном ее описание, отображает все основные процессы организации и взаимосвязанные с ними ресурсы, что, по факту, и является основными активами организации.