МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

УДК 004.4

Тези доповідей

VIII Міжнародної науково-практичної конференції

"Інформаційна безпека та комп'ютерні технології"

24-25 квітня 2025 року

Кропивницький 2025

УДК 004.4

Матеріали VIII Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології": тези доповідей, 24-25 квітня 2025 р. – Кропивницький: ЦНТУ, 2025. – 97 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

© Колектив авторів, 2025
© Центральноукраїнський національний технічний університет, 2025

УДК 004(056.53+413.4)::001.51

В.В. Мохор[1], О.О. Бакалинський[1], Я.Ю. Дорогий[2], В.В. Цуркан[1,3]
v.mokhor@gmail.com, baov@meta.ua, yaroslav.dorohyi@donntu.edu.ua, v.v.tsurkan@gmail.com
[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ
[2]Донецький національний технічний університет, Дрогобич
[3]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

СПОСОБИ ОБИРАННЯ МЕТОДУ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Відповідно до [1], організаціям незалежно від типу, розміру, сфери діяльності необхідно визначати та застосовувати процес поводження з ризиками. Насамперед це стосується розробляння і впроваджування інтегрованої системи управління інформаційною безпекою, кібербезпекою, приватністю, використанням штучного інтелекту [2, 3]. Визначенню її складників передує задання критеріїв прийнятності та оцінювання ризиків і, як наслідок, обирання відповідного методу на етапі встановлювання контексту [1, 4, 5]. Цим ураховуються як потреби, очікування, обмеження з боку зацікавлених сторін, так і особливості розробляння і впроваджування інтегрованої системи управління безпекою діяльності організації. Тож обирання методу оцінювання ризиків інформаційної безпеки є актуальним завданням.

Розробляння інтегрованої системи управління безпекою діяльності організації обумовлюється внутрішнім і зовнішнім контекстами. Це спонукає до врахування насамперед меж її впроваджування (частина організації, організація загалом); наявності інформації про вразливості інформаційних активів, заходів/засобів, загрози, наслідки реалізування загроз і мети оцінювання ризиків. Тому обирання відповідного методу може здійснюватися двома способами [5]. Першим з них визначаються і ураховується вплив відповідних характеристик з огляду на контекст діяльності організації. Тоді як другим – завдання оцінювання ризиків інформаційної безпеки. Приклад обирання методу аналізування впливу на приватність (англ. Privacy Impact Analysis, PIA) другим способом представлено табл. 1 [5] з урахуванням настанов [1, 4]. Так, він може застосовуватися для ідентифікування, визначання оцінок вірогідності, рівня ризику. До того ж завжди застосовується у межах виконання завдань визначання оцінок наслідків реалізування загрози та зіставляння ризиків інформаційної безпеки [4].

Таблиця 1

Приклад використання способу обирання методу оцінювання ризиків інформаційної безпеки відповідно до завдань

Метод оцінювання ризиків інформаційної безпеки	Оцінювання ризиків інформаційної безпеки				
	Ідентифікування ризиків інформаційної безпеки	Аналізування ризиків інформаційної безпеки			Зіставляння ризиків інформаційної безпеки
		Наслідки	Вірогідність	Рівень ризику	
Аналізування впливу на приватність	Застосовується	Завжди застосовується	Застосовується	Застосовується	Завжди застосовується

Отже, запорукою результативності розробляння і впроваджування інтегрованої системи управління безпекою є урахування внутрішнього і зовнішнього контекстів діяльності організацій. Це досягається встановлюванням критеріїв прийнятності, оцінювання ризиків інформаційної безпеки та, як наслідок, обиранням відповідного методу одним з або комбінуванням способів на основі характеристик і завдань.

Список літератури

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/27001 (accessed on: 08.04.2025).

2. The Integrated Use of Management System Standards (IUMSS). [Valid from 2018-11]. URL: https://www.iso.org/publication/PUB100435.html (accessed on: 08.04.2025).

3. Мохор В. В., Бакалинський О. О., Дорогий Я. Ю., Цуркан В. В. Симбіоз систем захисту інформації об'єктів критичної інфраструктури сфери енергетики. *Кібербезпека енергетики* : матеріали науково-практичної конференції (Київ, 31 травня 2023 р.). Київ, 2023. С. 107–108. DOI: https://doi.org/10.5281/ zenodo.14601428

4. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/80585.html (accessed on: 08.04.2025).

5. IEC 31010:2019. Risk management. Risk assessment techniques. [Valid from 2019-06-17; revised 2024-09-03]. URL: https://www.iso.org/standard/72140.html (accessed on: 08.04.2025).