МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

ПОЛОЖЕНЦЕВ АРТЕМ АНАТОЛІЙОВИЧ

УДК 004.738.5:159.923

ДИСЕРТАЦІЯ

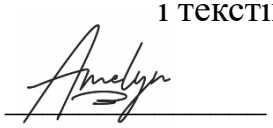
МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ІТ-ІНЦИДЕНТАМИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

122 «Комп’ютерні науки»

12 «Інформаційні технології»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.



_____ А.А. Положенцев

Науковий керівник:
Сидоренко Вікторія Миколаївна
кандидат технічних наук,
доцент

Київ – 2024

АНОТАЦІЯ

Положенцев А. А. Методи управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 12 «Інформаційні технології», за спеціальністю 122 «Комп’ютерні науки». — Національний авіаційний університет, м. Київ, 2024.

Дисертаційна робота присвячена дослідженню методів управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури, а саме – методу визначення стану захищеності об’єктів критичної інформаційної інфраструктури, методу визначення пріоритетів ІТ-інцидентів та управління ІТ-загрозами.

Проведено аналіз сучасних підходів до управління ІТ-інцидентами для ОКІІ держави. Встановлено, що існуючі методи оцінювання рівня кібербезпеки потребують оновлення індикаторів ІТ-безпеки та рівня цифрової трансформації, а також розробки рекомендацій для оптимізації захисту ОКІ. Відомі підходи до визначення пріоритетів ІТ-інцидентів не враховують ієрархічні структури потенційних загроз та ймовірності їх реалізації. Більшість методів оцінювання не використовують багатокритеріальні методи прийняття рішень і моделювання загроз, що обмежує їх ефективність. Розроблені методи спрямовані на подолання цих недоліків, забезпечуючи кількісну оцінку рівня захищеності, ефективне управління ІТ-загрозами та оптимальний розподіл ресурсів для захисту критичної інфраструктури. Проведений аналіз дозволив формалізувати завдання дисертаційного дослідження щодо розробки і вдосконалення методів управління ІТ-інцидентами на ОКІ.

Розроблено метод визначення стану захищеності об’єктів КІІ від ІТ-ризиків. Метод реалізується у кілька етапів, включаючи визначення загальних метрик ІТ-

безпеки, обчислення індексу цифрової трансформації, розрахунок кількісних параметрів стану захищеності та аналіз результатів з розробкою рекомендацій для оптимізації захисту. У результаті проведеного експериментального дослідження встановлено, що для сектору критичної інфраструктури "Цифрові технології" рівень захищеності $\mathbf{I}_{IT\,\mathrm{Sec}}$ становить 1.33%, що вказує на адекватний рівень безпеки відносно рівня цифрової трансформації $\mathbf{I}_{EGDI}$.

Розроблено метод визначення пріоритетів ІТ-інцидентів для забезпечення захисту критичної інфраструктури держави. Метод включає ідентифікацію та оцінку загроз, їх пріоритизацію за допомогою методу попарних порівнянь (AHP) і синтез локальних та глобальних пріоритетів. Метод допомагає зосередити ресурси на найбільш критичних загрозах, підвищуючи ефективність захисних заходів та забезпечуючи надійність і стійкість КІ. Експериментальне дослідження показало, що найбільш критичними загрозами є помилки користувачів, перебої в обслуговуванні та інциденти безпеки, що потребують першочергових заходів для їх нейтралізації.

Розроблено метод оцінювання ІТ-загроз на основі багатокритеріального прийняття рішень TODIM та моделі STRIDE для КІІ. Метод включає ідентифікацію загроз за методологією STRIDE, оцінювання та порівняння загроз за критеріями, використання функції проспективної цінності для моделювання ризиків, інтегративну оцінку корисності загроз і їх пріоритизацію. Експериментальне дослідження показало, що загроза Denial of Service (DoS) є найбільш критичною для КІІ, що потребує першочергових заходів для зменшення ризиків.

Ключові слова: критична інфраструктура, критична інформаційна інфраструктура, об’єкти критичної інфраструктури, кібербезпека, управління, оптимізація, інциденти, кіберінциденти, загрози, оцінка ризиків, оцінка загроз, модель загроз, виявлення атак, пріоритети інцидентів, STRIDE, TODIM, ITIL.

ABSTRACT

Polozhentsev A. Methods and means of IT Incident Management at Critical Information Infrastructure Facilities. – Qualification Scientific Work in the Form of a Manuscript. Dissertation for the Degree of Doctor of Philosophy in the Specialty 05.13.06 "Information Technology". – National Aviation University, Kyiv, 2024.

An analysis of current approaches to managing IT threats for the state's critical information infrastructure (CII) has been conducted. It was established that existing methods for evaluating the level of cybersecurity need updating of IT security indicators and the level of digital transformation, as well as the development of recommendations for optimizing the protection of critical infrastructure objects (CIO). Known approaches to determining IT threat priorities do not take into account the hierarchical structures of potential threats and the probability of their realization. Most methods for evaluating IT threats do not use multi-criteria decision-making methods and threat modeling, which limits their effectiveness. The developed methods aim to overcome these shortcomings, providing quantitative assessment of the level of protection, effective management of IT threats, and optimal allocation of resources for the protection of critical infrastructure. The analysis allowed formalizing the tasks of the dissertation research on the development and improvement of methods for managing IT incidents in CIO.

A method for determining the security status of CII objects from IT risks has been developed. The method is implemented in several stages, including the determination of general IT security metrics, calculation of the digital transformation index, quantitative parameters of the security status, and analysis of results with the development of recommendations for protection optimization. Experimental research found that for the "Digital Technologies" sector of critical infrastructure, the security level is 1.33%, indicating an adequate level of security relative to the level of digital transformation.

A method for determining the priorities of IT threats to ensure the protection of the state's critical infrastructure has been developed. The method includes identification and assessment of threats, their prioritization using the paired comparison method (AHP), and synthesis of local and global priorities. The method helps focus resources on the most critical threats, increasing the effectiveness of protective measures and ensuring the reliability and resilience of critical infrastructure. Experimental research showed that the most critical threats are user errors, service outages, and security incidents, requiring priority measures for their mitigation.

A method for evaluating IT threats based on the multi-criteria decision-making method TODIM and the STRIDE model for CII has been developed. The method includes identifying threats using the STRIDE methodology, evaluating and comparing threats by criteria, using a prospective value function to model risks, integrative assessment of threat utility, and prioritization. Experimental research showed that the Denial of Service (DoS) threat is the most critical for CII, requiring priority measures to reduce risks.

Keywords: critical infrastructure, critical information infrastructure, critical infrastructure facilities, cybersecurity, management, optimization, incidents, cyber incidents, threats, risk assessment, threat assessment, threat model, attack detection, incident priorities, STRIDE, TODIM, ITIL.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Розділ у колективній монографії:

1. Polozhentsev A., Fesenko A., Gnatyuk V, (2017) Method for CSIRT performance evaluation, *Project interdyscyplinarny projektem XXI wieku, Tom 2* (263-269).

Особистий внесок автора: проведено оцінку ефективності роботи команди реагування на інциденти комп'ютерної безпеки, визначено ключові показники ефективності, побудована панель індикаторів.

Статті у фахових наукових виданнях:

1. Положенцев А. А., Сидоренко В. М. Метод управління ІТ-загрозами на об’єктах критичної інформаційної інфраструктури. *Наукоємні технології*. 2024. Т. 2, № 62. С. 121–133.

Особистий внесок автора: проведено аналіз існуючих методів управління ІТ-загрозами, розроблено метод управління ІТ-загрозами для ОКІІ.

2. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління. 2024. Т. 2. №78. С. 68-80.

Особистий внесок автора: проведено аналіз підходів до визначення пріоритетів, розроблено етапи методу визначення пріоритетів ІТ-інцидентів.

3. Сидоренко В.М., Положенцев А.А., Гнатюк С.О. Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави. *Вісник інженерної академії України*. 2017. № 42. С. 81–89.

Особистий внесок автора: проведено аналіз підходів оцінювання рівня кібербезпеки об'єктів критичної інфраструктури держави.

4. Гнатюк С.О., Бердибаєв Р.Ш., Богун А.М., Сидоренко В.М., Положенцев А.А., Жигаревич О.К. Інтеграційна шина даних для ефективного функціонування системи управління подіями інформаційної безпеки. *Проблеми інформатизації та управління*. 2023. Т. 3. № 75. С. 29-40.

Особистий внесок автора: проаналізовано найпопулярніші сучасні рішення для побудови корпоративних сервісних шин.

5. Жигаревич О.К., Бердибаєв Р.Ш., Сидоренко В.М., Положенцев А.А., Кримська А.О. Модель онтоголіко-реляційного сховища даних для функціонування хмарної SIEM-системи. *Проблеми інформатизації та управління*. 2023. Т. 4. № 76. С. 17-27.

Особистий внесок автора: проведено аналіз використання хмарних SIEM-систем.

Статті у виданнях, які включено до міжнародних наукометричних баз:

1. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Fesenko, A., Akatayev, N., Zhilkishbayeva, G. Method of cybersecurity level determining for the critical information infrastructure of the state. *CEUR Workshop Proceedings*. 2020. Vol. 2616. P. 332-341. URL: https://ceur-ws.org/Vol-2616/paper28.pdf

Особистий внесок автора: представлено метод визначення рівня кібербезпеки об'єктів критичної інформаційної інфраструктури держави.

2. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Sotnichenko, Y. Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure. *IEEE International Conference on Problems of Infocommunications Science and Technology*. 2021. P. 757-764. DOI: https://doi.org/10.1109/PICST51311.2020.9467987.

Особистий внесок автора: визначено переваги та недоліки відомих підходів визначення рівня кібербпезки галузі цивільної авіації.

3. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., Polozhentsev, A. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. *CEUR Workshop Proceedings*, 2022. Vol. 3156. P. 390-399. URL: https://ceur-ws.org/Vol-3156/paper29.pdf

Особистий внесок автора: проведено аналіз існуючих методів та моделей оцінки рівня критичності ІТС.

4. Polozhentsev, A., Gnatyuk, S., Berdibayev, R., Sydorenko, V., Zhyharevych, O. Novel Cyber Incident Management System for 5G-based Critical Infrastructures. *IDAACS*. 2023, P. 1037-1041. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348645.

Особистий внесок автора: досліджено універсальну систему кореляції подій та управління інцидентами кібербезпеки для мереж 5G.

5. Lutskyi, M., Sydorenko, V., Polozhentsev, A., Apenko, N., Sydorenko, S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. *CEUR Workshop Proceedings*. 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf

Особистий внесок автора: запропоновано модель оцінки ефективності систем захисту інформації.

6. Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., Brzhanov, R. Method of Forming the Functional Security Profile for the Sectoral Information and Telecommunication Systems. *CEUR Workshop Proceedings*. 2021. Vol. 3179. P. 272-283. URL: https://ceur-ws.org/Vol-3179/Paper_25.pdf

Особистий внесок автора: запропоновано структурно-функціональний метод визначення функціонального профілю безпеки підсистеми галузевої ІТС.

7. Yarotskiy, S., Sydorenko, V., Lelechenko, A., Kolisnyk, O., Polozhentsev, A. Method of Determining the Importance Factor of IT Security Projects Investment Attractiveness in Critical Infrastructures. *CEUR Workshop Proceedings*. 2023. Vol. 3550. P. 181-190. URL: https://ceur-ws.org/Vol-3550/paper15.pdf

Особистий внесок автора: обґрунтовано, що оцінка ступеня інвестиційної привабливості об'єкта експертизи отримується за допомогою мультиплікативної функції агрегування, яка враховує нормовані коефіцієнти важливості.

8. Gnatyuk, S., Sydorenko, V., Yudin, O., Zhyharevych, O., Polozhentsev, A. Method for Calculating the Criticality Level of Sectoral Information and Telecommunication Systems. *CEUR Workshop Proceedings*. 2022. Vol. 3347. P. 234-245. URL: https://ceur-ws.org/Vol-3347/Paper_20.pdf

Особистий внесок автора: представлено метод розрахунку рівня критичності галузевої ІТС.

9. Gnatyuk, S., Sydorenko, V., Polozhentsev, A. Method for Cybersecurity Level Evaluation in the Civil Aviation Critical Infrastructure. *Lecture Notes in Networks and Systems*. 2023. Vol. 736. P. 206-218, DOI: https://doi.org/10.1007/978-3-031-38082-2_16.

Особистий внесок автора: проаналізовано перелік переваг та недоліків підходів визначення рівня кібербезпеки ОКІІ.

10. Sydorenko, V., Zhyharevych, O., Berdybaev, R., Polozhentsev, A., Fesenko, A. Ontological-Relational Data Store Model for a Cloud-based SIEM System Development. *CEUR Workshop Proceedings*. 2024. Vol. 3654. P. 343-354. URL: https://ceur-ws.org/Vol-3654/paper29.pdf

Особистий внесок автора: проведено аналіз сучасних типів баз даних, для обґрунтування вибору найбільш ефективних для створення моделі онтологічно-реляційного сховища даних.

11. Gnatyuk, S., Satybaldiyeva, F., Sydorenko, V., Zhyharevych, O., Polozhentsev, A. Model of Information Technology for Efficient Data Processing in Cloud-based Malware Detection Systems of Critical Information Infrastructure. *CEUR Workshop Proceedings*. 2023. Vol. 3421. P. 206-213. URL: https://ceur-ws.org/Vol-3421/short6.pdf

Особистий внесок автора: проведено дослідження імовірнісних та часових характеристик алгоритмів і програм генерації та обробки метаданих у хмарній системі виявлення шкідливого програмного забезпечення.

12. Lutskyi, M., Gnatyuk, S., Sydorenko, V., Yarotskiy, S., Polozhentsev, A. Study on the Evaluating the Degree of Investment Attractiveness of IT-Projects. *DESSERT*. 2023. P 1-7. DOI: https://doi.org/10.1109/DESSERT61349. 2023.10416440

Особистий внесок автора: проведено аналіз групових систем переваг експертів за комплексом характерних особливостей інвестиційної привабливості для оцінювання IT-проектів.

13. Semenchenko, A., Gurkovskyi, V., Romanenko, Y., Sydorenko, V., Kudrenko, S., Polozhentsev, A. Ukraine on the Road to the European Digital Market: Status and Tools for Implementing the European Digital Economy and Society Index in Ukraine. *CEUR Workshop Proceedings*. 2022. Vol. 3296. P. 18-28. URL: https://ceur-ws.org/Vol-3296/paper2.pdf

Особистий внесок автора: обґрунтовано актуальність та необхідність впровадження індексу цифрової економіки та суспільства в Україні.

14. Lutskyi, M., Gnatyuk, S., Verkhovets, O., Polozhentsev, A. Information Flows Formalization for BSD Family Operating Systems Security Against Unauthorized Investigation. Lect*ure Notes on Data Engineering and Communications Technologies*. 2023. Vol. 178. P. 235-246. DOI: https://doi.org/10.1007/978-3-031-35467-0_16.

Особистий внесок автора: проведено моделювання інформаційних потоків в операційних системах, що дозволяє більш ефективно виявляти загрози інформаційній безпеці.

15. Gnatyuk, S., Berdibayev, R., Sydorenko, V., Polozhentsev, A., Ryabyy, M. Enterprise Service Bus Construction in SOA Architecture for SIEM Implementation in Critical Information Infrastructure. *CEUR Workshop Proceedings*. 2022. Vol. 3288. P. 11-20. URL: https://ceur-ws.org/Vol-3288/paper2.pdf

Особистий внесок автора: проаналізовано найпопулярніші сучасні рішення для побудови корпоративних сервісних шин.

Наукові праці, які додатково відображають наукові результати дисертації:

1. Сидоренко В., Положенцев А., Юдін О., Жигаревич О. «Функціональна модель визначення критичності галузевих інформаційно-телекомунікаційних систем» АВІА-2023: XVI міжнар. наук.-техніч. конф., 18-20 квітня 2023 р.: тези доп., Київ: НАУ, 2023. С. 16.14-16.17.

Особистий внесок автора: розглянуто питання критичних галузевих інформаційно-телекомунікаційних систем.

2. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. «Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи», Кіберзахист особи, суспільства і держави: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.

Особистий внесок автора: проведено аналіз використання хмарних SIEM-систем.

3. А. Положенцев, В. Сидоренко, «Метод визначення рівня кібербезпеки об’єктів критичної інфраструктури держави», Матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2018. Сучасні проблеми науки», м. Київ, 4-6 квітня 2018 р., с. 102-103, 2018.

Особистий внесок автора: представлено метод визначення рівня кібербезпеки.

4. С. Гнатюк, В. Сидоренко, А. Положенцев. «Визначення показників рівня кібербезпеки об'єктів критичної інфраструктури авіаційної галузі». Матеріали VII Всеукр. наук.-практ. конф. «Перспективні напрямки захисту інформації», 30 серпня-03 вересня 2021 р.: тези доп. – Одеса, 2021. – С. 150-153.

Особистий внесок автора: проведено аналіз підходів визначення рівня кібербезпеки.

5. Ж. Алімсеітова, А. Положенцев. «Аналіз підходів до визначення терміну «критична інфраструктура» у різних країнах світу». Матеріали VI Міжн. наук.-практ. конф. «ITSEC», 17-19 травня 2016.: тези доп. – Київ, 2021. С. 62.

Особистий внесок автора: проведено аналіз підходів до визначення терміну «критична інфраструктура».

6. А. Положенцев. «Методи ведення кібервійни як потенційна загроза критичним авіаційним інформаційним системам». Матеріали IV Всеукраїнської наук.-практ. конф. молодих учених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики». тези доп., 28-29 жовтня 2015. К. С. 106.

Особистий внесок автора: висвітлено питання кібервійни як загрози критичним авіаційним інформаційним системам.

7. А. Положенцев. «Поняття кібервійни та їх прояв у сучасному світі». Матеріали наук.-практ. конф."Перспективні напрями захисту інформації": тези доп., 7-8 вересня 2015р., Одеса. – С. 79-80.

Особистий внесок автора: висвітлено поняття кібервійни та її прояв у сучасному світі.

8. А. Положенцев. «Інформаційна війна». Матеріали XV Міжн. наук.-практ. конф. молодих учених і студентів «Політ. Сучасні проблеми науки»:, 8-9 квітня 2015р.: тези доп. міжнар. наук.-практ. конф. – К., 2015. – С. 139.

Особистий внесок автора: проведено аналіз підходів до визначення поняття інформаційної війни.

9. В.О. Гнатюк, А.А. Положенцев. «Метод оцінки ефективності роботи груп реагування на кіберінциденти». Матеріали II всеукр. наук.-пр. конф. «Перспективні напрями захисту інформації». – м. Одеса, 03-07 вересня 2016 р. – Одеса: ОНАЗ, 2016. – С. 56-58.

Особистий внесок автора: проведено аналіз підходів реагування на кіберінциденти.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІКС	- інформаційно-комунікаційні системи;
ІКТ	- інформаційно-комунікаційні технології;
ІС	- інформаційна система;
ІТ	- інформаційні технології;
ІТС	- інформаційно-телекомунікаційні системи;
КІ	- критична інфраструктура;
КІІ	- критична інформаційна інфраструктура;
ОКІІ	- об’єкти критичної інформаційної інфраструктури
STRIDE	- Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TODIM	- метод прийняття рішень, який оцінює альтернативи на основі кількох критеріїв і враховуючи суб'єктивні переваги та ризики
ITIL	- бібліотека інфраструктури інформаційних технологій
AHP	- метод аналізу ієрархій

ВСТУП

Актуальність

В умовах швидкого розвитку інформаційних технологій та цифрової трансформації всіх сфер суспільного життя, захист ІТ-систем стає однією з ключових складових національної безпеки будь-якої держави. Питання захисту критичної інфраструктури (КІ) є важливими, оскільки від надійності цих систем залежить стабільне функціонування економіки, громадського порядку, охорони здоров'я та інших життєво важливих секторів.

КІ держави включає енергетичні, транспортні, фінансові, промислові, цифрові системи та інші важливі сектори, які, у разі порушення їх роботи, можуть призвести до серйозних наслідків для суспільства та держави в цілому. Зростаюча кількість та складність ІТ-загроз вимагає розробки нових підходів до оцінювання стану захищеності та управління ІТ-інцидентами для забезпечення надійного функціонування критичної інформаційної інфраструктури (КІІ).

КІІ держави є особливо вразливою до ІТ-інцидентів та загроз. Відсутність належного захисту КІІ може призвести до зупинки критичних функцій держави, що, в свою чергу, може мати катастрофічні наслідки для економіки та безпеки країни.

Важливість дослідження зумовлена необхідністю створення ефективних методів для управління та пріоритизації ІТ-загроз, що дозволить оптимально розподіляти ресурси для їх нейтралізації. Сучасні методи оцінювання стану ІТ-систем повинні враховувати не лише технічні аспекти, але й рівень цифрової трансформації, а також бути адаптованими до постійно змінюваного ландшафту загроз.

Питаннями захисту КІІ держави, зокрема від ІТ-інцидентів, займаються такі вітчизняні та закордонні вчені: К. Маклафлін, Р. Хан, Д. Лаверті, С. Сезер,

А.Б. Качинський, В.С. Харченко, В.В. Мохор, Ю.І. Хлапонін, О.Ю. Юдін, С.Ф. Гончар, П.М. Складанний, та ін.

Теоретична база дослідження питань оцінювання стану ІТ-систем та управління ІТ-загрозами є достатньо розвиненою, однак розробки щодо їх практичної реалізації в сучасних умовах майже відсутні. Більшість досліджень фокусуються на питаннях кібербезпеки, тоді як дослідження ІТ-інцидентів має свої особливості та відрізняється від загальних питань інформаційної безпеки.

Дослідження ІТ-інцидентів є важливим, оскільки вони безпосередньо впливають на працездатність та стабільність інформаційних систем. ІТ-інциденти можуть включати як зовнішні атаки, так і внутрішні помилки, збоїв в програмному забезпеченні та інші непередбачувані події, які можуть призвести до втрати даних, зупинки сервісів та інших негативних наслідків. Важливо швидко ідентифікувати та оцінювати ці інциденти для мінімізації їхнього впливу та забезпечення безперервності роботи систем.

Ця тематика відрізняється від загальних питань інформаційної безпеки тим, що вона охоплює не лише захист від зовнішніх загроз, але й управління внутрішніми ризиками та відновлення після інцидентів. В той час як інформаційної безпеки здебільшого фокусується на превентивних заходах, дослідження ІТ-інцидентів включає також реактивні та відновлювальні процеси, що є критично важливими для збереження функціональності інформаційних систем у випадку інциденту.

Таким чином, питання захисту КІ та КІІ є надзвичайно актуальними в сучасному світі, де інформаційні системи стають все більш інтегрованими та залежними від технологій, що створює нові виклики та ризики, які необхідно враховувати та активно управляти.

З огляду на зазначене, розроблення методів управління ІТ-інцидентами на ОКІ є актуальною науково-технічною задачею, що має теоретичне і практичне значення.

Тема дисертації відповідає освітньо-науковій програмі “Комп’ютерні науки” за спеціальністю 122 “Комп’ютерні науки” галузі знань 12 “Інформаційні технології” в Національному авіаційному університеті.

Зв’язок роботи з науковими програмами, планами, темами

Дисертаційна робота безпосередньо пов’язана з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2024–2028 роки», виконана в межах наукового напряму «Нові комп’ютерні засоби та технології інформатизації суспільства» визначеного пріоритетним у переліку актуальних проблем Міністерством освіти і науки України, концепції «Програми інформатизації НАН України на 2020-2024 роки за основними її напрямами». Теоретичні і практичні положення дисертаційної роботи були використані в науково-дослідних роботах, які виконувались у Національному авіаційному університеті, а саме «Алгоритмічно-програмне забезпечення універсальних методів захищеного передавання даних при використанні розвідувально-пошукового БПЛА (держ. реєстр. № 0120U101400) (2023-2024 рр.).

Мета і задачі дослідження

Метою дисертаційної роботи є удосконалення системи управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту.

Для досягнення поставленої мети необхідно розв’язати такі основні задачі:

– провести аналіз сучасних підходів до управління ІТ-інцидентами на об’єктах критичної інфраструктури держави;

– удосконалити метод оцінювання рівня захищеності та розробити відповідні рекомендації щодо оптимізації захисту об’єктів критичної інформаційної інфраструктури для визначення стану їх захищеності та управління захистом від ІТ-інцидентів.

– удосконалити метод визначення пріоритетів ІТ-інцидентів для кількісного визначення пріоритетів та управління ними.

– розробити метод оцінювання ІТ-загроз, для ідентифікації, оцінки та пріоритизації ІТ-загроз для оптимального розподілу ресурсів захисту критичної інформаційної інфраструктури.

– провести верифікацію розроблених методів з використанням розробленого програмного забезпечення з метою підтвердження їх ефективності та придатності для практичного застосування.

Об’єктом дослідження є процеси управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури.

Предметом дослідження є методи та засоби управління інцидентами на об'єктах критичної інформаційної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту.

Методи дослідження базуються на сучасних методах теорії захисту інформації, які використовуються для визначення метрик у методі оцінювання стану захищеності КІІ, теорії множин для формалізації етапів методів оцінювання ІТ-загроз, системного та структурного аналізу для визначення взаємозв'язків між

компонентами КІІ та моделювання загроз, методах багатокритеріального прийняття рішень для оцінювання та пріоритизації ІТ-загроз, а також теорії графів для відображення елементів КІІ та їх функціональних процесів.

Наукова новизна одержаних результатів полягає у наступному:

– *вперше* розроблено метод управління ІТ-загрозами, який за рахунок синтезу методів багатокритеріального прийняття рішень, моделювання загроз та функції перспективної цінності, дає змогу ідентифікувати, оцінювати та пріоритизувати ІТ-загрози для оптимального розподілу ресурсів захисту критичної інфраструктури держави.

– *удосконалено* метод визначення пріоритетів ІТ-інцидентів, який за рахунок представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації, дозволяє кількісно оцінити пріоритети ІТ-інцидентів та управляти ними для забезпечення необхідного рівня захисту життєво важливих інтересів громадян, суспільства, держави та правопорядку;

– *отримав подальшого розвитку* метод оцінювання рівня захищеності, який за рахунок використання нових індикаторів ІТ-безпеки та рівня цифрової трансформації, а також розроблених рекомендацій для оптимізації захисту дає змогу визначити стан захищеності об’єктів критичної інфраструктури (сектору/підсектору чи держави в цілому), а також управляти захистом зазначених об’єктів в умовах виникнення ІТ-інцидентів;

Практичне значення одержаних результатів. дисертаційного дослідження полягає у тому, що отримані результати можуть бути використані відповідними органами для ефективного оцінювання стану захищеності сектуру/підсектору КІІ, або управління ІТ-загрозами, крім цього було:

– реалізовано програмний застосунок, який автоматизує процес оцінки стану захищеності об’єктів критичної інформаційної інфраструктури, для

забезпечення структурованого підходу до збору даних, проведення оцінювання рівня захищеності та надає конкретні рекомендації для покращення безпеки критичної інформаційної інфраструктури.

– реалізовано методику, яку можна використовувати для визначення пріоритетів ІТ-інцидентів, що дозволяє ефективно ідентифікувати та пріоритизувати інциденти на ОКІІ та оптимізувати розподіл ресурсів, забезпечуючи надійність та стійкість критичних інформаційних систем.

– реалізовано програмний застосунок для управління ІТ-загрозами критичної інформаційної інфраструктури, який шляхом синтезу багатокритеріального методу прийняття рішень TODIM та моделлю загроз STRIDE, дозволяє ефективно ідентифікувати, оцінювати та пріоритизувати загрози, враховуючи їхню ймовірність, потенційний збиток та складність реалізації.

– теоретичні результати дисертації та результати експериментальних досліджень впроваджені і використовуються у науково-дослідній діяльності НДЛ протидії кіберзагрозам авіаційної галузі НАУ (акт впровадження від 11.12.2023), а також у ДержНДІ технологій кібербезпеки та захисту інформації для підвищення ефективності підготовки фахівців з ІТ та забезпечення захисту ОКІ (акт впровадження від 14.06.2024).

Особистий внесок здобувача

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні результати дисертаційної роботи були представлені та обговорені на таких міжнародних науково-технічних та науково-практичних конференціях: «12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications» (м. Дортмунд, 2023), «1st International Workshop on Social Communication and Information

Activity in Digital Humanities» (м. Львів, 2022), «VIII International conference “Information Technology and Implementation» (м. Київ, 2021), «The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security» (м. Хмельницький, 2022), «Перспективні напрямки захисту інформації», (м. Одеса, 2021) та ін.

Публікації. Основні наукові результати дисертаційної роботи опубліковані у 26 наукових публікаціях, із них: 0.5 розділу у колективній монографії, 3 наукових статей, надрукованих у вітчизняних фахових наукових виданнях, 15 публікацій, включених до міжнародних наукометричних баз Scopus, а також 7.5 тез доповідей на науково-практичних конференціях.

Основні наукові результати дисертаційної роботи опубліковані у 30 наукових працях, із них: 1 розділ у колективній монографії, 5 наукових статей, надрукованих у вітчизняних фахових наукових виданнях, 15 публікацій, включених до міжнародних наукометричних баз Scopus, а також 9 тез доповідей на науково-практичних конференціях.

Структура роботи та її обсяг. Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел до кожного розділу. Повний обсяг роботи становить 180 сторінок друкованого тексту, з них анотація – на 4 стор., зміст – на 2 стор., основний текст – на 151 стор., список із 125 використаних джерел – на 17 стор., додатки – на 29 стор. Дисертація містить 30 рисунків та 38 таблиць.

РОЗДІЛ 1

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ ІТ-ІНЦИДЕНТАМИ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Поняття захисту об’єктів критичної інфраструктури

Критична інфраструктура (КІ) є основою функціонування держави та забезпечення безпеки громадян. Вона включає об'єкти та системи, які є життєво необхідними для суспільства, економіки та національної безпеки [1-3]. Захист КІ є надзвичайно важливим завданням для будь-якої держави тому що є одним із головних напрямів забезпечення національної безпеки держави в цілому. Порушення роботи КІ може призвести до серйозних національних загроз. Наприклад, атака на енергетичні системи може залишити мільйони людей без електропостачання, що порушить нормальне функціонування всіх систем, та навіть може спричинити загрозу життю та здоров'ю населення.

КІ забезпечує стабільність економічних процесів [4], оскільки включає транспортні системи, фінансові послуги, комунікаційні мережі та інші життєво важливі сектори. Порушення їхнього функціонування може призвести до значних економічних втрат, зниження продуктивності, зривів у постачанні товарів та послуг, а також до руйнування бізнес-процесів.

Стабільна робота КІ є запорукою соціальної стабільності та громадського порядку. Аварії чи атаки на системи водопостачання, охорону здоров'я або транспорт можуть спричинити масові протести, погіршення суспільного здоров'я, зростання соціальної напруги та виникнення інших негативних соціальних наслідків.

КІ (рис. 1.1.) забезпечує функціонування державних та громадських служб, таких як охорона здоров'я, освіта, громадська безпека тощо. Її стабільна робота є

необхідною для безперебійного надання послуг населенню та підтримки нормального функціонування державних інституцій і багато іншого.

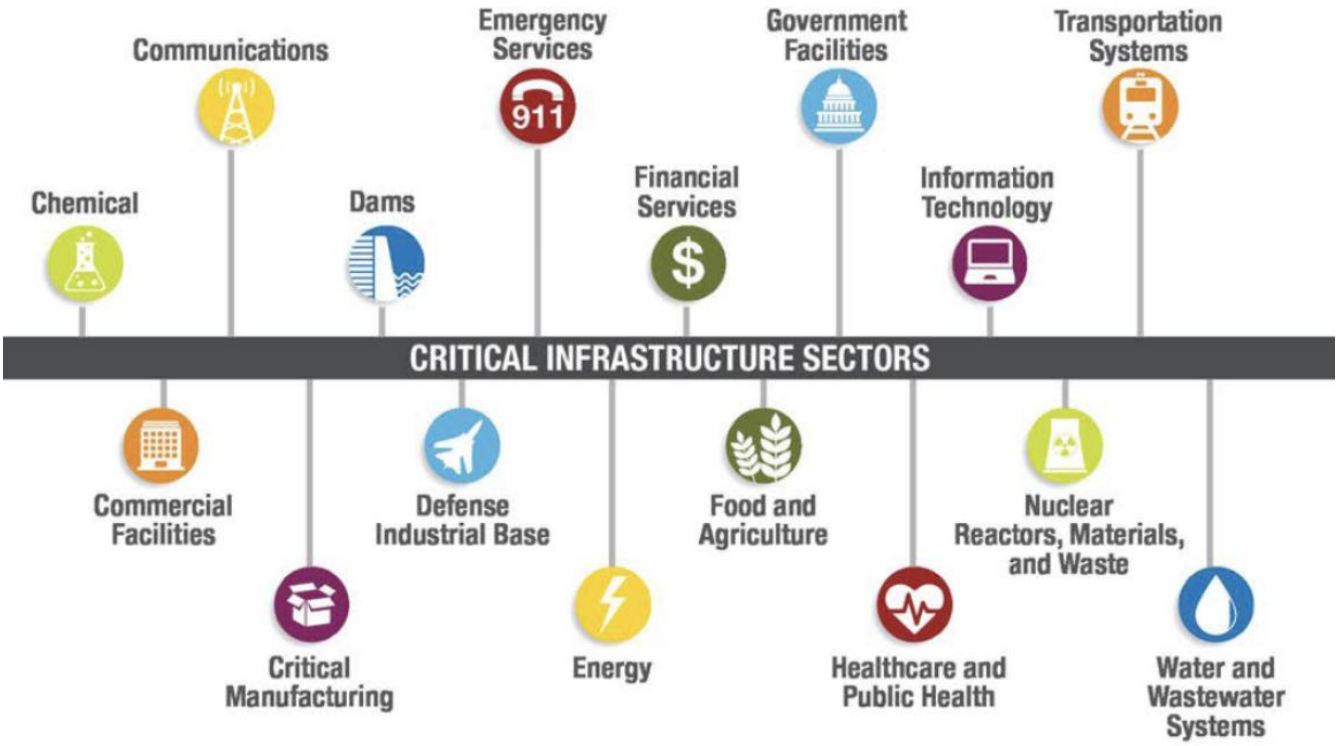


Рис. 1.1. Сектори КІ

Розглянемо основні підходи до захисту КІ в різних країнах світу [5-22].

В США захист КІ є пріоритетним завданням національної безпеки. Агентство з кібербезпеки та інфраструктурного захисту (CISA) відповідає за координацію зусиль у цій сфері. CISA працює під керівництвом Міністерства внутрішньої безпеки і займається оцінкою ризиків, розробкою стандартів безпеки та впровадженням найкращих практик для зниження вразливостей. Основні напрямки діяльності CISA включають ідентифікацію та оцінку ризиків, здійснення регулярних оцінок ризиків для різних секторів КІ, зокрема енергетики, водопостачання, транспорту, зв’язку та фінансів; розробку стандартів безпеки, встановлення

стандартів та керівних принципів для забезпечення безпеки ОКІ, наприклад, стандарти NIST (Національний інститут стандартів і технологій) є основою для багатьох політик та практик безпеки; навчання та тренування, організацію навчання та тренінгів для персоналу, відповідального за захист КІ, що включає симуляції атак, кризові навчання та розробку планів реагування; моніторинг і реагування на інциденти, здійснення моніторингу в режимі реального часу та координацію зусиль з реагування на інциденти; партнерства між державним та приватним секторами, активну співпрацю з приватними компаніями для забезпечення обміну інформацією про загрози та вразливості, а також розробку спільних стратегій захисту.

В ЄС захист КІ регулюється Директивою NIS (Network and Information Systems Directive), яка набрала чинності у 2018 році. Ця директива встановлює вимоги для держав-членів щодо забезпечення безпеки критичних секторів. Основні положення директиви включають національні стратегії безпеки, згідно з якими кожна держава-член повинна розробити та впровадити національну стратегію безпеки, яка охоплює захист КІ; операторські послуги та постачальники цифрових послуг, що зобов'язує операторів основних послуг та постачальників цифрових послуг впроваджувати відповідні заходи безпеки та повідомляти про значні інциденти; співпрацю та обмін інформацією, яка передбачає створення групи з співпраці, яка сприяє обміну інформацією між державами-членами, а також з CSIRT (команди реагування на інциденти у сфері комп'ютерної безпеки); контроль та нагляд, що зобов'язує кожну державу-член створити національні компетентні органи для контролю за виконанням вимог директиви.

У Великій Британії захист КІ координується Національним центром кібербезпеки (NCSC), який є частиною урядового агентства з комунікацій (GCHQ). Основні функції NCSC включають оцінку загроз та вразливостей, аналіз загроз та оцінку вразливостей для різних секторів КІ, надаючи рекомендації щодо їх усунення; підтримку та навчання, надання підтримки організаціям у підвищенні

рівня безпеки, включаючи розробку навчальних програм та проведення тренінгів; реагування на інциденти, координацію зусиль з реагування на інциденти, забезпечуючи оперативну допомогу у випадку атак; співпрацю з приватним сектором, активну співпрацю з приватними компаніями для забезпечення обміну інформацією про загрози та найкращі практики захисту.

У Канаді захист КІ здійснюється в рамках Програми захисту КІ, яка координується Міністерством громадської безпеки та підготовки до надзвичайних ситуацій. Основні аспекти програми включають ідентифікацію та оцінку ризиків, здійснення ідентифікації та оцінки ризиків для різних секторів КІ, забезпечуючи розробку відповідних заходів захисту; планування кризового реагування, розробку планів реагування на кризові ситуації, зокрема природні катастрофи, терористичні акти та інші загрози; партнерства та співпрацю, активну співпрацю уряду Канади з провінційними та територіальними урядами, а також з приватним сектором для забезпечення ефективного захисту КІ; навчання та тренування, проведення регулярних навчань та тренінгів для підвищення готовності до надзвичайних ситуацій.

