МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

МАТЕРІАЛИ

XII Всеукраїнської науково-технічної конференції з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2024

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю [Електронний ресурс]. – Миколаїв : НУК, 2024. – 234 с.

У збірнику подано матеріали XII Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

СЕКЦІЯ 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 004.056.5;057.2

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО РАНЖУВАННЯ ЗАГРОЗ ЗА ISO/IEC 27005:2022

Автор: *Іванюк А.О., магістриня, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Організаційно-технічна модель кіберзахисту 2021 року [1], Стратегія кібербезпеки України [2] і планb її реалізації [3, 4] передбачають розвиток систем виявлення та реагування на кіберзагрози з метою ефективного управління ризиками інформаційної безпеки (РІБ) і забезпечення кіберготовності та кіберстійкості об'єктів інформаційної діяльності (ОІД), особливо об'єктів критичної інфраструктури.

Захист кіберпростору передбачає організацію ефективної протидії актуальним загрозам, визначення котрих передбачає проведення моніторингу і аналізу стану кіберпростору, створення і застосування ефективної системи індикаторів кіберзагроз, прогнозування появи загроз різних типів, їх очікуваних наслідків і визначення відповідних ризиків.

На даний час прийнято проводити аналіз факторів РІБ і оцінювання ризиків шляхом евристичних експертних оцінок. При цьому можуть застосовуватися десятки методів оцінки ризиків [5], вибір серед яких складно здійснити [6]. Визначення РІБ проводиться на основі прийнятих дослідником класифікації загроз, моделі загроз і методів оцінки ризиків, які мають узгоджуватися з діючими нормативними документами. Цим питанням присвячені роботи багатьох науковців та практиків як в Україні, так за кордоном [6-14], однак залишається невирішеною задача автоматизації процесів визначення рангів загроз за їх критичністю згідно із відповідності з міжнародними стандартами.

Метою даної роботи є розробка системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– провести аналіз відкритої нормативно-правової бази і визначити принципи та процедури ранжування загроз;

– визначити критерії і правила прийняття рішень щодо рангів загроз;

– розробити основні алгоритми і структуру системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022.

Ранжування загроз – це процес віднесення загроз до певного поіменованого діапазону заданого заданого критерію. Ранг загрози визначається за асоційованою із загрозою мірою ризику. Міра ризику може бути кількісною або якісною. Існує багато кількісних мір ризиків, які різняться як за розрахунковими формулами, так і за розмірністю: можуть бути виражені у грошовій або безрозмірній формі. Ризик, асоційований із загрозою, у кількісній формі є очікуваним збитком в разі успішної реалізації загрози. Якісна міра ризику є поіменованим діапазоном кількісної міри, наприклад, «високий», «середній», «низький», тобто фактично визначає ранг ризику з міркувань його критичності. Таким чином, для визначення рангів загроз необхідно сформувати перелік загроз, які підлягатимуть аналізу, обрати міру ризику і спосіб її визначення. Для складання переліку загроз необхідно прийняти певну класифікацію загроз. На даний час існує багато класифікацій загроз, наприклад, виділяють:

– в НД ТЗІ [15]: загрози конфіденційності, цілісності, доступності і спостережуваності інформації;

– в моделі STRIDE [16]: підміна мережевих об'єктів, модифікація даних, відмова від авторства, розголошування інформації, відмова в обслуговуванні, несанкціоноване підвищення рівня привілеїв;

– загрози, що характерні для певної предметної галузі, наприклад: загрози безпеці державних інформаційних ресурсів [14], загрози соціального інжинірингу [9], загрози критичній інфраструктурі [11], загрози для соціально-економічних процесів [13] тощо;

– в ISO/IEC 27005 [17], якому відповідає ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT), ідентифікація ризику передбачає обов'язкову ідентифікацію джерел ризику, подій, їх причин та потенційних наслідків,

а також може включати історичні дані, теоретичний аналіз, інформовані та експертні думки та потреби стейкхолдерів. Наприклад, джерелом загроз може бути людина, яка створює загрозу цілеспрямовано або внаслідок випадкової помилки, або природа, дії якої не є цілеспрямованими. В ISO/IEC 27005:22 передбачено, що від певних джерел можуть надходити загрози різних типів, наприклад: технічні відмови; втрата необхідних сервісів; компрометація інформації і функцій; несанкціоновані дії тощо;

– в моделі загроз DSECCT компанії Digital Security [18]: загрози класифікуються за характером загрози, видом впливу, джерелаами та за цільовими об'єктами загрози;

– в моделі OCTAVE [19]: передбачено різний ступінь деталізації первинного опису загроз і ризиків для великого і малого бізнесу тощо.

В даній роботі за основу прийнято класифікацію загроз, наведену в [12].

