УДК 004.056:005.3

SNW-АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Ібрагімова Д. Ф., Добринін І. С.
e-mail: ibrahimova.diana@nure.ua, e-mail: ihor.dobrynin@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В. В. Поповського
м. Харків, Україна

This work compares the risk-based and game-theoretic approaches to building an Information Security Management Systems (ISMS). The study estimates these methods based on criteria such as risk assessment methodology, adaptability to evolving threats, implementation complexity, and consideration of attacker behavior. The risk-based approach ensures compliance with international standards and provides a structured methodology for security management. In contrast, the game-theoretic approach enables adaptive decision-making by anticipating an attacker's strategies. The analysis highlights the strengths and limitations of both methods, demonstrating that their combination offers a more effective ISMS model.

Із розвитком галузі інформаційних технологій кібератаки стають дедалі більш складними та небезпечними, отже виникає гостра потреба ефективного захисту інформаційних активів організацій. Найкращою практикою щодо вирішення цього питання є впровадження систем управління інформаційною безпекою (СУІБ), про що свідчать стандарти і нормативні акти, наприклад ISO/IEC 27001:2022 [1], Постанова №95 від 28.09.2017 Правління НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [2], тощо. Відомі різні підходи до побудови СУІБ. Найбільш вживаним є ризик-орієнтовний підхід, який використовується стандартом ISO/IEC 27001:2022 для створення СУІБ. У роботі [3] описано використання іншого підходу – теоретико-ігрового. Хоча обидва підходи спрямовані на забезпечення надійного та ефективного функціонування СУІБ, вони суттєво відрізняються за принципами аналізу та прийняття рішень. Метою даної роботи є порівняння зазначених підходів за ключовими критеріями та визначення їхніх сильних та слабких аспектів у контексті побудови СУІБ.

Ризик-орієнтовний підхід ґрунтується на аналізі активів, загроз і вразливостей, визначенні ймовірності реалізації ризиків та оцінюванні їхнього впливу [4]. Оцінка здійснюється через експертні висновки. Такий підхід дозволяє структурувати СУІБ, визначаючи ключові напрями захисту, спираючись на критичні ризики. Теоретико-ігровий підхід розглядає побудову СУІБ на основі динамічного процесу взаємодії між зловмисником та офіцером із інформаційної безпеки (CISO – Chief Information Security Officer) у вигляді гри, в якій опоненти мають свої цілі, ресурси, обмеження

та стратегії. Основна увага приділяється пошуку оптимальних стратегій протидії атакам, що дозволяє мінімізували можливі втрати шляхом оцінювання параметрів та властивостей конкретної організації.

Теоретико-ігровий підхід забезпечує більшу адаптивність, яка обумовлена можливістю прогнозувати дії зловмисників та відповідно до цього коригувати стратегії кіберзахисту, що є перевагою в середовищах, де загрози швидко змінюються. Ризик-орієнтовні методи використовують статичний аналіз загроз [4], який потребує періодичного оновлення оцінок. Таким чином ризик-орієнтовний підхід може бути недостатньо динамічними для реагування на нетипові загрози, отже СУІБ, побудована виключно на цьому підході, може виявитися недостатньо гнучкою для швидкої адаптації до змін у кіберпросторі.

Ризик-орієнтовний підхід задокументовано в багатьох стандартах, він є широко використовуваним та розвиненим, що дозволяє простіше його впроваджувати в організації, створюючи нову СУІБ або інтегруючи у вже наявну. За цієї ж причини такий підхід забезпечує дотримання певних нормативних вимог. Теоретико-ігрові методи для побудови СУІБ вимагають більш складних індивідуальних математичних розрахунків, особливо при моделюванні багатофакторних сценаріїв, що створює труднощі у вигляді потреби в додаткових ресурсах для обчислень і побудові моделей. Тобто, практичне застосування теоретико-ігрового підходу може бути обмеженим у випадках відсутності апріорної аналітики.

Теоретико-ігровий підхід передбачає аналіз поведінки атакуючих та прогнозування їхніх дій, що робить СУІБ здатною не лише до реактивного, а й до проактивного захисту, в той час як ризик-орієнтовний підхід не враховує мотиви та можливі стратегії атакуючих, оскільки зосереджується на технічних параметрах ризиків.

За результатами наведеного порівняння, у таблиці 1 надано SNW-аналіз досліджуваних підходів до побудови СУІБ, який якісно оцінює досліджувані об’єкти (у нашому випадку – підходи) за певними позиціями, використовуючи 3 стани: сильний (S), нейтральний (N) та слабкий (W).

Таблиця 1 – SNW-аналіз ризик-орієнтовного та теоретико-ігрового підходів

№ з/п	Найменування критерію оцінки	Ризик-орієнтовний підхід			Теоретико-ігровий підхід		
		S	N	W	S	N	W
1	2	3	4	5	6	7	8
1	Відповідність стандартам	X				X	
2	Легкість впровадження	X					X
3	Врахування динамічних змін		X		X		

Продовження таблиці 1

1	2	3	4	5	6	7	8
4	Широке практичне застосування	X				X	
5	Гнучкість (адаптивність)			X	X		
6	Здатність прогнозування			X	X		
7	Вартість реалізації		X				X
8	Можливість моделювання		X		X		
9	Швидкість реагування			X	X		

Аналіз таблиці 1 показує, що ризик-орієнтовний підхід забезпечує простоту реалізації та відповідність міжнародним стандартам, що робить його ефективним для організацій, які прагнуть дотримуватися регуляторних вимог. Теоретико-ігровий підхід пропонує можливість прогнозування дій зловмисників, завдяки чому може застосовуватись в нестабільному середовищі загроз. Таким чином, у реальних умовах найбільш ефективним є поєднання обох підходів, використовуючи їхні переваги та усуваючи недоліки. Зокрема, вважаємо за доцільне поєднати структурованість ризик-орієнтовного аналізу з адаптивністю теоретико-ігрового методу, таким чином отримуючи модель побудови СУІБ, яка буде водночас гнучкою, відповідати вимогам нормативно-правових документів так і оперативно враховувати потенційні кіберінциденти.

Список використаних джерел:

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 20.02.2025)

2. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Нац. банку України від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 20.02.2025).

3. Ібрагімова Д. Ф., Добринін І. С. Визначення стратегії захисту інформації при біматричній грі зловмисника та CISO. *«Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2024))* : Міжнар. науково-техн. конф., м. Харків, 13 – 14 листоп. 2024 р. 2024. С. 172 – 174.

4. The risk-based approach to cybersecurity / J. Boehm et al. *McKinsey & Company*. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity#/ (дата звернення: 21.02.2025).