У Німеччині захист КІ регулюється Федеральним відомством з інформаційної безпеки (BSI). Основні напрямки діяльності BSI включають розробку стандартів та керівних принципів, розробку стандартів безпеки для різних секторів КІ, включаючи енергетику, транспорт, зв'язок та водопостачання; оцінку ризиків та вразливостей, проведення регулярних оцінок ризиків та вразливостей, надаючи рекомендації щодо підвищення рівня безпеки; навчання та консультації, організацію навчань та надання консультацій для організацій, які відповідають за захист КІ; моніторинг та реагування, здійснення моніторингу загроз та координацію зусиль з реагування на інциденти.

В Австралії захист КІ координується Австралійським центром кібербезпеки (Australian Cyber Security Centre, ACSC), який є частиною Австралійської

сигналізаційної дирекції (Australian Signals Directorate). Основні функції ACSC включають оцінку та управління ризиками, здійснення оцінки ризиків для критичних секторів та надання рекомендацій щодо їх зменшення; навчання та тренування, проведення навчань та тренінгів для підвищення кваліфікації фахівців з безпеки; моніторинг та реагування на інциденти, забезпечення моніторингу та оперативне реагування на інциденти; співпрацю з приватним сектором, активну співпрацю з приватними компаніями для забезпечення обміну інформацією про загрози та кращі практики захисту.

У Японії захист КІ координується Національним центром готовності та стратегії (NISC). Основні напрямки діяльності NISC включають розробку національних стратегій та політик, розробку національних стратегій та політик щодо забезпечення безпеки КІ; оцінку загроз та вразливостей, здійснення оцінки загроз та вразливостей для різних секторів, надаючи рекомендації щодо підвищення рівня безпеки; підтримку та консультування, надання підтримки та консультацій для організацій, відповідальних за захист КІ; навчання та тренування, організацію навчань та тренінгів для фахівців з безпеки.

Захист КІ в Україні

Захист КІ є однією з ключових задач для забезпечення національної безпеки України, особливо в умовах воєнного стану, викликаного збройною агресією російської федерації. Важливість нормативно-правового регулювання у цій сфері [23-35] обумовлена численними загрозами, які включають природні та техногенні катастрофи, терористичні акти, військові дії та атаки у інформаційному просторі.

Відповідні законодавчі акти щодо захисту КІ в Україні починали приймати ще з 2007 року, вони були спрямовані на створення і вдосконалення системи захисту КІ, відображають реагування на ці виклики.

Державна політика у сфері захисту КІ в Україні визначена низкою нормативно-правових актів, які розроблялися і впроваджувалися протягом останніх

десятиліть. Зокрема, починаючи з 2007 року, коли було затверджено Стратегію національної безпеки України [36], питання захисту критичної інфраструктури набуло державного значення. У 2015 році Рада національної безпеки і оборони України ухвалила нову Стратегію національної безпеки, яка вимагала від уряду розробити комплексні пропозиції щодо реформування сектору безпеки і оборони. Основою для подальшого розвитку системи захисту критичної інфраструктури стала Концепція створення державної системи захисту критичної інфраструктури, затверджена у 2017 році.

Ця концепція визначала пріоритети реформування, включаючи створення єдиної системи захисту КІ, усунення нормативно-правових прогалин, координацію дій між державними органами та власниками ОКІ, а також розробку методологій для оцінки загроз і категоризації об’єктів. У 2019 році був запропонований проект Закону "Про критичну інфраструктуру та її захист", який передбачав створення умов для ефективної реалізації державної політики у цій сфері. Однак, цей проект був відкликаний, і лише у 2020 році Кабінет Міністрів України затвердив Постанову "Деякі питання об’єктів критичної інфраструктури" [28], яка встановила порядок віднесення об’єктів до критичної інфраструктури, методику їх категоризації та основні терміни.

Прийняття Закону України "Про критичну інфраструктуру" [27] у 2021 році стало значним кроком вперед у формуванні національної системи захисту КІ. Закон визначає термін "захист критичної інфраструктури" як сукупність заходів, спрямованих на забезпечення безпеки об’єктів критичної інфраструктури, включаючи виявлення, запобігання і нейтралізацію загроз. Законодавче визначення цього терміну в Україні наближається до європейських стандартів, що підкреслює важливість міжнародного співробітництва у цій сфері.

Особливу роль у захисті КІ під час воєнного стану виконує Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку). Відповідно

до законодавства, Держспецзв’язку наділена повноваженнями координувати діяльність суб’єктів національної системи захисту критичної інфраструктури, вести реєстр об’єктів, оцінювати ризики та створювати бази даних загроз. Це забезпечує централізоване управління та координацію заходів з безпеки на національному рівні [37].

Державна політика у сфері захисту КІ в Україні зазнала значних змін та вдосконалень протягом останніх років. Було створено нормативно-правове підґрунтя для ефективного функціонування системи захисту, визначено ключові завдання та повноваження відповідальних органів. Впровадження цих заходів сприяє підвищенню рівня національної безпеки та стійкості критичної інфраструктури до різноманітних загроз.

Станом на сьогодні, згідно із Законом України "Про критичну інфраструктуру", КІ – це сукупність об'єктів, які є стратегічно важливими для економіки і національної безпеки [27]. Порушення їхнього функціонування може завдати шкоди життєво важливим національним інтересам. Захист КІ включає:

– визначення секторів КІ та встановлення відповідальних суб'єктів захисту для цих секторів;

– категоризацію ОКІ для визначення рівня вимог до забезпечення їхнього захисту;

– складання та ведення Національного переліку КІ;

– паспортизацію ОКІ;

– визначення режимів функціонування КІ та розроблення планів реагування на кризові ситуації;

– взаємодію та обмін інформацією між суб'єктами державної системи захисту КІ та визначення рівня доступу до такої інформації третіх осіб;

– контроль за рівнем безпеки ОКІ та їх стійкості;

– взаємодію між органами державної влади та приватним сектором у сфері захисту КІ;

– запровадження критеріїв та методології віднесення об'єктів до КІ;

– оцінка загроз об'єктам КІ та реагування на них.

– запобігання інцидентам інформаційної безпеки та ліквідація їх наслідків, відновлення сталості та надійності функціонування комунікаційних і технологічних систем.

1.2. Аналіз підходів для визначення стану захищеності об’єктів критичної інформаційної інфраструктури

Зважаючи на те, що все більше у нашому суспільстві з’являється інформаційних технологій, питання захисту критичної інформаційної інфраструктури (КІІ) стає дуже актуальним завданням. Сучасні інформаційні та комунікаційні системи (ІКТ) пронизують всі аспекти нашого життя – від урядових та фінансових послуг до охорони здоров'я, транспорту та енергетики. Відмова або порушення функціонування цих систем може призвести до хаосу, значних фінансових збитків та навіть загрози життю. В той же час, більшість людей схильна приймати стабільність і надійність цих систем як належне, поки не відбувається серйозних інцидентів. Енергетичні та транспортні мережі, урядові та військові об’єкти є життєво важливими компонентами сучасного суспільства, тому забезпечення їх безпеки і захист КІІ в цілому є надзвичайно важливим завданням.

Визначення стану захищеності ОКІІ є складним і багатоаспектним завданням, яке включає різні методології та підходи, розглянемо деякі з них:

ICT Development Index (IDI) [38] – це індекс, розроблений Міжнародним союзом електрозв'язку (International Telecommunication Union, ITU), який використовується для вимірювання рівня розвитку ІКТ у різних країнах світу. Індекс

базується на трьох основних компонентах: доступ (access), використання (use) та навички (skills), як видно з рис. 1.2. Компонент доступ включає показники, такі як кількість фіксованих телефонних ліній на 100 жителів, кількість мобільних телефонних підписок на 100 жителів, кількість міжнародних інтернет-шлюзів на 100 жителів, частку домогосподарств із комп'ютером та частку домогосподарств із доступом до інтернету. Компонент використання включає показники, такі як частка індивідуальних користувачів інтернету, частка фіксованих широкосмугових підписок на 100 жителів та частка мобільних широкосмугових підписок на 100 жителів. Компонент навички включає показники, такі як рівень грамотності дорослого населення, частка осіб із середньою освітою та частка осіб із вищою освітою. IDI дозволяє країнам оцінювати свої досягнення в галузі ICT та визначати області, які потребують покращення. Він також допомагає урядам і політикам розробляти стратегії для подальшого розвитку інформаційно-комунікаційних технологій, сприяючи економічному зростанню та соціальному розвитку. Порівняння індексу між країнами дозволяє виявити лідерів та відстаючих, а також вивчити найкращі практики в галузі ICT.

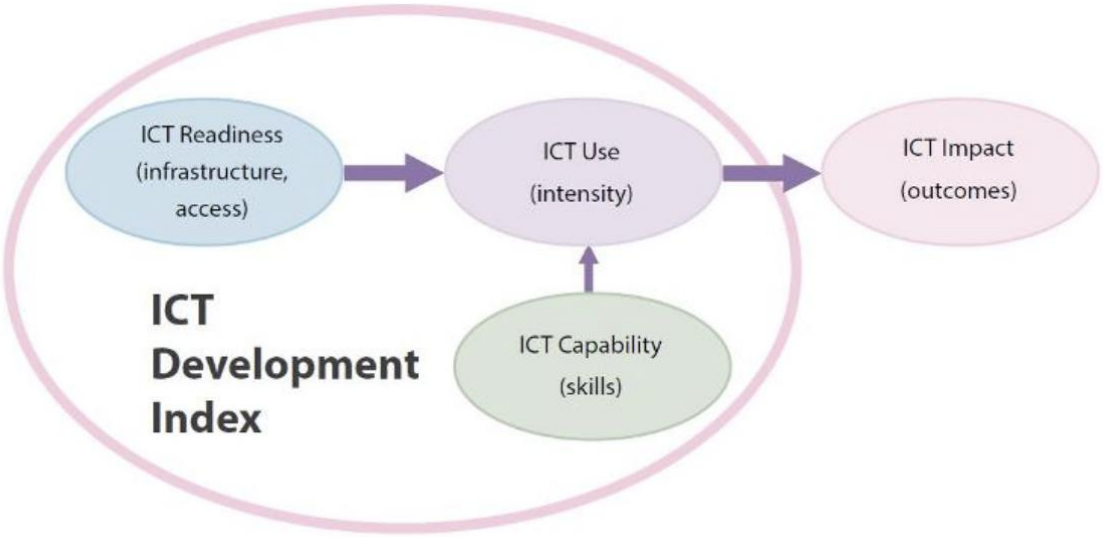


Рис. 1.2. Структура ICT Development Index

E-Government Development Index (EGDI) [39] розроблений Організацією Об'єднаних Націй і є комплексним показником, що оцінює рівень розвитку електронного уряду в різних країнах світу. EGDI вимірює, наскільки ефективно уряди використовують ІКТ для надання публічних послуг, забезпечення громадської участі та сприяння прозорості та підзвітності. EGDI складається з трьох основних компонентів: онлайн-послуги, телекомунікаційна інфраструктура та людський капітал (рис. 1.3). Онлайн-послуги оцінюють доступність і якість урядових веб-сайтів, що забезпечують доступ до інформації, інтерактивних послуг і можливості для громадян взаємодіяти з урядом. Цей компонент також включає оцінку рівня інтерактивності веб-сайтів, їхню зручність у користуванні та доступність. Телекомунікаційна інфраструктура вимірює наявність та доступність базових ІСТ інфраструктур, таких як інтернет-доступ, мобільні телефонні мережі, широкосмуговий інтернет та інші комунікаційні технології. Важливими показниками є кількість користувачів інтернету, мобільних телефонів і фіксованих широкосмугових підписок на 100 жителів. Людський капітал охоплює рівень освіти та навичок населення, необхідних для ефективного використання ІСТ. Цей компонент включає показники, такі як рівень грамотності серед дорослих, частка населення з середньою та вищою освітою, а також рівень підготовки кадрів у сфері ІСТ. Оцінка людського капіталу важлива для розуміння, наскільки населення країни здатне використовувати та впроваджувати ІСТ у повсякденному житті та бізнесі. EGDI дозволяє країнам оцінювати свої досягнення в галузі електронного уряду і визначати області, які потребують покращення. Використання цього індексу допомагає урядам і політикам розробляти стратегії для подальшого розвитку електронного уряду, сприяючи ефективнішому наданню публічних послуг і залученню громадян до процесів управління. Порівняння EGDI між країнами дозволяє виявити лідерів та відстаючих, а також вивчити найкращі практики в галузі

електронного уряду, що сприяє обміну досвідом і впровадженню успішних рішень в інших країнах.

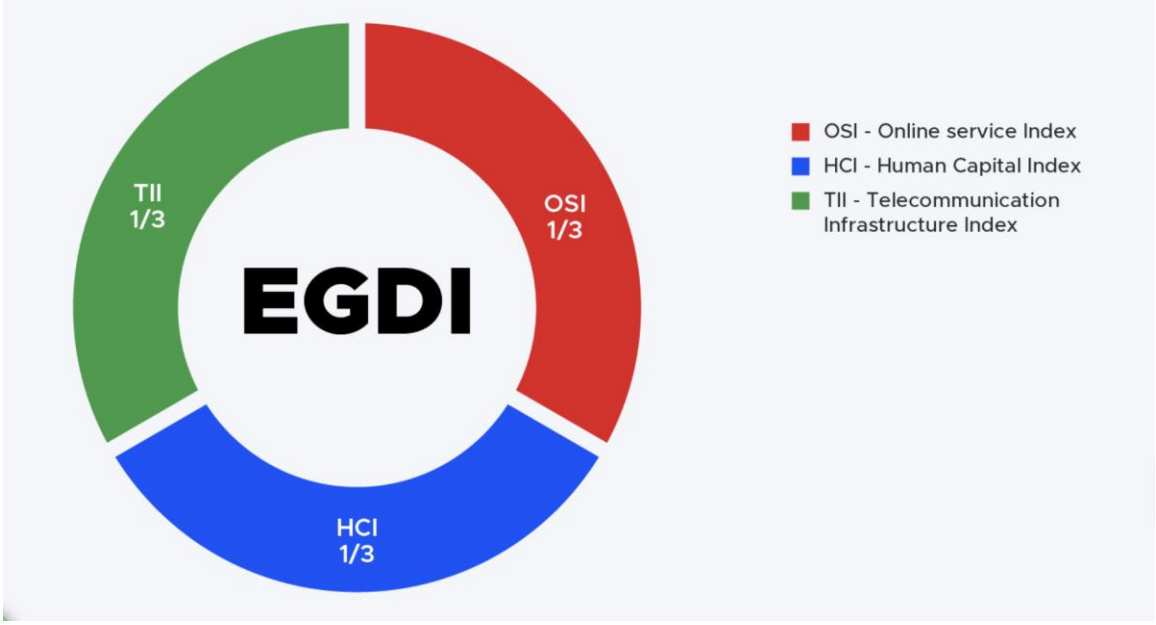


Рис. 1.3. Структура E-Government Development Index

National Cyber Security Index (NCSI) [40] – це індекс, розроблений e-Governance Academy Foundation (eGA), який вимірює рівень кібербезпеки в різних країнах світу. Він оцінює здатність держав запобігати кіберзагрозам та реагувати на них, забезпечуючи тим самим кіберстійкість національної інфраструктури.

NCSI складається з різних індикаторів, які згруповані в кілька основних категорій (рис. 1.4). Ці категорії включають: правові заходи, технічні заходи, організаційні заходи, розвиток потенціалу, співпраця та участь у міжнародних ініціативах. Кожен індикатор оцінюється за шкалою, і сукупний бал кожної країни визначає її позицію в рейтингу NCSI. Індекс надає комплексне уявлення про стан кібербезпеки в різних країнах, допомагаючи урядам, організаціям та дослідникам аналізувати поточний рівень захисту та визначати області, що потребують покращення. Інформація, зібрана за допомогою NCSI, також сприяє розробці

політики та стратегій для підвищення кібербезпеки на національному та міжнародному рівнях.

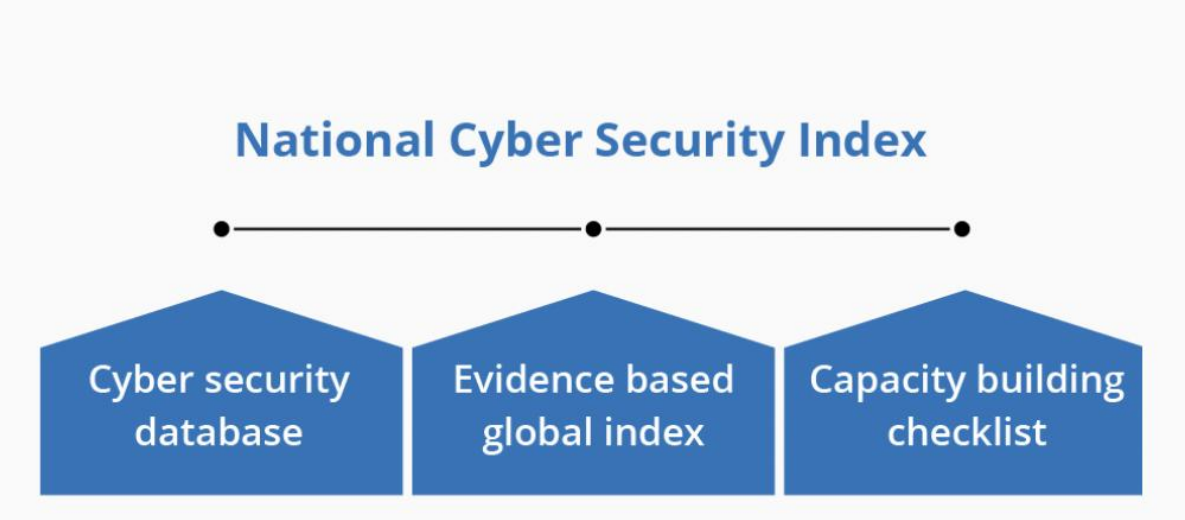


Рис. 1.4. Структура National Cyber Security Index

Методологія оцінки кіберризиків NIST Cyber Risk Scoring (CRS) [41] розроблена Національним інститутом стандартів і технологій США і являє собою комплексний підхід для оцінки та управління кібербезпековими ризиками організацій. Ця методологія допомагає організаціям зрозуміти їхній ризиковий профіль, використовуючи кількісні вимірювання для оцінки кібербезпеки. NIST надає всебічний погляд на стан безпеки організації, враховуючи різні аспекти, такі як ризики, пов'язані з внутрішніми та зовнішніми чинниками. Методологія включає в себе оцінку ризикових факторів на основі їхнього потенційного впливу на організацію, що призводить до "рейтингів впливу". Чим вищий рейтинг, тим вищий ризик, і тим більше організація повинна вживати заходів для усунення цих ризиків. Основні категорії ризиків, які оцінюються в рамках CRS, включають внутрішні та зовнішні ризики (рис. 1.5). Внутрішні ризики оцінюються на основі факторів, які безпосередньо пов'язані з операційною діяльністю, процесами, ресурсами та загальним бізнес-середовищем організації. Зовнішні ризики, навпаки, оцінюються

на основі зовнішніх чинників, таких як ринкові умови, галузеві тренди, зміни в регуляторних вимогах, економічні показники та геополітичні події. Процес оцінки ризиків включає кілька ключових етапів: ідентифікацію ризикових факторів, визначення метрик і базових значень для кожного фактора, присвоєння ваги кожному фактору на основі його значущості, оцінку рівня ризику для кожного фактора, розрахунок рейтингів впливу та сумарного ризику, інтерпретацію результатів та впровадження стратегій зниження ризику. Це дозволяє організаціям зрозуміти, де їхні найбільші вразливості, і ефективно розподілити ресурси для зменшення цих ризиків. Методологія також забезпечує можливість порівняння з галузевими стандартами та демонстрацію відповідності кращим практикам кібербезпеки. Вона допомагає організаціям покращити комунікацію та співпрацю між зацікавленими сторонами, пріоритизувати інвестиції в безпеку, а також регулярно переглядати та оновлювати свої підходи до управління ризиками відповідно до змін у бізнес-середовищі та ефективності реалізованих заходів.

Рис. 1.5. Підхід NIST Cyber Risk Scoring

Розроблений у праці [42] метод оцінки сумарного ризику кібербезпеки ОКІ може ефективно використовуватись для визначення рівня захищеності держави. Цей метод базується на визначенні максимальних значень наслідків для кожного ризику та включає як графічний, так і аналітичний підходи. Він дозволяє оцінити загальний ризик кібербезпеки, максимальні збитки та ймовірність їх виникнення через множинні кіберзагрози. Основна перевага цього методу полягає в його здатності визначати максимальні значення наслідків для кожного ризику, що дозволяє оцінити

загальний рівень кібербезпеки. Метод включає як графічний, так і аналітичний підходи, що забезпечує точність і наочність оцінок. Використання цього методу дає можливість державним органам розробляти ефективні стратегії захисту, оцінювати економічну доцільність різних заходів та приймати обґрунтовані рішення щодо підвищення рівня захищеності країни від різних загроз. Це забезпечує комплексний підхід до управління кібербезпекою на національному рівні та сприяє зміцненню кіберстійкості КІ.

В табл. 1.1. відображені порівняння підходів до захисту КІ держави за такими критеріями:, гнучкість (FL), застосування для сфери КІ (CI), використання ІТ інцидентів (IT), вартість впровадження (CT), час впровадження (TT), масштабованість (SC), підтримка міжнародних стандартів (IS).

Таблиця 1.1

Порівняння підходів щодо визначення стану захищеності

Критерій / Підхід	FL	CI	IT	CT	TT	SC	IS
ICT Development Index (IDI)	-	+	-	-	-	-	+
E-Government Development Index (EGDI)	+	+	-	-	-	+	+
National Cyber Security Index (NSCI)	+	+	+	-	-	+	+
NIST Cyber Risk Scoring (CRS)	-	-	-	-	-	-	+
Метод оцінки сумарного ризику ОКІ	-	+	-	+	+	-	-

Отже, як видно з табл. 1.1, проведений аналіз показав, що підходи IDI, EGDI, NSCI, NIST CRS та метод оцінки сумарного ризику ОКІ мають як переваги, так і недоліки. Серед недоліків можна виділити обмежену гнучкість та відсутність орієнтації на критичну інфраструктуру та ІТ інциденти у IDI, високу вартість та тривалий час впровадження для EGDI та CRS, а також меншу гнучкість та

масштабованість методу ОКІ. З огляду на необхідність забезпечення можливості комплексної оцінки рівня захищеності КІІ, доцільно розробити новий метод, який враховуватиме всі сильні сторони, щоб ефективно оцінювати та покращувати рівень захищеності КІІ держави.

1.3. Аналіз підходів для визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури

Захист ОКІІ від ІТ-інцидентів є ключовим завданням для забезпечення національної безпеки та безперервного функціонування життєво важливих сервісів. Різні підходи та методології використовуються для ідентифікації, оцінки та управління ризиками, пов’язаними з ІТ-інцидентами (рис. 1.6).

Незважаючи на важливість забезпечення ІТ-безпеки КІІ, станом на сьогодні немає достатньої кількості наукових досліджень, щодо розроблення та впровадження методів визначення пріоритетів ІТ-інцидентів, як на міжнародному, так і вітчизняному просторі. Тому, при проведені аналізу, було досліджено підходи щодо управління інцидентами у різних сферах КІ.

Рис. 1.6. Процес управління ІТ-інцидентами

У статті [43] представлено систематичний підхід до оцінки ризиків у телекомунікаційних системах, зокрема у внутрішньоплатіжних банківських

системах. Основна мета дослідження полягає у побудові та аналізі моделі оцінки ризику реалізації загроз для телекомунікаційних систем, а також у розробці методики оцінки ризику загроз і ефективності засобів захисту даних. У роботі детально розглядається функціональний тип математичних моделей "чорного ящика", побудованих відповідно до методології IDEF0 з використанням Case-засобу Bpwin. Для оцінки економічного збитку при реалізації загроз використовується узагальнена картка експерта-аналітика, яка дозволяє визначити найбільш уразливі місця і оцінити ризики. Модель оцінки ризику враховує конфіденційність, цілісність та доступність даних. Запропонована методика дозволяє обґрунтувати вибір відповідних засобів захисту для критичних систем, включаючи банківські системи та системи управління залізничним транспортом.

У статті [44] розглядається проблема управління кіберризиками в інформаційних системах об'єктів критичної інфраструктури. Основна мета дослідження полягає у розробці методів і моделей оцінки та управління ризиками, зокрема векторної та інтегральної моделей ризику. Векторна модель ризику використовує набір параметрів для визначення рівня ризику, для якого присвоюється ваговий коефіцієнт, і загальний ризик розраховується як векторна сума параметрів з врахуванням їх вагових коефіцієнтів. Ця модель дозволяє ідентифікувати найбільш критичні компоненти ризику та легко візуалізувати і розуміти ризики на різних рівнях системи. Інтегральна модель ризику включає комплексний підхід до оцінки ризиків, враховуючи взаємозв'язки між різними параметрами. На практиці ці системи використовуються для моніторингу та управління кібербезпекою в різних секторах критичної інфраструктури, таких як енергетика, транспорт, охорона здоров'я. Результати дослідження показують, що запропоновані векторна та інтегральна моделі ризику є ефективними інструментами для оцінки та зниження кіберризиків, забезпечуючи надійний захист інформаційних систем критичної інфраструктури від кіберзагроз.

У статті [45] розглядаються математичні методи захисту критичної інфраструктури від небажаних інцидентів. Основна мета дослідження полягає у створенні шаблону для аналізу та покращення захисту та стійкості критичної інфраструктури. Оцінка інцидентів включає моделі ймовірності відмови компонентів системи та очікуваних втрат від таких відмов. Для кібербезпеки розглядаються методи оцінки вразливостей і часу реагування на інциденти. Метрики стійкості охоплюють індекс стійкості, що вимірює здатність системи до відновлення після збоїв, та цільовий час відновлення, що визначає максимально допустимий час простою системи. Застосування цих математичних методів дозволяє кількісно оцінювати інциденти, оцінювати ефективність заходів кібербезпеки та покращувати співпрацю між зацікавленими сторонами, що підтверджує практичну цінність розроблених методів для ефективного управління захистом критичної інфраструктури.

У статті [46] представлено модель індексу ризику для пріоритизації інцидентів безпеки. Модель оцінює індекс ризику для кожного інциденту на основі показників, отриманих з середовища активів та характеристик інцидентів. Основними факторами моделі є вплив на актив та ймовірність загроз і вразливостей, які додатково оцінюються за допомогою показників, таких як критичність, підтримуваність, замінність, надійність та контроль. Розподіл показників на основні та бажані дозволяє точно оцінювати інциденти та впроваджувати динамічні зміни індексу ризику для покращення процесу пріоритизації..

У статті [47] представлено розробку алгоритму, призначеного для пріоритизації кіберзагроз у системі кібербезпеки, враховуючи їх високу ймовірність реалізації. Основна мета дослідження полягає у створенні алгоритму, що включає ієрархічну модель системи кібербезпеки з трьома рівнями: кібербезпека, загрози та ризики. У статті детально розглянуто метод аналізу ієрархій (AHP) [48], який дозволяє оцінювати та порівнювати пріоритети загроз. Ключові кіберзагрози, такі

як трояни, віруси та хробаки, мають найвищі пріоритети, що потребують зосереджених заходів для їх пом'якшення. Результати дослідження підтверджують практичну цінність розробленого методу, який допомагає систематично пріоритизувати загрози та ефективно керувати кібербезпекою.

Отже, в табл. 1.2 пропонується порівняти вище описані підходи, які можна застосувати для розробки методу визначення пріоритетів ІТ-інцидентів за наступними критеріями: простота використання (EU), фокус на критичну інфраструктуру (CI), об'єктивність (OB), можливість застосування для ІТ-інцидентів (IT).

Таблиця 1.2

Порівння підходів щодо пріоритизації ІТ-інцидентів

Критерій / Підхід	EU	CI	OB	IT
Метод оцінювання ризику реалізації загроз безпеки у телекомунікаційних системах	-	+	+	-
Метод оцінювання ризиків кібербезпеки інф. систем ОКІ	-	+	+	-
Методологія для ранжування кіберсценаріїв та критичних об'єктів	-	-	+	-
Метод індексу ризику (RIM)	-	-	+	+
Метод оцінки пріоритетів системи кібернетичної безпеки	+	+	+	-

Таким чином, з табл. 1.2 видно, що метод, розроблений авторами у дослідженні [47] є кращим підходом на основі якого можна розробити метод визначення пріоритетів ІТ-інцидентів для забезпечення безпеки КІІ оскільки він є простим у використанні, завдяки чіткій ієрархічній моделі, яка робить процес оцінки інцидентів зрозумілим і доступним для користувачів, включає конкретні механізми для оцінки і пріоритизації загроз саме для ОКІІ, а використання методу аналізу ієрархій надає об'єктивність в оцінці загроз, оскільки дозволяє

систематично і прозоро порівнювати та ранжувати загрози на основі встановлених критеріїв.

1.4. Аналіз підходів для управління ІТ-загрозами на об’єктах критичної інформаційної інфраструктури

У сучасному світі цифрових технологій захист КІ є одним із найважливіших завдань для організацій та держави. Зростання кількості загроз, пов'язаних із розвитком інформаційних технологій, підвищує необхідність впровадження надійних заходів безпеки. КІІ включає в себе системи та мережі, які є життєво важливими для функціонування суспільства у сферах енергетики, транспорту, фінансів, зв'язку та охорони здоров'я. Вихід з ладу або компрометація таких компонентів можуть мати серйозні наслідки для національної безпеки, економіки та суспільного добробуту. Для ефективного захисту КІІ необхідно правильно ідентифікувати, оцінити та управляти ІТ-загрозами, особливо в умовах обмежених ресурсів захисту. Все це, свідчить про наявність важливого наукового завдання щодо розробки та впровадження ефективного методу управління ІТ-інцидентами на ОКІІ.

Незважаючи на важливість забезпечення ІТ-безпеки КІІ, станом на сьогодні немає достатньої кількості наукових досліджень, щодо розроблення та впровадження методів управління ІТ-загрозами, як на міжнародному, так і вітчизняному просторі (Рис. 1.7). Проте, при проведені аналізу, було досліджено підходи щодо управління загрозами у різних сферах КІ.

У дослідженні [51] автори розробили алгоритм оцінки загроз кібербезпеки для систем управління навчанням (LMS). Поєднавши модель STRIDE з багатокритеріальним методом підтримки прийняття рішень TODIM та дадавши нечіткі множини, вони оцінили платформи LMS, а саме Moodle, Atutor та Ilias. У дослідженні брали участь три експерти з кібербезпеки, які оцінювали безпеку за допомогою лінгвістичних змінних, демонструючи ефективність алгоритму у

виявленні та ранжуванні кіберзагроз у середовищах LMS. Дане дослідження найбільше стосується фахівців з кібербезпеки, які є відповідальним за безпеку освітніх технологій та зможуть використати методологію для посилення безпеки LMS.

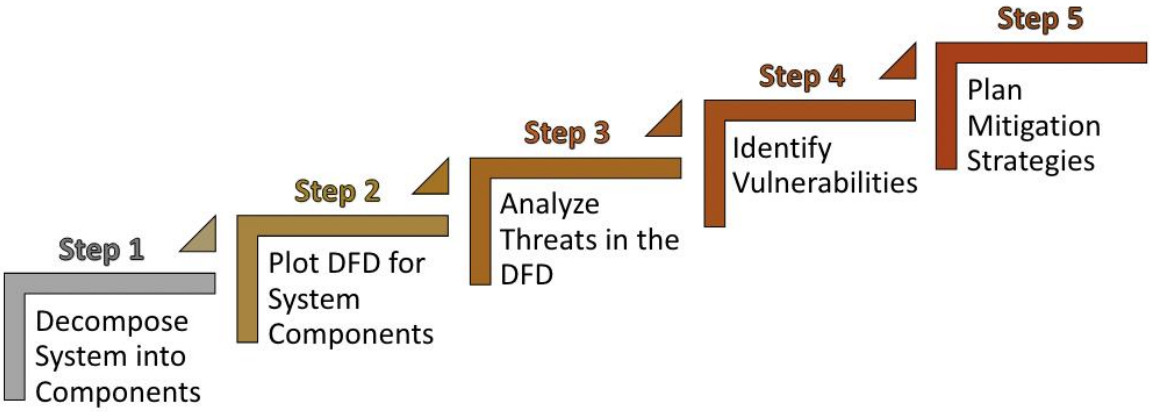


Рис. 1.7. Процес управління IT-загрозами

У статті [52] автори досліджують застосування моделі STRIDE для оцінки загроз кібербезпеки в транспортній галузі КІ. У статті висвітлено, як інтеграція STRIDE з методом аналізу небезпек і оцінки ризиків (HARA), що отримав назву SAHARA-підхід, забезпечує всеосяжну основу для оцінки ризиків безпеки на ранніх етапах розробки. Цей комбінований підхід дозволяє ідентифікувати та класифікувати загрози безпеці, забезпечуючи впровадження відповідних контрзаходів для захисту автомобільних систем від потенційних кібератак, тим самим підтримуючи послідовну та безпечну розробку продукту протягом усього життєвого циклу.

У дослідженні [53] розглядаються питання покращення безпеки та конфіденційності, а також вразливості мереж 5G з акцентом на захисті КІ. Незважаючи на досягнення в порівнянні з попередніми поколіннями, мережі 5G все ще мають слабкі місця в технічній безпеці, які можуть бути використані. У документі використовується модель класифікації загроз STRIDE для виявлення та

аналізу одинадцяти сценаріїв загроз в екосистемі 5G, що підкреслює важливість впровадження надійних заходів безпеки для зменшення цих ризиків.

У дослідженні [54] було встановлено, що критичні об'єкти інфраструктури та промислові системи управління є складними кібер-фізичними системами (КФС). Забезпечення надійної роботи таких систем вимагає комплексного моделювання загроз під час проектування та валідації системи. У цій статті представлено комплексну методологію моделювання загроз для КФС з використанням STRIDE - системного підходу до забезпечення безпеки системи на компонентному рівні. Методологію застосовано до реального випробувального стенду синхронної ізольованої системи на основі синхрофазору. Дослідження визначає типи загроз, які можуть виникнути в кожному компоненті системи, і те, як вразливості в компоненті можуть поставити під загрозу безпеку всієї системи. Доведено, що STRIDE є легкою та ефективною методологією моделювання загроз для КФС, що спрощує завдання для аналітиків з безпеки.

Встановлено, що на даний момент не існує реалізованого методу, який би дозволяв ефективно управляти ІТ-загрозами на ОКІІ.

У зв’язку з тим, що попередній аналіз існуючих досліджень щодо ідентифікації, оцінки та управління ІТ-загрозами не дав змогу знайти єдиний формалізований підхід, було прийнято рішення розробки нового, більш універсального методу управління ІТ-загрозами на ОКІІ. Для цього необхідно провести додатковий аналіз ефективності міжнародних практик та методологій моделювання загроз за наступними критеріями: простота використання (EU) – оцінка легкості застосування методу на практиці, комплексність (CM) – наскільки метод охоплює всі аспекти управління ІТ-загрозами, інтеграція з іншими системами (IS) – наскільки метод дозволяє інтегруватися з іншими системами безпеки та управління, фокус на КІ (CI) – чи враховує метод специфіку ОКІІ, об'єктивність (OB)

– наскільки метод зменшує суб'єктивність у процесі прийняття рішень, час на застосування (ET) – час, необхідний для застосування методу.

Методика класифікації загроз STRIDE [57] є популярним інструментом для аналізу загроз безпеки, розробленим Microsoft. Цей акронім розшифровується як Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. Ця методологія допомагає виявити слабкі місця в інформаційних системах, дозволяючи розробникам і спеціалістам з безпеки проактивно вживати заходів для їх усунення. Серед переваг STRIDE – комплексність, оскільки метод охоплює широкий спектр загроз, чіткість і структурованість з чітко визначеними категоріями загроз, а також можливість інтеграції з іншими методами та інструментами безпеки. Однак, для ефективного використання даної методології потрібні глибокі знання в області IT-безпеки.

Нормативний документ NIST SP 800-30 [58] від Національного інституту стандартів і технологій є стандартом для управління ризиками в інформаційних системах, що надає всебічний підхід до ідентифікації, оцінки та управління ризиками, враховуючи специфіку організаційних процесів і активів. Основними перевагами NIST SP 800-30 є комплексний підхід, який охоплює всі етапи управління ризиками, від ідентифікації загроз до розробки стратегії реагування, та визнання стандарту у багатьох організаціях. Однак, впровадження цього стандарту може вимагати значних ресурсів і часу, а також складнощів для малих організацій через обмежені ресурси.

Міжнародний стандарт ISO/IEC 27005 [59] надає вказівки щодо управління ризиками інформаційної безпеки, пропонуючи структурований підхід до ідентифікації, оцінки та обробки ризиків. Переваги ISO/IEC 27005 включають узгодженість з іншими стандартами ISO, що дозволяє інтегрувати управління ризиками в загальну систему управління організацією, та структурованість підходу.

Недоліками є вимогливість до ресурсів для впровадження стандарту і складність для малих організацій, які можуть зіткнутися з труднощами при впровадженні.

Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [60] розроблена для оцінки і управління ризиками інформаційної безпеки, зосереджуючись на критичних активах організації. Вона дозволяє визначити та захистити найважливіші активи організації та проводити самооцінку, залучаючи внутрішні ресурси. Однак, OCTAVE потребує значної участі співробітників на всіх рівнях організації і може бути складною для координації у великих організаціях.

Фреймворк COBIT (Control Objectives for Information and Related Technologies) [61] є фреймворком для управління IT, який включає аспекти управління ризиками, забезпечуючи інтеграцію IT з бізнес-цілями. Серед переваг COBIT є інтеграція з бізнес-процесами, що допомагає узгодити управління IT з загальними бізнес-цілями організації, та всеохоплюючий підхід, що охоплює всі аспекти управління IT. Однак, впровадження фреймворку може вимагати значних ресурсів, і малі організації можуть зіткнутися з труднощами через недостатні ресурси для повного впровадження.

Отже, в табл. 1.3 відображені порівняння підходів до визначення пріоритетів IT-загроз за такими критеріями: EU – простота використання, CM – комплексність, IS – інтеграція з іншими системами, CI – фокус на KI, OB – об'єктивність та ET – час на застосування.

Таблиця 1.3

Порівняння підходів до визначення пріоритетів IT-загроз

Критерій / Підхід	EU	CM	IS	CI	OB	ET
STRIDE	+	+	+	-	+	+

Продовження табл. 1.3

NIST SP 800-30	-	+	-	+	-	-
ISO/IEC 27005	-	+	+	-	-	+
OCTAVE	-	+	-	-	+	+
COBIT	-	+	-	+	-	+

Зважаючи на аналіз зазначених критеріїв, підхід STRIDE (рис. 1.8) є надзвичайно ефективним і всебічним підходом до визначення IT-загроз. Його чітка структура, можливість інтеграції з іншими методами та акцент на різноманітних типах загроз роблять його ідеальним інструментом для підвищення безпеки інформаційних систем. STRIDE дозволяє організаціям не лише ідентифікувати загрози, але й оцінити їх критичність, розробити відповідні методи захисту і забезпечити комплексний підхід до управління ризиками.

Рис. 1.8. Методологія моделювання IT-загроз STRIDE

Крім цього, для визначення пріоритетів IT-загроз, необхідно розглянути питання **методів прийняття рішень** —підходів, які допомагають аналізувати складні проблеми та вибирати найкращий шлях дій з урахуванням різних можливих

альтернатив. Ці методи включають ряд технік та інструментів, які допомагають в оцінці різних параметрів та вагомості критеріїв, з метою досягнення об'єктивного, зваженого рішення.

Аналітичний ієрархічний процес (AHP) [63], розроблений Томасом Сааті у 1980-х роках, допомагає розбити проблему прийняття рішень на ієрархію менших складових, що включає цілі, критерії, підкритерії та альтернативи. Використовуючи математичні принципи для оцінки важливості критеріїв та вибору оптимального варіанту, AHP є інтуїтивно зрозумілим і здатним об'єднувати кількісні та якісні критерії. Однак, метод може бути схильним до суб'єктивності у вагах і вимагає значної кількості часу та даних для аналізу.

Метод багатокритеріального аналізу рішень TODIM [64] є мультикритеріальним методом ухвалення рішень, заснованим на теорії перспектив Даніеля Канемана та Амоса Тверскі. Метод використовує принципи теорії корисності для моделювання вподобань особи, яка приймає рішення, в умовах невизначеності та супутніх ризиків. Основні кроки методу включають визначення критеріїв та альтернатив, оцінювання альтернатив за кожним критерієм, присвоєння ваг критеріям, розрахунок домінування кожної альтернативи над іншими з урахуванням ваг, використання функції проспективної цінності для врахування ставлення до ризику, підсумовування проспективних цінностей для отримання оцінки корисності та вибір альтернативи з максимальною оцінкою корисності. Метод включає ризики та невизначеність і є інтуїтивно зрозумілим, але вимагає складних обчислень і суб'єктивної оцінки вагів [65-66].

Техніка оцінки та перегляду варіантів (TOPSIS) [67] визначає оптимальну альтернативу шляхом вибору найближчої альтернативи до ідеальної точки. Метод враховує відстані до ідеального (найкращого) та анти-ідеального (найгіршого) рішення. TOPSIS є простим у реалізації та чітко визначає кращу альтернативу, але

він чутливий до відносних значень критеріїв і може бути впливовим до некоректного масштабування [68].

Отже, в табл. 1.4 відображено порівняння методів прийняття рішень, за допомогою яких можливо оцінювати ІТ-загрози. Аналіз проведено за такими критеріями: CI – можливість застосування у галузі КІ, FL – гнучкість, SC – масштабованість, CR – врахування ризиків та невизначеності, EU – простота використання.

Таблиця 1.4

Огляд популярних методів багатокритеріального прийняття рішень

Критерій / Підхід	CI	FL	SC	CR	EU
AHP	+	+	+	-	+
TODIM	+	+	+	+	+
TOPSIS	-	-	+	-	+

Зважаючи на аналіз зазначених критеріїв, підхід TODIM є найбільш придатним для застосування у галузі КІІ. Метод ефективно враховує ризики та невизначеність, що є важливим аспектом для ОКІІ, і демонструє високу гнучкість у врахуванні різноманітних критеріїв.

1.5. Висновки до першого розділу

Отже, у першому розділі було проаналізовано основні підходи до захисту КІ України та у інших країнах світу. Розглянуто методи та стандарти, що використовуються для забезпечення безпеки КІ, включаючи підходи в США, ЄС, Великій Британії, Канаді, Німеччині, Австралії та Японії. Оцінено нормативні вимоги та практики, визначено ключові напрямки та методи покращення захисту

критичної інфраструктури. Також проаналізовано сучасні методи управління ІТ інцидентами, що дозволяють ефективно ідентифікувати, оцінювати та управляти ризиками, пов’язаними з ІТ інцидентами на ОКІІ. Визначено переваги та недоліки цих методів, а також можливості їх інтеграції для підвищення рівня захищеності КІ.

1.6. Список літератури до першого розділу

1. С. Гнатюк, М. Рябий, В. Лядовська. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. *Зв'язок*. 2014. №4, С. 3-7.

2. С. Гнатюк, В. Сидоренко, О. Дуксенко. Сучасні підходи до виявлення та ідентифікації найбільш важливих об’єктів критичної інфраструктури». *Безпека інформації*. Том 21, №3, с. 269-275, 2015.

3. С.О. Гнатюк, В.М. Сидоренко, О.П. Дуксенко. Сучасні підходи до виявлення та ідентифікації найбільш важливих об’єктів критичної інфраструктури. *Безпека інформації*, Т 21, №3. С. 269-275. 2015.

4. Brunner, E., & Suter, M. (2021). Enhancing the protection and cyber-resilience of critical information infrastructure. *Digital Regulation Platform*. URL: https://digitalregulation.org/enhancing-cyber-resilience (дата звернення: 01.06.2024).

5. Hintze, K., Graham, S., Dunlap, S., & Sweeney, P. (2021). InfiniBand network monitoring: Challenges and possibilities. In *Critical Infrastructure Protection XV: 15th IFIP WG 11.10 International Conference* (pp. 187-208). SpringerLink. URL: https://link.springer.com/chapter/10.1007/978-3-030-78021-2_9 (дата звернення: 01.06.2024).

6. Katzke, S. W., Oldehoeft, A., & Radack, S. M. (2021). Critical infrastructures protection: Research agendas for information systems security. *NIST*. URL: https://www.nist.gov/publications/critical-infrastructures-protection-research-agendas-information-systems-security (дата звернення: 01.06.2024).

7. Manjikian, M., & Romaniuk, S. N. (2021). Routledge companion to global cyber-security strategy. Routledge. ISBN 9780367024239.

8. Osama, A., & et al. (2021). Threats, vulnerabilities, and security functions in critical information infrastructure. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/9354300 (дата звернення: 01.06.2024).

9. RAND Corporation. (2021). Critical infrastructure protection: Research and analysis. *RAND*. URL: https://www.rand.org/topics/critical-infrastructure-protection.html (дата звернення: 01.06.2024).

10. Schmitt, M. N. (2021). Tallinn manual 2.0 on the international law applicable to cyber warfare. Cambridge University Press. ISBN 9781107177222.

11. TNO. (2021). Critical information infrastructure protection for governmental policy-makers. *GFCE-Meridian*. URL: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf (дата звернення: 01.06.2024).

12. Critical infrastructures protection: Conference papers from CRITIS 2021. *SpringerLink*. URL: https://link.springer.com/book/10.1007/978-3-030-78021-2 (дата звернення: 01.06.2024).

13. Aleksandar S. Jovanovic, Somik Chakravarty, and Marjan Jelic. (2021). *Resilience and Situational Awareness in Critical Infrastructure Protection: An Indicator-Based Approach*. In *IntechOpen*. URL: https://www.intechopen.com/chapters/75135 (дата звернення: 01.06.2024).

14. Andrea Carpignano, Daniele Grosso, Raffaella Gerboni, and Andrea Bologna. (2021). *Resilience of Critical Infrastructures: A Risk Assessment Methodology for Energy Corridors*. In *IntechOpen*. URL: https://www.intechopen.com/chapters/75136 (дата звернення: 01.06.2024).

15. Chiara Foglietta and Stefano Panzieri. (2021). *Resilience in Critical Infrastructures: The Role of Modelling and Simulation*. In *IntechOpen*. URL: https://www.intechopen.com/chapters/75137 (дата звернення: 01.06.2024).

16. European Commission. (2021). *Critical Infrastructure Resilience: News, Updates and Events*. URL: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC125587/cir_newsletter_june_2021.pdf (дата звернення: 01.06.2024).

17. European Commission. (2021). *Technical Guidance on Climate Proofing of Infrastructure 2021-2027*. URL: https://ec.europa.eu/newsroom/cipr/items/722278/ (дата звернення: 01.06.2024).

18. John D'Avanzo, Gebhard Geiger, Sascha Goldner, Claudia Lorenz, Alf Papproth, and Mara Cole. (2021). *Optimisation of Critical Infrastructure Protection: The SiVe Project on Airport Security*. In *SpringerLink*. URL: https://link.springer.com/chapter/10.1007/978-3-030-65813-8_27 (дата звернення: 01.06.2024).

19. Klaver, M., Kotzanikolaou, P., Theoharidou, M., and Gritzalis, D.. (2021). *Assessing n-order Dependencies Between Critical Infrastructures*. In *SpringerLink*. URL: https://link.springer.com/chapter/10.1007/978-3-319-71643-0_5 (дата звернення: 01.06.2024).

20. Kotzanikolaou, P., Theoharidou, M., and Gritzalis, D.. (2021). *Methodologies and Strategies for Critical Infrastructure Protection*. In *SpringerLink*. URL: https://link.springer.com/chapter/10.1007/978-3-030-65813-8_1 (дата звернення: 01.06.2024).

21. National Technical University of Athens. (2021). *European Programme for Critical Infrastructure Protection (EPCIP)*. URL: https://joint-research-centre.ec.europa.eu (дата звернення: 01.06.2024).

22. Illiashenko, O., Kharchenko, V., & Odarushchenko, O. (2023). Towards Evidence-Based Cybersecurity Assessment of Programmable Systems to Ensure the Protection of Critical IT Infrastructure, *IDAACS 2023* (pp. 1178-1183). Hybrid, Dortmund, September 7-9, 2023. IEEE. URL: https://doi.org/10.1109/IDAACS58523.2023.10348834. (дата звернення: 01.06.2024).

23. Закон України. Про основні засади забезпечення кібербезпеки України. від 15.10.2017, №2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19(дата звернення: 01.06.2024).

24. Захист об’єктів критичної інфраструктури. URL: https://ssu.gov.ua/zakhystobiektiv-krytychnoi-infrastruktury (дата звернення: 01.06.2024).

25. Green paper on a European programme for critical infrastructure protection (COM/2005/576 final). URL: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.

26. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ. 2015. 31 с. URL: https://cdn.regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua_File_188.pdf (дата звернення: 01.06.2024).

27. Закон України про критичну інфраструктуру. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.06.2024).

28. Кабінет Міністрів України. (2020). Деякі питання об’єктів критичної інфраструктури: Постанова від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 01.06.2024).

29. Кабінет Міністрів України. (2018). Про затвердження переліку особливо важливих об’єктів електроенергетики, у тому числі територій забороненої зони та контрольованої зони гідротехнічних споруд, які підлягають охороні відомчою

воєнізованою охороною. Постанова від 4 липня 2018 р. № 575. URL: https://zakon.rada.gov.ua/laws/show/575-2018-%D0%BF#Text (дата звернення: 01.06.2024).

30. Кабінет Міністрів України. (2009). Про затвердження переліку особливо важливих об'єктів нафтогазової галузі. Розпорядження від 27.05.2009 № 578-р. URL: https://zakon.rada.gov.ua/laws/show/578-2009-%D1%80#Text (дата звернення: 01.06.2024).

31. Кабінет Міністрів України. (2018). Про деякі питання запобігання виникненню надзвичайних ситуацій природного та техногенного характеру. Постанова від 26 вересня 2018 р. № 779. URL: https://zakon.rada.gov.ua/laws/show/779-2018-%D0%BF#Text (дата звернення: 01.06.2024).

32. Кабінет Міністрів України. (2018). Про затвердження категорій об’єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах. Постанова від 21 листопада 2018 р. № 975. URL: https://zakon.rada.gov.ua/laws/show/975-2018-%D0%BF#Text (дата звернення: 01.06.2024).

33. Кабінет Міністрів України. (2012). Про затвердження Порядку ведення Державного земельного кадастру. Постанова від 17 жовтня 2012 р. № 1051. URL: https://zakon.rada.gov.ua/laws/show/1051-2012-%D0%BF#Text (дата звернення: 01.06.2024).

34. Кабінет Міністрів України (2016). Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави». Постанова від 23.08.2016, №563. URL: http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF.

35. Кабінет Міністрів України. (2015). Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки

держави: Постанова від 4 березня 2015 р. № 83. URL: https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF#n10 (дата звернення: 01.06.2024).

36. Указ Президента України. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 01.06.2024).

37. Адміністрація державної служби спеціального зв'язку та захисту інформації України. Наказ про внесення змін до наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 26 грудня 2022 року № 832. URL: https://zakon.rada.gov.ua/laws/show/z0102-24#Text (дата звернення 01.06.2024).

38. International Telecommunication Union (ITU). Core ICT Indicators. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/coreindicators/Core_ICT_Indicators_E.pdf.

39. Knoema. UN E-Government Development Index. URL: https://ru.knoema.com/infographics/mctunlb/un-e-government-development-index?indicator=Telecommunication%20Infrastructure%20Index%20(TII) (дата звернення 01.06.2024).

40. National Cyber Security Index. URL: http://ncsi.ega.ee/ncsi-index/ (дата звернення 01.06.2024).

41. NIST Cyber Risk Scoring (CRS) Program Overview. URL: https://csrc.nist.gov/CSRC/media/Presentations/nist-cyber-risk-scoring-crs-program-overview/images-media/NIST%20Cyber%20Risk%20Scoring%20(CRS)%20-%20Program%20Overview.pdf (дата звернення 01.06.2024).

42. Mokhor, V., Gonchar, S., & Dybach O. (2019). Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. *Ядерна та радіаційна*

безпека, (2(82), 4-8. https://doi.org/10.32918/nrs.2019.2(82).01 (дата звернення 01.06.2024).

43. Король О.Г., Огурцова К.В., Євсеєв С.П. Оцінка ризику реалізації загроз безпеки у телекомунікаційних системах. Автоматика, телемеханіка, зв'язок. Збірник наукових праць ДонІЗТ. 2013. № 36. С. 55-63.

44. Mokhor, V. V., G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine, Honchar, S. F., & G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine. (2019). Evaluation of risks of cyber security of information systems of objects of critical infrastructure. Elektronnoe Modelirovanie, 41(6), 65–76. https://doi.org/10.15407/emodel.41.06.065

45. Jablanski, D. (2023). Method for Determining the State of Protection of Critical Information Infrastructure Objects from IT Risks. Наукові дослідження з кібербезпеки. URL: https://www.researchcybersecurity.com/state-protection-method/ (дата звернення: 01.06.2024).

46. N. Anuar, S. Furnell, M. Papadaki, and N. Clarke, "A risk index modelfor security incident prioritisation," in Proceedings of the 9th AustralianInformation Security Management Conference (AISM), 2011, pp. 25–39 (3) (PDF) A Response Cost Model for Advanced Metering Infrastructures. Available from: https://www.researchgate.net/publication/279164404_A_Response_Cost_Model_for_Advanced_Metering_Infrastructures [accessed Jun 01 2024].

47. Качинський А.Б., Варичева Д.І., Свириденко С.В. (2016). Ефективне управління IT-інцидентами в критичній інформаційній інфраструктурі. Інформація і право, № 2(17), с. 114-126.

48. Nosal, K., & Solecka, K. (2014). Application of AHP method for multi-criteria evaluation of variants of the integration of urban public transport. Transportation

Research Procedia, 3, 269–278. URL: https://doi.org/10.1016/j.trpro.2014.10.006 (дата звернення: 11.06.2024).

49. Nosal, K., & Solecka, K. (2014). Application of AHP method for multi-criteria evaluation of variants of the integration of urban public transport. Transportation Research Procedia, 3, 269–278. URL: https://doi.org/10.1016/j.trpro.2014.10.006 (дата звернення: 11.06.2024).

50. Axelos. (2019). ITIL Foundation: ITIL 4 Edition. ITIL 4 Best Practice. URL: https://www.axelos.com/certifications/itil-certifications/itil-foundation (дата звернення: 01.06.2024).

51. T. Lechachenko, T. Gancarczyk, T. Lobur, A. Postoliuk. «Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems». *CITI* 2023: 250-256.

52. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016). Threat and risk assessment methodologies in the automotive domain. Procedia Computer Science, 83, 1288–1294. URL: https://doi.org/10.1016/j.procs.2016.04.268 (дата звернення: 01.06.2024).

53. G. Holtrup, W. Blonay, M. Strohmeier, A. Mermoud, J. -P. Chavanne and V. Lenders, "Modeling 5G Threat Scenarios for Critical Infrastructure Protection," 2023 *15th International Conference on Cyber Conflict: Meeting Reality* (CyCon), Tallinn, Estonia, 2023, pp. 161-180. DOI: 10.23919/CyCon58705.2023.10 (дата звернення: 01.06.2024).

54. R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 2017, pp. 1-6, doi: 10.1109/ISGTEurope.2017.8260283 (дата звернення: 01.06.2024).

55. Wang J, Wei G, Lu M. TODIM Method for Multiple Attribute Group Decision Making under 2-Tuple Linguistic Neutrosophic Environment. *Symmetry*. 2018; 10(10):486. https://doi.org/10.3390/sym10100486 (дата звернення: 01.06.2024).

56. M. Abomhara, M. Gerdes, and G. M. Koien, “A STRIDE-Based Threat Model for Telehealth Systems”, *NISK*, 2015.

57. Microsoft Corporation. The STRIDE Threat Model, 2005.

58. Ross, R. (2012). *Guide for Conducting Risk Assessments, Special Publication (NIST SP) 800-30 Rev 1*. National Institute of Standards and Technology, Gaithersburg, MD. Available at NIST.

59. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO. Available at ISO.

60. Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Carnegie Mellon University, Software Engineering Institute. Available at SEI CMU.

61. ISACA. (2019). *COBIT 2019 Framework: Governance and Management Objectives*. Information Systems Audit and Control Association (ISACA). Available at ISACA.

62. Hamed Taherdoost. Decision Making Using the Analytic Hierarchy Process (AHP). A Step by Step Approach. International Journal of Economics and Management System, 2017. ffhal-02557320f

63. Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83. URL: https://doi.org/10.1504/ijssci.2008.017590 (дата звернення: 01.06.2024).

64. Llamazares, B. (2018). An analysis of the generalized TODIM method. *European Journal of Operational Research*, *269*(3), 1041–1049. URL: https://doi.org/10.1016/j.ejor.2018.02.054 (дата звернення: 01.06.2024).

65. Wakker, P. P. (2010). Prospect theory: For risk and ambiguity. Cambridge University Press. URL: https://doi.org/10.1017/CBO9780511779329 (дата звернення: 01.06.2024).

66. Barberis, N. C. (2013). Thirty years of prospect theory in economics: A review and assessment. Journal of Economic Perspectives, 27(1), 173-196. URL: https://doi.org/10.1257/jep.27.1.173 (дата звернення: 01.06.2024).

67. El Alaoui, M. (2021). Fuzzy TOPSIS: Logic, Approaches, and Case Studies. New York: CRC Press. URL: DOI:10.1201/9781003168416. ISBN 978-0-367-76748-8. S2CID 233525185.

68. Tzeng, G. H., & Huang, J. J. (2011). *Multiple attribute decision making: methods and applications*. CRC press.

69. В. Сидоренко, С. Гнатюк, О. Юдін. Експериментальне дослідження методу визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації. *Захист інформації*. Том 19, №2. с. 155-172, 2017.

70. Хлапонін Ю.І, Тернавська В.М. Кібербезпека як засіб забезпечення інформаційного суверенітету держави: техніко-юридичний аналіз: збірник тез наукових доповідей Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2021). Миколаїв- Коблево: 2021. С. 47-49. URL: http://bit.nau.edu.ua/wp-content/uploads/2021/07/Zbirnyk-tez-Koble vo- 2021.pdf

71. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. *Альфа реклама*. 2019. 176с. Київ.

72. Шевченко, С., Жданова, Ю., Складанний, П., & Спасітєлєва, С. (2021). Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. Кібербезпека: освіта, наука, техніка, 1(13), 133–144.

РОЗДІЛ 2

РОЗРОБКА МЕТОДУ ВИЗНАЧЕННЯ СТАНУ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ВІД ІТ-РИЗИКІВ

2.1. Розробка методу визначення пріоритетів ІТ-інцидентів на об'єктах критичної інформаційної інфраструктури

Загальний опис та роз'яснення методу

Відповідно до [1,2, 4-7], розроблений метод визначення стану захищеності об'єктів КІІ реалізується у такі 4 етапи:

Етап 1. Визначення загальних метрик ІТ-безпеки для ОКІІ;

Крок 1.1. Формування множин метрик ІТ-безпеки для ОКІІ

Крок 1.2. Обчислення індексу, що характеризує стан захищеності ОКІІ

Етап 2. Визначення загальних метрик рівня цифрової трансформації у галузі КІІ;

Крок 2.1. Визначення загальних метрик рівня цифрової трансформації у галузі КІІ.

Крок 2.2 – Обчислення індексу рівня цифрової трансформації

Етап 3. Розрахунок кількісних параметрів, що визначають стан захищеності ОКІІ держави від ІТ-ризиків.

Етап 4. Аналіз отриманих результатів та розроблення рекомендацій для оптимізації захисту об'єкту КІІ

Крок 4.1. Аналіз отриманих результатів визначення стану захищеності ОКІІ

Крок 4.2. Розроблення рекомендацій для оптимізації захисту ОКІІ

Схема реалізації розробленого методу відображена на рис 2.1:

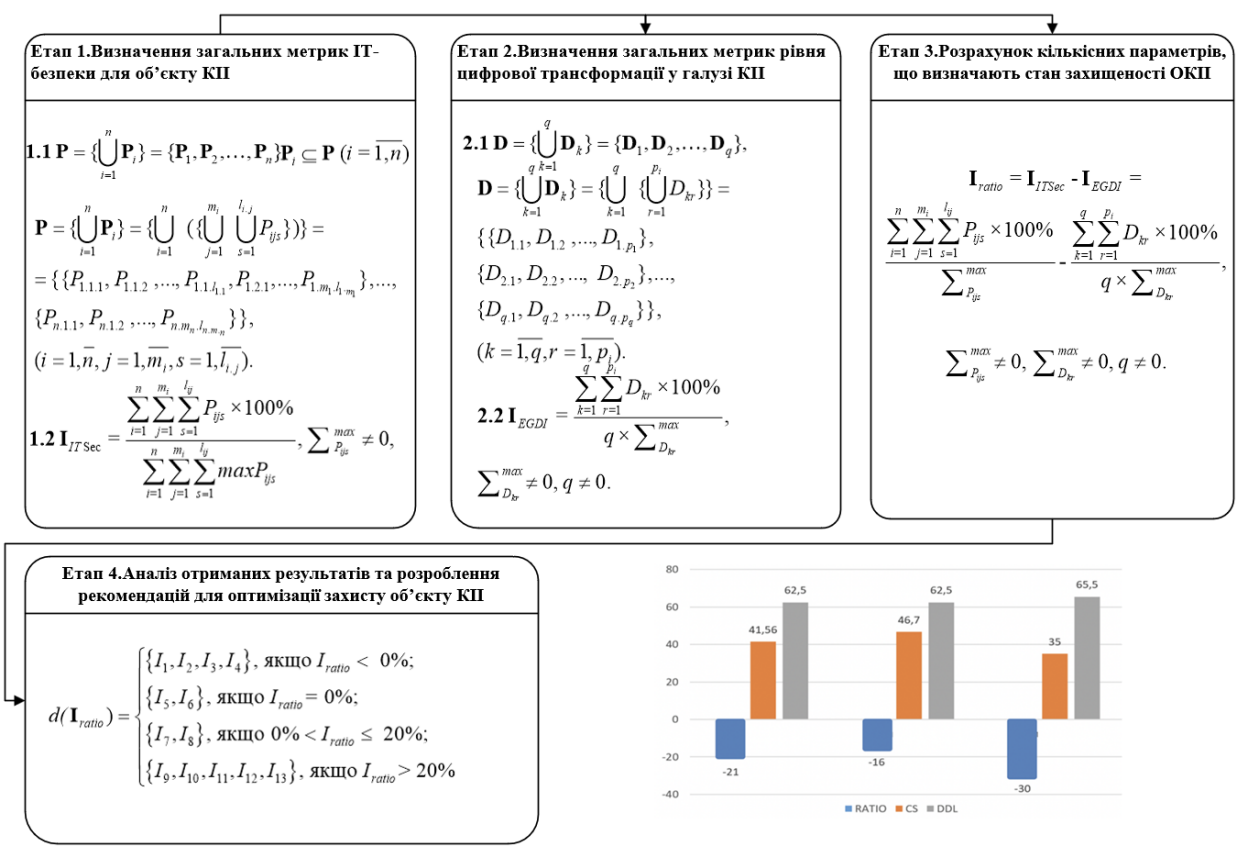


Рис. 2.1. Схема реалізації методу визначення стану захищеності ОКІІ

Отже, розглянемо детально та проаналізуємо кожний етап розробленого методу:

ЕТАП 1 – Визначення загальних метрик ІТ-безпеки для ОКІІ

Крок 1.1 – Формування множин метрик ІТ-безпеки для ОКІІ

$$\mathbf{P} = \{\bigcup_{i=1}^{n} \mathbf{P}_i\} = \{\mathbf{P}_1, \mathbf{P}_2, \ldots, \mathbf{P}_n\}, \tag{2.1}$$

де $\mathbf{P}_i \subseteq \mathbf{P}\ (i = \overline{1,n})$ підмножина наборів метрик.

Множина $\mathbf{P}_i$ може бути представлена у вигляді системи підмножин:

$$\mathbf{P}_i = \{\bigcup_{j=1}^{m_i} P_{ij}\} = \{P_{i.1}, P_{i.2}, \ldots, P_{i.m_i}\}, \tag{2.2}$$

де P_{ij} $(i=\overline{1,n},\ j=\overline{1,m_i})$ метрики *i*-го набору (діапазон значень метрик визначається згідно відповідних стандартів та рекомендованих практик у відповідній галузі КІІ), m_i – кількість метрик і-го набору.

Отже, множину $\mathbf{P}_i$ можна представити у такому вигляді:

$$\mathbf{P}=\{\bigcup_{i=1}^{n}\mathbf{P}_i\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}P_{ij}\}\}=\{\{P_{1.1},P_{1.2},...,P_{1.m_1}\},\{P_{2.1},P_{2.2},...,P_{2.m_2}\},...,\{P_{n.1},P_{n.2},...,P_{n.m_n}\}\},(i=\overline{1,n},\ j=\overline{1,m_i}). \tag{2.3}$$

Крім цього, відповідно до [1] множину $\mathbf{P}_i$ можна розширити за допомогою додаткових показників, що допоможе отримати точнішу оцінку, і представити у вигляді:

$$\mathbf{P}=\{\bigcup_{i=1}^{n}\mathbf{P}_i\}=\{\bigcup_{i=1}^{n}(\{\bigcup_{j=1}^{m_i}\bigcup_{s=1}^{l_{i.j}}P_{ijs}\})\}=\{\{P_{1.1.1},P_{1.1.2},...,P_{1.1.l_{1.1}},P_{1.2.1},...,P_{1.m_1.l_{1.m_1}}\},...,\{P_{n.1.1},P_{n.1.2},...,P_{n.m_n.l_{n.m_n}}\}\},(i=\overline{1,n},\ j=\overline{1,m_i},s=\overline{1,l_{i.j}}). \tag{2.4}$$

Крок 1.2 – Обчислення індексу, що характеризує стан захищеності ОКІІ

Обчислення індексу, що характеризує стан захищеності об'єкту КІІ від ІТ-ризиків, можна виразити наступним чином:

$$\mathbf{I}_{IT\,\mathrm{Sec}}=\frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{s=1}^{l_{ij}}P_{ijs}\times 100\%}{\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{s=1}^{l_{ij}}maxP_{ijs}},\ \sum{}^{max}_{P_{ijs}}\neq 0, \tag{2.5}$$

де $\sum{}^{max}_{P_{ij}}$ максимально можлива сума значень індексу $\mathbf{P}_i$

ЕТАП 2 – Визначення метрик рівня цифрової трансформації ОКІІ

Крок 2.1 – Визначення загальних метрик рівня цифрової трансформації у галузі КІІ

Введемо множину метрик, які характеризують рівень цифрової трансформації об'єкту КІІ **D**:

$$\mathbf{D} = \{\bigcup_{k=1}^{q} \mathbf{D}_k\} = \{\mathbf{D}_1, \mathbf{D}_2, \ldots, \mathbf{D}_q\}, \tag{2.6}$$

де $\mathbf{D}_k \subseteq \mathbf{D}\ (k = \overline{1,q})$ – підмножина індексу цифрової трансформації, q – кількість підмножин метрик.

Множина $\mathbf{D}_k$ може бути представлена у вигляді системи підмножин:

$$\mathbf{D}_k = \{\bigcup_{r=1}^{p_i} D_{kr}\} = \{D_{k.1}, D_{k.2}, \ldots, D_{k.p_i}\}, \tag{2.7}$$

де D_{kr} $(k = \overline{1,q}, r = \overline{1,p_i})$ - метрики i-ї множини, P_i – кількість метрик i-ї множини.

Аналогічно, вираз можна представити у вигляді:

$$\begin{gathered}\mathbf{D} = \{\bigcup_{k=1}^{q} \mathbf{D}_k\} = \{\bigcup_{k=1}^{q} \{\bigcup_{r=1}^{p_i} D_{kr}\}\} = \{\{D_{1.1}, D_{1.2}, \ldots, D_{1.p_1}\}, \\ \{D_{2.1}, D_{2.2}, \ldots, D_{2.p_2}\}, \ldots, \{D_{q.1}, D_{q.2}, \ldots, D_{q.p_q}\}\}, \\ (k = \overline{1,q}, r = \overline{1,p_i}).\end{gathered} \tag{2.8}$$

Крок 2.2 – Обчислення індексу рівня цифрової трансформації

Метрики, що характеризують рівень цифрової трансформації ОКІІ обчислюються згідно наступного виразу:

$$\mathbf{I}_{EGDI} = \frac{\sum_{k=1}^{q}\sum_{r=1}^{p_i} D_{kr} \times 100\%}{q \times \sum_{D_{kr}}^{max}}, \sum_{D_{kr}}^{max} \neq 0,\ q \neq 0. \tag{2.9}$$

де $\sum_{D_{kr}}^{max}$ – максимально допустиме значення метрик D_{kr}.

ЕТАП 3 – Розрахунок кількісних параметрів, що визначають стан захищеності ОКІІ держави від ІТ-ризиків

На основі виразів $\mathbf{I}_{IT\,\mathrm{Sec}}$ та $\mathbf{I}_{EGDI}$ можемо отримати кількісні параметри, які визначають стан захищеності об'єкту КІІ держави від ІТ-ризиків $\mathbf{I}_{ratio}$:

$$\mathbf{I}_{ratio} = \mathbf{I}_{ITSec} - \mathbf{I}_{EGDI} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{s=1}^{l_{ij}} P_{ijs} \times 100\%}{\sum_{P_{ijs}}^{max}} - \frac{\sum_{k=1}^{q}\sum_{r=1}^{p_i} D_{kr} \times 100\%}{q \times \sum_{D_{kr}}^{max}}, \quad (2.10)$$

$$\sum_{P_{ijs}}^{max} \neq 0,\ \sum_{D_{kr}}^{max} \neq 0,\ q \neq 0.$$

Етап 4. Аналіз отриманих результатів та розроблення рекомендацій для оптимізації захисту об'єкту КІІ

Крок 4.1. Аналіз отриманих результатів визначення стану захищеності ОКІІ

Індекс $\mathbf{I}_{ratio}$ може приймати значення в діапазоні від -99% до +99%. Ці межі визначають ступінь відповідності або невідповідності стану захищеності ІТ-систем об'єкту КІІ до рівня його цифрової трансформації.

Введемо множину $\mathbf{I}_{ratio}$, де n=13:

$$d(\mathbf{I}_{ratio}) = \begin{cases} \{I_1, I_2, I_3, I_4\}, \text{ якщо } I_{ratio} < 0\%; \\ \{I_5, I_6\}, \text{ якщо } I_{ratio} = 0\%; \\ \{I_7, I_8\}, \text{ якщо } 0\% < I_{ratio} \leq 20\%; \\ \{I_9, I_{10}, I_{11}, I_{12}, I_{13}\}, \text{ якщо } I_{ratio} > 20\% \end{cases} \quad (2.11)$$

Оцінка та інтерпретація значень індексу $\mathbf{I}_{ratio}$

Після розрахунку індексу $\mathbf{I}_{ratio}$, важливо розглянути та інтерпретувати його значення, щоб визначити відповідність рівня захищеності ІТ-систем об'єкту КІІ до рівня його цифрової трансформації. Інтерпретація значень індексу $\mathbf{I}_{ratio}$ дозволяє виявити поточний стан безпеки, потенційні вразливості, та визначити необхідні дії для оптимізації захисту [9-12]. Розглянемо різні діапазони значень індексу та відповідні рекомендації.

Від'ємне значення $\mathbf{I}_{ratio}$ (< 0%): Це вказує на те, що стан захищеності КІІ є недостатнім у порівнянні з рівнем цифрової трансформації. Тобто, цифрові активи і системи розвиваються швидше, ніж вживаються заходи щодо їх захисту. Це може свідчити про потенційні вразливості і збільшений ризик ІТ-інцидентів, які можуть негативно вплинути на діяльність організації.

$$I_{ratio} < 0\% \Rightarrow \begin{cases} I_1 : \text{Підвищення інвестицій у ІТ-безпеку;} \\ I_2 : \text{Оновлення захисного ПО;} \\ I_3 : \text{Проведення аудиту безпеки;} \\ I_4 : \text{Навчання персоналу.} \end{cases} \tag{2.12}$$

Нульове значення $\mathbf{I}_{ratio}$ (0%): Показує, що рівень захищеності КІІ в точності відповідає поточному рівню цифровізації. Заходи безпеки адекватні сучасному стану цифрових технологій у КІІ, але це також може означати потребу уважного моніторингу з метою уникнення відставання в майбутньому.

$$I_{ratio} = 0\% \Rightarrow \begin{cases} I_5 : \text{Моніторинг і аналіз;} \\ I_6 : \text{Оптимізація ресурсів.} \end{cases} \tag{2.13}$$

Позитивне значення $\mathbf{I}_{ratio}$ (від 0% до 20%): Свідчить про те, що заходи щодо захисту КІІ не тільки відповідають, а й можуть перевищувати поточний рівень

цифрового розвитку. Це означає, що організація добре захищена від поточних ІТ-ризиків і має запас міцності для забезпечення безпеки при майбутніх технологічних змінах.

$$0\% < I_{ratio} \le 0\% \Rightarrow \begin{cases} I_7 : \text{Періодичний перегляд політик безпеки;} \\ I_8 : \text{Збалансоване вкладання.} \end{cases} \quad (2.14)$$

Значення $\mathbf{I}_{ratio}$ вище 20% Таке значення свідчить про високий рівень безпеки, який значно перевищує потреби цифрової трансформації. Хоча це може бути позитивним показником, існує ризик нераціонального розподілу ресурсів, де занадто багато вкладається в захист, що може призвести до зменшення інвестицій в інші необхідні аспекти розвитку КІІ.

$$I_{ratio} > 20\% \Rightarrow \begin{cases} I_9 : \text{Аналіз ефективності інвестицій у безпеку;} \\ I_{10} : \text{Оптимізація бюджету ІТ-безпеки;} \\ I_{11} : \text{Переоцінка стратегії безпеки;} \\ I_{12} : \text{Підвищення ефективності використання наявних технологій;} \\ I_{13} : \text{Вдосконалення аналітичних здібностей.} \end{cases} \quad (2.15)$$

Кожне з цих значень вимагає адекватної реакції та може бути використане для коригування стратегії безпеки та розподілу ресурсів, щоб забезпечити оптимальний баланс між безпекою та інноваційним розвитком.

Крок 4.2. Розроблення рекомендацій для оптимізації захисту ОКІІ

На цьому кроці формуються конкретні рекомендації на основі аналізу індексу $\mathbf{I}_{ratio}$ з метою досягнення або підтримки його оптимального значення (0% до 20%). Ці рекомендації спрямовані на забезпечення адекватного рівня захисту КІІ відповідно до рівня цифрової трансформації.

Для випадків, коли $\mathbf{I}_{ratio}$ є від'ємним, що означає термінову необхідність підвищення рівня захищеності ОКІІ, можна застосувати наступні підходи, [13, 14]**:**

1. Підвищення інвестицій у IT-безпеку: Збільшити бюджет на IT-безпеку для вдосконалення захисних технологій і методів.

2. Оновлення захисного програмного забезпечення: Регулярне оновлення антивірусних програм, файєрволів та інших систем безпеки.

3. Проведення аудиту безпеки: Регулярні аудити для ідентифікації та усунення вразливостей у системах КІІ.

4. Навчання персоналу. Організація тренінгів з IT-безпеки для співробітників для підвищення їхньої обізнаності щодо потенційних загроз.

Для випадків, коли I_{ratio} є нульовим:

1. Моніторинг і аналіз. Постійний моніторинг систем для виявлення та реагування на нові загрози є ключовим аспектом забезпечення кібербезпеки. Це включає наступні підходи [15]:

- Впровадження системи безперервного моніторингу. Використання спеціалізованих інструментів для автоматичного відстеження та аналізу активності в реальному часі.
- Використання штучного інтелекту (AI) та машинного навчання (ML). Застосування AI та ML для аналізу великих обсягів даних і виявлення аномалій, які можуть свідчити про потенційні IT-загрози.
- Регулярне оновлення програмного забезпечення безпеки. Постійне оновлення антивірусних програм, файєрволів та інших інструментів безпеки для захисту від новітніх загроз.

2. Оптимізація витрат на IT-безпеку включає перегляд бюджетів та ресурсів для забезпечення адекватного рівня захисту при мінімальних витратах. Це включає наступні підходи [16]:

- Аналіз поточних витрат та їх ефективності: Проведення аналізу всіх витрат на заходи безпеки для виявлення можливостей для оптимізації.
- Пріоритезація загроз та ризиків: Визначення найбільш критичних загроз та зосередження ресурсів на їх усуненні.
- Використання економічно ефективних технологій: Вибір та впровадження технологій, які забезпечують максимальний захист при відносно низьких витратах.

Для випадків, коли I_{ratio} є достатнім (0% до 20%):

1. Періодичний перегляд політик безпеки. Регулярний перегляд і оновлення політик та процедур безпеки є необхідним для забезпечення актуальності заходів безпеки у відповідності до змін у технологіях та загрозах, що включає наступні кроки [17]:
   - Встановлення регулярного графіку перегляду. Визначення чітких інтервалів для перегляду політик безпеки, таких як щоквартально або щорічно, щоб забезпечити своєчасне оновлення.
   - Оцінка відповідності поточним загрозам. Аналіз новітніх IT-загроз та атак для визначення, чи поточні політики безпеки адекватно захищають організацію.
   - Адаптація до нових технологій. Перегляд політик для врахування нових технологій, які впроваджуються в організації, таких як хмарні обчислення, штучний інтелект тощо.
   - Тестування та симуляції. Проведення тестувань та симуляцій для перевірки ефективності оновлених політик та процедур у реальних умовах.
2. Збалансоване вкладення. Означає уникнення перевитрат на заходи безпеки, які не приносять пропорційного зниження ризику. Це включає наступні підходи [18-21]:
   - Оцінка ризиків: визначення і пріоритезація ризиків, щоб сконцентрувати ресурси на найбільш критичних загрозах.

- Аналіз витрат та вигод. проведення аналізу витрат та вигод для кожного заходу безпеки, щоб визначити його економічну доцільність.
- Використання ефективних технологій. інвестування в рішення, які пропонують високий рівень захисту при відносно низьких витратах.
- Моніторинг ефективності. постійний моніторинг ефективності заходів безпеки та їх відповідність змінам у загрозах.

Для випадків, коли I_{ratio} перевищує 20%:

1. Аналіз інвестицій у безпеку є важливим для виявлення можливих надмірних витрат, які не приносять пропорційної користі. Це включає оцінку всіх витрат на заходи безпеки та порівняння їх з отриманими перевагами. Зокрема, необхідно з'ясувати, чи вкладення в безпеку не здійснюються за рахунок інших критичних потреб організації, таких як розвиток IT-інфраструктури, навчання персоналу або інноваційні проекти. Аналіз ефективності інвестицій може включати наступні кроки [22-25]:
   - Збір даних про витрати та результати. Включає інформацію про всі витрати на безпеку, а також про кількість і типи попереджених загроз та інцидентів.
   - Оцінка віддачі від інвестицій (ROI). Аналізує економічну ефективність витрат на безпеку у відношенні до зменшення кількості інцидентів і їх вартості.
   - Порівняльний аналіз. Порівняння витрат на безпеку з аналогічними організаціями або галузевими стандартами для виявлення надмірних витрат.
2. Оптимізація бюджету безпеки. Передбачає перерозподіл ресурсів з метою збереження адекватного рівня захисту IT-систем, скорочуючи при цьому надмірні заходи. Можливі кроки [26]:

- Ідентифікація ключових пріоритетів. Визначення найважливіших аспектів безпеки, які забезпечують максимальний захист за мінімальних витрат.
- Використання ризик-менеджменту. Оцінка ризиків для визначення областей, де можна скоротити витрати без значного збільшення ризиків.
- Інвестування в ефективні технології. Використання сучасних інструментів та технологій, які забезпечують вищий рівень захисту при менших витратах.

3. Переоцінка стратегії безпеки. Включає аналіз поточних заходів захисту та їх відповідність сучасним загрозам та технологіям. Це допомагає уникнути перевантаження системи непотрібно складними заходами, які можуть ускладнювати управління IT-системами і знижувати їхню ефективність. Рекомендації [27]:

- Оцінка поточного стану безпеки. Аналіз існуючих політик і процедур для виявлення надлишкових або неефективних заходів.
- Впровадження нових підходів. Використання новітніх методологій та технологій, таких як адаптивна безпека або проактивне управління IT-загрозами.
- Навчання персоналу. Забезпечення регулярного навчання для оновлення знань та навичок співробітників у сфері IT-безпеки.

4. Підвищення ефективності використання наявних технологій полягає у максимізації користі від вже встановлених систем безпеки. Можливі кроки [28]:

- Оцінка поточного використання. Аналіз того, як використовуються наявні технології, та визначення можливостей для їх покращення.
- Оптимізація налаштувань. Налаштування систем безпеки для підвищення їх ефективності, зокрема шляхом оновлення програмного забезпечення та оптимізації конфігурацій.
- Аудит та тестування. Регулярні аудити та тестування систем для виявлення і усунення вразливостей.

5. Вдосконалення аналітичних здібностей організації може значно покращити її здатність розуміти ступінь і характер загроз. Це включає [29]:

- Інвестування в аналітичні інструменти. Використання інструментів для аналізу великих обсягів даних про загрози та вразливості.
- Розробка аналітичних моделей. Створення моделей для прогнозування та ідентифікації загроз.
- Спільне використання даних. Налагодження співпраці з іншими організаціями та обмін даними для підвищення загальної ситуаційної обізнаності.

2.2. Висновки до другого розділу

У даному розділі було удосконалено метод визначення рівня захищеності об'єктів критичної інформаційної інфраструктури шляхом використання нових індикаторів IT-безпеки та рівня цифрової трансформації. Використання нових індикаторів дозволяє детальніше оцінити стан безпеки, аналіз цифрової трансформації допомагає виявити слабкі місця та потенційні ризики, а розроблені рекомендації щодо оптимізації захисту об'єктів критичної інформаційної інфраструктури сприяють більш точному визначенню стану їх захищеності та ефективному управлінню захистом від IT-інцидентів.

2.3. Список літератури до другого розділу

1. National Cyber Security Index. Methodology. URL https://ncsi.ega.ee/methodology/ (дата звернення 01.06.2024).

2. UN-library. Nations E-Government Survey. URL: https://www.un-ilibrary.org/content/periodicals/2411829x (дата звернення 01.06.2024).

3. Revisions and additions to the core list of ict indicators. URL: https://unstats.un.org/unsd/statcom/doc09/bg-ictindicators.pdf (дата звернення 01.06.2024).

4. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Fesenko, A., Akatayev, N., Zhilkishbayeva, G. «Method of cybersecurity level determining for the critical information infrastructure of the state» CEUR Workshop Proceedings, 2020, Vol. 2616, pp. 332-341.

5. Gnatyuk, S., Sydorenko, V., Polozhentsev, A. «Method for Cybersecurity Level Evaluation in the Civil Aviation Critical Infrastructure» Lecture Notes in Networks and Systems, 2023, Vol. 736, pp. 206-218, DOI: 10.1007/978-3-031-38082-2_16.

6. В. Сидоренко, А. Положенцев, С. Гнатюк, «Метод визначення рівня захищеності критичної інформаційної інфраструктури держави», Вісник інженерної академії України, вип. 42, с. 81- 89, 2017.

7. А. Положенцев, В. Сидоренко, «Метод визначення рівня кібербезпеки об’єктів критичної інфраструктури держави», Матеріали IX міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2018. Сучасні проблеми науки», К., 4-6 квітня 2018 р., с. 102-103, 2018.

8. Gnatyuk S., Polishchuk Yu., Sydorenko V., Sotnichenko Yu. “Determining the level of importance for critical information infrastructure objects”, Proceedings of 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, Kyiv, Ukraine, October 8-11, 2019, pp. 829-834.

9. Cybersecurity and Infrastructure Security Agency (CISA). (2023). FY2024-2026 Cybersecurity Strategic Plan. URL: https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf (дата звернення 01.06.2024).

10. U.S. Government Accountability Office (GAO). (2019). Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks

Facing the Electric Grid. URL: https://www.gao.gov/assets/gao-19-332.pdf (дата звернення 01.06.2024).

11. Smith, M. J., & Williams, K. R. (2020). "Enhancing Cybersecurity Measures for Critical Infrastructure Systems Using AI and Machine Learning." Journal of Cybersecurity and Privacy, 2(3), 145-160. URL: https://doi.org/10.3390/jcp2030145 (дата звернення 01.06.2024).

12. Chen, Y., & Xiao, L. (2021). "Building Resilient Critical Infrastructure: Approaches and Challenges." Journal of Infrastructure Systems, 27(1), URL: https://doi.org/10.1061/(ASCE)IS.1943-555X.0000611 (дата звернення 01.06.2024).

13. International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information Security Management. ISO. Retrieved from https://www.iso.org/standard/54534.htmlNational Institute of Standards and Technology. (n.d.). NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework (дата звернення 01.06.2024).

14. Managing the Adoption of New Technologies in the Financial Sector. (2021). Journal of Financial Services. Retrieved from https://www.journaloffinancialservices.com/article/2021-managing-new-tech (дата звернення 01.06.2024).

15. Security Policy Development and Implementation. (2019). Information Security Journal, 28(2), 100-110. https://doi.org/10.1080/19393555.2019.1605489 (дата звернення 01.06.2024).

16. Cybersecurity Incident Response: Testing and Drills. (2020). Cybersecurity Journal, 32(4), 45-55. https://doi.org/10.1016/j.cybsec.2020.04.005 (дата звернення 01.06.2024).

17. National Institute of Standards and Technology. (2019). Risk Management Framework for Information Systems and Organizations. NIST Special Publication 800-

37. Retrieved from https://doi.org/10.6028/NIST.SP.800-37r2 (дата звернення 01.06.2024).

18. Cost-Benefit Analysis of Information Security. (2021). Journal of Information Security, 12(1), 45-60. https://doi.org/10.4236/jis.2021.121003 (дата звернення 01.06.2024).

19. Efficient Cybersecurity Solutions for Small and Medium Enterprises. (2020). Cybersecurity Review, 10(3), 98-110. https://doi.org/10.1016/j.cybsec.2020.03.008 (дата звернення 01.06.2024).

20. Continuous Monitoring for Cybersecurity. (2019). Cybersecurity Techniques, 14(2), 100-120. https://doi.org/10.1016/j.cybsec.2019.02.007 (дата звернення 01.06.2024),

21. Adaptive Security Budget Allocation. (2021). Journal of Cybersecurity, 18(3), 200-215. https://doi.org/10.1093/cybsec/2021.200 (дата звернення 01.06.2024).

22. Continuous Security Monitoring for Risk Management. (2021). Risk Management Journal, 24(2), 140-155. https://doi.org/10.1016/j.rm.2021.02.005 (дата звернення 01.06.2024).

23. Artificial Intelligence and Machine Learning for Cybersecurity. (2020). Journal of Cyber Intelligence, 22(3), 88-105. https://doi.org/10.1016/j.jci.2020.03.006 (дата звернення 01.06.2024).

24. Best Practices for Security Software Updates. (2019). Information Security Journal, 20(4), 45-60. https://doi.org/10.1080/19393555.2019.1605498 (дата звернення 01.06.2024).

25. Log Analysis for Security Monitoring. (2021). Cybersecurity and Data Analysis, 16(1), 77-89. https://doi.org/10.1016/j.cybsec.2021.01.006 (дата звернення 01.06.2024).

26. Cyber Threat Intelligence: Improving Security Posture. (2020). Journal of Cyber Threat Intelligence, 12(2), 99-115. https://doi.org/10.1016/j.jcti.2020.02.004 (дата звернення 01.06.2024).

27. Cost-Effective Strategies for Cybersecurity. (2019). Cybersecurity Review, 11(3), 55-70. https://doi.org/10.1016/j.cybsec.2019.03.009 (дата звернення 01.06.2024).

28. Efficient Cybersecurity Technologies for Small Businesses. (2021). Journal of Small Business Cybersecurity, 19(1), 35-50. https://doi.org/10.1016/j.jsbc.2021.01.002 (дата звернення 01.06.2024).

29. Outsourcing Cybersecurity: Benefits and Risks. (2020). Cybersecurity Management, 21(2), 112-130. https://doi.org/10.1016/j.cybsec.2020.02.010 (дата звернення 01.06.2024).

РОЗДІЛ 3

РОЗРОБКА МЕТОДІВ УПРАВЛІННЯ ТА ВИЗНАЧЕННЯ ПРІОРИТЕТІВ ІТ-ІНЦИДЕНТІВ

3.1. Розробка методу визначення пріоритетів ІТ-інцидентів

Розроблений метод складається з наступних етапів:

Етап 1. Визначення структури управління ІТ-інцидентами об’єкта критичної інформаційної інфраструктури.

На цьому етапі необхідно створити структуру для управління ІТ-інцидентами, що включає визначення ключових інцидентів та їх класифікацію наприклад, проблеми з фізичними пристроями, програмним забезпеченням, інциденти безпеки, тощо, а також створити відповідну ієрархічну модель.

Етап 2. Оцінка інцидентів та їхніх пріоритетів як на локальному, так і на глобальному рівнях в системі ІТ безпеки

На даному етапі необхідно оцінити пріоритетність кожного ІТ-інциденту, враховуючи його вплив на різні рівні (локальний та глобальний) ІТ-безпеки, застосувавши метод попарних порівнянь (AHP) [1,2] для оцінки впливу кожного інциденту, обчислити локальні та глобальні пріоритети загроз, щоб визначити найбільш критичні для управління та мінімізації ризиків.

Етап 3. Проведення порівнянь елементів системи ІТ безпеки на різних рівнях для оцінки їх впливу та встановлення пріоритетів за допомогою методу попарних порівнянь (AHP).

Крок 3.1. Побудова матриць парних порівнянь

На цьому кроці необхідно сформувати матрицю парних порівнянь, яка дозволяє оцінити відносну важливість кожного критерію чи альтернативи в системі. Цей крок забезпечує структуру для проведення подальших розрахунків. Для цього

створюємо матрицю A розміром n×n, де кожен елемент a_{ij} представляє відношення важливості між критерієм i та критерієм j. Елементи матриці розташовані таким чином:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1i} \\ \vdots & \ddots & \vdots \\ a_{1j} & \cdots & a_{ij} \end{pmatrix} \tag{3.1}$$

де A —матриця попарних порівнянь, a_{ij} — елементи матриці парних порівнянь.

Крок 3.2. Нормалізація матриць парних порівнянь

На цьому кроці необхідно провести нормалізацію матриць парних порівнянь, щоб забезпечити, що сума всіх елементів у кожному стовпці матриці дорівнює 1. Це дозволяє порівняти різні критерії та їхні ваги на основі єдиної шкали.

$$a'_{ij} = \frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}} \tag{3.2}$$

де a'_{ij} — нормалізований елемент матриці парних порівнянь, a_{ij} — початковий елемент матриці парних порівнянь.

Після нормалізації всіх елементів матриці отримуємо нормалізовану матрицю A':

$$A' = \begin{pmatrix} a'_{11} & \cdots & a'_{1i} \\ \vdots & \ddots & \vdots \\ a'_{1j} & \cdots & a'_{ij} \end{pmatrix} \tag{3.3}$$

де, A' — нормалізована матриця попарних порівнянь, a'_{ij} — нормалізований елемент матриці парних порівнянь

Крок 3.3. Обчислення векторів ваг, та вектору Ax

На цьому кроці необхідно обчислити вектори ваг W для кожного критерію на основі нормалізованої матриці парних порівнянь A', що необхідно для визначення

відносної важливості кожного критерію та для подальшого аналізу їхнього впливу на загальний результат.

$$W_i = \frac{1}{n}\sum_{j=1}^{n} a'_{ij} \tag{3.4}$$

де W_i – вагового коефіцієнта для i-го критерію, a'_{ij} — нормалізований елемент матриці парних порівнянь, n – кількість критеріїв.

Для розрахунку вектору, який представляє відносну важливість кожного критерію і буде використаний для подальших розрахунків, скористаємось наступною формулою:

$$W = \begin{pmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{pmatrix} \tag{3.5}$$

де W – це вектори ваг критеріїв порівняння.

Далі, для оцінки узгодженості матриці парних порівнянь і точності визначених вагових коефіцієнтів, що є критично важливим для прийняття обґрунтованих рішень у методі аналізу ієрархій, необхідно розрахувати вектор Ax:

$$Ax = A \times W \tag{3.6}$$

де A — початкова матриця парних порівнянь, W — вектор ваг.

Отже, вектор Ax допомагає нам зрозуміти, як кожен критерій впливає на загальний результат, враховуючи відносну важливість кожного критерію.

Крок 3.4. Розрахунок індексу та коефіцієнту узгодженості

На цьому кроці необхідно розрахувати індекс узгодженості та коефіцієнт узгодженості для перевірки консистентності матриці парних порівнянь, що є

важливим кроком для оцінки надійності прийнятих рішень на основі вагових коефіцієнтів.

Для перевірки консистентності матриці парних порівнянь, що забезпечує логічну узгодженість і надійність визначених вагових коефіцієнтів, розрахуємо найбільше власне число:

$$\lambda_{\max} = \frac{1}{n}\sum_{i=1}^{n}\frac{(Ax)_i}{W_i} \tag{3.7}$$

де $\lambda_{\max}$ — найбільше власне число, n — кількість критеріїв, Ax — елементи векторів, W_i — елементи вектора ваг.

Індекс узгодженості визначає, наскільки узгодженою є матриця парних порівнянь:

$$CI = \frac{\lambda_{\max} - n}{n-1} \tag{3.8}$$

де CI – індекс узгодженості, $\lambda_{\max}$ — найбільше власне число, n — кількість критеріїв.

$$CR = \frac{CI}{RI} \tag{3.9}$$

де CR – коефіцієнт узгодженості, CI – індекс узгодженості, RI – випадковий індекс узгодженості, залежить від кількості критеріїв і визначається таблицею для відповідних значень n.

– Якщо $CR < 0.1$, – матриця парних порівнянь вважається узгодженою.

– Якщо $CR \geq 0.1$, це означає, що матриця має значні розбіжності і потребує перегляду парних порівнянь для досягнення кращої узгодженості.

Цей крок є критичним для забезпечення надійності та обґрунтованості прийнятих рішень, оскільки дозволяє виявити і усунути можливі невідповідності в матриці парних порівнянь.

Етап 4. Синтез локальних і глобальних пріоритетів для системи IT-безпеки

На цьому етапі необхідно синтезувати локальні і глобальні пріоритети для системи ІТ-безпеки, що дозволить визначити загальну важливість кожного альтернативного рішення з урахуванням ваг критеріїв та їхніх пріоритетів.

Для кожного критерію C_i визначаємо локальні пріоритети альтернатив A_j. Локальний пріоритет альтернативи A_j за критерієм C_i позначається як $W_{Ci, Aj}$.

Глобальний пріоритет альтернативи A_j обчислюється як сума добутків ваг критеріїв на локальні пріоритети відповідних альтернатив. Формула для обчислення глобального пріоритету виглядає наступним чином:

$$G_{A_j} = \sum_{i=1}^{m} (W_{C_i} \times W_{C_i, A_j}) \quad (3.10)$$

де G_{A_j} - глобальний пріоритет альтернативи A_j, W_{C_i} - вага критерію C_i, W_{C_i, A_j} - локальний пріоритет альтернативи A_j за критерієм C_i, m – кількість критеріїв.

Після обчислення глобальних пріоритетів для кожної альтернативи, буде отримано вектор глобальних пріоритетів, що дозволяє визначити загальну важливість кожної альтернативи у системі ІТ-безпеки та зробити обґрунтовані висновки щодо вибору найбільш пріоритетних альтернативних рішень для системи ІТ-безпеки. Альтернатива з найвищим глобальним пріоритетом має найбільшу важливість і повинна отримати пріоритет при реалізації.

Етап 5. Отримання результатів оцінки та коригування пріоритетів ІТ-безпеки

На цьому етапі необхідно обчислити остаточні результати оцінки пріоритетів для системи ІТ-безпеки та при необхідності коригуємо ці пріоритети. Це забезпечує точне і обґрунтоване визначення найважливіших аспектів для захисту критичної інформаційної інфраструктури.

$$\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{n1} & a'_{n2} & \cdots & a'_{nn} \end{pmatrix} \times \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} a'_{11}w_1 + a'_{12}w_2 + \cdots + a'_{1n}w_n \\ a'_{21}w_1 + a'_{22}w_2 + \cdots + a'_{2n}w_n \\ \vdots \\ a'_{n1}w_1 + a'_{n2}w_2 + \cdots + a'_{nn}w_n \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{pmatrix} \qquad (3.11)$$

де a_{ij} – елемент матриці парних порівнянь, а i — номер рядка, j — номер стовпця, a'_{ij} – нормалізований елемент матриці парних порівнянь, w_1, w_2,… w_n – вагові коефіцієнти (пріоритети), що визначаються для кожного критерію, Y_1, Y_2,… Y_n – результати, отримані після множення нормалізованої матриці на вектор вагових коефіцієнтів.

Отримані результати Y_1, Y_2,… Y_n відображають відносну важливість кожного критерію або альтернативи в контексті ІТ-безпеки. Аналіз цих результатів дозволяє визначити, які аспекти потребують найбільшої уваги і ресурсів для забезпечення ефективного захисту.

На основі отриманих і скоригованих результатів приймаються рішення щодо пріоритетних напрямків захисту щодо ІТ-інцидентів. Це допомагає ефективно розподілити ресурси і зосередитися на найбільш критичних аспектах захисту критичної інформаційної інфраструктури.

Схема реалізації розробленого методу відображена на рис. 3.1:

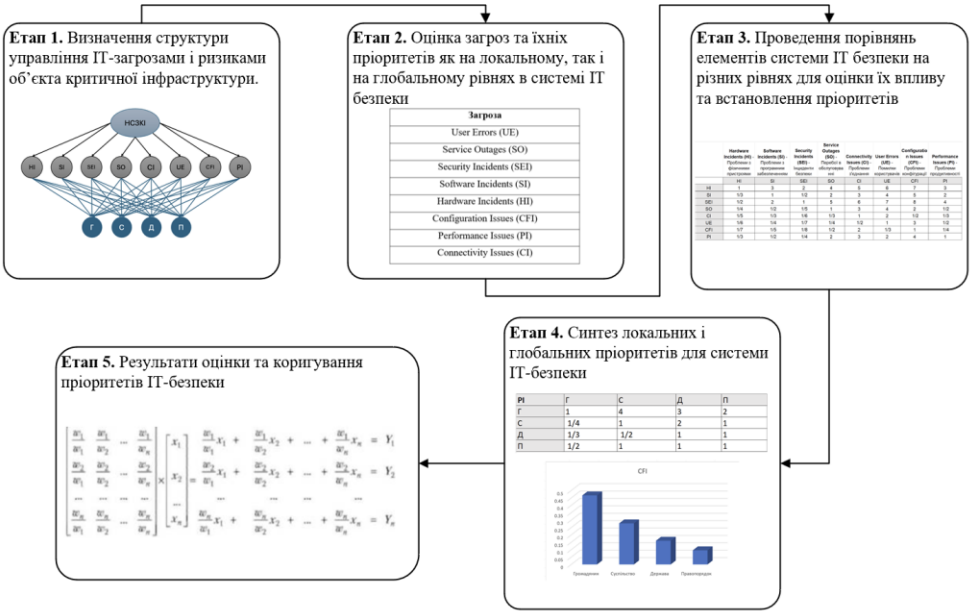


Рис. 3.1. Схема реалізації методу визначення пріоритетів IT-загроз

3.2. Розробка методу управління IT-загрозами на об'єктах критичної інформаційної інфраструктури

Запропонований метод складається з наступних 7 етапів (схема реалізації відображена на рис. 3.2)**.**

Етап 1. Ідентифікація IT-загроз для об'єктів критичної інформаційної інфраструктури.

Етап 2. Визначення критеріїв оцінки IT-загроз для критичної інформаційної інфраструктури.

Етап 3. Отримання та нормалізація даних IT-загроз для критичної інформаційної інфраструктури.

Етап 4. Визначення вагових коефіцієнтів критеріїв для IT-загроз критичної інформаційної інфраструктури.

Етап 5. Проведення парних порівнянь альтернативних загроз для критичної інформаційної інфраструктури.

Етап 6. Отримання інтегративної оцінки альтернативних ІТ-загроз для критичної інформаційної інфраструктури.

Етап 7. Пріоритизація та ухвалення рішень щодо ІТ-загроз для критичної інформаційної інфраструктури.

Отже, розглянемо кожний етап методу детальніше:

Етап 1. Ідентифікація ІТ-загроз для ОКІІ.

Ідентифікація ІТ-загроз є важливим етапом у процесі управління ІТ-загрозами для ОКІІ. Метою цього етапу є виявлення потенційних загроз, які можуть вплинути на нормальну роботу критичних інформаційних систем. На цьому етапі можна вибрати загрози за різними міжнародними підходами, такими як STRIDE, NIST SP 800-30, ISO/IEC 27005, OCTAVE або COBIT, в залежності від особливостей ОКІІ. Позначимо множину потенційних ІТ загроз як множину U_i:

$$U_i = \{U_1, U_2, \ldots, U_n\} \tag{3.12}$$

де U_i:– сукупність ідентифікованих потенційних ІТ-загроз, $U_1, U_2, \ldots, U_n$ - це конкретні потенційні ІТ-загрози.

Етап 2. Визначення критеріїв оцінки ІТ-загроз для КІІ.

Для кожної загрози U_i та кожного критерію k, введемо множину критеріїв оцінки K:

$$K = \{k_1, k_2, \ldots, k_m\} \tag{3.13}$$

де K - це множина критеріїв, за якими буде проводитися оцінка ІТ-загроз, $k_1, k_2, \ldots, k_m$ - це конкретні критерії оцінки.

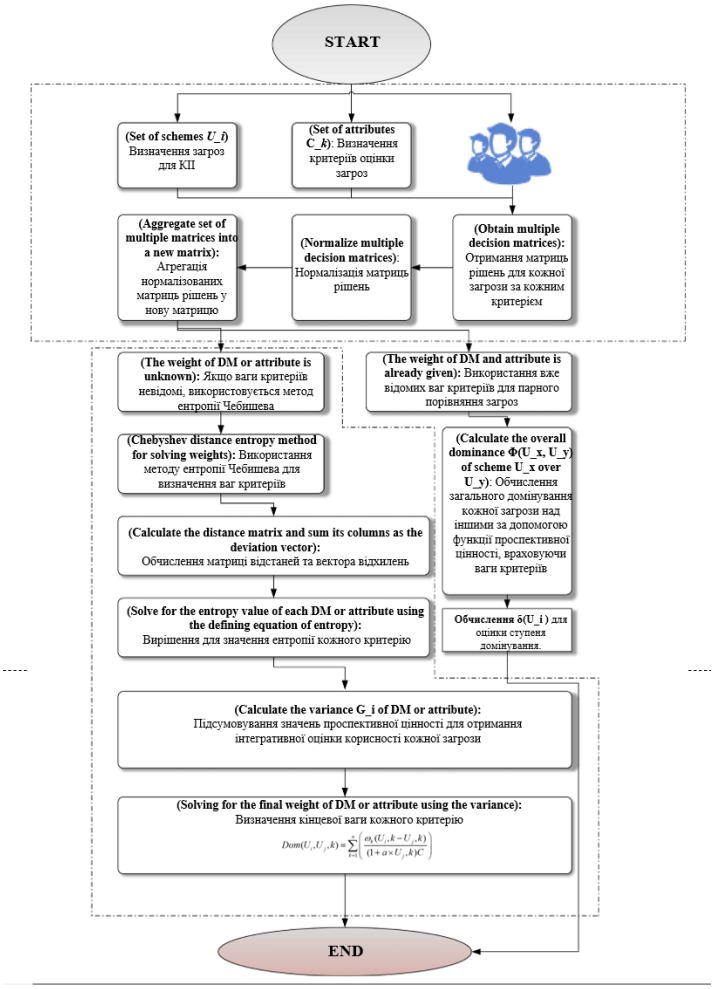


Рис. 3.2. Схема реалізації методу управління ІТ-загрозами

Кожна потенційна загроза U_i повинна бути оцінена за критеріями K, що дозволить визначити її вплив та пріоритетність.

$$vU_i, k, \tag{3.14}$$

де vU_i,k — оцінка i-ї загрози за k-им критерієм, Ui — i-та загроза, k — критерій оцінки.

Етап 3. Отримання та нормалізація даних ІТ-загроз для КІІ.

На цьому етапі необхідно провести збір, оцінку та нормалізацію даних щодо ІТ-загроз для КІІ. Цей процес забезпечує об'єктивність та збалансованість підходу до оцінки загроз. Кожна загроза U_i оцінюється за визначеними критеріями K.

Наприклад, експерти можуть оцінити ймовірність виникнення загрози, можливий збиток, складність реалізації тощо. Кожен критерій оцінки k має відповідний ваговий коефіцієнт w_k, де сума всіх коефіцієнтів дорівнює 1:

$$\sum_{k=1}^{K} \omega_k = 1, \tag{3.15}$$

де K – загальна кількість критеріїв, w_k – ваговий коефіцієнт для критерію k.

Етап 4. Визначення вагових коефіцієнтів критеріїв для ІТ-загроз КІІ.

Визначення вагових коефіцієнтів для кожного критерію оцінки ІТ-загроз є важливим кроком, що дозволить врахувати відносну важливість різних аспектів загроз. Це допомагає забезпечити об'єктивність і збалансованість у процесі оцінювання ІТ-загроз. Кожен критерій оцінюється за попередньо встановленою шкалою. Автори у своїй роботі пропонують застосовувати шкалу від 1 до 5, де 5 вказує на найвищу ймовірність, шкоду або складність, а 1 - на найнижчу. Така шкала є інтуїтивно зрозумілою та легкою для використання, що спрощує процес оцінки для експертів. Для кожного критерію обчислюємо середнє геометричне оцінок, наданих експертами наступним чином:

$$k = (\prod_{j=1}^{n} \nu k_j)^{1/n} \tag{3.16}$$

де νk_j - оцінка критерію k експертом j, n - кількість експертів.

Далі, на цьому етапі створюємо вектор вагових коефіцієнтів та обчислюємо їх шляхом нормалізації середніх геометричних оцінок:

$$W = (W_1, W_2, \ldots, W_n)^T \tag{3.17}$$

де W_i – це ваговий коефіцієнт для кожного критерію i.

$$W_{jr} = \frac{W_j}{\sum_{r=1}^{n} W_r} \tag{3.18}$$

де W_j – середнє геометричне для критерію j, W_r – сума середніх геометричних для всіх критеріїв.

Етап 5. Проведення парних порівнянь альтернативних загроз для КІІ.

Використовуємо парне порівняння для визначення домінування кожної загрози над іншими, застосовуючи функцію проспективної цінності, яка враховує ваги критеріїв і оцінки альтернатив за кожним критерієм.

$$Dom(U_i, U_j, k) = \omega_k \times \left(\frac{\nu U_i, k - \nu U_j, k}{1 + a \times \nu U_j, k} \right), \tag{3.19}$$

де U_i та U_j — загрози, які порівнюються; k — критерій, за яким ведеться порівняння; W_k — вага критерію; vUi,k та vUj,k — оцінки загроз за критерієм; α — параметр, який відображає ставлення до ризику.

Врахування категорій ОКІ

Відповідно до Закону України «Про критичну інфраструктуру» [15], зокрема відповідно до Статті 10 "Категоризація ОКІ", ОКІ поділяються на категорії залежно від їхньої важливості та потенційного впливу на безпеку держави чи регіону. Введення змінної критичності C дозволяє інтегрувати ці категорії як додаткові критерії у багатокритеріальний аналіз за розробленим методом, що підвищує точність оцінки потенційного впливу загроз на різні рівні критичності.

Змінна критичності C приймає значення від 1 до 4, які відображають рівень критичності об'єкту інфраструктури: Категорія I **(C=1)**: Особливо важливі об'єкти з загальнодержавним значенням. Порушення їхнього функціонування може спричинити кризу державного масштабу. Категорія II **(C=2)**: Життєво важливі

об'єкти, чиє порушення може викликати регіональну кризу. Категорія III **(C=3)**: Важливі об'єкти, порушення яких може призвести до місцевої кризи. Категорія IV **(C=4)**: Необхідні об'єкти, чиє порушення може викликати локальні кризові ситуації.

$$Dom(U_i, U_j, k) = \sum_{k=1}^{n} \left(\frac{\omega_k(U_i, k - U_j, k)}{(1 + a \times U_j, k)C} \right) \tag{3.20}$$

де U_i та U_j — загрози, які порівнюються; k — критерій, за яким ведеться порівняння; W_k — вага критерію; vUi,k та vUj,k — оцінки загроз за критерієм; α — параметр, який відображає ставлення до ризику, C – змінна критичності.

Етап 6. Отримання інтегративної оцінки альтернативних ІТ-загроз для КІІ.

На даному етапі необхідно вирахувати значення проспективної цінності, щоб отримати оцінку корисності для кожної загрози.

$$Score(U_i) = \sum_{j \neq i} \sum_{k=1}^{K} Dom(U_i, U_j, k) \tag{3.21}$$

де Score(U_i) - інтегративна оцінка корисності для загрози a.

Етап 7. Пріоритизація та ухвалення рішень щодо ІТ-загроз для КІІ.

На даному етапі необхідно провести пріоритизацію виявлених ІТ-загроз та ухвалити відповідні рішення щодо заходів з їхнього усунення або мінімізації. Це досягається шляхом обчислення відносної важливості кожної загрози та ранжування їх на основі отриманих оцінок.

$$p(U_i) = \frac{Score(U_i)}{\sum_{i=1}^{n} Score(U_i)} \tag{3.22}$$

де $p(U_i)$ - відносна важливість кожної потенційної ІТ-загрози.

Далі, ІТ-загрози необхідно ранжувати від найвищого до найнижчого значення $p(U_i)$. Загрози з найвищими значеннями є найбільш критичними і потребують

першочергового реагування. Виходячи з результату ранжування загроз, ухвалюються рішення щодо необхідних заходів для усунення або мінімізації кожної загрози. Це можуть бути технічні, організаційні або процедурні заходи.

3.3. Висновки до третього розділу

У даному розділі було удосконалено метод визначення пріоритетів ІТ-інцидентів шляхом представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації та розроблено метод оцінювання ІТ-загроз, який за рахунок синтезу методів багатокритеріального прийняття рішень, моделювання загроз та функції проспективної цінності, дозволяє ідентифікувати, оцінювати та пріоритизувати ІТ-загрози для оптимального розподілу ресурсів захисту критичної інфраструктури держави

3.4. Список літератури до третього розділу

1. Качинський А.Б., Варичева Д.І., Свириденко С.В. (2016). Ефективне управління ІТ-інцидентами в критичній інформаційній інфраструктурі. Інформація і право, № 2(17), с. 114-126.

2. Nosal, K., & Solecka, K. (2014). Application of AHP method for multi-criteria evaluation of variants of the integration of urban public transport. Transportation Research Procedia, 3, 269–278. URL: https://doi.org/10.1016/j.trpro.2014.10.006 (дата звернення: 11.06.2024).

3. Saaty, T. L. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1), 83. https://doi.org/10.1504/ijssci.2008.017590

4. T. Lechachenko, T. Gancarczyk, T. Lobur, A. Postoliuk. “Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems”. CITI 2023: 250-256.

5. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016). Threat and risk assessment methodologies in the automotive domain. Procedia Computer Science, 83, 1288–1294. https://doi.org/10.1016/j.procs.2016.04.268

6. G. Holtrup, W. Blonay, M. Strohmeier, A. Mermoud, J. -P. Chavanne and V. Lenders, "Modeling 5G Threat Scenarios for Critical Infrastructure Protection," 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia, 2023, pp. 161-180, doi: 10.23919/CyCon58705.2023.10

7. R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 2017, pp. 1-6, doi: 10.1109/ISGTEurope.2017.8260283.

8. Wang J, Wei G, Lu M. TODIM Method for Multiple Attribute Group Decision Making under 2-Tuple Linguistic Neutrosophic Environment. Symmetry. 2018; 10(10):486. https://doi.org/10.3390/sym10100486

9. M. Abomhara, M. Gerdes, and G. M. Koien, “A STRIDE-Based Threat Model for Telehealth Systems”, NISK, 2015.

10. Microsoft Corporation. The STRIDE Threat Model, 2005.

11. Ross, R. (2012). Guide for Conducting Risk Assessments, Special Publication (NIST SP) 800-30 Rev 1. National Institute of Standards and Technology, Gaithersburg, MD. Available at NIST.

12. International Organization for Standardization. (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO. Available at ISO.

13. Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University, Software Engineering Institute. Available at SEI CMU.

14. ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association (ISACA). Available at ISACA.

15. Llamazares, B. (2018). An analysis of the generalized TODIM method. European Journal of Operational Research, 269(3), 1041–1049. https://doi.org/10.1016/j.ejor.2018.02.054

16. Tzeng, G. H., & Huang, J. J. (2011). Multiple attribute decision making: methods and applications. CRC press.

17. Положенцев А. А., Сидоренко В. М. Метод управління ІТ-загрозами на об’єктах критичної інформаційної інфраструктури. *Наукоємні технології*. 2024. Т. 2, № 62. С. 121–133.

18. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління. 2024. Т. 2. №78. С. 68-80.

РОЗДІЛ 4

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ МЕТОДІВ УПРАВЛІННЯ ІТ-ІНЦИДЕНТАМИ

4.1. Експериментальне дослідження методу визначення стану захищеності об’єктів критичної інфраструктури та його практична реалізація

Застосуємо розроблений метод на прикладі сектору КІ держави «Цифрові технології». Згідно з Законом України «Про критичну інфраструктуру» [1-2], до них найчастіше відносять системи та мережі електронного урядування, інформаційні системи органів державної влади, державні реєстри, електронні платформи для надання публічних послуг, а також критичні елементи національних інформаційних та телекомунікаційних мереж. Наприклад, це можуть бути Державний реєстр виборців, Єдина державна електронна система у сфері будівництва, платформа "Дія", системи забезпечення електронного документообігу у державних установах, а також мережі національних операторів зв'язку.

Етап 1. Визначення загальних метрик ІТ-безпеки для об’єкту КІІ у секторі «Цифрові технології».

Крок 1.1. Формування множин метрик ІТ-безпеки для ОКІІ. При $n = 3$, визначимо повну множину метрик ІТ-безпеки наступним чином, відповідно до (2.1):

$$\mathbf{P}_{ITSec} = \{\bigcup_{i=1}^{3} \mathbf{P}_i\} = \{\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3\} = \{\mathbf{P}_{GSI}, \mathbf{P}_{SRI}, \mathbf{P}_{RMI}\} \quad (4.1)$$

де $\mathbf{P}_1 = \mathbf{P}_{GSI}$ – множина стратегічних індикаторів ІТ-управління, $\mathbf{P}_2 = \mathbf{P}_{SRI}$ – множина профілактичних індикаторів управління ІТ, $\mathbf{P}_3 = \mathbf{P}_{RMI}$ – множина реагуючих індикаторів управління ІТ.

При n=3, m_1=4, представимо множину $\mathbf{P}_1 = \mathbf{P}_{GSI}$ у такому вигляді:

$$\mathbf{P}_1 = \mathbf{P}_{GSI} = \{\bigcup_{j=1}^{4} P_{1j}\} = \{P_{11}, P_{12}, P_{13}, P_{14}\} = \{P_{ITP}, P_{GCI}, P_{EPD}, P_{ITRD}\}, \quad (4.2)$$

де $P_{11} = P_{ITP}$ – множина індикаторів IT-політики, $P_{12} = P_{GCI}$ – множина індикаторів глобального внеску в IT, $P_{13} = P_{EPD}$ – множина індикаторів освіти та професійного розвитку в IT, $P_{14} = P_{ITRD}$ - множина індикаторів дослідження та розвитку в IT.

Аналогічно до $\mathbf{P}_1 = \mathbf{P}_{GSI}$, представимо $\mathbf{P}_2 = \mathbf{P}_{SRI}$ при $m_2 = 4$:

$$\mathbf{P}_2 = \mathbf{P}_{SRI} = \{\bigcup_{j=1}^{4} P_{2j}\} = \{P_{21}, P_{22}, P_{23}, P_{24}\} = \{P_{CII}, P_{DE}, P_{TAA}, P_{PD}\}, \quad (4.3)$$

де $P_{21} = P_{CII}$ – множина індикаторів стійкості IT Інфраструктури, $P_{22} = P_{DE}$ – множина індикаторів безпеки та управління цифровими засобами, $P_{23} = P_{TAA}$ – множина індикаторів аналізу IT-загроз, $P_{24} = P_{PD}$ - множина індикаторів захисту даних та приватності.

Аналогічно, представимо $\mathbf{P}_3 = \mathbf{P}_{RMI}$, при m_3=4:

$$\mathbf{P}_3 = \mathbf{P}_{RMI} = \{\bigcup_{j=1}^{4} P_{3j}\} = \{P_{31}, P_{32}, P_{33}, P_{34}\} = \{P_{IRM}, P_{CCM}, P_{FCT}, P_{MCD}\}, \quad (4.4)$$

де $P_{31} = P_{IRM}$ – множина індикаторів управління IT Інцидентами, $P_{32} = P_{CCM}$ – множина індикаторів управління IT-кризами, $P_{33} = P_{FCT}$ – множина індикаторів злочинності та шахрайства в IT, $P_{34} = P_{MCD}$ - множина індикаторів залучення IT в забезпечення оборони.

З урахуванням визначених метрик, множина **P** може бути представлена у вигляді:

$$\mathbf{P} = \{\bigcup_{i=1}^{3} \mathbf{P}_i\} = \{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{m_i} P_{ij}\}\} = \{\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3\} = \{\mathbf{P}_{GSI}, \mathbf{P}_{SRI}, \mathbf{P}_{RMI}\} =$$
$$= \{\{P_{11}, P_{12}, P_{13}, P_{14}\}, \{P_{21}, P_{22}, P_{23}, P_{24}\}, \{P_{31}, P_{32}, P_{33}, P_{34}\}\} = \quad (4.5)$$
$$= \{\{P_{ITP}, P_{GCI}, P_{EPD}, P_{ITRD}\}, \{P_{CII}, P_{DE}, P_{TAA}, P_{PD}\}, \{P_{IRM}, P_{CCM}, P_{FCT}, P_{MCD}\}\}, (i = \overline{1,n}, j = \overline{1,m_i}).$$

Відповідно до [3,4], можемо представити множини $\mathbf{P}_{GSI}, \mathbf{P}_{SRI}, \mathbf{P}_{RMI}$ у вигляді підмножин, з індексами $(i = 1,\overline{n}, j = 1,\overline{m_i}, s = 1,\overline{l_{i.j}})$:

Отже, множина $\mathbf{P}_1 = \mathbf{P}_{GSI}$ при n=3, $m_1 = 4$ а $l_{1.1}$=5, $l_{1.2}$=3, $l_{1.3}$=5, $s_{1.4}$=2 може бути представлена наступним чином:

$$P_{1.1=}\{\bigcup_{s=1}^{5} P_{1.1.s}\} = \{P_{1.1.1}, P_{1.1.2}, P_{1.1.3}, P_{1.1.4}, P_{1.1.5}\} =$$
$$= \{ITP_{IL}, ITP_{PD}, ITP_{PC}, IPT_{NIS}, IPT_{NISA}\} \quad (4.6)$$

де $P_{1.1.1} = ITP_{IL}$ – Лідерство в IT на вищому рівні ($ITP_{IL} \in [0;3]$), $P_{1.1.2} = ITP_{PD}$ – Розроблення IT політики ($ITP_{PD} \in [0;3]$), $P_{1.1.3} = ITP_{PC}$ – Координація IT політики між відділами ($ITP_{PC} \in [0;3]$), $P_{1.1.4} = ITP_{NIS}$ - Національна IT стратегія ($ITP_{NIS} \in [0;3]$), $P_{1.1.5} = ITP_{NISA}$ - План дій для реалізації національної IT стратегії ($ITP_{NISA} \in [0;3]$).

$$P_{1.2=}\{\bigcup_{s=1}^{3} P_{1.2.s}\} = \{P_{1.2.1}, P_{1.2.2}, P_{1.2.3}\} = \{GCI_{ID}, GCI_{IL}, GCI_{CB}\} \quad (4.7)$$

де $P_{1.2.1} = GCI_{ID}$ – IT дипломатія та міжнародна співпраця ($GCI_{ID} \in [0;3]$), $P_{1.2.2} = GCI_{IL}$ – Дотримання міжнародних IT стандартів і законів ($GCI_{IL} \in [0;1]$), $P_{1.2.3} = GCI_{CB}$ – Внесок у міжнародний розвиток IT потенціалу ($GCI_{CB} \in [0;2]$).

$$P_{1.3} = \{\bigcup_{s=1}^{5} P_{1.3.s}\} = \{P_{1.3.1}, P_{1.3.2}, P_{1.3.3}, P_{1.3.4}, P_{1.3.5}\} =$$
$$= \{EPD_{CPE}, EPD_{CSE}, EPD_{UE}, EPD_{GE}, EPD_{AITP}\} \quad (4.8)$$

де $P_{1.3.1} = EPD_{CPE}$ – Компетенції з ІТ у початковій освіті ($EPD_{CPE} \in [0;2]$), $P_{1.3.2} = EPD_{CSE}$ – Компетенції з ІТ у середній освіті ($EPD_{CSE} \in [0;2]$), $P_{1.3.3} = EPD_{UE}$ – Освіта в ІТ на рівні бакалаврату ($EPD_{UE} \in [0;2]$), $P_{1.3.4} = EPD_{GE}$ – Освіта в ІТ на рівні магістратури та наукові програми ($EPD_{GE} \in [0;3]$), $P_{1.3.5} = EPD_{AITP}$ – Асоціація Професіоналів в ІТ-сфері ($EPD_{AITP} \in [0;1]$).

$$P_{1.4} = \{\bigcup_{s=1}^{2} P_{1.4.s}\} = \{P_{1.4.1}, P_{1.4.2}\} = \{ITRD_{RDP}, ITRD_{DS}\} \tag{4.9}$$

де $P_{1.4.1} = ITRD_{RDP}$ – Програми досліджень та інновацій в ІТ ($ITRD_{RDP} \in [0;2]$), $P_{1.4.2} = ITRD_{DS}$ – Докторські студії в галузі ІТ ($ITRD_{DS} \in [0;2]$).

Аналогічно до $\mathbf{P}_{GSI}$, множина $\mathbf{P}_2 = \mathbf{P}_{SRI}$ при $m_2 = 4$, $s_{2.1}$=4, $s_{2.2}$=6, $s_{2.3}$=4, $s_{2.4}$=2 може бути представлена наступним чином:

$$P_{2.1=}\{\bigcup_{s=1}^{4} P_{2.1.s}\} = \{P_{2.1.1}, P_{2.1.2}, P_{2.1.3}, P_{2.1.4}\} = \{CII_{II}, CII_{CRO}, CII_{CRP}, CII_{CSA}\} \tag{4.10}$$

де $P_{2.1.1} = CII_{II}$ – Ідентифікація та управління критичною ІТ інфраструктурою ($CII_{II} \in [0;3]$), $P_{2.1.2} = CII_{CRO}$ – Вимоги до стійкості операторів ІТ інфраструктури ($CII_{CRO} \in [0;3]$), $P_{2.1.3} = CII_{CRP}$ – Планування стійкості для ІТ сервісів державного сектору ($CII_{CRP} \in [0;3]$), $P_{2.1.4} = CII_{CSA}$ - Уповноважений орган нагляду за ІТ інфраструктурою ($CII_{CSA} \in [0;3]$).

$$\begin{aligned} P_{2.2} &= \{\bigcup_{s=1}^{6} P_{2.2.s}\} = \{P_{2.1.1}, P_{2.1.2}, P_{2.1.3}, P_{2.1.4}, P_{2.1.5}, P_{2.1.6}\} = \\ &= \{DE_{SEI}, DE_{ES}, DE_{TS}, DE_{STS}, DE_{CCS}, DE_{SCS}\} \end{aligned} \tag{4.11}$$

де $P_{2.2.1} = DE_{SEI}$ – Управління безпечною електронною ідентифікацією ($DE_{SEI} \in [0;2]$), $P_{2.2.2} = DE_{ES}$ – Послуги електронного підпису ($DE_{ES} \in [0;2]$), $P_{2.2.3} = DE_{TS}$ – Автентифікація та довірчі послуги ($DE_{TS} \in [0;2]$), $P_{2.2.4} = DE_{STS}$ - Регуляторний орган цифрових послуг ($DE_{STS} \in [0;2]$), $P_{2.2.5} = DE_{CCS}$ - Управління та безпека хмарних сервісів ($DE_{CCS} \in [0;2]$), $P_{2.2.6} = DE_{SCS}$ - Управління та безпека ланцюгів поставок ІТ ($DE_{SCS} \in [0;2]$).

$$P_{2.3} = \{\bigcup_{s=1}^{4} P_{2.3.s}\} = \{P_{2.3.1}, P_{2.3.2}, P_{2.3.3}, P_{2.3.4}\} = \\ = \{TAA_{ITA}, TAA_{PTR}, TAA_{PAR}, TAA_{CAR}\} \tag{4.12}$$

де $P_{2.3.1} = TAA_{ITA}$ – Аналіз ІТ загроз і ризиків ($TAA_{ITA} \in [0;3]$), $P_{2.3.2} = TAA_{PTR}$ – Публічне звітування про ІТ загрози ($TAA_{PTR} \in [0;3]$), $P_{2.3.3} = TAA_{PAR}$ – Публічна освіта та підвищення обізнаності з ІТ ($TAA_{PAR} \in [0;3]$), $P_{2.3.4} = TAA_{CAR}$ - Координація програм з підвищення обізнаності з ІТ ($TAA_{CAR} \in [0;3]$).

$$P_{2.4} = \{\bigcup_{s=1}^{2} P_{2.4.s}\} = \{P_{2.4.1}, P_{2.4.2}\} = \{PD_{PDL}, PD_{PDA}\} \tag{4.13}$$

де $P_{2.4.1} = PD_{PDL}$ – Законодавство та відповідність у сфері захисту даних ($PD_{PDL} \in [0;2]$), $P_{2.4.2} = PD_{PDA}$ – Орган захисту даних та нагляд ($PD_{PDA} \in [0;2]$).

Аналогічно, множина $\mathbf{P}_3 = \mathbf{P}_{RMI}$ при $m_3 = 4$, $s_{2.1}$=5, $s_{2.2}$=4, $s_{2.3}$=6, $s_{2.4}$=3 може бути представлена наступним чином:

$$P_{3.1=}\{\bigcup_{s=1}^{5} P_{3.1.s}\} = \{P_{3.1.1}, P_{3.1.2}, P_{3.1.3}, P_{3.1.4}, P_{3.1.5}\} = \\ = \{IRM_{NIM}, IRM_{IRO}, IRM_{IRT}, IRM_{SPC}, IRM_{PIIC}\} \tag{4.14}$$

де $P_{3.1.1} = IRM_{NIM}$ – Національна спроможність управління ІТ інцидентами ($IRM_{NIM} \in [0;3]$), $P_{3.1.2} = IRM_{IRO}$ – Механізми звітування про ІТ інциденти ($IRM_{IRO} \in [0;3]$), $P_{3.1.3} = IRM_{IRT}$ – Інструменти для відстеження та аналізу ІТ інцидентів ($IRM_{IRT} \in [0;2]$), $P_{3.1.4} = IRM_{SPC}$ - Центральна точка координації ІТ інцидентів ($IRM_{SPC} \in [0;3]$), $P_{3.1.5} = IRM_{PIIC}$ - Міжнародна співпраця у сфері управління ІТ інцидентами ($IRM_{PIIC} \in [0;3]$).

$$P_{3.2} = \{\bigcup_{s=1}^{4} P_{3.2.s}\} = \{P_{3.2.1}, P_{3.2.2}, P_{3.2.3}, P_{3.2.4}\} = \{CCM_{CMP}, CCM_{NCM}, CCM_{ICM}, CCM_{OCR}\} \quad (4.15)$$

де $P_{3.2.1} = CCM_{CMP}$ – Планування управління ІТ кризами та відновлення ($CCM_{CMP} \in [0;2]$), $P_{3.2.2} = CCM_{NCM}$ – Національні тренування та симуляції ІТ криз ($CCM_{NCM} \in [0;3]$), $P_{3.2.3} = CCM_{ICM}$ – Міжнародні вправи з управління ІТ кризами ($CCM_{ICM} \in [0;2]$), $P_{3.2.4} = CCM_{OCR}$ - Резерви оперативної неперервності ІТ сервісів ($CCM_{OCR} \in [0;2]$).

$$\begin{aligned} P_{3.3} &= \{\bigcup_{s=1}^{6} P_{3.3.s}\} = \{P_{3.3.1}, P_{3.3.2}, P_{3.3.3}, P_{3.3.4}, P_{3.3.5}, P_{3.3.6}\} = \\ &= \{FCT_{ITL}, FTC_{PLP}, FCT_{CC}, FCT_{CIC}, FCT_{DFC}, FCT_{CPI}\} \end{aligned} \quad (4.16)$$

де $P_{3.3.1} = FCT_{ITL}$ – Правові порушення та дотримання у сфері ІТ ($FCT_{ITL} \in [0;3]$), $P_{3.3.2} = FCT_{PLP}$ – Процесуальні правила для розслідування ІТ злочинів ($FCT_{PLP} \in [0;3]$), $P_{3.3.3} = FCT_{CC}$ – Дотримання міжнародних конвенцій щодо ІТ злочинності ($FCT_{CC} \in [0;2]$), $P_{3.3.4} = FCT_{CIC}$ - Спроможності розслідування ІТ злочині ($FCT_{CIC} \in [0;3]$), $P_{3.3.5} = FCT_{DFC}$ - Спроможності цифрової форензики для ІТ

інцидентів ($FCT_{DFC} \in [0;2]$), $P_{3.3.6} = FCT_{CPI}$ - Цілодобова координація реагування на ІТ злочинність ($FCT_{CPI} \in [0;3]$).

$$P_{3.4} = \{\bigcup_{s=1}^{3} P_{3.4.s}\} = \{P_{3.4.1}, P_{3.4.2}, P_{3.4.3}\} = \{MCD_{MCR}, MCD_{MD}, MCD_{MDE}\} \qquad (4.17)$$

де $P_{3.4.1} = MCD_{MCR}$ – Спроможності та готовність військової оборони ІТ ($MCD_{MCR} \in [0;2]$), $P_{3.4.2} = MCD_{MD}$ – Доктрина та стратегія військової оборони ІТ ($MCD_{MD} \in [0;2]$), $P_{3.4.3} = MCD_{MDE}$ – Навчання та вправи військової оборони ІТ ($MCD_{MDE} \in [0;2]$).

Отже, відповідно до [3,4] виконаємо оцінювання показників $\mathbf{P}_{ITSec}$ сектору КІ «цифрові технології»:

У табл. 4.1 відобразимо Стратегічні індикатори ІТ-Управління $\mathbf{P}_{GSI}$, а саме GSI_{ITP}

Таблиця 4.1

Стратегічні індикатори ІТ-Управління

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
GSI_{ITP} - **ІТ Політика**	**15**	**10**
ITP_{IL} - Лідерство в ІТ на вищому рівні	3	2
ITP_{PD} - Розроблення ІТ політики	3	2
ITP_{PC} - Координація ІТ політики між відділами	3	2
IPT_{NIS} - Національна ІТ стратегія	3	2
IPT_{NISA} - План дій для реалізації національної ІТ стратегії	3	2

Аналогічно, проведемо оцінювання індикаторів GSI_{GCI} - Глобальний внесок в IT, табл. 4.2:

Таблиця 4.2

Індикатори Глобальний внесок в IT

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
GSI_{GCI} - **Глобальний Внесок в IT**	**6**	**4**
GCI_{ID} - IT дипломатія та міжнародна співпраця	3	2
GCI_{IL} - Дотримання міжнародних IT стандартів і законів	1	1
GCI_{CB} - Внесок у міжнародний розвиток IT потенціалу	2	1

У табл. 4.3 відобразимо оцінювання індикаторів GSI_{EPD} - Освіта та професійний розвиток в IT:

Таблиця 4.3

Освіта та професійний розвиток в IT

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
GSI_{EPD} - **Освіта та професійний розвиток в IT**	**10**	**9**
EPD_{CPE} - Компетенції з IT у початковій освіті	2	2
EPD_{CSE} - Компетенції з IT у середній освіті	2	2
EPD_{UE} - Освіта в IT на рівні бакалаврату	2	2
EPD_{GE} - Освіта в IT на рівні магістратури та наукові програми	3	2
EPD_{AITP} - Асоціація Професіоналів в IT-сфері	1	1

У табл. 4.4 відобразимо оцінювання індикаторів GSI_{ITRD} - Дослідження та Розвиток в ІТ:

Таблиця 4.4

Дослідження та Розвиток в ІТ

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
GSI_{ITRD} - **Дослідження та Розвиток в ІТ**	**4**	**3**
$ITRD_{RDP}$ - Програми досліджень та інновацій в ІТ	2	2
$ITRD_{DS}$ - Докторські студії в галузі ІТ	2	1

Аналогічно, відповідно до [3,4] виконаємо оцінювання показників Профілактичні індикатори ІТ-Управління $\mathbf{P}_{SRI}$, а саме SRI_{CII} , SRI_{DE} , SRI_{TAA} та SRI_{PD} .

У табл. 4.5 відобразимо оцінювання Профілактичних індикаторів ІТ-Управління:

Таблиця 4.5

Профілактичні індикатори ІТ-Управління

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
SRI_{CII} - **Стійкість ІТ Інфраструктури**	**12**	**8**
CII_{II} - Розроблення ІТ політики	3	2
CII_{CRO} - Вимоги до стійкості операторів ІТ інфраструктури	3	2
CII_{CRP} - Планування стійкості для ІТ сервісів державного сектору	3	2
CII_{CSA} - Уповноважений орган нагляду за ІТ інфраструктурою	3	2

Аналогічно, проведемо оцінювання індикаторів SRI_{DE} - Безпека та управління цифровими засобами, відповідно до табл. 4.6:

Таблиця 4.6

Безпека та управління цифровими засобами

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
SRI_{DE} - **Безпека та управління цифровими засобами**	**12**	**10**
DE_{SEI} - IT дипломатія та міжнародна співпраця	2	1
DE_{ES} - Послуги електронного підпису	2	1
DE_{TS} - Автентифікація та послуги довіри	2	2
DE_{STS} - Регуляторний орган цифрових послуг	2	2
DE_{CCS} - Управління та безпека хмарних сервісів	2	2
DE_{SCS} -Управління та безпека ланцюгів поставок IT	2	2

У табл. 4.7 відобразимо оцінювання індикаторів SRI_{TAA} - Аналіз та освіта щодо IT загроз:

Таблиця 4.7

Аналіз та освіта щодо ІТ загроз

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
SRI_{TAA} - **Аналіз та освіта щодо ІТ загроз**	**12**	**8**
TAA_{ITA} - Аналіз ІТ загроз і ризиків	3	2
TAA_{PTR} - Публічне звітування про ІТ загрози	3	2
TAA_{PAR} - Публічна освіта та підвищення обізнаності з ІТ	3	2
TAA_{CAR} - Координація програм з підвищення обізнаності з ІТ	3	2

Аналогічно, відобразимо оцінювання індикаторів SRI_{PD} - Захист даних та приватності, у табл. 4.8:

Таблиця 4.8

Захист даних та приватності

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
SRI_{PD} - **Захист даних та приватності**	**4**	**3**
PD_{PDL} - Законодавство та відповідність у сфері захисту даних	2	1
PD_{PDA} - Орган захисту даних та нагляд	2	2

Аналогічно, виконаємо оцінювання показників Реагуючі індикатори ІТ-Управління $\mathbf{P}_{RMI}$, а саме RMI_{IRM} , RMI_{CCM} , RMI_{FCT} та RMI_{MCD} .

Відобразимо оцінювання індикаторів RMI_{IRM} - Реагуючі індикатори IT-Управління, у табл. 4.9:

Таблиця 4.9

Реагуючі індикатори IT-Управління

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
RMI_{IRM} - **Управління IT Інцидентами**	**15**	**13**
IRM_{NIM} - Національна спроможність управління IT інцидентами	3	3
IRM_{IRO} - Механізми звітування про IT інциденти	3	2
IRM_{IRT} - Інструменти для відстеження та аналізу IT інцидентів	3	2
IRM_{SPC} - Центральна точка координації IT інцидентів	3	3
IRM_{PIIC} - Міжнародна співпраця у сфері управління IT інцидентами	3	3

Аналогічно, проведемо оцінювання індикаторів RMI_{CCM} - Управління IT кризами, у табл. 4.10:

Таблиця 4.10

Управління IT кризами

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
RMI_{CCM} - **Управління IT кризами**	**9**	**8**
CCM_{CMP} - Планування управління IT кризами та відновлення	2	2

Продовження табл. 4.10

CCM_{NCM} - Національні тренування та симуляції ІТ криз	3	2
CCM_{ICM} - Міжнародні вправи з управління ІТ кризами)	2	2
CCM_{OCR} - Резерви оперативної неперервності ІТ сервісів	2	2

Проведемо оцінювання індикаторів RMI_{FCT} - Управління ІТ злочинністю та шахрайством, у табл. 4.11:

Таблиця 4.11

Управління ІТ злочинністю та шахрайством

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
RMI_{FCT} - **Управління ІТ злочинністю та шахрайством**	**16**	**12**
FCT_{ITL} - Правові порушення та дотримання у сфері ІТ	3	2
FCT_{PLP} - Процесуальні правила для розслідування ІТ злочинів	3	2
FCT_{CC} - Дотримання міжнародних конвенцій щодо ІТ злочинності	2	2
FCT_{CIC} - Спроможності розслідування ІТ злочинів	3	2
FCT_{DFC} - Спроможності цифрової форензики для ІТ інцидентів	2	2
FCT_{CPI} - Цілодобова координація реагування на ІТ злочинність	3	2

Аналогічно, проведемо оцінювання індикаторів RMI_{MCD} - Військова оборона в ІТ, відповідно до табл. 4.12:

Таблиця 4.12

Військова оборона в IT

Індикатор	**Максимальна оцінка**	**Оцінка експерта**
RMI_{MCD} - **Військова оборона в IT**	**6**	**5**
MCD_{MCR} - Спроможності та готовність військової оборони IT	2	2
MCD_{MD} - Доктрина та стратегія військової оборони IT	2	2
MCD_{MDE} - Навчання та вправи військової оборони IT	2	1

Отже, відповідно до [5-8] розрахуємо індикатори **P_1, P_2, P_3:**

Стратегічні індикатори (GSI):

$$\begin{aligned}\mathbf{P}_1 = \mathbf{P}_{GSI} = ITP_{IL} + ITP_{PD} + ITP_{PC} + IPT_{NIS} + IPT_{NISA} + \\ + GCI_{ID} + GCI_{IL} + GCI_{CB} + EPD_{CPE} + EPD_{CSE} + EPD_{UE} + EPD_{GE} + EPD_{AITP} + \\ + ITRD_{RDP} + ITRD_{DS} = 2+2+2+2+2+2+1+1+2+2+2+2+1+2+1=26\end{aligned} \quad (4.18)$$

Профілактичні індикатори (SRI):

$$\begin{aligned}\mathbf{P}_2 = \mathbf{P}_{SRI} = CII_{II} + CII_{CRO} + CII_{CRP} + CII_{CSA} + DE_{SEI} + DE_{ES} + DE_{TS} + DE_{STS} \\ + DE_{CCS} + DE_{SCS} + TAA_{ITA} + TAA_{PTR} + TAA_{PAR} + TAA_{CAR} + PD_{PDL} + PD_{PDA} = \\ = 2+2+2+2+1+1+2+2+2+2+2+2+2+2+2+2=28\end{aligned} \quad (4.19)$$

Реагуючі індикатори (RMI):

$$\begin{aligned}\mathbf{P}_3 = \mathbf{P}_{RMI} = IRM_{NIM} + IRM_{IRO} + IRM_{IRT} + IRM_{SPC} + IRM_{PIIC} + CCM_{CMP} + \\ + CCM_{NCM} + CCM_{ICM} + CCM_{OCR} + FCT_{ITL} + FCT_{PLP} + FCT_{CC} + FCT_{CIC} + FCT_{DFC} + \\ + FCT_{CPI} + MCD_{MCR} + MCD_{MD} + MCD_{MDE} = 3+2+2+3+3+2+2+2+2+ \\ +2+2+2+2+2+2+1=34\end{aligned} \quad (4.20)$$

Отже, показник $\mathbf{I}_{IT\,\mathrm{Sec}}$ можна визначити за наступною формулою:

$$\mathbf{I}_{IT\,\mathrm{Sec}} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{s=1}^{l_{ij}} P_{ijs} \times 100\%}{\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{s=1}^{l_{ij}} maxP_{ijs}} = \frac{26+28+35\times 100\%}{35+40+45} = \frac{88\times 100\%}{120} = 73.33\% \qquad (4.21)$$

ЕТАП 2. Визначення загальних метрик рівня цифрової трансформації у галузі КІІ.

Крок 2.1. Сформуємо метрики, які характеризують рівень цифрової трансформації ОКІІ.

$$\mathbf{D}_{EGDI} = \{\bigcup_{k=1}^{3} \mathbf{D}_k\} = \{\mathbf{D}_1, \mathbf{D}_2, \mathbf{D}_3\} = \{\mathbf{D}_{OSI}, \mathbf{D}_{HCI}, \mathbf{D}_{TII}\}, \qquad (4.22)$$

де $\mathbf{D}_1 = \mathbf{D}_{OSI}$ це обсяг та якість онлайн-послуг, $\mathbf{D}_2 = \mathbf{D}_{HSI}$ - Індекс людського капіталу та $\mathbf{D}_3 = \mathbf{D}_{TII}$ - Стан розвитку телекомунікаційної інфраструктури, відповідно до рис 4.1:

Figure A.1. The three components of the E-Government Development Index (EGDI)

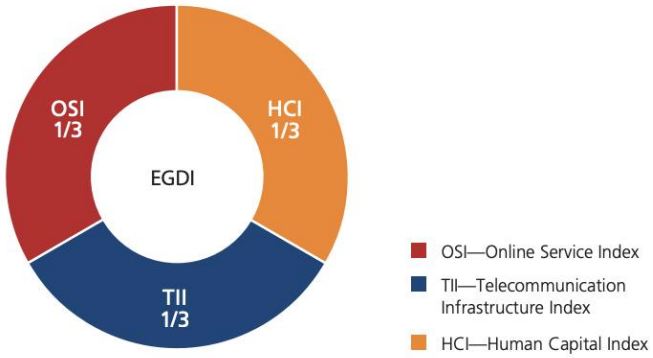


Рис. 4.1. Структура індексу EGDI

Розглянемо кожний показник більш детально:

$$\mathbf{D}_1 = \mathbf{D}_{OSI} = \{\bigcup_{r=1}^{5} D_{1r}\} = \{D_{11}, D_{12}, D_{13}, D_{14}, D_{15}\} = \{D_{INS}, D_{CTP}, D_{SRP}, D_{PTE}, D_{TEC}\}, \qquad (4.23)$$

де $D_{11} = D_{INS}$ - це рівень інституційної структури, ($D_{INS} \in [0;10]$), $D_{12} = D_{CTP}$ надання контенту, ($D_{CTP} \in [0;10]$), $D_{13} = D_{SRP}$ надання послуг ($D_{SRP} \in [0;10]$), $D_{14} = D_{PTE}$ участь та залучення ($D_{PTE} \in [0;10]$), $D_{15} = D_{TEC}$ технології ($D_{TEC} \in [0;10]$).

$$\mathbf{D}_2 = \mathbf{D}_{HCI} = \{\bigcup_{r=1}^{4} D_{2r}\} = \{D_{21}, D_{22}, D_{23}, D_{24}\} = \{D_{ALR}, D_{GER}, D_{EYS}, D_{AYS}\}, \quad (4.24)$$

де $D_{21} = D_{ALR}$ - це рівень грамотності дорослих, ($D_{ALR} \in [0;10]$), $D_{22} = D_{GER}$ - відсоток зарахувань до навчальних закладів, ($D_{GER} \in [0;10]$), $D_{23} = D_{EYS}$ - це очікувана тривалість навчання ($D_{EYS} \in [0;10]$), $D_{24} = D_{AYS}$ - це фактична тривалість навчання ($D_{AYS} \in [0;10]$), відповідно до рис. 4.2:

Figure A.3. Human Capital Index (HCI) and its components

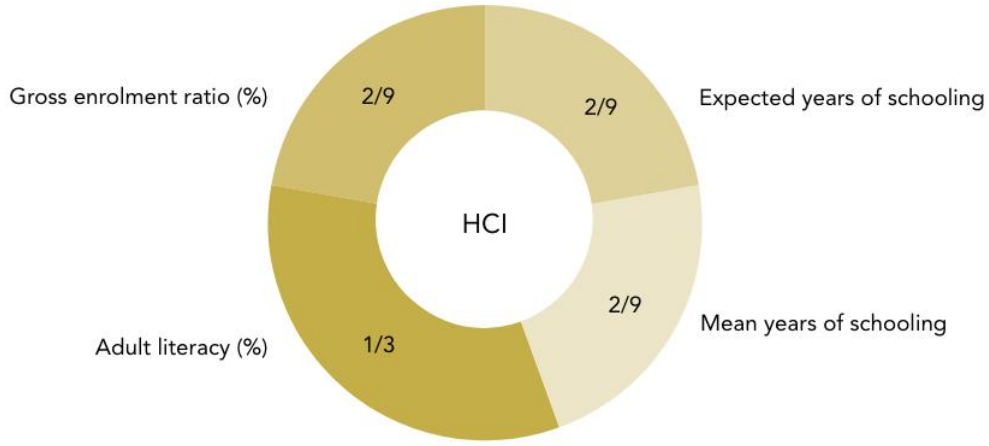


Рис. 4.2. Структура показника HCI

$$\mathbf{D}_3 = \mathbf{D}_{TII} = \{\bigcup_{r=1}^{5} D_{3r}\} = \{D_{31}, D_{32}, D_{33}, D_{34}, D_{35}\} = \{D_{IUI}, D_{FTL}, D_{MSI}, D_{WBI}, D_{FBI}\}, \quad (4.25)$$

де $D_{31} = D_{IUI}$ індекс користувачів інтернету, ($D_{IUI} \in [0;10]$), $D_{32} = D_{FTL}$ - індекс стаціонарних телефонних ліній, ($D_{FTL} \in [0;10]$), $D_{33} = D_{MSI}$ індекс мобільних абонентів ($D_{MSI} \in [0;10]$), $D_{34} = D_{WBI}$ - індекс стаціонарного широкосмугового доступ ($D_{WBI} \in [0;10]$), $D_{55} = D_{FBI}$ технології ($D_{FBI} \in [0;10]$), відповідно до рис. 4.3:

Figure A.2. Telecommunication Infrastructure Index (TII) and its components

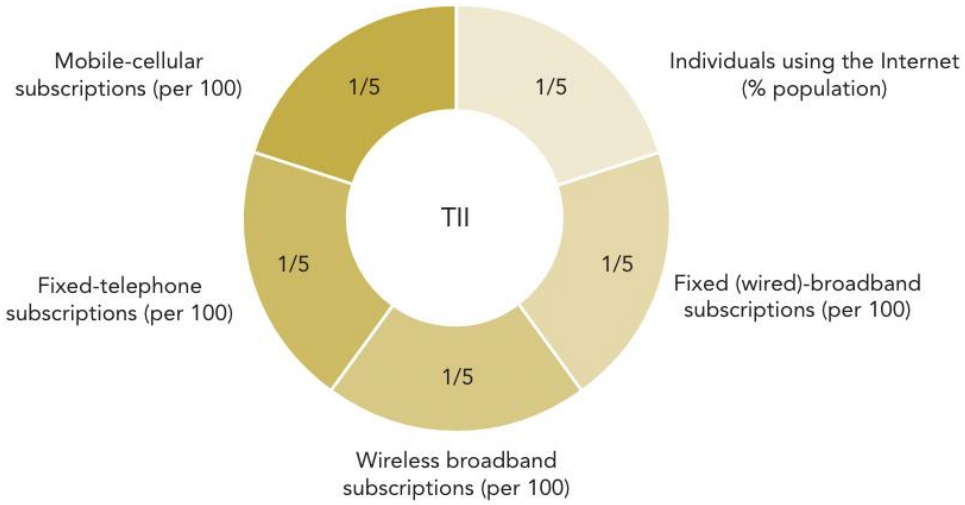


Рис. 4.3. Структура показника TII

$$\mathbf{D} = \{\bigcup_{k=1}^{q}\mathbf{D}_k\} = \{\{\bigcup_{k=1}^{q}\{\bigcup_{r=1}^{p_i}D_{kr}\}\} = \{\mathbf{D}_1,\mathbf{D}_2,\mathbf{D}_3\} = \{D_{\text{OSI}},D_{\text{HCI}},D_{\text{TII}}\}$$
$$= \{\{D_{11},D_{12},D_{13},D_{14},D_{15}\},\{D_{21},D_{22},D_{23},D_{24}\},\{D_{31},D_{32},D_{33},D_{34},D_{35}\}\} = \quad (4.26)$$
$$= \{\{D_{INS},D_{CTP},D_{SRP},D_{PTE},D_{TEC}\},\{D_{ALR},D_{GER},D_{EYS},D_{AYS}\},\{D_{IUI},D_{FTL},D_{MSI},D_{\text{WBI}},D_{FBI}\}\},$$
$$(k=\overline{1,q},r=\overline{1,p_i}).$$

Проведено оцінку показників, що характеризують рівень цифрової трансформації **D** (табл. 4.13), відповідно до [9,10]:

Крок 2.2 – Обчислення індексу рівня цифрової трансформації

Відповідно до [9], розрахуємо індекс $\mathbf{D}_{OSI}$ - Обсяг та якість онлайн-послуг:

$$\mathbf{D}_1 = \mathbf{D}_{OSI} = \frac{D_{INS}+D_{CTP}+D_{SRP}+D_{PTE}+D_{TEC}}{5} = \frac{8+7+8+7+6}{5} = 7.2 \quad (4.27)$$

Таблиця 4.13

Показники, що характеризують рівень цифрової трансформації D

D_{EGDI} max – **10 (середнє арифм)**	**D_{OSI} Обсяг та якість онлайн-послуг (OSI)** max – **10**	**D_{ISN}** Рівень інституційної структури Оцінка – **8**	**D_{CTP}** Надання контенту Оцінка – **7**	**D_{SRP}** Надання послуг Оцінка – **8**	**D_{PTE}** Участь та залучення Оцінка – **7**	**D_{TEC}** Технології Оцінка – **6**
	D_{HCI} Індекс людського капіталу (HCI) max – **10** (середнє арифм)	**D_{ALR}** Індекс грамотності дорослих Оцінка – **9**	**D_{GER}** Індекс зарахувань до навчальних закладів Оцінка – **8**	**D_{EYS}** Очікувана тривалість навчання Оцінка – **8**	**D_{AYS}** Фактична тривалість навчання Оцінка – **7**	
	D_{TII} Стан розвитку телекомунікаційної інфраструктури (TII) max – **10** (середнє арифм.)	**D_{IUI}** Індекс користувачів Інтернету Оцінка – **8**	**D_{FTL}** Індекс стаціонарних телефонних ліній Оцінка – **6**	**D_{MSI}** Індекс мобільних абонентів Оцінка – **7**	**D_{WBI}** Індекс бездротового широкосмугового доступу Оцінка – **6**	**D_{FBI}** Індекс стаціонарного широкосмугового доступу Оцінка – **5**

Аналогічно до [9], розрахуємо $\mathbf{D}_{HCI}$ - Індекс людського капіталу:

$$\mathbf{D}_2 = \mathbf{D}_{HCI} = \frac{D_{ALR}, D_{GER}, D_{EYS}, D_{AYS}}{4} = \frac{9+8+8+7}{4} = 8.0 \qquad (4.28)$$

Та, відповідно, розрахуємо індекс $\mathbf{D}_{TII}$ - Стан розвитку телекомунікаційної інфраструктури:

$$\mathbf{D}_3 = \mathbf{D}_{TII} = \frac{D_{IUI} + D_{FTL} + D_{MSI} + D_{WBI} + D_{FBI}}{5} = \frac{8+6+7+6+5}{5} = 6.4 \qquad (4.29)$$

Отже, рівень цифрової трансформації сектору критичної інфраструктури «Цифрові технології» можна розрахувати наступним чином:

$$I_{\text{EGDI}} = \frac{D_{\text{OSI}} + D_{\text{HCI}} + D_{\text{TII}} \times 100\%}{3} = \frac{7.2 + 8.0 + 6.4 \times 100\%}{3} = 72\% \qquad (4.30)$$

Етап 3. Розрахунок кількісних параметрів, що визначають стан захищеності об’єкту КІІ держави від ІТ-ризиків

Отже, показник $\mathbf{I}_{ratio}$ можна визначити за формулою:

$$\mathbf{I}_{ratio} = \mathbf{I}_{ITSec} - \mathbf{I}_{EGDI} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i}\sum_{s=1}^{l_{ij}} P_{ijs} \times 100\%}{\sum^{max}_{P_{ijs}}} - \frac{\sum_{k=1}^{q}\sum_{r=1}^{p_i} D_{kr} \times 100\%}{q} = \qquad (4.31)$$

$$= 73.33\% - 72\% = 1.33\%$$

Етап 4. Аналіз отриманих результатів визначення стану захищеності об’єкту КІІ

Відповідно до [5] показник $\mathbf{I}_{ratio}$ сектору критичної інфраструктури держави «Цифрові технології» дорівнює 1.33%, що, відповідно до наданих у розробленому методі рекомендацій означає:

$$0\% < I_{ratio} \le 0\% \Rightarrow \begin{cases} I_7 : \text{Періодичний перегляд політик безпеки;} \\ I_8 : \text{Збалансоване вкладання.} \end{cases}$$

Для перевірки правильності роботи методу при зміні вхідних даних було проведено три додаткові експерименти (рис. 4.4-4.6):

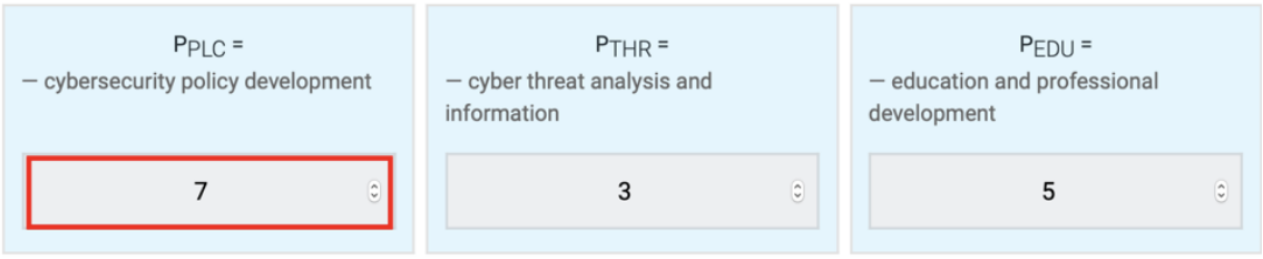


Рис. 4.4. Зміна індикатора P_{PLC} для верифікації методу

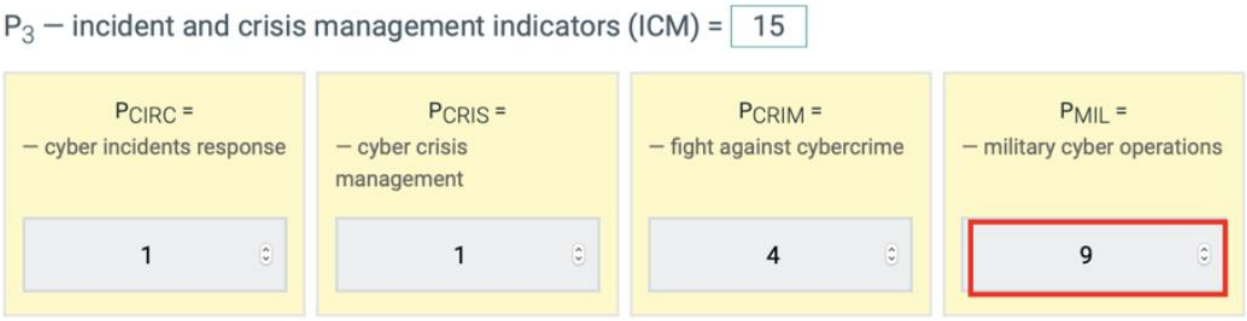


Рис. 4.5. Зміна індикатору P_{MIL} для верифікації методу

Рис. 4.6. Зміна індикатору M_{POL} для верифікації методу

Отримані результати (рис. 4.6) підтвердили можливість використання розробленого методу для розрахунку кількісних параметрів, що характеризують рівень захищеності ОКІІ. Цей метод дозволяє точно визначити ступінь захищеності та вразливості різних об'єктів, що є важливим для ефективного планування заходів безпеки та розподілу ресурсів.

4.2. Експериментальне дослідження методу визначення пріоритетів ІТ-інцидентів та його практична реалізація

Для експериментального дослідження розробленого методу, застосуємо його для сектору КІ «Інформаційні послуги», підсектору «Засоби масової інформації», до якого відноситься, наприклад, надання послуг у сфері телебачення та радіомовлення [8-9].

Етап 1. Визначення структури управління ІТ-інцидентами об’єкта критичної інформаційної інфраструктури.

У нашій моделі перший рівень ієрархії має одну мету: надійність та стійкість захисту КІІ (НСЗКІ). Значення її пріоритету приймається рівним одиниці.

Далі, для формування другого рівня ієрархії, пропонується, відповідно проведеного аналізу застосувати міжнародний стандарт ITIL [10].

Саме тому, другий рівень ієрархії включає різні види загроз, класифіковані за ITIL:

– проблеми з фізичними пристроями (Hardware Incidents);
– проблеми з програмним забезпеченням (Software Incidents);
– інциденти безпеки (Security Incidents);
– перебої в обслуговуванні (Service Outages);

– проблеми з'єднання (Connectivity Issues);
– помилки користувачів (User Errors);
– проблеми конфігурації (Configuration Issues);
– проблеми продуктивності (Performance Issues).

Пріоритети цих загроз розраховуються за допомогою матриці попарних порівнянь загроз щодо НСЗКІ у спосіб порівняння елементів другого рівня ієрархії відносно першого рівня.

Третій рівень ієрархії охоплює вплив на громадянина, суспільство, державу і правопорядок. Оцінка впливу загроз на ці три категорії також здійснюється за допомогою матриці попарних порівнянь, що дозволяє визначити пріоритети загроз для кожної категорії.

Отже, структуру управління ІТ-інцидентами на ОКІІ можна зобразити наступним чином (рис. 4.7):

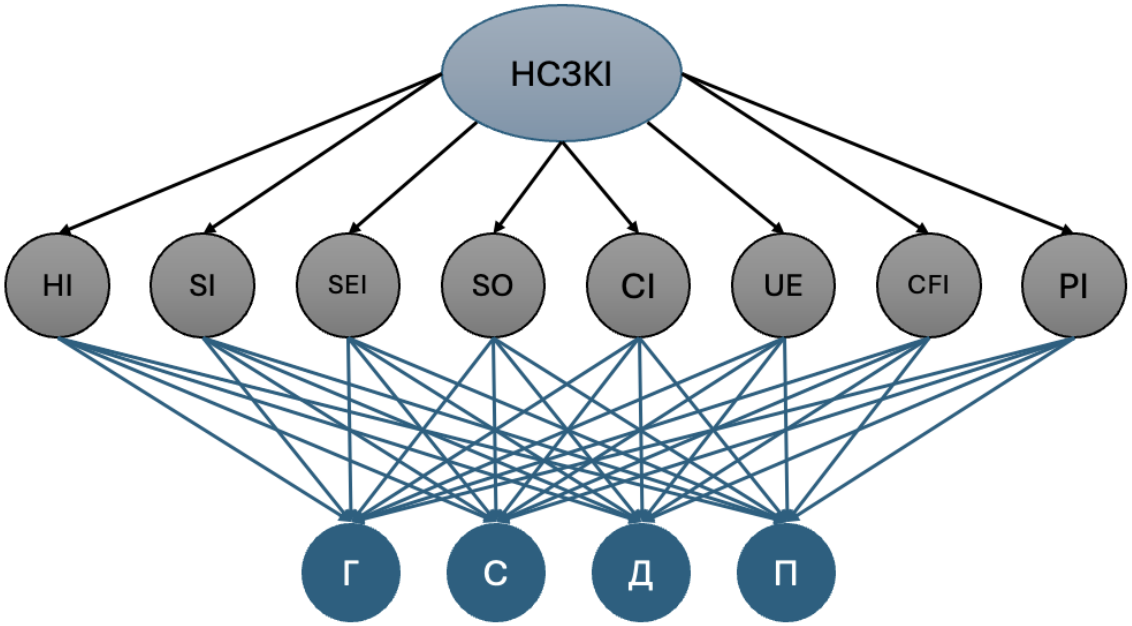


Рис. 4.7. Структура управління ІТ-інцидентами на ОКІІ

ЕТАП 2. Оцінка загроз та їхніх пріоритетів як на локальному, так і на глобальному рівнях в системі ІТ безпеки

Оцінки в матриці Сааті виставлені на основі відносної важливості загроз для забезпечення надійності та стійкості критичної інформаційної інфраструктури (НСЗКІ). Вони враховують можливий вплив кожної загрози на загальний рівень безпеки та функціональність системи:

- Проблеми з фізичними пристроями (**HI**) оцінені як менш важливі порівняно з іншими загрозами, оскільки проблеми з обладнанням можуть бути відносно легко виявлені та виправлені.

- Проблеми з програмним забезпеченням (**SI**) мають середню важливість, оскільки помилки програмного забезпечення можуть призвести до збоїв, але їх теж можна виправити через оновлення або виправлення.

- Інциденти безпеки (**SEI**) мають високий пріоритет, оскільки вони можуть призвести до значних втрат даних або порушень безпеки.

- Перебої в обслуговуванні (**SO**) оцінені як дуже важливі, оскільки вони безпосередньо впливають на доступність критичних послуг.

- Проблеми з'єднання (**CI**) також мають високий пріоритет, оскільки вони можуть впливати на зв'язок між системами та користувачами.

- Помилки користувачів (**UE**) мають високий пріоритет, оскільки людські помилки можуть часто спричиняти значні збої та порушення в роботі систем.

- Проблеми конфігурації (**CFI**) оцінені як дуже важливі, оскільки неправильна конфігурація може призвести до серйозних збоїв у роботі систем.

- Проблеми продуктивності (**PI**) мають середній пріоритет, оскільки вони впливають на ефективність роботи систем, але не завжди мають негайний критичний вплив.

Етап 3. Проведення порівнянь елементів системи ІТ безпеки на різних рівнях для оцінки їх впливу та встановлення пріоритетів за допомогою методу попарних порівнянь (AHP).

Побудуємо матрицю попарних порівнянь, яка, заснована. Матриця має наступний вигляд (табл. 4.14):

Таблиця 4.14

Матриця попарних порівнянь на шкалі важливості Т. Сааті

	Hardware Incidents (HI) -	**Software Incidents (SI)**	**Security Incidents (SEI)**	**Service Outages (SO)**	**Connectivity Issues (CI)**	**User Errors (UE)**	**Configuration Issues (CFI) -**	**Performance Issues (PI)**
	HI	SI	SEI	SO	CI	UE	CFI	PI
HI	1	3	2	4	5	6	7	3
SI	1/3	1	1/2	2	3	4	5	2
SEI	1/2	2	1	5	6	7	8	4
SO	1/4	1/2	1/5	1	3	4	2	1/2
CI	1/5	1/3	1/6	1/3	1	2	1/2	1/3
UE	1/6	1/4	1/7	1/4	1/2	1	3	1/2
CFI	1/7	1/5	1/8	1/2	2	1/3	1	1/4
PI	1/3	1/2	1/4	2	3	2	4	1

Глобальні пріоритети показують відносну силу, величину та важливість кожного окремого елемента системи ІТ безпеки. На основі проведених розрахунків найбільший локальний пріоритет щодо ІТ безпеки в порівнянні з іншими загрозами має User Errors (UE) – 0,25. На другому місці Service Outages (SO) з глобальним

пріоритетом 0,20. Третє місце займає Security Incidents (SEI) з глобальним пріоритетом 0,15.

Окрім цього, важливими є Software Incidents (SI) та Hardware Incidents (HI) з глобальними пріоритетами 0,12 та 0,10 відповідно. Проблеми з конфігурацією (Configuration Issues, CFI) також заслуговують на увагу з глобальним пріоритетом 0,08. Для решти загроз глобальні пріоритети наступні: Performance Issues (PI) – 0,06, Connectivity Issues (CI) – 0,04.

Отримані значення глобальних пріоритетів дозволяють визначити, які загрози є найбільш критичними для забезпечення надійності та стійкості критичної інформаційної інфраструктури. Зосередження уваги на найбільш пріоритетних загрозах допомагає ефективно управляти IT безпекою та мінімізувати ризики для громадянина, суспільства, держави та правопорядку (табл. 4.15):

Таблиця 4.15

Значення глобальних пріоритетів IT-інцидентів ОКІІ

Загроза	**Глобальний пріоритет**
User Errors (UE)	0,25
Service Outages (SO)	0,20
Security Incidents (SEI)	0,15
Software Incidents (SI)	0,12
Hardware Incidents (HI)	0,10
Configuration Issues (CFI)	0,08
Performance Issues (PI)	0,06
Connectivity Issues (CI)	0,04

Таким чином, матриця парних порівнянь дозволяє визначити, які з загроз є найбільш критичними для забезпечення IT безпеки. Це допомагає зосередити

ресурси та зусилля на найважливіших проблемах, мінімізуючи вплив потенційних загроз на систему.

Отримані значення глобальних пріоритетів дозволяють визначити, які загрози є найбільш критичними для забезпечення надійності та стійкості критичної інформаційної інфраструктури. Зосередження уваги на найбільш пріоритетних загрозах допомагає ефективно управляти ІТ безпекою та мінімізувати ризики для громадянина, суспільства, держави та правопорядку.

Етап 4. Синтез локальних і глобальних пріоритетів для системи ІТ-безпеки

Основним завданням цього етапу МАІ є визначення локальних пріоритетів ризиків об’єктів захисту через проміжний другий рівень – загрози за допомогою матриць попарних порівнянь щодо цих загроз. У такий спосіб за допомогою групи матриць парних порівнянь, для вище наведених загроз, послідовно формуємо множину локальних пріоритетів третього рівня щодо ризиків особи, суспільства та держави.

У табл. 4.16 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Проблеми з фізичними пристроями».

Таблиця 4.16

Значення локальних пріоритетів – Проблеми з фізичними пристроями

НІ	**Г**	**С**	**Д**	**П**
Г	1	1/3	1/5	1/2
С	3	1	1/2	2
Д	5	2	1	3
П	2	1/2	1/3	1

Значення локальних пріоритетів ризиків об’єктів захисту щодо зазначених загроз наведені у табл. та рис. нижче. Ці значення визначають рівень важливості кожного об’єкта захисту відносно конкретних загроз, що дозволяє пріоритизувати заходи безпеки та ресурси, необхідні для їхнього захисту:

На рис. 4.8 нижче представлено графічне відображення значень локальних пріоритетів ризиків для різних об'єктів захисту щодо зазначених загроз. Діаграма дозволяє візуально порівняти рівні ризиків для кожного об'єкта та визначити, які з них потребують більшої уваги та захисту.

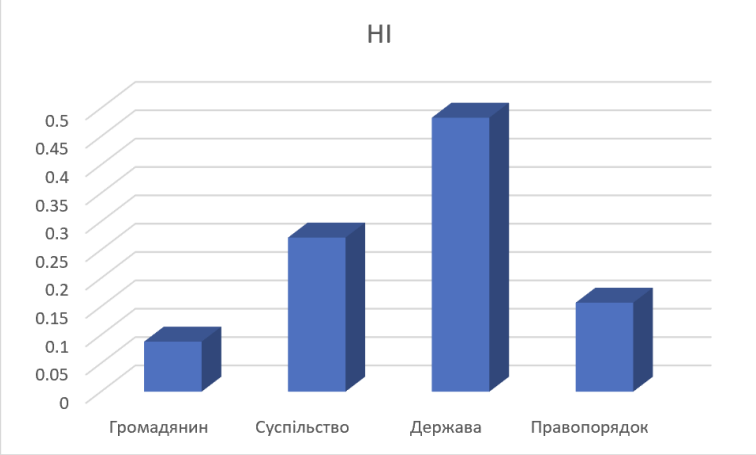


Рис. 4.8. Проблеми з фізичними пристроями

У табл. 4.17 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Проблеми з програмним забезпеченням».

Таблиця 4.17

Значення локальних пріоритетів – Проблеми з програмним забезпеченням

SI	**Г**	**С**	**Д**	**П**
Г	1	3	5	7
С	1/3	1	4	6
Д	1/5	1/4	1	3
П	1/7	1/6	1/3	1

Відповідно до наданих даних у табл. 4.17, діаграма локальних пріоритетів зображена на рис. 4.9, ілюструючи порівняльний аналіз ризиків для різних об'єктів захисту.

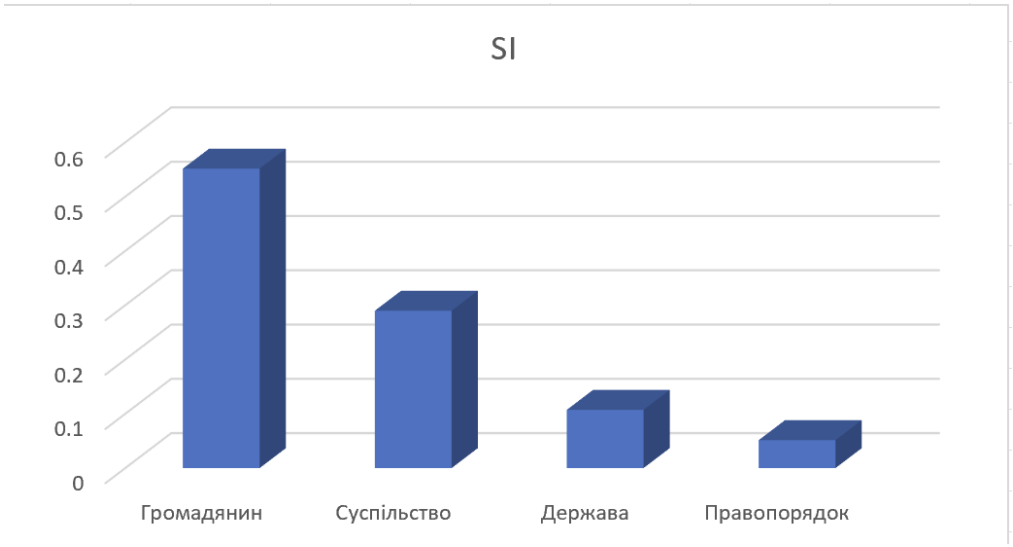


Рис. 4.9. Проблеми з програмним забезпеченням

У табл. 4.18 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Інциденти безпеки».

Таблиця 4.18

Значення локальних пріоритетів – Інциденти безпеки

SEI	**Г**	**С**	**Д**	**П**
Г	1	3	6	8
С	1/3	1	4	7
Д	1/6	1/4	1	5
П	1/8	1/7	1/5	1

Виходячи з інформації, представленої у таблиці, діаграма локальних пріоритетів, наведена на рис. 4.10 нижче:

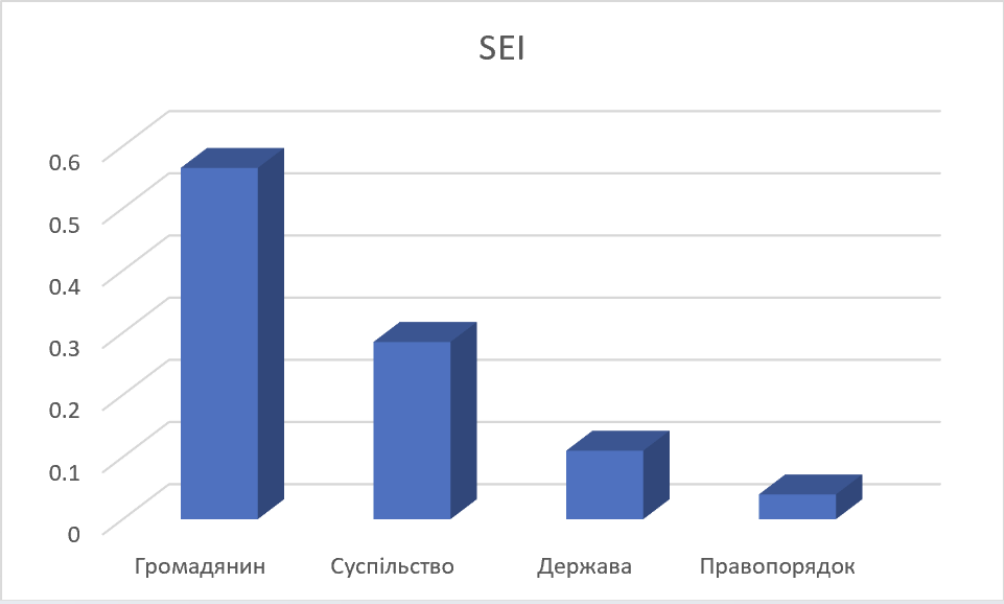


Рис. 4.10. Інциденти безпеки

У табл. 4.19 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Перебої в обслуговуванні».

Таблиця 4.19

Значення локальних пріоритетів – Перебої в обслуговуванні

SO	**Г**	**С**	**Д**	**П**
Г	1	3	5	7
С	1/3	1	4	6
Д	1/5	1/4	1	3
П	1/7	1/6	1/3	1

Як показано у таблиці, діаграма локальних пріоритетів на рис. 4.11 нижче відображає співвідношення ризиків для різних об'єктів захисту:

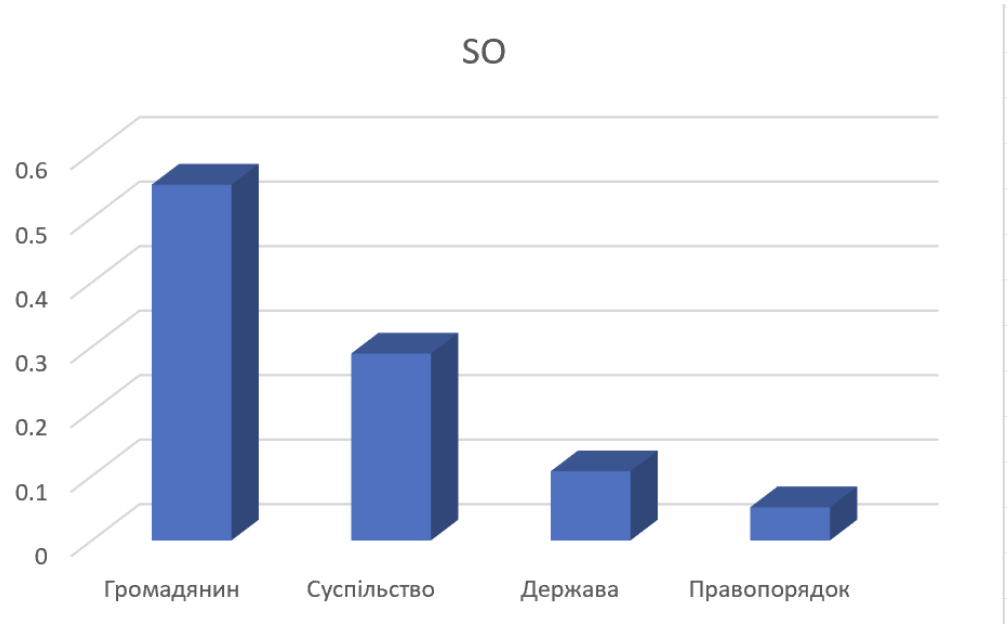


Рис. 4.11. Перебої в обслуговуванні

У табл. 4.20 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Проблеми з'єднання».

Таблиця 4.20

Значення локальних пріоритетів – Проблеми з'єднання

СІ	**Г**	**С**	**Д**	**П**
Г	1	3	2	4
С	1/3	1	2	3
Д	1/2	½	1	2
П	1/4	1/3	1/2	1

Відповідно до табл. 4.20, діаграма локальних пріоритетів, представлена на рис. 4.12 нижче:

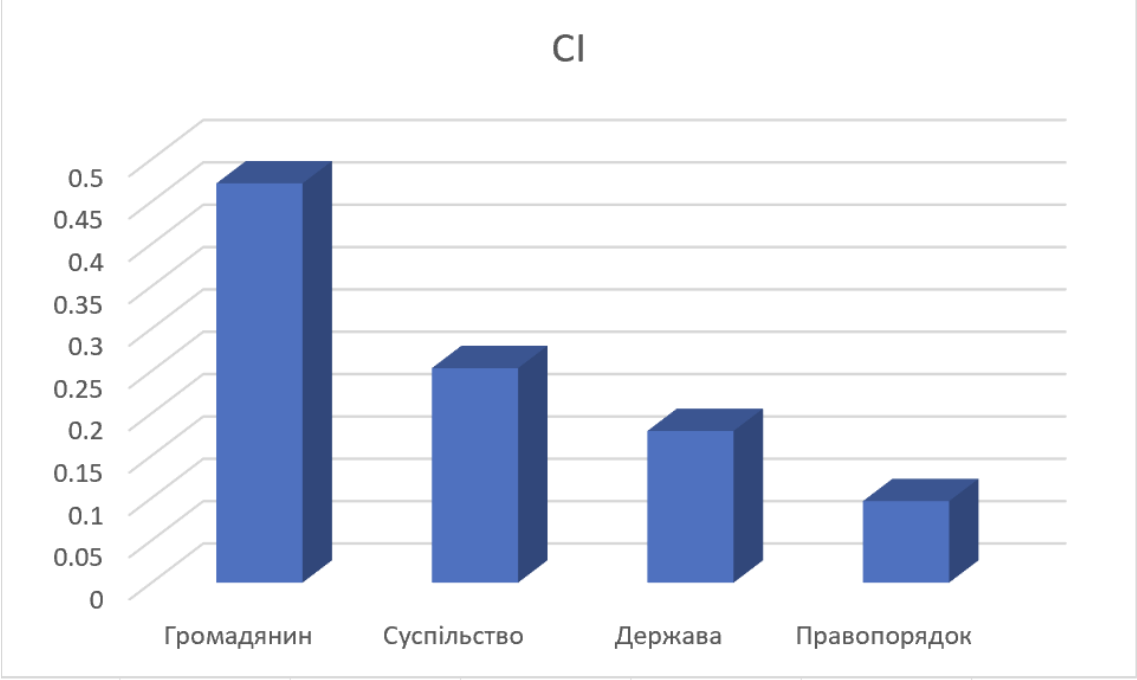


Рис. 4.12. Проблеми з'єднання

У табл. 4.21 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Помилки користувачів».

Таблиця 4.21

Значення локальних пріоритетів – Помилки користувачів

UE	Г	С	Д	П
Г	1	2	3	4
С	1/2	1	2	3
Д	1/3	1/2	1	2
П	1/4	1/3	1/2	1

Відповідно до табл. 4.21, діаграма локальних пріоритетів, представлена на рис. 4.13 нижче:

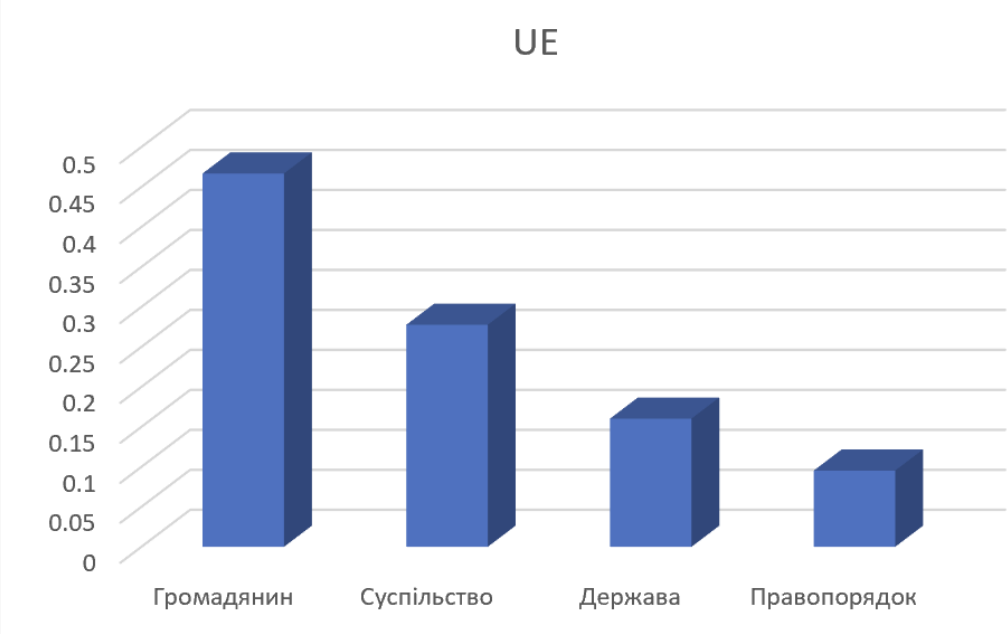


Рис. 4.13. Помилки користувачів

У табл. 4.22 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Проблеми конфігурації».

Таблиця 4.22

Значення локальних пріоритетів – Проблеми конфігурації

CFI	**Г**	**С**	**Д**	**П**
Г	1	2	3	4
С	1/2	1	2	3
Д	1/3	1/2	1	2
П	1/4	1/3	1/2	1

Відповідно до табл. 4.22, діаграма локальних пріоритетів, представлена на рис. нижче:

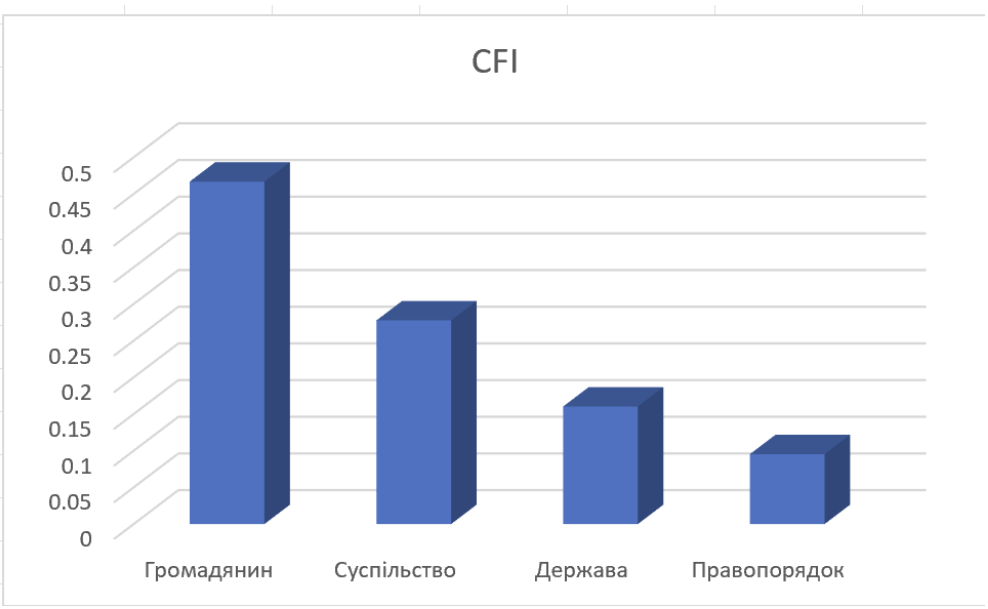


Рис. 4.14. Проблеми конфігурації

У табл. 4.23 наведено значення локальних пріоритетів ризиків об'єктів захисту стосовно загрози «Проблеми продуктивності».

Таблиця 4.23

Значення локальних пріоритетів – Проблеми продуктивності

РІ	**Г**	**С**	**Д**	**П**
Г	1	4	3	2
С	1/4	1	2	1
Д	1/3	1/2	1	1
П	1/2	1	1	1

Відповідно до табл. 4.23, діаграма локальних пріоритетів, представлена на рис. 4.15 нижче:

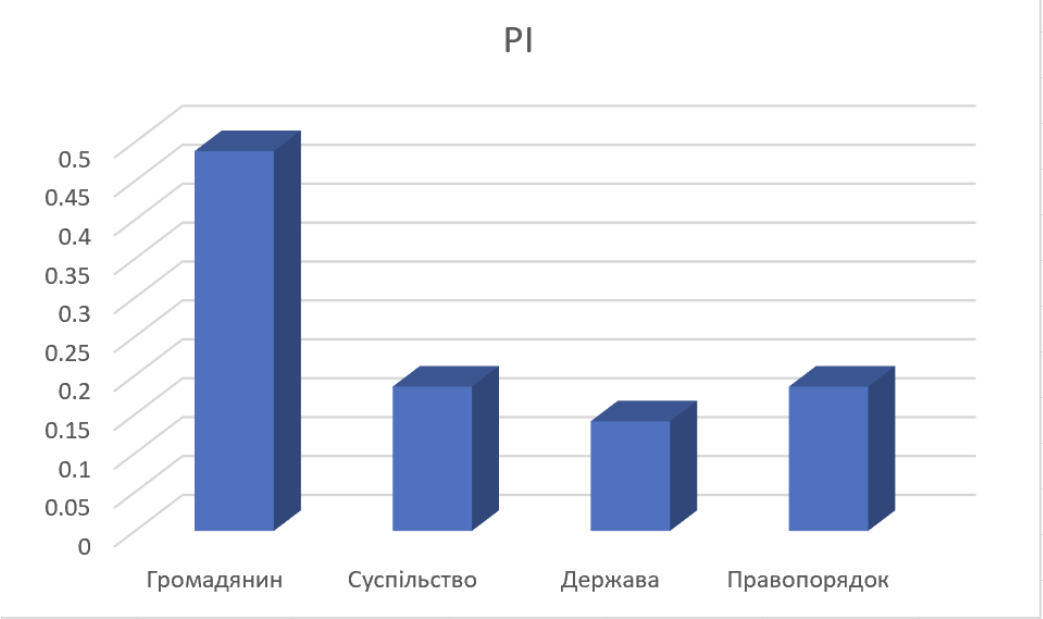


Рис. 4.15. Проблеми продуктивності

ЕТАП 5. Оцінка та коригування результатів

Разом з матрицями парних порівнянь будуть отримані міри оцінок відхилення від узгодженості, які в узагальненому вигляді подані в табл. 4.24 нижче.

Таблиця 4.24

Міри оцінок відхилення від узгодженості

Рівні	**Пріоритети**	**n**	**λmax**	**CR**
1	НСЗКІ	8	8.57373	0.05812
2	HI	4	4.01452	0.005
2	SI	4	4,17244	0,05748
2	SEI	4	4,27255	0,09085
2	SO	4	4,17244	0,05748
2	CI	4	4,12326	0,04109
2	UE	4	4,03098	0,01033
2	CFI	4	4,03098	0,01033
2	PI	4	4,13199	0,04400

Отже, відповідно до отриманих результатів видно, що IT-інциденти мають різний вплив на громадян, суспільство, державу та правопорядок. Нижче наведено аналіз впливу кожного типу інциденту.

Розглянемо результати оцінювання щодо кожної загрози:

Проблеми з фізичними пристроями (Hardware Incidents, HI):

Громадяни: **0.088** – Найменш вразлива категорія. Проблеми з фізичними пристроями, як правило, не мають значного впливу на індивідуальних користувачів.

Суспільство: **0.272** – Суспільство відчуває помірний вплив від таких інцидентів, зокрема в контексті громадських сервісів.

Держава: **0.483** – Найбільш вразлива категорія. Проблеми з фізичними пристроями можуть суттєво впливати на функціонування державних установ і критичних інфраструктур.

Правопорядок: **0.157** – Вразливість правопорядку до проблем з фізичними пристроями є менш значною порівняно з іншими категоріями.

Проблеми з програмним забезпеченням (Software Incidents, SI):

Громадяни: **0.552** – Найбільш вразлива категорія. Проблеми з програмним забезпеченням можуть значно впливати на повсякденне життя користувачів.

Суспільство: **0.290** – Помірний вплив. Суспільні сервіси можуть відчувати перебої через проблеми з програмним забезпеченням.

Держава: **0.107** – Найменш вразлива категорія. Держава має засоби для мінімізації таких інцидентів.

Правопорядок: **0.051** – Вплив на правопорядок незначний.

Інциденти безпеки (Security Incidents, SEI):

Громадяни: **0.565** – Найбільш вразлива категорія. Інциденти безпеки, такі як витік даних, можуть суттєво вплинути на особисту інформацію громадян.

Суспільство: **0.285** – Суспільство відчуває значний вплив від інцидентів безпеки, що можуть порушити громадський порядок.

Держава: **0.110** – Вплив на державу є помірним.

Правопорядок: **0.040** – Найменший вплив серед усіх категорій.

Перебої в обслуговуванні (Service Outages, SO):

Громадяни: **0.552** – Найбільш вразлива категорія. Перебої в обслуговуванні можуть суттєво впливати на доступ до важливих сервісів.

Суспільство: **0.290** – Помірний вплив на суспільство.

Держава: **0.107** – Держава має ресурси для швидкого реагування на перебої в обслуговуванні.

Правопорядок**: 0.051** – Найменший вплив серед усіх категорій.

Помилки користувачів (User Errors, UE):

Громадяни: **0.467** – Значний вплив. Помилки користувачів можуть призвести до втрати даних або інших проблем.

Суспільство: **0.278** – Помірний вплив на суспільство.

Держава: **0.160** – Вплив на державу є суттєвим, але меншим ніж на громадян.

Правопорядок: **0.095** – Вплив на правопорядок є відносно незначним.

Проблеми конфігурації (Configuration Issues, CFI):

Громадяни: **0.467** – Значний вплив. Неправильна конфігурація може призвести до проблем у функціонуванні систем.

Суспільство: **0.278** – Помірний вплив на суспільство.

Держава: **0.160** – Вплив на державу є суттєвим.

Правопорядок: **0.095** – Вплив на правопорядок є відносно незначним.

Проблеми продуктивності (Performance Issues, PI):

Громадяни: **0.488** – Значний вплив на користувачів. Проблеми продуктивності можуть знижувати ефективність роботи.

Суспільство: **0.185** – Вплив на суспільство є найменшим серед усіх категорій.

Держава: **0.141** – Держава може адаптуватися до проблем продуктивності.

Правопорядок: **0.185** – Значний вплив на правопорядок.

Отже, Апаратні інциденти (HI) мають найвищий пріоритет для держави (0.483), що підкреслює критичну необхідність підтримки і захисту фізичної інфраструктури. Програмні інциденти (SI) та інциденти безпеки (SEI) найбільш критичні для громадян (0.552 та 0.565 відповідно), що вимагає посиленої уваги до розробки надійного програмного забезпечення та заходів кібербезпеки. Перебої в обслуговуванні (SO) суттєво впливають на громадян та суспільство, але мають менший вплив на державу і правопорядок. Проблеми продуктивності (PI), помилки користувачів (UE) та проблеми конфігурації (CFI) мають значний вплив на громадян, вимагаючи зусиль для покращення якості IT-послуг і навчання користувачів.

Верифікація розробленого методу

Для проведення верифікації розробленого методу, проведено додаткові експерименти. Застосуємо розроблений метод для секторів КІІ «Захист інформації» (табл. 4.25-4.26) та «Національна безпека» (табл. 4.27-4.28).

Таблиця 4.25

Матриця попарних порівнянь для сектору КІІ «Захист інформації»

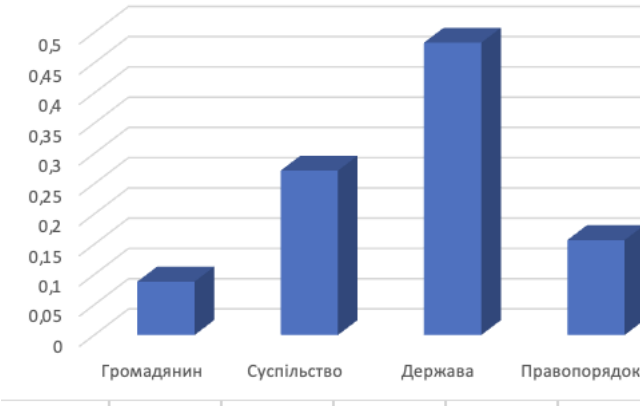
	Hardware Incidents (HI) -	**Software Incidents (SI)**	**Security Incidents (SEI)**	**Service Outages (SO)**	**Connectivity Issues (CI)**	**User Errors (UE)**	**Configuration Issues (CFI) -**	**Performance Issues (PI)**
	HI	SI	SEI	SO	CI	UE	CFI	PI
HI	1	3	2	4	5	6	7	3
SI	1/3	1	1/2	2	3	4	5	2
SEI	1/2	2	1	5	6	7	8	4
SO	1/4	1/2	1/5	1	3	4	2	1/2
CI	1/5	1/3	1/6	1/3	1	2	1/2	1/3
UE	1/6	1/4	1/7	1/4	1/2	1	3	1/2
CFI	1/7	1/5	1/8	1/2	2	1/3	1	1/4
PI	1/3	1/2	1/4	2	3	2	4	1

Відповідно до розробленого методу представимо значення локальних пріоритетів ІТ-інцидентів ОКІІ галузі у табл. 4.26:

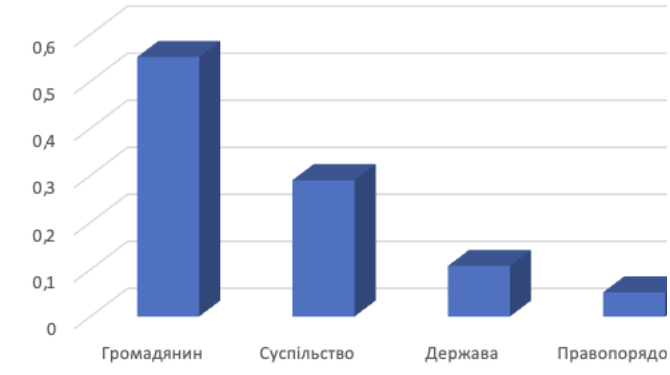
Таблиця 4.26

Значення локальних пріоритетів ІТ-інцидентів ОКІІ галузі «Захист інформації»

Hardware Incidents (HI) - Проблеми з фізичними пристроями

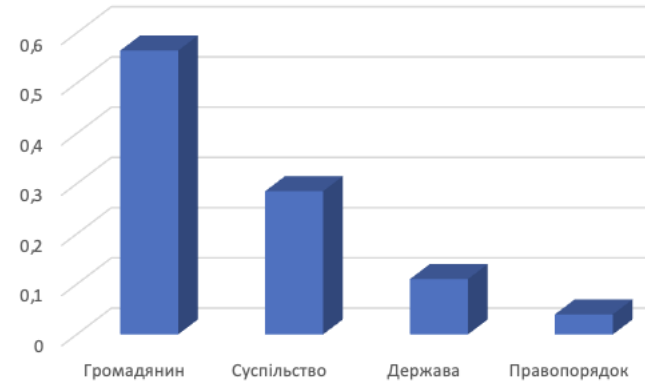


Software Incidents (SI) - Проблеми з програмним забезпеченням



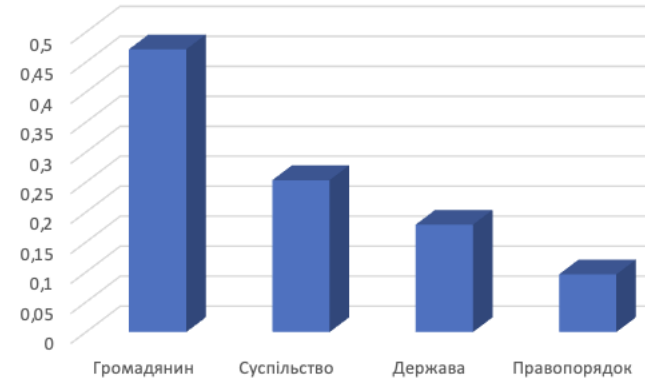
Security Incidents (SEI) - Інциденти безпеки

Service Outages (SO) - Перебої в обслуговуванні

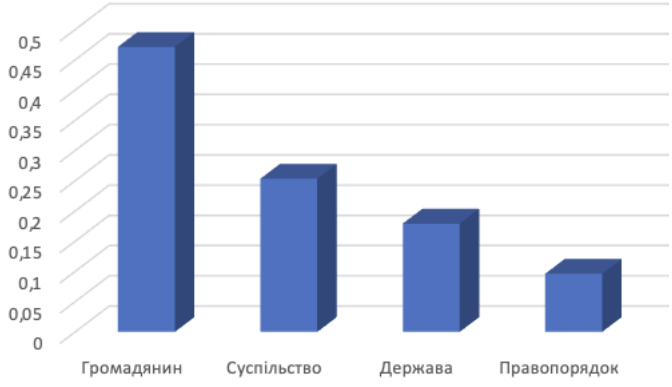


Connectivity Issues (CI) - Проблеми з'єднання

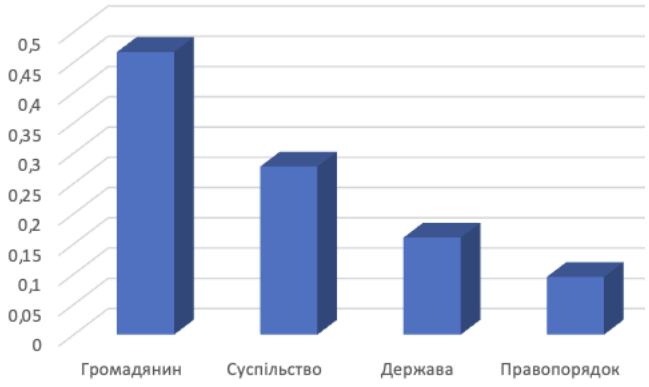
User Errors (UE) - Помилки користувачів

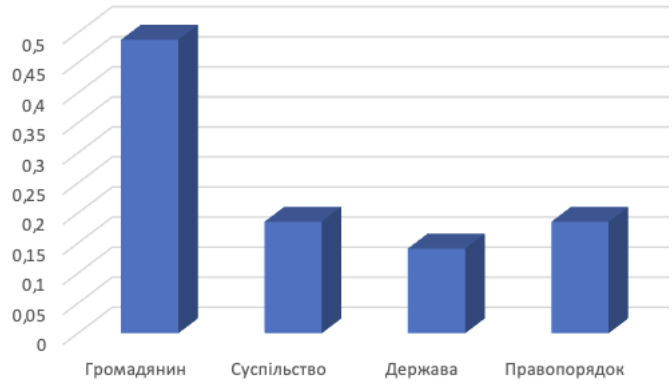


Configuration Issues (CFI) - Проблеми конфігурації



Performance Issues (PI) - Проблеми продуктивності





На основі проведеного експерименту з оцінки впливу різних типів IT-інцидентів на різні категорії захисту КІІ можна зробити такі висновки: апаратні інциденти (HI) мають найвищий пріоритет для держави (0.483), що підкреслює необхідність підтримки і захисту фізичної інфраструктури; для громадян (0.088) і суспільства (0.272) цей тип інцидентів має менший вплив, але все ж важливий.

Програмні інциденти (SI) є найбільш критичними для громадян (0.552), що вимагає уваги до надійного програмного забезпечення, вони також суттєво впливають на суспільство (0.290). Інциденти безпеки (SEI) мають найвищий пріоритет для громадян (0.565), що вказує на необхідність посиленої уваги до кібербезпеки. Перебої в обслуговуванні (SO) суттєво впливають на громадян (0.552) і суспільство (0.290), але менш впливають на державу (0.107) і правопорядок (0.051). Проблеми продуктивності (PI) (0.488), помилки користувачів (UE) (0.471) та проблеми конфігурації (CFI) (0.467) мають значний вплив на громадян, потребуючи покращення IT-послуг і навчання користувачів. Проблеми з'єднання (CI) також значно впливають на громадян (0.471) та суспільство (0.253).

Тепер, застосуємо розроблений метод для сектору для сектору КІІ «Національна безпека». У табл. 4.27 представимо матрицю попарних порівнянь:

Таблиця 4.27

Матриця попарних порівнянь для сектору КІІ «Національна безпека»

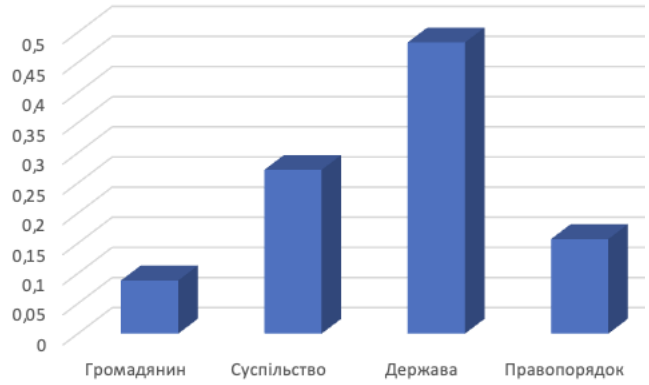
	Hardware Incidents (HI) -	**Software Incidents (SI)**	**Security Incidents (SEI)**	**Service Outages (SO)**	**Connectivity Issues (CI)**	**User Errors (UE)**	**Configuration Issues (CFI) -**	**Performance Issues (PI)**
	HI	SI	SEI	SO	CI	UE	CFI	PI
HI	1	4	3	5	6	7	8	4
SI	1/4	1	1/3	2	3	4	5	2
SEI	1/3	3	1	6	7	8	9	5
SO	1/5	1/2	1/6	1	4	5	3	1/2
CI	1/6	1/3	1/7	1/4	1	3	1/2	1/4
UE	1/7	1/4	1/8	1/5	1/3	1	4	1/3
CFI	1/8	1/5	1/9	1/3	2	1/4	1	1/5
PI	1/4	1/2	1/5	2	3	2	5	1

Аналогічно, відповідно до розробленого методу представимо значення локальних пріоритетів ІТ-інцидентів ОКІІ галузі «Національна безпека», у табл. 4.28:

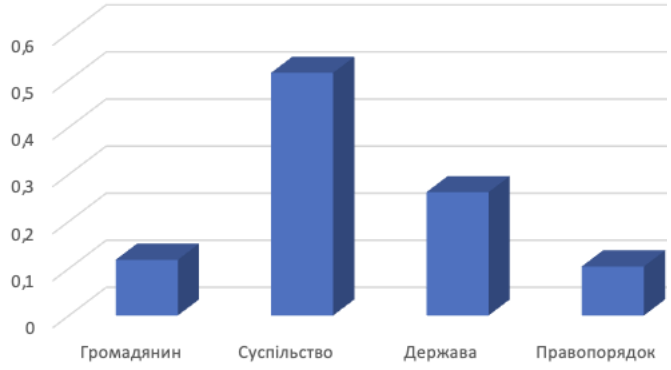
Таблиця 4.28

Значення локальних пріоритетів ІТ-інцидентів ОКІІ галузі «Національна безпека»

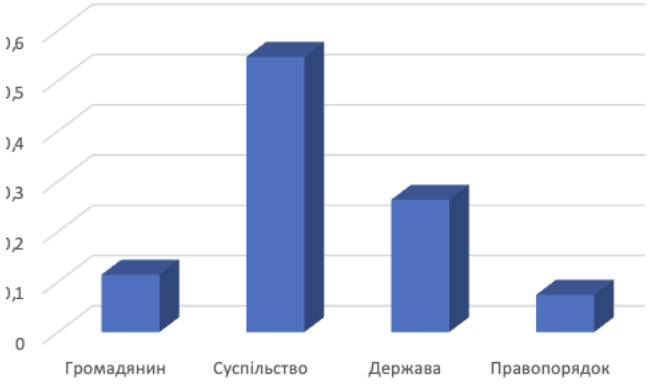
Hardware Incidents (HI) - Проблеми з фізичними пристроями



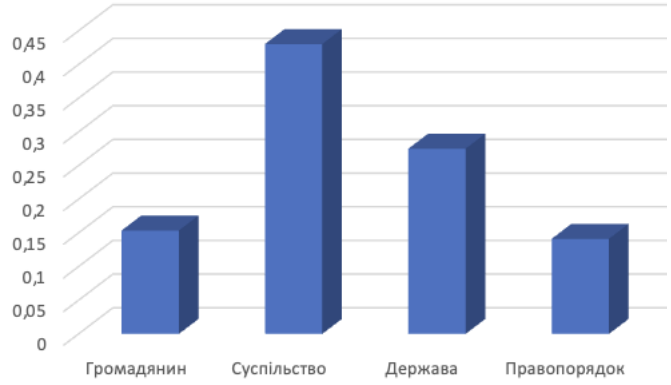
Software Incidents (SI) - Проблеми з програмним забезпеченням



Security Incidents (SEI) - Інциденти безпеки

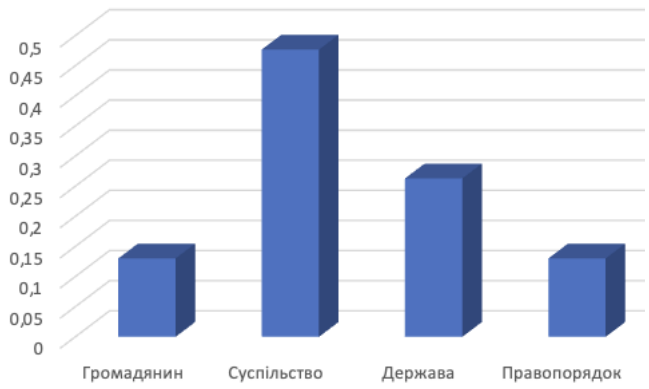


Service Outages (SO) - Перебої в обслуговуванні

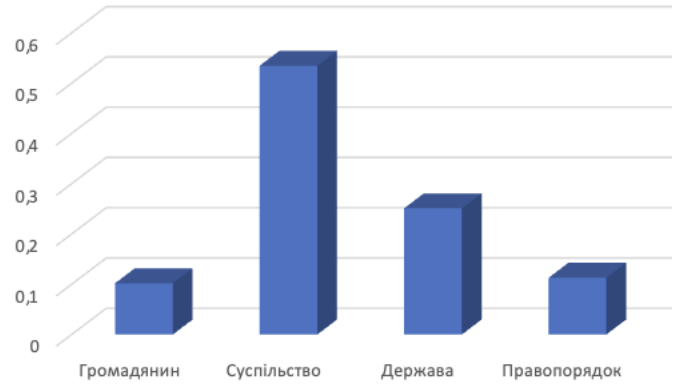


Connectivity Issues (CI) - Проблеми з'єднання

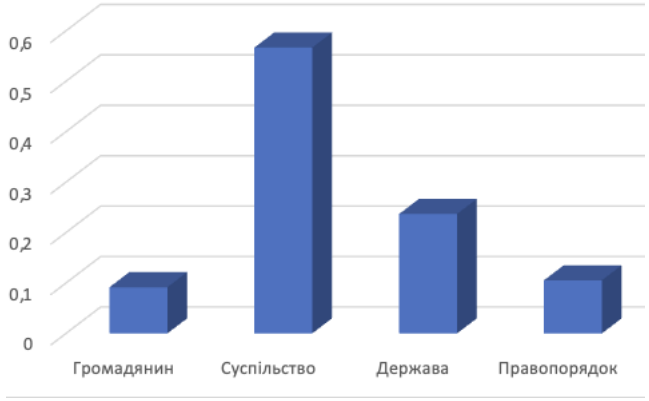
User Errors (UE) - Помилки користувачів

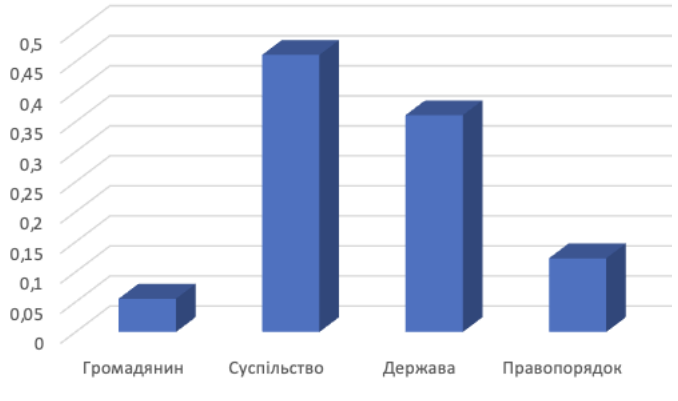


Configuration Issues (CFI) - Проблеми конфігурації



Performance Issues (PI) - Проблеми продуктивності





На основі проведеного експерименту з оцінки впливу різних типів IT-інцидентів на сектор «Національна безпека» можна зробити наступні висновки: апаратні інциденти (HI) мають найвищий пріоритет для держави (0.483), що підкреслює необхідність підтримки фізичної інфраструктури; для громадян (0.088) і суспільства (0.272) цей тип інцидентів має менший вплив. Програмні інциденти (SI) є критичними для суспільства (0.516) та громадян (0.118), що вимагає уваги до надійного програмного забезпечення. Інциденти безпеки (SEI) також мають високий пріоритет для суспільства (0.548) та громадян (0.114), що вказує на необхідність посиленої уваги до кібербезпеки. Перебої в обслуговуванні (SO) суттєво впливають на суспільство (0.430) та громадян (0.154), а також на державу (0.275). Помилки користувачів (UE) та проблеми конфігурації (CFI) значно впливають на суспільство (0.534 та 0.567 відповідно), потребуючи покращення IT-послуг і навчання

користувачів. Проблеми продуктивності (PI) мають значний вплив на державу (0.361) та суспільство (0.461), потребуючи покращення продуктивності систем. Проблеми з'єднання (CI) суттєво впливають на суспільство (0.477) та громадян (0.130), вказуючи на необхідність забезпечення надійного зв'язку.

Отже, відповідно до проведених експериментів з оцінки впливу різних типів IT-інцидентів на сектори КІІ «Інформаційні послуги», «Захист інформації» та «Національна безпека», можна зробити висновок, що метод адекватно реагує на змінні дані в кожному з цих секторів. Результати показують, що пріоритети загроз змінюються в залежності від категорій впливу, що свідчить про гнучкість та точність методу.

4.3. Експериментальне дослідження методу управління IT-загрозами та його практична реалізація

Застосуємо даний метод для сектору КІІ «Цифрові технології», а саме підсектору «Електронні комунікації», відповідно до [16].

Етап 1. Ідентифікація IT-загроз для ОКІІ.

Для покращення IT-безпеки ОКІІ були визначені такі IT-загрози, відповідно до методології STRIDE:

1. **Spoofing** (Підроблення ідентичності):

Загроза втручання в систему шляхом використання підроблених даних або ідентифікаційних даних для отримання несанкціонованого доступу. Наприклад, хакер може використати підроблені сертифікати для доступу до мережі енергетичної компанії.

2. **Tampering** (Маніпуляція даними):

Внесення неправомірних змін у дані або конфігурації системи. Це може включати зміну логічних команд управління на ОКІ, що може призвести до фізичних збоїв.

3. **Repudiation** (Заперечення):

Неможливість відстеження або доведення здійснення дій користувачем. Наприклад, відсутність журналів аудиту може дозволити зловмисникам заперечувати факт здійснення шкідливих дій у мережі управління водопостачанням.

4. **Information disclosure** (Розголошення інформації):

Несанкціонований доступ до конфіденційної інформації. Наприклад, витік секретних даних з баз даних урядових агентств може призвести до серйозних наслідків для національної безпеки.

5. **Denial of Service (DoS)** (Відмова у обслуговуванні):

Атаки, які спрямовані на перешкоджання нормальній роботі системи, зокрема, за допомогою перевантаження ресурсів. Наприклад, DoS-атака на системи управління транспортною інфраструктурою може зупинити всі перевезення.

6. **Elevation of Privilege** (Підвищення привілеїв):

Загроза, що дозволяє зловмисникам отримати більші права, ніж вони мають, і використовувати їх для неправомірного доступу до систем або даних. Наприклад, зловмисник може отримати права адміністратора в системах управління здоров'ям та зловживати цими правами.

Етап 2: Визначення критеріїв оцінки ІТ-загроз для КІІ.

Даний етап передбачає детальне визначення критеріїв для оцінки кожної ІТ-загрози U_i. Критерії оцінки є ключовими параметрами, які дозволяють проводити

всебічний аналіз загроз та визначати їх пріоритетність для подальшого управління. Для кожної ІТ-загрози U_i та кожного критерію k пропонується застосувати наступні параметри, відповідно до (2, 3):

– **Імовірність виникнення загрози** (І): Оцінка ймовірності, з якою конкретна ІТ-загроза може реалізуватися. Це дозволяє визначити, наскільки часто можна очікувати виникнення даної загрози.

– **Можливий збиток від загрози** (З): Оцінка потенційних збитків, які можуть бути завдані КІІ у разі реалізації загрози. Враховуються як фінансові втрати, так і можливий вплив на безпеку та функціонування системи.

– **Складність реалізації загрози** (С): Оцінка технічної складності, з якою загроза може бути реалізована зловмисниками. Це включає аналіз необхідних знань, інструментів та ресурсів для здійснення атаки.

Правильне визначення критеріїв дозволяє забезпечити більш глибокий та всебічний аналіз загроз, підвищуючи ефективність управління ризиками та захисту КІІ. Оптимальна кількість критеріїв для оцінки ІТ-загроз на ОКІІ залежить від складності проблеми та доступних даних. Використання 3-7 критеріїв, відповідно до [12] є стандартною практикою для забезпечення всебічного аналізу. Це дозволяє врахувати різні аспекти загроз і ризиків, забезпечуючи збалансований підхід до ухвалення рішень щодо захисту ОКІІ.

Етап 3. Отримання та нормалізація даних ІТ-загроз для КІІ.

Даний етап передбачає детальний процес збору, оцінки та нормалізації даних щодо ІТ-загроз для ОКІІ. Важливою частиною цього етапу є визначення вагових коефіцієнтів для кожного критерію оцінки, що дозволяє забезпечити об'єктивність та збалансованість у підході до оцінки загроз.

Вагові коефіцієнти для оцінки ІТ-загроз на ОКІІ мають бути визначені на основі їх відносної важливості. Імовірність виникнення загрози отримала високий коефіцієнт через її значний вплив на ризик реалізації загрози. Можливий збиток від

загрози має найвищий коефіцієнт, оскільки потенційні втрати від загрози критично впливають на функціонування ОКІІ. Складність реалізації загрози отримала нижчий коефіцієнт через її відносно меншу важливість у порівнянні з іншими критеріями, але все ж важливість для оцінки технічних аспектів захисту.

Відповідно до попередніх кроків, кожен критерій оцінки k має відповідний ваговий коефіцієнт w_k, де сума всіх коефіцієнтів дорівнює 1, згідно з (4), що відображено нижче у табл. 4.29:

Таблиця 4.29

Таблиця критеріїв оцінки ІТ-загроз

Критерій, $\boldsymbol{k}$	Опис	Ваговий коефіцієнт, $\boldsymbol{w_k}$
Імовірність виникнення загрози (І)	Оцінка ймовірності того, що загроза може реалізуватися	0.4
Можливий збиток від загрози (З)	Оцінка потенційних втрат або збитків, які можуть бути завдані в разі реалізації загрози.	0.5
Складність реалізації загрози (С)	Оцінка складності технічної реалізації загрози, що враховує необхідні ресурси, знання та інструменти.	0.1

Етап 4. Визначення вагових коефіцієнтів критеріїв для ІТ-загроз КІІ.

Для більш точного визначення критеріїв, використовується шкала оцінки від 1 до 5, де 1 вказує на найнижчий рівень (низька ймовірність, мінімальний збиток, низька складність) і 5 вказує на найвищий рівень (висока ймовірність, максимальний збиток, висока складність). Далі ці оцінки використовуються для парного порівняння загроз, що дозволяє визначити їх відносну важливість та критичність для ОКІІ. На основі цих критеріїв здійснюється інтегративна оцінка та пріоритизація загроз, що є основою для ухвалення управлінських рішень щодо заходів безпеки та захисту.

Отже, відповідно до (5, 7), застосуємо зазначену шкалу для оцінювання альтернатив, за вказаними критеріями. Нижче наведено таблицю оцінок альтернатив за критеріями (табл. 4.30):

Таблиця 4.30

Оцінка альтернатив за критеріями

Загроза	Імовірність (I)	Збиток (З)	Складність (С)
Spoofing	2	4	3
Tampering	3	5	2
Repudiation	1	3	4
Information disclosure	4	5	2
Denial of Service	5	5	1
Elevation of Privilege	2	4	3

Далі ці оцінки використовуються для парного порівняння загроз, що дозволяє визначити їх відносну важливість та критичність для ОКІІ. Це порівняння допомагає встановити, які загрози є найбільш серйозними і потребують першочергових заходів захисту. Після цього здійснюється інтегративна оцінка та пріоритизація загроз на основі отриманих результатів, що є основою для ухвалення управлінських рішень щодо заходів безпеки та захисту ОКІІ.

Етап 5. Проведення парних порівнянь альтернативних загроз для КІІ.

Відповідно до (8), на цьому етапі використовується метод парних порівнянь для визначення домінування кожної загрози над іншими. Цей метод дозволяє оцінити відносну важливість та критичність кожної загрози шляхом порівняння їх за визначеними критеріями. Застосування функції проспективної цінності враховує ваги критеріїв та оцінки альтернатив за кожним критерієм.

– **Внесення даних**: Після проведення оцінки всіх загроз за визначеними критеріями на попередньому етапі, ці дані заносяться у спеціально розроблене програмне забезпечення, для проведення розрахунків.

– **Визначення параметра α**: Параметр α встановлюється для врахування ставлення до ризику. Значення α можуть приймати значення залежно від конкретної ситуації, але зазвичай знаходяться в діапазоні від 0 до 1. Низькі значення α зменшують вплив ризику, тоді як високі значення підсилюють його значення.

– **Парне порівняння загроз**: Кожна загроза порівнюється з іншими по всіх критеріях. Для кожної пари загроз розраховується значення домінування за допомогою вищевказаної формули.

– **Розрахунок сумарного домінування**: Після порівняння всіх пар загроз за кожним критерієм обчислюється сумарне значення домінування для кожної загрози. Це значення використовується для ранжування загроз і визначення їх пріоритетності.

Отже, цей етап дозволяє провести детальний і об'єктивний аналіз загроз, що забезпечує надійну основу для прийняття управлінських рішень щодо захисту КІІ.

Етап 6. Отримання інтегративної оцінки альтернативних ІТ-загроз для КІІ.

На цьому етапі, для автоматизації цього процесу та підвищення точності розрахунків, використовується розроблений програмний застосунок для методу управління ІТ-загрозами. Цей застосунок інтегрує всі дані, проведені парні порівняння та вагові коефіцієнти для обчислення підсумкових оцінок корисності. Відповідно до (10), підсумовуємо значення проспективної цінності, щоб отримати оцінку корисності для кожної загрози. Отже, застосувавши розроблений програмний застосунок для методу управління ІТ-загрозами, отримуємо наступний результат (рис. 4.16):

0.02	0.5	0.2	0.3	Dom	Rank
S	2	4	3	2.406	3
T	3	5	2	-1.564	5
R	1	3	4	5.789	2
I	4	5	2	-1.004	4
D	5	5	1	9.145	1
E	2	4	3	-13.338	6

Рис. 4.16. Результат застосування програмного застосунку для управління IT-загрозами

Етап 7. Пріоритизація та ухвалення рішень щодо IT-загроз для КІІ.

На основі проведеного аналізу за розробленим методом, загрози було ранжовано згідно їх сумарного домінування. Представимо пріоритизацію загроз, де загрози з вищими значеннями сумарного домінування мають бути адресовані як найбільш критичні (табл. 4.31):

Таблиця 4.31

Ранжовані загрози сектору КІІ «Цифрові технології»

Загроза	**Рівень – Dom**	**Пріоритет**
Denial of Service (DoS)	**9.145**	**Найвищий**. Загроза DoS є найбільш критичною та має бути адресована першочергово для зниження ризиків відмови в обслуговуванні, що може призвести до значних збоїв в роботі КІ

Продовження табл. 4.31

Repudiation	**5.789**	**Високий**. Загрози, пов'язані з запереченням дій користувачів, вимагають удосконалення систем журналювання та аудиту для забезпечення відповідності та прозорості операцій
Spoofing	**2.406**	**Середній**. Ця загроза вимагає зміцнення аутентифікаційних процедур та поліпшення систем ідентифікації та верифікації для запобігання несанкціонованому доступу
Information disclosure	**-1.004**	**Середній**. Необхідно зміцнити механізми захисту даних, особливо щодо конфіденційної інформації, щоб уникнути її несанкціонованого розголошення
Tampering	**-1.564**	**Низький**. Потрібно забезпечити захист від несанкціонованого втручання в дані, але це не є так критично, як інші загрози.
Elevation of Privilege	**-13.338**	**Низький**. Хоча це серйозна загроза, вона має найнижчий показник домінування і може бути адресована після інших, більш нагальних проблем.

На рис. 4.17 представлено результати оцінювання ІТ-загроз для підсектору КІ «електронні комунікації», відповідно до табл. 4.31.

Отже, відповідно до результатів, отриманих за допомогою розробленого спеціального програмного забезпечення, отримали наступні рекомендації щодо ІТ-загроз:

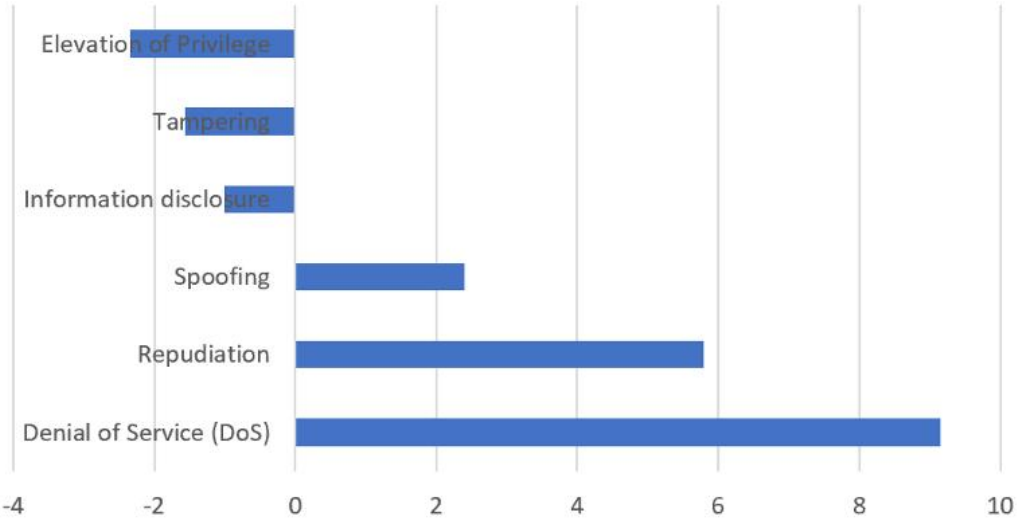


Рис. 4.17. Результати оцінювання IT-загроз для підсектору КІ «Електронні комунікації»

– Denial of Service (DoS): Найбільш критична загроза, що потребує першочергового усунення для зниження ризиків відмови в обслуговуванні, які можуть призвести до значних збоїв в роботі КІ. Рекомендується впровадити стійкі системи проти DoS-атак, використовуючи методи розподілу навантаження та захисту на рівні мережі.

– Repudiation: Вимагає удосконалення систем журналювання та аудиту для забезпечення відповідності та прозорості операцій. Слід впровадити надійні механізми логування та збереження журналів дій користувачів, а також регулярні аудити для виявлення та запобігання спробам заперечення дій.

– Spoofing: Необхідно зміцнити аутентифікаційні процедури та поліпшити системи ідентифікації та верифікації для запобігання несанкціонованому доступу. Рекомендується використовувати багатофакторну аутентифікацію та вдосконалені методи верифікації користувачів.

– Information Disclosure: Необхідно посилити механізми захисту даних, особливо конфіденційної інформації, щоб уникнути її несанкціонованого

розголошення. Варто впровадити шифрування даних як під час передачі, так і під час зберігання, а також використовувати системи моніторингу та виявлення витоків інформації.

– Tampering: Потрібно забезпечити захист від несанкціонованого втручання в дані, хоча ця загроза не є настільки критичною, як інші. Слід використовувати контроль цілісності даних та впроваджувати системи виявлення змін у даних.

– Elevation of Privilege: Хоча це серйозна загроза, вона має найнижчий показник домінування і може бути адресована після більш нагальних проблем. Для запобігання підвищенню привілеїв необхідно реалізувати принцип найменших привілеїв, регулярні перевірки прав доступу та використання інструментів для виявлення та блокування спроб підвищення прав користувачів.

Верифікація розробленого методу

Для перевірки адекватної роботи методу, було проведено 3 додаткові експерименти для паливно-енергетичного сектору КІ, охорони здоров’я та сектору транспорт і пошта.

Застосуємо розроблений метод для пріоритизації загроз «Паливно-енергетичого» сектору КІІ. Результати відображено у табл. 4.32:

Таблиця 4.32

Ранжовані загрози «Паливно-енергетичого» сектору КІІ

Загроза	**Рівень – Dom**	**Пріоритет**
Denial of Service (DoS)	8.215	**Найвищий**. Потрібні стійкі системи проти DoS-атак.
Repudiation	5.789	**Високий**. Загрози, пов'язані з запереченням дій користувачів, вимагають удосконалення систем журналювання та аудиту для забезпечення відповідності та прозорості операцій

Продовження табл. 4.32

Spoofing	4.678	**Високий.** Необхідне покращення аутентифікаційних процедур.
Information disclosure	2.134	**Середній**. Середній. Потрібні кращі механізми захисту даних.
Tampering	-0.789	**Низький**. Низький. Потрібен захист від втручання в дані.
Elevation of Privilege	-3.256	**Низький**. Можна адресувати після критичніших загроз.

Найвищий пріоритет був наданий загрозі Denial of Service (DoS) з рівнем Dom 8.215, що підтверджує критичну важливість безперервності електропостачання. Інші загрози, такі як Spoofing та Information disclosure, також були належним чином оцінені, що свідчить про здатність методу враховувати різні типи загроз.

Застосуємо розроблений метод для пріоритизації загроз сектору КІІ «Охорони здоров'я». Результати відображено у табл. 4.33:

Таблиця 4.33

Ранжовані загрози сектору КІ «Охорони здоров'я»

Загроза	**Рівень – Dom**	**Пріоритет**
Information disclosure	9.567	**Найвищий.** Потрібні надійні механізми захисту даних пацієнтів.
Denial of Service (DoS)	6.234	**Високий.** Потрібні стійкі системи проти DoS-атак.

Продовження табл. 4.43

Spoofing	3.678	**Середній.** Необхідне покращення аутентифікаційних процедур.
Tampering	2.123	**Середній**. Потрібен захист від втручання в дані.
Elevation of Privilege	-1.123	**Низький.** Можна адресувати після критичніших загроз.
Repudiation	-2.789	**Низький.** Вимагає удосконалення систем журналювання та аудиту.

На рис. 4.18 представлено результати оцінювання ІТ-загроз для сектору КІІ «Охорона здоров'я», відповідно до табл. 4.33:

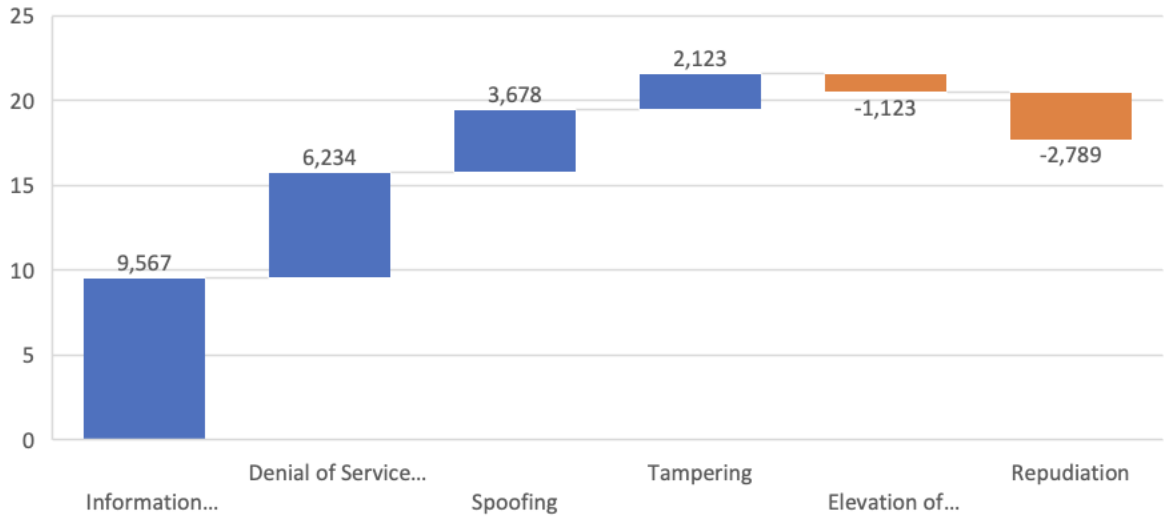


Рис. 4.18. Результати оцінювання ІТ-загроз для сектору КІІ «Охорона здоров'я»

Найбільший пріоритет отримала загроза Information disclosure (Dom 9.567), що підкреслює важливість захисту конфіденційних даних пацієнтів. Denial of

Service (DoS) також показала високий пріоритет, що вказує на необхідність забезпечення доступності медичних послуг.

Застосуємо розроблений метод для пріоритизації загроз сектору КІІ «Транспорт і пошта». Результати відображено у табл. 4.34:

Таблиця 4.34

Ранжовані загрози сектору КІІ «Транспорт і пошта»

Загроза	**Рівень – Dom**	**Пріоритет**
Denial of Service (DoS)	7.986	**Найвищий**. Найвищий. Потрібні стійкі системи проти DoS-атак.
Spoofing	4.567	**Високий.** Необхідне покращення аутентифікаційних процедур.
Information disclosure	2.345	**Середній**. Потрібні кращі механізми захисту даних.
Tampering	1.789	**Середній**. Потрібен захист від втручання в дані..
Elevation of Privilege	-0.789	Низький. Можна адресувати після критичніших загроз.
Repudiation	-2.123	**Низький**. Вимагає удосконалення систем журналювання та аудиту.

На рис. 4.19 представлено результати оцінювання ІТ-загроз для сектору КІІ «Транспорт і пошта», відповідно до табл. 4.34

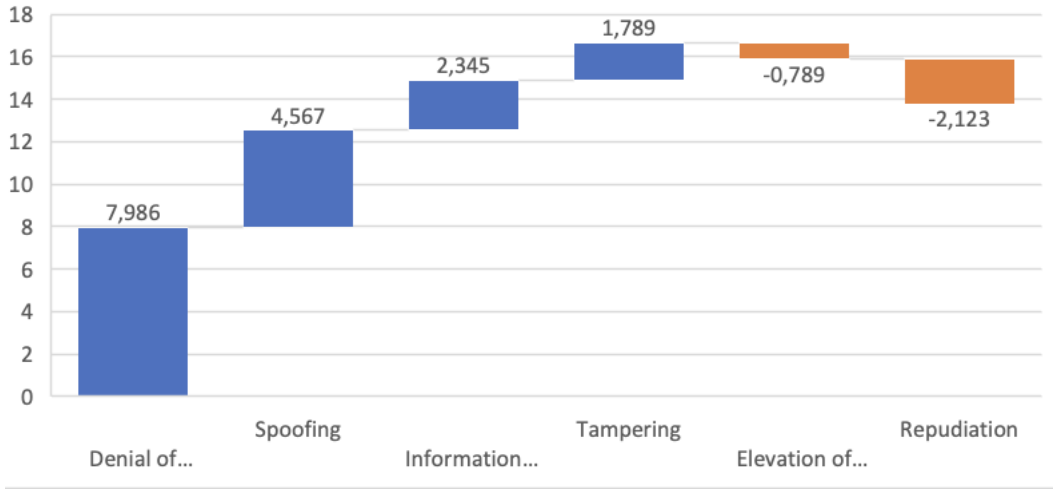


Рис. 4.19. Результати оцінювання IT-загроз для сектору КІІ «Транспорт і пошта»

Найвищий пріоритет був наданий загрозі Denial of Service (DoS) з рівнем Dom 7.986, що підкреслює важливість безперервності транспортних систем. Загрози Spoofing та Information disclosure були відповідно оцінені, підтверджуючи ефективність методу для різних аспектів безпеки.

Отже, проведені додаткові експерименти для різних галузей КІ (енергетика, охорона здоров'я та транспорт) демонструють адекватність і універсальність розробленого методу оцінки IT-загроз. Зміна вхідних даних відповідно до специфічних загроз кожної галузі не вплинула на здатність методу ефективно визначати та пріоритизувати ризики.

4.4. Висновки до четвертого розділу

Отже, у цьому розділі на основі розробленого спеціалізованого програмного забезпечення були проведені експериментальні дослідження для різних секторів КІ, таких як цифрові технології, телекомунікації, енергетика, охорона здоров'я, транспорт та ін., чим було верифіковано розроблені у роботі методи управління IT-інцидентами на ОКІІ.

4.5. Список літератури до четвертого розділу

1. Закон України про критичну інфраструктуру. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 01.06.2024).

2. Кабінет Міністрів України. (2020). Деякі питання об'єктів критичної інфраструктури: Постанова від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 01.06.2024).

3. National Cyber Security Index. URL: http://ncsi.ega.ee/ncsi-index/

4. E-Government Development Index (EGDI). URL: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index (дата звернення 01.06.2024).

5. Knoema. UN E-Government Development Index. Retrieved from https://ru.knoema.com/infographics/mctunlb/un-e-government-development-index?indicator=Telecommunication%20Infrastructure%20Index%20(TII).

6. International Telecommunication Union (ITU). Core ICT Indicators. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/coreindicators/Core_ICT_Indicators_E.pdf.

7. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Fesenko, A., Akatayev, N., Zhilkishbayeva, G. «Method of cybersecurity level determining for the critical information infrastructure of the state» CEUR Workshop Proceedings, 2020, Vol. 2616, pp. 332-341.

8. Gnatyuk, S., Sydorenko, V., Polozhentsev, A. «Method for Cybersecurity Level Evaluation in the Civil Aviation Critical Infrastructure» Lecture Notes in Networks and Systems, 2023, Vol. 736, pp. 206-218, DOI: 10.1007/978-3-031-38082-2_16.

9. В. Сидоренко, А. Положенцев, С. Гнатюк, «Метод визначення рівня кібербезпеки галузі критичної інформаційної інфраструктури держави», Вісник інженерної академії України, вип. 42, С. 81- 89, 2017.

10. А. Положенцев, В. Сидоренко, «Метод визначення рівня кібербезпеки галузі критичної інформаційної інфраструктури держави», Матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2018. Сучасні проблеми науки», К., 4-6 квітня 2018 р., с. 10-13, 2018.

11. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Sotnichenko, Y. Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure. *IEEE International Conference on Problems of Infocommunications Science and Technology*. 2021. P. 757-764. DOI: https://doi.org/10.1109/PICST51311.2020.9467987.

12. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., Polozhentsev, A. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. *CEUR Workshop Proceedings*, 2022. Vol. 3156. P. 390-399. URL: https://ceur-ws.org/Vol-3156/paper29.pdf

13. Положенцев А. А., Сидоренко В. М. Метод управління ІТ-загрозами на об’єктах критичної інформаційної інфраструктури. Наукоємні технології. 2024. Т. 2, № 62. С. 121–133.

14. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління. 2024. Т. 2. №78. С. 68-80.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв’язання актуальної та важливої науково-технічної задачі розроблення методів управління ІТ-інцидентами об’єктів критичної інформаційної інфраструктури.

У результаті виконання дисертаційної роботи було отримано такі наукові та практичні результати:

1. Проведено аналіз сучасних підходів до оцінювання стану захищеності об’єктів критичної інфраструктури держави. Вивчено існуючі методології та стандарти в сфері ІТ-безпеки, ідентифіковано основні недоліки та області для покращення.

2. Удосконалено метод визначення рівня захищеності об'єктів критичної інформаційної інфраструктури за рахунок використання нових індикаторів ІТ-безпеки та рівня цифрової трансформації, дає змогу визначити стан захищеності об’єктів критичної інфраструктури. Розроблено рекомендації для ефективного управлінню захистом від ІТ-інцидентів а також створено спеціалізоване програмне забезпечення для автоматизації процесу визначення стану захищеності об’єктів критичної інформаційної інфраструктури.

3. Удосконалено метод визначення пріоритетів ІТ-інцидентів шляхом представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації. Створено ієрархічні структури, які дозволяють систематизувати та класифікувати потенційні ІТ-інциденти, розроблено модель для розрахунку ймовірності реалізації кожної загрози, визначено пріоритетність загроз на основі кількісного аналізу.

4. Розроблено метод оцінювання ІТ-загроз, для ідентифікації, оцінки та пріоритизації ІТ-загроз для оптимального розподілу ресурсів захисту критичної інформаційної інфраструктури. Крім цього, було розроблено спеціалізоване

програмне забезпечення для визначення пріоритетів ІТ-загроз, що дозволяє ефективно ідентифікувати та пріоритизувати ІТ-загрози.

5. Проведено верифікацію розроблених методів для підтвердження їх ефективності та придатності до практичного застосування. Виконано тестування розроблених методів в реальних умовах, підтверджено ефективність методів на практиці, виявлено потенційні напрямки для подальшого вдосконалення. Результати дисертаційного дослідження впроваджені і використовуються у науково-дослідній діяльності НДЛ протидії кіберзагрозам авіаційної галузі НАУ (акт впровадження від 11.12.2023 р.), а також у ДержНДІ технологій кібербезпеки та захисту інформації для підвищення ефективності підготовки фахівців з ІТ та забезпечення захисту ОКІ (акт впровадження від 14.06.2024 р.).

Додаток А. Лістинг (код) програмного застосунку визначення стану захищеності об’єктів критичної інформаційної інфраструктури

```
<html>
  <head>
    <title>"Method for cybersecurity level determination</title>
    <link href="https://fonts.googleapis.com/css?family=Roboto:300,400,500,700&display=swap&subset=cyrillic"
      rel="stylesheet"
    />
    <style>
      /* Generic styles */
      html {
        scroll-behavior: smooth;
      }

      body {
        margin: 0;
        background-color: #f4f4f4;
        font-size: 10px;
      }
      * {
        font-family: "Roboto", "Segoe UI", Tahoma, Geneva, Verdana, sans-serif;
      }

      h1,
      h2,
      h3,
      h4,
      h5,
      h6 {
        color: #455a64;
        font-weight: 400;
      }
      h1 {
        font-weight: 600;
        font-size: 2rem;
      }
      h2 {
```

```
  font-size: 1.5rem;
}

.wrapper {
  background-color: #fff;
  max-width: 1024px;
  padding: 2rem 3rem;
  margin: auto;
  box-shadow: 0 0 10px 0px #ccc;
}

.center {
  text-align: center;
}

sub,
sup {
  font-weight: 300;
}

/* Styles for the hero image */
.hero {
  /* Photo by mnm.all on Unsplash */
  box-shadow: 0 0 0 1px #455a64 inset;
  border-radius: 0.5rem;
  padding: 4rem 2rem;
  /* grid styles */
  display: grid;
  grid-template-columns:     repeat(auto-fit,
minmax(240px, 1fr));
  align-items: center;
}

.hero > * {
  color: #263238;
}

.hero > h1 {
  font-size: 3rem;
  font-weight: 400;
  padding-bottom: 1rem;
}
```

```
.hero > article > p > img {
  width: 100%;
}

/* grid styles */
.grid {
  padding: 2rem 0;
  color: #666666;
}

.grid h2 {
  margin-top: 5rem;
}

.grid > ul {
  list-style: none;
  display: grid;
  grid-template-columns: repeat(auto-fit, minmax(200px, 1fr));
  grid-row-gap: 1rem;
  grid-column-gap: 0.5rem;
  padding: 0;
}

.grid > ul > li {
  border: 1px solid #e2e2e2;
  font-size: 1rem;
  line-height: 1.5;
  padding: 1rem 0.75rem;
  display: flex;
  flex-direction: column;
  justify-content: space-between;
}

.grid input {
  display: block;
  width: 100%;
  background: #eceff1;
  font-size: 1.2rem;
  margin-top: 1rem;
  padding: 1rem 0.5rem;
```

```
  border: 1px solid #cfd8dc;
  text-align: center;
}
.small-input {
  display: inline;
  padding: 0.2rem 1rem;
}
.small-input:not(:empty) {
  box-shadow: 0 0 0 1px #009688 inset;
}

.blue-bg {
  background-color: #e1f5fe;
}
.blue-text {
  color: #263238;
}
.gray-bg {
  background-color: #fafafa;
}
.yellow-bg {
  background-color: #fff9c4;
}
.green-bg {
  background-color: #e8f5e9;
}

hr {
  border: none;
  border-top: 2px solid #607d8b;
  margin: 5rem 0;
}

.darkblue-bg {
  background-color: #e3f2fd;
}
.orange-bg {
  background-color: #fff3e0;
}
.red-text {
  color: #880e4f;
}
```

```
    .green-text {
      color: #00695c;
    }
    .formula {
      display: inline-block;
      margin-bottom: -1rem;
      position: relative;
      top: 1.1rem;
      padding: 0 1rem;
    }
    .formula > span:first-child {
      display: block;
      border-bottom: 2px solid;
    }
    .formula > span:last-child {
      display: block;
    }
  </style>
</head>
<body>
  <main class="wrapper">
        <section class="hero">
          <h1>                                    </h1>
          <article>
            <p>

            </p>
          </article>
        </section>
        <section class="grid">
          <div class="center">
            <h1>
              P<sub>CS</sub> = P<sub>1</sub> +
P<sub>2</sub> + P<sub>3</sub>+
              P<sub>4</sub>
            </h1>
          </div>

          <!-----------------------------------------------
------------------------------------>
          <h2>
```

```
        P<sub>1</sub> &mdash; general cybersecurity indicators (GEN) =
        <span class="small-input" id="p-1-val"></span>
       </h2>
       <ul>
        <li class="blue-bg">
         <div>
          <div class="center blue-text">P<sub>PLC</sub> =</div>
          <div>&mdash; cybersecurity policy development </div>
         </div>
         <div>
          <input
           type="number"
           min="0"
           max="8"
           step="1"
           id="p-plc"
           placeholder="value from 0 t0 8"
          />
         </div>
        </li>
        <li class="blue-bg">
         <div>
          <div class="center blue-text">P<sub>THR</sub> =</div>
          <div>&mdash; cyber threat analysis and information </div>
         </div>
         <div>
          <input
           type="number"
           min="0"
           max="4"
           step="1"
           id="p-thr"
           placeholder="value from 0 to 4"
          />
         </div>
        </li>
```

```
        <li class="blue-bg">
          <div>
            <div class="center blue-text">P<sub>EDU</sub> =</div>
            <div>
              &mdash; education and professional development
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="p-edu"
              placeholder="value from 0 to 10"
            />
          </div>
        </li>
      </ul>

      <!-------------------------------------------------------------------------->
      <h2>
        P<sub>2</sub> &mdash; baseline cybersecurity indicators (BAS) =
        <span class="small-input" id="p-2-val"></span>
      </h2>
      <ul>
        <li class="gray-bg">
          <div>
            <div class="center blue-text">P<sub>BASS</sub> =</div>
            <div>&mdash; cybersecurity baselines</div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="11"
```

```
            step="1"
            id="p-dsp"
            placeholder="value from 0    11"
           />
          </div>
         </li>
         <li class="gray-bg">
          <div>
           <div          class="center          blue-
text">P<sub>ESEV</sub> =</div>
           <div>
            &mdash; E-services protection
           </div>
          </div>
          <div>
           <input
            type="number"
            min="0"
            max="4"
            step="1"
            id="p-essp"
            placeholder="value from 0 t0 4"
           />
          </div>
         </li>
         <li class="gray-bg">
          <div>
           <div          class="center          blue-
text">P<sub>EIDN</sub> =</div>
           <div>
            &mdash; E-identification and trust
services
           </div>
          </div>
          <div>
           <input
            type="number"
            min="0"
            max="8"
            step="1"
            id="p-eits"
            placeholder="value from 0 to 8"
           />
```

```
        </div>
      </li>
      <li class="gray-bg">
        <div>
          <div class="center blue-text">P<sub>CIIP</sub> =</div>
          <div>
            &mdash; critical information infrastructure protection
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="6"
            step="1"
            id="p-pdp"
            placeholder="value from 0 to 6"
          />
        </div>
      </li>
      </ul>

      <!----------------------------------------------
------------------------------------>
      <h2>
        P<sub>3</sub> &mdash; incident and crisis management indicators (ICM) =
        <span class="small-input" id="p-3-val"></span>
      </h2>
      <ul>
        <li class="yellow-bg">
          <div>
            <div class="center blue-text">P<sub>CIRC</sub> =</div>
            <div>&mdash; cyber incidents response </div>
          </div>
          <div>
            <input
              type="number"
```

```
            min="0"
            max="9"
            step="1"
            id="p-circ"
            placeholder="value from 0 to 9"
          />
        </div>
      </li>
      <li class="yellow-bg">
        <div>
          <div class="center blue-text">P<sub>CRIS</sub> =</div>
          <div>&mdash; cyber crisis management</div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="9"
            step="1"
            id="p-cris"
            placeholder="value from 0 to 9"
          />
        </div>
      </li>
      <li class="yellow-bg">
        <div>
          <div class="center blue-text">P<sub>CRIM</sub> =</div>
          <div>
            &mdash; fight against cybercrime
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="10"
            step="1"
            id="p-crim"
            placeholder="value from 0 to 10"
```

```
        />
      </div>
    </li>
    <li class="yellow-bg">
      <div>
        <div class="center blue-text">P<sub>MIL</sub> =</div>
        <div>
          &mdash; military cyber operations
        </div>
      </div>
      <div>
        <input
          type="number"
          min="0"
          max="10"
          step="1"
          id="p-mil"
          placeholder="value from 0 to 10"
        />
      </div>
    </li>
  </ul>

  <!-------------------------------------------------
------------------------------------>
  <h2>
    P<sub>4</sub> &mdash; international impact indicators
    (INT) =
    <span class="small-input" id="p-4-val"></span>
  </h2>
  <ul>
    <li class="green-bg">
      <div>
        <div class="center blue-text">P<sub>INT</sub> =</div>
        <div>&mdash; set of international impact indicators </div>
      </div>
      <div>
        <input
```

```
            type="number"
            min="0"
            max="1"
            step="1"
            id="p-conv"
            placeholder="value from 0 to 1"
          />
        </div>
      </li>
      <li class="green-bg">
        <div>
          <div class="center blue-text">P<sub>INTC</sub> =</div>
          <div>
            &mdash; Representation in international cybersecurity unions
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="1"
            step="1"
            id="p-intc"
            placeholder="value from 0 to 1"
          />
        </div>
      </li>
      <li class="green-bg">
        <div>
          <div class="center blue-text">P<sub>INTS</sub> =</div>
          <div>
            &mdash; The presence of international organizations on cyber security
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="3"
            step="1"
```

```
            id="p-ints"
            placeholder="value from 0 to 3"
           />
          </div>
         </li>
         <li class="green-bg">
          <div>
           <div class="center blue-text">P<sub>DEV</sub> =</div>
           <div>
            &mdash; Development of cybersecurity solutions for the international community
           </div>
          </div>
          <div>
           <input
            type="number"
            min="0"
            max="1"
            step="1"
            id="p-dev"
            placeholder="Value from 0 to 1"
           />
          </div>
         </li>
        </ul>

        <!---------------------------------------------
-------------------------------------->
        <div class="center">
         <h1>
          P<sub>CS</sub> = P<sub>1</sub> + P<sub>2</sub> + P<sub>3</sub>+
          P<sub>4</sub> =
          <span class="small-input" id="p-cs"></span>
         </h1>
         <h2>
          P<sub>CS</sub>% =
((P<sub>PLC</sub> + P<sub>THR</sub> + P<sub
           >EDU</sub
```

```
        >
        +           P<sub>DSP</sub>          +
P<sub>ESSP</sub>  +  P<sub>EITS</sub>  +
P<sub
         >PDP</sub
        >
        +           P<sub>CIRC</sub>         +
P<sub>CRIS</sub>  +  P<sub>CRIM</sub>  +
P<sub
         >MIL</sub
        >
        +           P<sub>INT</sub>          +
P<sub>CONV</sub>  +  P<sub>INTC</sub>  +
P<sub
         >INTS</sub
        >
        + P<sub>DEV</sub>) / 77) * 100% =
        <span  class="small-input"  id="p-cs-
perc"></span>
       </h2>
      </div>
```

```
      <hr />
      <div class="center">
       <h1 class="red-text">
        M<sub>DDL</sub> =
        <span class="formula">
         <span>M<sub>IDI</sub>          +
M<sub>NRI</sub></span>
         <span>2</span>
        </span>
       </h1>
      </div>
      <!-----------------------------------------------
------------------------------------->
      <h2>
       M<sub>IDI</sub>  &mdash;  ICT
Development Index (IDI) =
       <span  class="small-input"  id="m-
idi"></span>
      </h2>
```

```
<ul>
 <li class="darkblue-bg">
  <div>
   <div class="center blue-text">M<sub>ACC</sub> =</div>
   <div>&mdash; ICT access</div>
  </div>
  <div>
   <input
    type="number"
    min="0"
    max="10"
    step="1"
    id="m-acc"
    placeholder="value from 0 to 10"
   />
  </div>
 </li>
 <li class="darkblue-bg">
  <div>
   <div class="center blue-text">M<sub>USE</sub> =</div>
   <div>
    &mdash; ICT use
   </div>
  </div>
  <div>
   <input
    type="number"
    min="0"
    max="10"
    step="1"
    id="m-use"
    placeholder="value from 0 to 10"
   />
  </div>
 </li>
 <li class="darkblue-bg">
  <div>
   <div class="center blue-text">M<sub>SKI</sub> =</div>
```

```
          <div>
            &mdash; ICT skills
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="10"
            step="1"
            id="m-ski"
            placeholder="value from 0 to 10"
          />
        </div>
      </li>
    </ul>
    <!-----------------------------------------------
------------------------------------>
    <h2>
      M<sub>NRI</sub> &mdash; Networked
Readiness Index (NRI) =
          <span class="small-input" id="m-
nri"></span>
    </h2>
    <ul>
      <li class="orange-bg">
        <div>
          <div class="center blue-
text">M<sub>POL</sub> =</div>
          <div>
            &mdash; political and regulatory
environment
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="10"
            step="1"
            id="m-pol"
            placeholder="value from from 0 to
10"
```

```
        />
      </div>
    </li>
    <li class="orange-bg">
      <div>
        <div class="center blue-text">M<sub>INN</sub> =</div>
        <div>
          &mdash; business and innovation environment
        </div>
      </div>
      <div>
        <input
          type="number"
          min="0"
          max="10"
          step="1"
          id="m-inn"
          placeholder="value from from 0 to 10"
        />
      </div>
    </li>
    <li class="orange-bg">
      <div>
        <div class="center blue-text">M<sub>RDN</sub> =</div>
        <div>
          &mdash; ICT readiness
        </div>
      </div>
      <div>
        <input
          type="number"
          min="0"
          max="10"
          step="1"
          id="m-rdn"
          placeholder="value from from 0 to 10"
        />
      </div>
```

```
        </li>
        <li class="orange-bg">
          <div>
            <div class="center blue-text">M<sub>AFF</sub> =</div>
            <div>
              &mdash; ICT accessibility
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="m-aff"
              placeholder="value from from 0 to 10"
            />
          </div>
        </li>
        <li class="orange-bg">
          <div>
            <div class="center blue-text">M<sub>BUS</sub> =</div>
            <div>
              &mdash; business sector usage
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="m-bus"
              placeholder="value from from 0 to 10"
            />
          </div>
        </li>
        <li class="orange-bg">
```

```
          <div>
            <div class="center blue-text">M<sub>GOV</sub> =</div>
            <div>
              &mdash; governance support
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="m-gov"
              placeholder="value from from 0 to 10"
            />
          </div>
        </li>
        <li class="orange-bg">
          <div>
            <div class="center blue-text">M<sub>SOC</sub> =</div>
            <div>
              &mdash; social impacts
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="m-soc"
              placeholder="value from from 0 to 10"
            />
          </div>
        </li>
        <li class="orange-bg">
          <div>
```

```
            <div class="center blue-
text">M<sub>SKIL</sub> =</div>
            <div>
              &mdash; ICT efficiency
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="m-skil"
              placeholder="value from from 0 to
10"
            />
          </div>
        </li>
        <li class="orange-bg">
          <div>
            <div class="center blue-
text">M<sub>USE</sub> =</div>
            <div>
              &mdash; efforts to improve the ICT
usage
            </div>
          </div>
          <div>
            <input
              type="number"
              min="0"
              max="10"
              step="1"
              id="m-use2"
              placeholder="value from from 0 to
10"
            />
          </div>
        </li>
        <li class="orange-bg">
          <div>
```

```
          <div class="center blue-text">M<sub>IMP</sub> =</div>
          <div>
            &mdash; ICT improving impact
          </div>
        </div>
        <div>
          <input
            type="number"
            min="0"
            max="10"
            step="1"
            id="m-imp"
            placeholder="value from from 0 to 10"
          />
        </div>
      </li>
    </ul>

    <div class="center">
      <h1 class="red-text">
        M<sub>DDL</sub> =
        <span class="formula">
          <span>M<sub>IDI</sub> + M<sub>NRI</sub></span>
          <span>2</span>
        </span>
        <span class="small-input" id="m-ddl"></span>
      </h1>
    </div>
    <div class="center">
      <h1 class="red-text">
        M<sub>DDL</sub>% =
        <span class="formula">
          <span>
            (M<sub>IDI</sub> + M<sub>NRI</sub>) / 2
          </span>
          <span>
            10
          </span>
```

```
        </span>
        *
        100% =
        <span class="small-input" id="m-ddl-perc"></span>
      </h1>
    </div>

    <hr />
    <div class="center">
      <h1 class="green-text">
        I<sub>ratio</sub> = P<sub>CS</sub>% - M<sub>DDL</sub> % =
        <span class="small-input" id="i-ratio"></span>
      </h1>
    </div>
  </section>
 </main>

<script>
document.addEventListener("DOMContentLoaded", function() {
  const inputs = document.querySelectorAll("input[type='number']");

  function updateValues() {
    let pCs = 0;
    const maxScores = {
      pPlc: 8, pThr: 4, pEdu: 10, pDsp: 11, pEssp: 4, pEits: 8, pPdp: 6, pCirc: 9,
      pCris: 9, pCrim: 10, pMil: 10, pConv: 1, pIntc: 1, pInts: 3, pDev: 1,
      mAcc: 10, mUse: 10, mSki: 10, mPol: 10, mInn: 10, mRdn: 10, mAff: 10,
      mBus: 10, mGov: 10, mSoc: 10, mSkil: 10, mUse2: 10, mImp: 10
    };
    const pCsMax = 77; // Sum of max scores for cybersecurity indicators
```

```
    const mDdlMax = 20; // Sum of max scores for two main ICT indicators divided by 2

    inputs.forEach(input => {
        const id = input.id;
        const value = parseFloat(input.value) || 0;
        pCs += Math.min(value, maxScores[id] || 0); // Ensure value does not exceed max score
    });

    const pCsPercent = (pCs / pCsMax) * 100;
    const mIdi = ["mAcc", "mUse", "mSki"].reduce((acc, curr) => acc + (parseFloat(document.getElementById(curr).value) || 0), 0) / 3;
    const mNri = ["mPol", "mInn", "mRdn", "mAff", "mBus", "mGov", "mSoc", "mSkil", "mUse2", "mImp"].reduce((acc, curr) => acc + (parseFloat(document.getElementById(curr).value) || 0), 0) / 10;
    const mDdl = ((mIdi + mNri) / 2) * 10; // Adjusted to fit into the same scale as P_CS
    const mDdlPercent = (mDdl / mDdlMax) * 100;
    const iRatio = pCsPercent - mDdlPercent;

    document.getElementById("p-cs-perc").textContent = pCsPercent.toFixed(2) + "%";
    document.getElementById("m-ddl-perc").textContent = mDdlPercent.toFixed(2) + "%";
    document.getElementById("i-ratio").textContent = iRatio.toFixed(2) + "%";
  }

  inputs.forEach(input => input.addEventListener("input", updateValues));
  updateValues(); // Initial calculation on page load
});
```

```
</body>
</script>
</html>
```

Додаток Б. Лістинг (код) програмного застосунку методу визначення пріоритетів ІТ-загроз

```
// Define the headers
const headers = [
    "Type", "HI", "SI", "SEI", "SO", "CI", "UE", "CFI", "PI",
    "M", "V", "W - Vector", "Vector Ax", "Weighted Vector",
    "Lmax", "CI", "CR", "n", "RI (8x8)"
];

// Define the input data
const inputData = [
    ["HI", 1, 1/3, 1/2, 1/4, 1/5, 1/6, 1/7, 1/3],
    ["SI", 3, 1, 2, 4, 6, 4, 5, 2],
    ["SEI", 2, 1/2, 1, 5, 6, 7, 8, 1/4],
    ["SO", 4, 2, 1/5, 1, 1/3, 1/2, 1/7, 2],
    ["CI", 5, 3, 6, 3, 1, 1/2, 2, 3],
    ["UE", 6, 4, 7, 4, 2, 1, 3, 4],
    ["CFI", 7, 5, 8, 7, 3, 2, 1, 1/2],
    ["PI", 3, 2, 4, 1/2, 1/3, 1/4, 2, 1]
];

const M_VALUES = [15120, 40, 6720, 0.3, 0.001, 0.001, 0, 2];
```

```
const V_VALUES = [3.330, 1.586, 3.009, 0.860, 0.433, 0.428, 0.362, 1.091];
const W_VECTORS = [0.30004, 0.14289, 0.27112, 0.07751, 0.03901, 0.03852, 0.03265, 0.09826];
const VECTOR_AX = [2.53051648, 1.16438576, 2.25244806, 0.66374131, 0.3437942, 0.34895577, 0.29216545, 0.8172094];
const WEIGHTED_VECTORS = [8.43392409, 8.1489176, 8.3083117, 8.56294551, 8.81295128, 9.05885652, 8.9471714, 8.31704582];
const LMAX_VALUES = [8.57373981, 8.57373981, 8.57373981, 8.57373981, 8.57373981, 8.57373981, 8.57373981, 8.57373981];
const CI_VALUES = [0.08196, 0.08196, 0.08196, 0.08196, 0.08196, 0.08196, 0.08196, 0.08196];
const CR_VALUES = [0.05812, 0.05812, 0.05812, 0.05812, 0.05812, 0.05812, 0.05812, 0.05812];
const N_VALUES = [8, 8, 8, 8, 8, 8, 8, 8];
const RI_VALUES = [1.41, 1.41, 1.41, 1.41, 1.41, 1.41, 1.41, 1.41];

// Generate the data dynamically
const data = inputData.map((row, index) => {
    return [
        ...row,
        M_VALUES[index],
        V_VALUES[index],
```

```
        W_VECTORS[index],
        VECTOR_AX[index],
        WEIGHTED_VECTORS[index],
        LMAX_VALUES[index],
        CI_VALUES[index],
        CR_VALUES[index],
        N_VALUES[index],
        RI_VALUES[index]
    ];
});

// Function to display the data
function displayData(data, headers) {
    console.log(headers.join('\t'));
    data.forEach(row => {
        console.log(row.join('\t'));
    });
}

// Display the data
displayData(data, headers);
```

```
// Example of manipulating the data
function calculateTotals(data) {
    const totals = Array(data[0].length).fill(0);
    data.forEach(row => {
        row.forEach((value, index) => {
            if (!isNaN(value)) {
                totals[index] += value;
            }
        });
    });
    return totals;
}

const totals = calculateTotals(data);
console.log("Totals:", totals);

// Convert Excel-like structure to JavaScript variables
const incidentTypes = data.map(row => row[0]);
const hardwareIncidents = data.map(row => row[1]);
const softwareIncidents = data.map(row => row[2]);
```

```
const securityIncidents = data.map(row => row[3]);

const serviceOutages = data.map(row => row[4]);

const connectivityIssues = data.map(row => row[5]);

const userErrors = data.map(row => row[6]);

const configurationIssues = data.map(row => row[7]);

const performanceIssues = data.map(row => row[8]);

const mValues = data.map(row => row[9]);

const vValues = data.map(row => row[10]);

const wVectors = data.map(row => row[11]);

const vectorAx = data.map(row => row[12]);

const weightedVectors = data.map(row => row[13]);

const lmaxValues = data.map(row => row[14]);

const ciValues = data.map(row => row[15]);

const crValues = data.map(row => row[16]);

const nValues = data.map(row => row[17]);

const riValues = data.map(row => row[18]);


console.log("Incident Types:", incidentTypes);

console.log("Hardware Incidents:", hardwareIncidents);

console.log("Software Incidents:", softwareIncidents);

console.log("Security Incidents:", securityIncidents);
```

```
console.log("Service Outages:", serviceOutages);

console.log("Connectivity Issues:", connectivityIssues);

console.log("User Errors:", userErrors);

console.log("Configuration Issues:", configurationIssues);

console.log("Performance Issues:", performanceIssues);

console.log("M Values:", mValues);

console.log("V Values:", vValues);

console.log("W Vectors:", wVectors);

console.log("Vector Ax:", vectorAx);

console.log("Weighted Vectors:", weightedVectors);

console.log("Lmax Values:", lmaxValues);

console.log("CI Values:", ciValues);

console.log("CR Values:", crValues);

console.log("N Values:", nValues);

console.log("RI Values:", riValues);
```