Оскільки ранжування загроз здійснюється за рівнем асоційованих з ними ризиків, то воно може бути проведене тільки після оцінювання ризиків як процедура перевірки належності відповідного ризику певному діапазону чи групі діапазонів ризиків. Після цього за правилами, визначеними в процесі менеджменту ризиків на етапах визначення контексту та ідентифікації ризиків, загрози певних рангів визнаються критичними у різному ступені.

Таким чином, вхідними даними для СППР ранжування загроз є дані, які мають бути отримані на етапі визначення контексту та ідентифікації ризиків, зокрема:

– сфера управління ризиками і джерела загроз;

– перелік інформаційних активів із визначеною цінністю, з переліками наявних вразливостей; і переліків асоційованих з ними загроз;

– перелік сценаріїв виникнення і реалізації загроз із визначеними джерелами загроз, активами-об’єктами атаки, ймовірностями виникнення кожного сценарію.

Опис сценаріїв також включає в себе:

– оцінки ймовірностей виникнення кожної загрози, асоційованої з певним активом;

– оцінки ймовірностей експлуатації кожною загрозою певних вразливостей, асоційованих з певним активом;

– оцінки ймовірностей успіху реалізації загроз при експлуатації певних вразливостей кожного активу;

– оцінки наслідків успіху реалізації загроз при експлуатації певних вразливостей кожного активу.

Визначення, оцінювання і аналіз ризиків здійснюється для кожного сценарію. Аналіз ризиків може здійснюватися для всієї множини обчислених ризиків або для окремої вибірки, яка формується за заданим ОПР критерієм, наприклад, ризики для певного активу або ризики, що асоційовані із загрозою порушення цілісності даних. Ранжовані ризики є основою для визначення рангів загроз, після чого СППР формує і видає ОПР звіт про отримані результати. На підставі цього звіту ОПР приймає рішення або про обробку ризиків або про проведення повторного аналізу загроз за біль детальним сценарієм.

Узагальнений алгоритм ранжування загроз за міжнародним стандартом ISO/IEC 27005:2022 наведено на рис.1.

Ранжування ризиків здійснюється за алгоритмом, наведеним на рис.2. При цьому користувач має задати кількість рангів ризиків NR і граничні значення ризиків a_n, b_n, що відповідають кожному n-ому рангу. На вхід блоку ранжування ризиків подається множина ризиків $\{R_{ijk}\}$, де i – номер активу, j – номер загрози, k – номер вразливості за рахунок успішної експлуатації котрої реалізується загроза. Ці номери визначаються із опису сценаріїв.

Ранжування загроз здійснюється за алгоритмом, наведеним на рис.3, який передбачає, що аналіз проводиться для певного активу. Кількість рангів загроз NZ задається ОПР. Послідовно переглядаються всі загрози і їх ранг визначається як m при умові, що сумарний ризик, асоційований із загрозою потрапляє в діапазон, обмежений значеннями $c_m = 1 + (m-1)\frac{NR}{NZ}$ і $d_m = c_m \frac{NR}{NZ}$. Ранги присвоюються у порядку зростання ризиків, тому, якщо загроза за різними сценаріями може експлуатувати різні вразливості, що матиме різні наслідки і, відповідно, ризики, то ранг цієї загрози буде перевизначатися. Остаточно загрозі буде присвоєно ранг, що відповідатиме максимальному ризику.

