УДК 004/056

ОБҐРУНТУВАННЯ ВИБОРУ ПІДХОДУ ДО ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Усенко М.О., Добринін І.С.
e-mail: maksym.usenko1@nure.ua, e-mail: ihor.dobrynin@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

This work is devoted to comparing four internationally recognized standards – BSI Standard 200-3, ISO/IEC 27005:2022, IEC 31010:2019, and NIST SP 800-30 Rev. 1. By utilizing the Analytic Hierarchy Process (AHP), this research evaluates the strengths and weaknesses of each standard, providing insights into their applicability and effectiveness in different organizational contexts. The findings contribute to the selection of the most suitable risk assessment methodology.

У сучасному світі безпека інформаційних систем є дуже важливим питанням для організацій різного рівня. Важливою частиною її забезпечення є визначення та мінімізація інформаційних ризиків. Оцінювання інформаційних ризиків є важливим процесом для організацій, оскільки воно дозволяє їм ідентифікувати, аналізувати та керувати ризиками, пов'язаними з інформаційними активами. Для оцінювання ризиків можуть бути використані різноманітні методики та стандарти [1].

Аналіз сучасної літератури за зазначеною тематикою показав, що наразі найбільш вживаними стандартами з оцінювання інформаційних ризиків є: BSI Standard 200-3, ISO/IEC 27005:2022, IEC 31010:2019 і NIST SP 800-30 Rev. 1. Вочевидь, кожний із зазначених стандартів має певні недоліки та переваги.

Метою даної роботи є обґрунтування вибору підходу до оцінювання ризиків інформаційної безпеки на основі чинних міжнародних стандартів.

Зазначена задача відноситься до задач багатокритеріальної оптимізації. В теорії математики показано, що для вирішення складних задач прийняття рішень, де присутні множинні, часто суперечливі критерії, може бути використаний метод аналізу ієрархій (Analytic Hierarchy Process, AHP), розроблений Томасом Сааті [2]. Загальна ідея цього методу полягає в декомпозиції проблеми вибору на більш прості складові та обробку суджень особою, яка приймає рішення. Через міркування визначається відносна значимість досліджуваних альтернатив за всіма критеріями, що є в ієрархії. На основі порівнянь критеріїв та альтернатив за кожним із критеріїв обчислюються коефіцієнти важливості критеріїв, оцінки альтернатив та знаходиться загальна оцінка, як виважена сума оцінок критеріїв. Альтернативний варіант, вага якого максимальна, вважається найкращим.

Отже, відповідно до [2], перш за все слід визначити критерії, які будуть використовуватись у процесі аналізу. Їх можна отримати, спираючись на результати SNW-аналізу, які надані в [3]. Визначимо наступні критерії:

– включення процесу обробки ризиків – стандарт включає не тільки безпосередньо процес оцінювання ризику, але також і обробки;

– використання різних методик оцінювання – розглядається використання якісного, напівкількісного та кількісного оцінювань;

– надання додаткового матеріалу, що вводить додаткові можливості до процесу – залучення додаткових таблиць та методів, що доповнюють або спрощують процес;

– варіативність – пропонування декількох методів та шляхів виконання етапів процесу;

– розширення процесу оцінювання ризиків у організації за межі інформаційної системи – розглядання аспектів ззовні інформаційної системи, що впливають на процес оцінювання або безпосередньо на ризики;

– простота та швидкість впровадження.

Використовуючи математичний апарат, зазначений в [2], з урахуванням обраних альтернатив (стандартів) та критеріїв, отримуємо результати, які надані в таблиці 1.

Таблиця 1 – Результати вибору найкращого стандарту оцінювання ризиків інформаційної безпеки

Стандарт	BSI Standard 200-3	ISO/IEC 27005:2022	IEC 31010:2019	NIST 800-30 Rev. 1
Оцінка	0,18	0,17	0,40	0,25

Результати, надані в таблиці 1 показують, що найкращим стандартом для оцінювання ризиків інформаційної безпеки є IEC 31010:2019. Проте, в окремих випадках, організації можуть використовувати і інші стандарти.

Список використаних джерел:

1. О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, *Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія*, Київ, ЦП «Компринт», 2017 – 435 с.

2. Saaty T.L. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process. Pittsburgh: RWS Publications, 2013. 477 p.

3. Усенко М. О., Добринін І. С. SNW-аналіз міжнародних стандартів з оцінювання інформаційних ризиків. м. Харків, 13 листоп. 2024 р. Харків, 2024. URL: https://ice.nure.ua/wp-content/uploads/2024/12/40_Usenko-M.O.-Dobrynin-I.S._Str.167-169.pdf (дата звернення: 02.03.2025).