УДК 004.056

Головкова Елена Александровна,
к.т.н., доцент, Ангарский государственный технический университет,
e-mail: temnikova_ea@bk.ru

КОМПЛЕКСНЫЙ ПОДХОД К УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Golovkova E.A.

INTEGRATED APPROACH TO INFORMATION SECURITY RISK MANAGEMENT

Аннотация. Предложен комплексный риск-ориентированный подход управления информационной безопасностью, основанный на экспертных оценках, описана процессная модель управления рисками.

Ключевые слова: риск-ориентированный подход, информационная безопасность, оценка возврата инвестиций.

Abstract. A comprehensive risk-oriented approach to information security management based on expert assessments is proposed, and a process model of risk management is described.

Keywords: risk-based approach, information security, investment return assessment.

Основной целью обработки рисков является выбор наиболее эффективных мер, обеспечивающих сокращение среднегодовых потерь организации от инцидентов информационной безопасности (ИБ) при максимальном возврате инвестиций.

При управлении ИБ (анализе уязвимостей и угроз, возможного ущерба и рисков) рассматривают три свойства информации: конфиденциальность (к), целостность (ц) и доступность (д).

Процесс управления рисками ИБ состоит из 6 этапов, его можно представить в виде IDEF0-диаграммы, как показано на рисунке 1.

1 этап: определение активов организации и их ценности, анализ категории пользователей, имеющих доступ к информации.

2 этап: анализ возможного ущерба (коммерческим интересам организации и ущерб репутации).

3 этап: анализ возможных угроз и уязвимостей, ассоциированных с активами организации. Групповой уровень уязвимостей рассчитывается по формуле, где $Р_{уу}$ – это уровни уязвимости, а $Р_{МК}$ – уровни механизмов контроля.

$$\Gamma_{у} = \sum_{i=1}^{n} Р_{уу} - \sum_{i=1}^{n} Р_{МК}.$$

4 этап: определение величины риска, по матрице из рисунка 2.

5 этап: определение среднегодового ущерба (ALE) по формуле:

$$ALE = РУ \times k \times Р_{ру},$$

где РУ – размер ущерба; k – количество инцидентов в год; РРУ – вероятность успешной реализации угрозы.

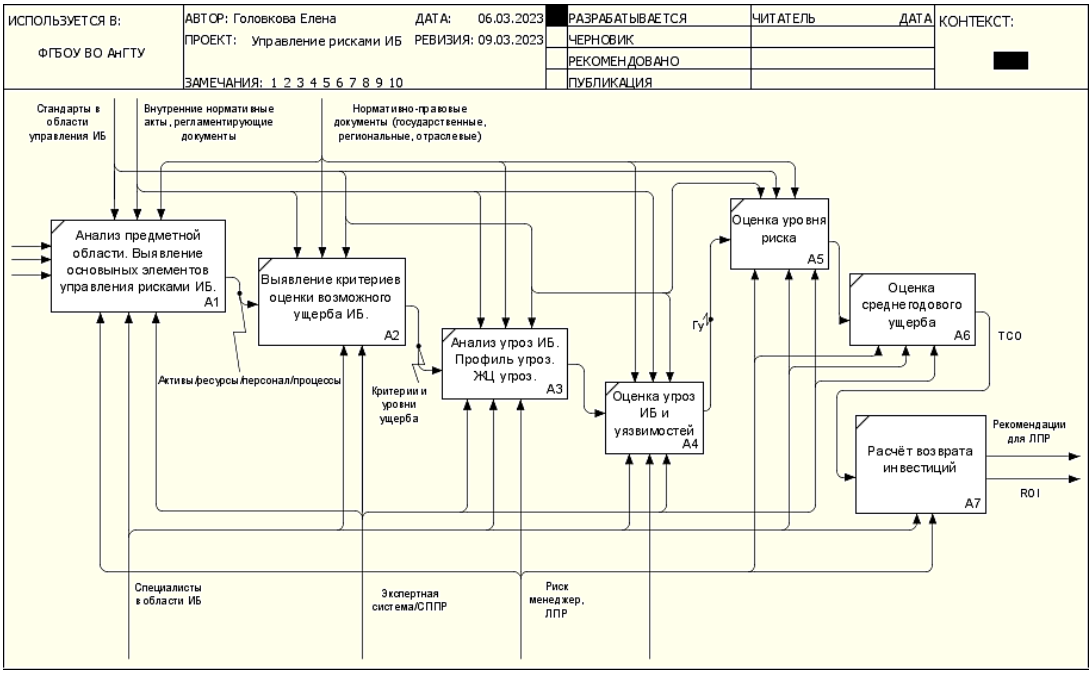

Рисунок 1 – Диаграмма декомпозиции процесса управления рисками ИБ

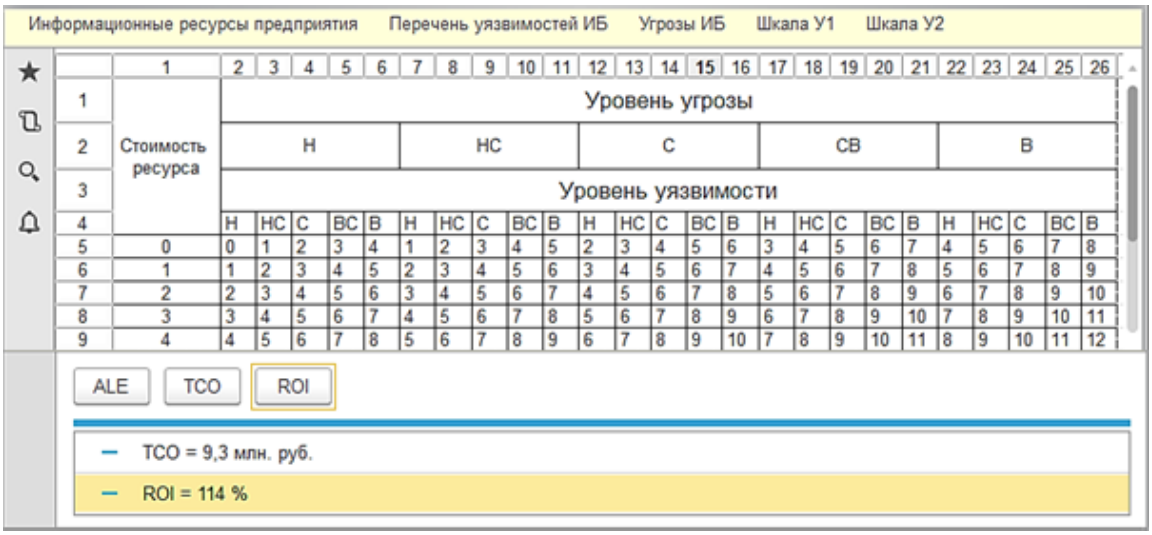

Рисунок 2 – Матрица величин риска

6 этап: расчёт коэффициента возврата инвестиций (ROI) по формуле:

$$\mathrm{ROI} = \frac{\mathrm{ALE}-\mathrm{TCO}}{\mathrm{TCO}} \times 100\ \%.$$

где TCO (Total Cost of Ownership) – это стоимость защитных мер:

$$\mathrm{TCO} = \mathrm{ПР} + \mathrm{К1} + \mathrm{К2},$$

где К1, К2 – косвенные затраты первой и второй групп, ПР – сумма капитальных затрат и расходов на управление. ROI > 100% свидетельствует о том, что затраты на ИБ окупились, есть прибыль от вложений (ROI = 100% – это точка безубыточности, 0 < ROI < 100% – возвращается часть затрат).

ЛИТЕРАТУРА

1. **Дорофеев, А. В.** Менеджмент информационной безопасности: основные концепции / Дорофеев А. В. – Текст : непосредственный // Вопросы кибербезопасности.– 2014, № 1(2). – С. 67-73.