УДК 004.056

Ожгибесова А.С., Шабуров А.С., Южаков А.А.
Пермский национальный исследовательский
политехнический университет, Пермь

О РАЗРАБОТКЕ МЕТОДА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Приводится обзор существующих методов оценки рисков информационной безопасности. Предлагается подход по совершенствованию методов оценки рисков, ориентированный на сохранении живучести информационных систем. Приведена математическая постановка задачи оценки рисков на основе применения методов нечеткой логики.

Ключевые слова: риск информационной безопасности, защита информации, живучесть информационных систем, нечеткая когнитивная карта.

В условиях количества и сложности кибератак оценка рисков информационной безопасности (ИБ) становится важнейшим инструментом для защиты данных, инфраструктуры и бизнес-процессов. Традиционные методы оценки рисков ИБ имеют общие недостатки, ограничивающие эффективность их применения [1]. Как правило, реализация традиционных подходов либо требует значительного количества ресурсов, либо имеют ограничения по применению (CRAMM, OCTAVE). Часть методов недостаточно гибки и сложно адаптируются к применению современных технологий (COBIT for Risk), или субъективны, узконаправленны и игнорируют устойчивость и возможность восстановления (FRAP, OCTAVE), акцентируя оценку на сохранении традиционных критериев обеспечения ИБ, а не на сохранении устойчивости функционирования систем в условиях риска и т. д.

Для преодоления этих недостатков необходимы новые, более гибкие подходы, ориентированные на противодействие современным киберугрозам и позволяющие автоматизировать процессы управления рисками ИБ в режиме реального времени, на основе применения технологий IoT, ML, AI и т. п.

В то же время значительное повышение актуальности проблем кибербезопасности, особенно для объектов класса КИИ, требует оценивать риски ИБ, с учетом сохранения надежности и работоспособности объектов защиты информации, а также сохранении живучести подобных систем [2], даже в условиях реализации стратегии принятия рисков ИБ.

К методам оценки рисков ИБ, ориентированных на сохранении живучести систем, способности их восстановления после инцидентов, а также устойчивости информационных систем, относятся: Survivability Analysis Framework (SAF), Mission-Oriented Riskand Design Analysis (MORDA), Resilience-Based Risk Management (RBRM) и Cyber Resilience Review (CRR). Каждый из данных методов имеет свои уникальные особенности, цели и подходы к оценке рисков, основные из которых приведены в табл. 1.

Анализ сравнительных характеристик базовых методов оценки рисков ИБ, позволяет сделать следующие выводы:

1) SAF подходит для глубокого анализа критических функций системы, но требует значительных затрат ресурсов;

2) MORDA ориентирована на системы, где важно выполнение конкретных миссий, но менее применима для систем общего назначения;

3) RBRM фокусируется на восстановлении после инцидентов, что делает ее полезной для систем с высокой важностью непрерывности, но требует значительных ресурсов для анализа рисков;

4) CRR – простой и доступный инструмент для оценки киберустойчивости, но не обеспечивает глубокого анализа данных.

Таблица 1

Сравнительные характеристики методов оценки рисков ИБ

	SAF	**MORDA**	**RBRM**	**CRR**
Основная цель	Сохранение критических функций	Оценка рисков для выполнения миссии	Повышение устойчивости и восстановления	Оценка киберустойчивости
Область приме-нения	Универсальная	Критические системы	Системы с высокой важностью непрерывности	Организации любого уровня
Методы анализа	Анализ угроз, уязвимостей	Сценарии угроз, анализ миссии	Анализ восстановления, сценарии инцидентов	Анкетирование, самооценка
Глубина анализа	Высокая	Высокая	Средняя	Низкая-средняя
Ресур-соемкость	Высокая	Высокая	Средняя	Низкая
Резуль-таты	Стратегии повышения живучести	Меры по снижению рисков для миссии	Планы повышения устойчивости	Рекомендации по улучшению

Таким образом, необходимо совершенствовать методы оценки рисков ИБ, с учетом ориентированности оценки на сохранении живучести ИС в условиях сохранения риска, путем нахождения оптимального баланса между универсальностью применения, необходимой глубиной анализа, оптимальной ресурсоемкостью и простотой применения технологий оценки. При этом, оценку целесообразно осуществлять на основе построения нечетких когнитивных карт (НКК), что неоднократно подтверждено [3, 4].

Для постановки задачи нахождения приемлемого уровня риска ИБ с учетом ориентированности на сохранении живучести ИС, обозначим:

$A = \{a_1, a_2, \dots a_n\}$ – множество ключевых активов;

$T = \{t_1, t_2, \dots t_p\}$ – множество угроз;

$V = \{v_1, v_2, \dots v_q\}$ – множество уязвимостей.

Для каждого актива $a_i \in A$ определяется подмножество соответствующих угроз $T_i \subseteq T$ и уязвимостей $V_i \subseteq V$. При этом, связь формализуется как:

$$R = \{(a_i, t_j, v_k) | a_i \in A, t_j \in T_i, v_k \in V_i\}. \quad (1)$$

Определим множество функциональных состояний ИС $S = \{s_1, s_2, \dots s_m\}$, где каждое состояние s_k характеризует степень работоспособности при частичных отказах ИС.

Живучесть системы L можно формализовать как функцию:

$L: S \to [0,1]$, $L(s_k)$-уровень живучести в состоянии s_k.

Для каждого состояния s_k вычисляется:

$$L(s_k) = \frac{\sum_{i=1}^{n} \alpha_i \cdot \delta_i(s_k)}{\sum_{i=1}^{n} \alpha_i}, \quad (2)$$

где α_i вес (значимость) актива a_i; $\delta_i(s_k) \in \{0,1\}$ – индикатор функционирования актива в состоянии s_k.

Построение НКК для оценки рисков ИБ предполагает представление ее в виде графа $G = (C, E, W)$, где $C = \{c_1, c_2, \dots c_l\}$ – концепты (факторы риска, уязвимости, угрозы); $E \subseteq C \times C$ – множество направленных связей; $W = \{w_{ij}\}, w_{ij} \in [-1,1]$ – веса влияния концепта c_j на концепт c_i.

Нечеткие значения концептов $A = \{a_1, a_2, \dots a_n\}$ задаются в виде чисел в интервале [0,1] и обновляются по формуле:

$$a_i^{(t+1)} = f\left(\sum_{j=1}^{l} w_{ij} \cdot a_i^{(t)}\right), \quad (3)$$

где $f(x)$ – функция активации, например:

$f(x) = \frac{1}{1+e^{-x}}$, или $f(x) = \min(1, \max(0, x))$.

Для каждого пути P_{ij} между концептами $c_j \to c_i$ можно вычислить агрегированное влияние с учетом длины пути и затухания:

$$Imp(c_j, c_i) = \sum_{k=1}^{K} \lambda^k \cdot \prod_{(u,v) \in P_{ij}^{(k)}} w_{uv}, \quad (4)$$

где $\lambda \in [0,1]$ – коэффициент затухания; K – максимальная длина пути; $P_{ij}^{(k)}$ – пути длины k между c_j и c_i.

Расчет уровня риска для актива α_i, связанного с угрозой t_j и уязвимостью v_k, определяется как нечеткая функция:

$$R_{ijk} = \mu T(t_j) \otimes \mu V(v_k) \otimes \mu C(c_m), \quad (5)$$

где $\mu T(t_j), \mu V(v_k), \mu C(c_m) \in [0,1]$ – степени принадлежности соответствующих концептов;

$\otimes$ – нечеткая операция агрегации (например, минимум, произведение или правило Мамдани).

Тогда общий риск для ИС будет определяться как:

$$R_{общ} = \sum_{(\alpha_i, t_j, v_k) \in R} \beta_{ijk} \cdot R_{ijk}, \quad (6)$$

где β_{ijk} – весовая значимость тройки (α_i, t_j, v_k).

Итоговый риск корректируется коэффициентом живучести ИС:

$$R_{кор} = R_{общ} \cdot (1 - L(s_{тек})), \quad (7)$$

где $L(s_{тек})$ – живучесть в текущем состоянии системы.

Разработанная математическая постановка задачи может являться основой предлагаемого метода оценки рисков ИБ, учитывающего особенности обеспечения живучести ИС различного назначения.

Список использованных источников:

1. Плетнёв П. В., Белов В. М. Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. 2011. № 3-1. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-suschestvuyuschih-metodov-opredeleniya-riskov-informatsionnoy-bezopasnosti (дата обращения: 13.04.2025).
2. Махутов Н.А., Петров В.П., Резников Д.О. Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47–66. (дата обращения: 17.04.2025).
3. Ожгибесова А. С. Об оценке рисков информационной безопасности на основе применения нечетких когнитивных карт в интеллектуальных транспортных системах управления дорожным движением / А.С. Ожгибесова, А.С. Шабуров, А.А. Южаков // Вестник УрФО. 2024. № 2(52). С. 56–67.
4. Васильев В.И. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт / В.И. Васильев, Р.Т. Кудрявцева, В.А. Юдинцев // Вестник УГАТУ. 2014. Т. 18, № 3 (64). С. 253–260. (дата обращения: 28.04.2025).

Ozhgibesova A.S., Shaburov A.S., Yuzhakov A.A.
Perm National Research Polytechnic University, Perm

ON THE DEVELOPMENT OF A METHOD FOR ASSESSING INFORMATION SECURITY RISKS

Abstract. This paper provides an overview of existing methods for assessing information security risks. A proposed approach for improving risk assessment methods is focused on maintaining the resilience of information systems. A mathematical formulation of the risk assessment problem is presented based on the application of fuzzy logic methods.

Keywords: information security risk, information protection, survivability of information systems, fuzzy cognitive map.