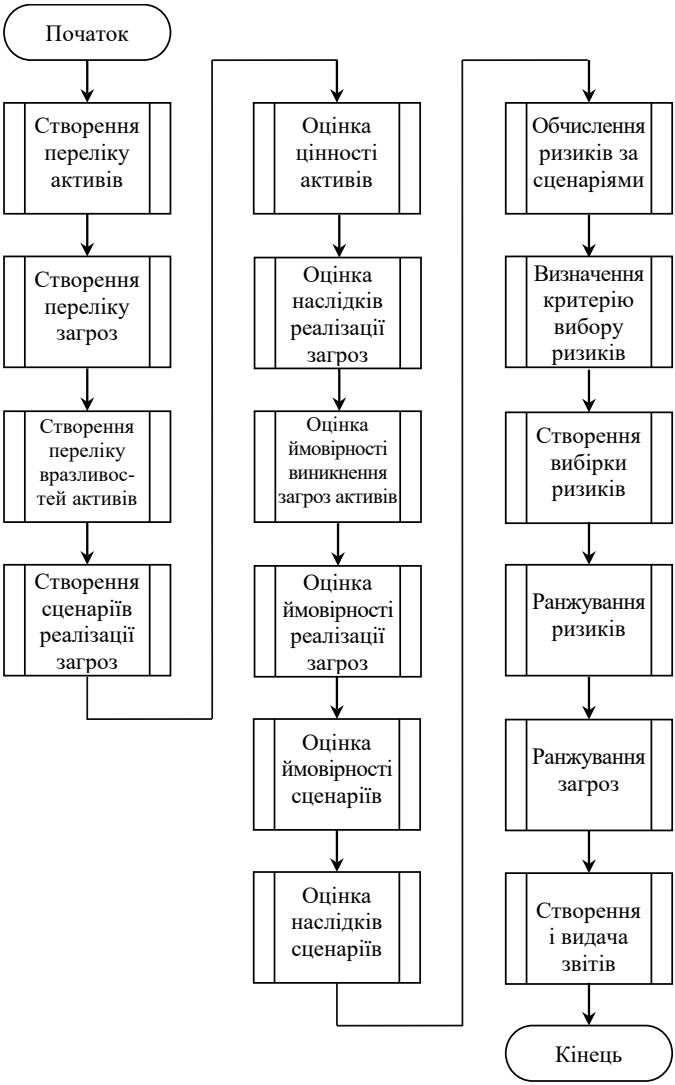

Рисунок 1 – Узагальнений алгоритм ранжування загроз за міжнародним стандартом ISO/IEC 27005:2022

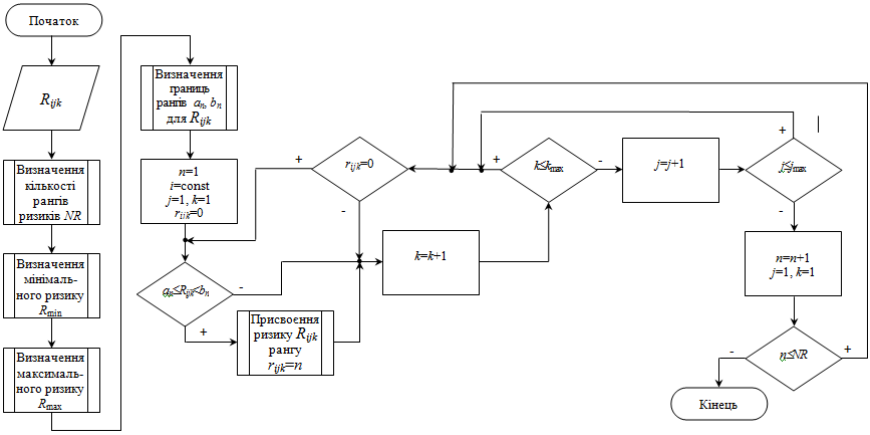

Рисунок 2 – Алгоритм блоку «Ранжування ризиків»

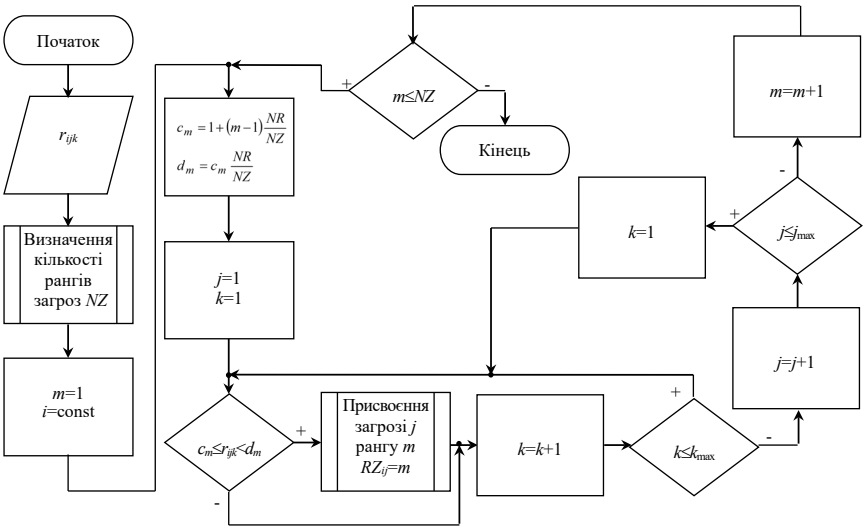

Рисунок 3 – Алгоритм блоку «Ранжування загроз» для і-го активу

Розроблена структура СППР наведена на рис.4 і передбачає, що користувачами СППР будуть ОПР та адміністратор СППР, який може вносити зміни в СППР на вимогу ОПР.

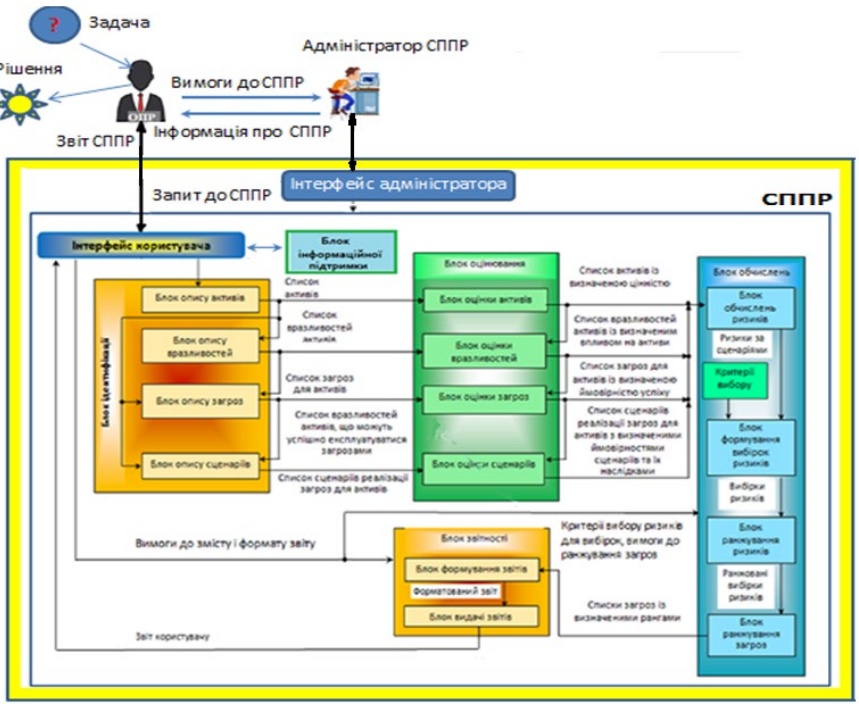

Рисунок 4. – Структура і користувачі СППР

Висновки

В даній роботі проведено аналіз відкритої нормативно-правової бази і визначені принципи та процедури ранжування загроз, критерії і правила прийняття рішень щодо рангів загроз; розроблено основні алгоритми і структуру СППР щодо ранжування загроз за ISO/IEC 27005:2022.

Список літератури:

1. Положення про організаційно-технічну модель кіберзахисту. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

2. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7

3. План реалізації Стратегії кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/ show/n0087525-21#Text

4. План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

5. ДСТУ EN IEC 31010:2022 Керування ризиками – методи оцінки ризиків (EN IEC 31010:2019, IDT; IEC 31010:2019, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100889

6. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології*. 2021. №1(23). С.62–68. URL: http://tst.stu.cn.ua/article/view/233549/232282

7. Carfora M., Martinelli F. Cyber Risk Management: An Actuarial Point of View. *Journal of Operational Risk*. 2021. Vol.4. №4. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778061

8. Top 10 emerging cyber-security threats for 2030. URL: https://www.enisa.europa.eu/news/ cybersecurity-threats-fast-forward-2030

9. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

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

11. Салієва О.В., Яремчук Ю.Є. Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз. *Реєстрація, зберігання і обробка даних*. 2020. Т. 22. № 2. С.63-76. URL: http://drsp.ipri.kiev.ua/article/view/211279

12. Турти М.В.; Доценко В.В. Інформаційна модель ранжування загроз за BS ISO/IEC 27005:2011. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2022. С.134-140.

URL: https://www.nuos.edu.ua/wp-content/uploads/2023/05/SPIBT-2022-Materiali-s-obkladinkoju.pdf

13. Шандрівська О. Є., Шинкаренко Н. В. Прикладна оцінка ризиків у системі забезпечення безпеки соціально-економічних процесів у кіберпросторі. *Вісник Національного університету "Львівська політехніка". Серія "Проблеми економіки та управління"*. 2020. №2(8). С.94-104.

14. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. К.: НАУ, 2015. 214 с. URL: https://er.nau.edu.ua/ bitstream/NAU/31911/1/Monogr_klas_ zagroz_Yudin_Buchyk.pdf

15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: http://www.dsszzi.gov.ua/dsszzi/doccatalog/ document ?id=106342

16. Зубок В.Ю. Оцінювання ризиків глобальної маршрутизації. *Електронне моделювання*. 2019. Т.41. №2. С.97-109. URL: https://www.emodel. org.ua/images/em/41-2/Zubok.pdf

17. ISO/IEC 27005:2022(en) Information security, cybersecurity and privacy protection — Guidance on managing information security risks URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en

18. Лисенко І. А. Методичні вказівки до виконання практичних робіт з навчальної дисципліни "Основи управління кібербезпекою". Кропивницький: ЦНТУ, 2018. 64 с. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/3256be49-4ce2-4178-a396-1c1136b8a237/content

19. Alberts C., Dorofee A., Stevens J., Woody C. Introduction to the OCTAVE® Approach. Pittsburgh, Pennsylvania, United States: Carnegie Mellon University. 2003. 27 p. URL: https://www.itgovernanceusa.com/files/Octave.pdf

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

XII Всеукраїнська науково-технічна конференція
з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич