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»

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

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

© Національний університет кораблебудування імені адмірала Макарова, 2024

9. IACS UR E27 Cyber resilience of on-board systems and equipment. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf

10. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

11. Naval Dome. URL: https://navaldome.com/index.html

12. Anomaly-Based Intrusion Detection Systems Using Machine Learning. Journal of Cybersecurity and Information Managemen. 2024. Vol. 14. No. 01. PP. 20-33. URL: https://americaspg.com/article/pdf/2836

13. Стефанюк Ю.В. Інтелектуальні засоби в системах виявлення та запобігання вторгнень. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.129-133. URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf

УДК 004.056.5

ЗВАЖЕНЕ ОЦІНЮВАННЯ КРИТИЧНОСТІ ОБ'ЄКТІВ МОРСЬКОГО ТА РІЧКОВОГО ТРАНСПОРТУ

Автор: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Морський та річковий транспорт є підсектором сектору «Транспорт і пошта», критичної інфраструктури (КІ) України, що підпорядковується Мінінфраструктури. Кібербезпеці об'єктів КІ (ОКІ) і об'єктів критичної інформаційної інфраструктури (ОКІІ) приділяється особлива увага як на міжнародному, так і на національному рівнях, оскільки ці об'єкти надають послуги, що є життєво важливими для населення та держави, а часто – і для інших держав.

Наприклад, у червні 2024 року Норвегія, Фінляндія та Швеція прийняли рішення про створення військово-транспортного коридору крізь північні території цих країн, який сприятиме швидкому переміщенню персоналу та матеріалів із портів Норвегії через Швецію до Фінляндії [1].

Зерновим коридором, який був запущений у липні 2022 року, з України експортували щонайменше 33 мільйонів тонн зерна, а після того як Росія вийшла з угоди у 2023 році, Україна у серпні 2023 року оголосила створення "гуманітарного коридору", щоб продовжувати постачання продовольства до африканських та азійських ринків [2]. Перша заступниця голови транспортного комітету ВРУ про Чорне море Юлія Клименко в своєму інтерв'ю [3] зазначила, що «Морська економіка і морська безпека мають розвиватися паралельно», оскільки блокада українських портів Росією є економічною блокадою, що має на меті подолання України як конкурента на міжнародних ринках і «не має нічого спільного з військовими діями». Однак, саме витискання російського флоту з Чорного моря дозволило Україні у 2024 році відправити морським коридором 66 мільйонів тонн вантажів і вийти на довоєнний рівень експорту 2021 року [2]. На даний час «свобода навігації … досягається виключно озброєнням нашого військово-морського флоту, коли ми можемо захистити наші порти, пробити собі морські коридори, ні у кого не питаючи дозволу, а виключно на основі міжнародного права» [3].

Таким чином, безпека річкового і морського транспорту є складовою національної економічної безпеки, а Стратегія розвитку водного транспорту має передбачати різні типи заходів, які дозволять відстояти інтереси України. Передумовою впровадження різних заходів і засобів захисту на ОКІ є визначення їх категорії критичності. Категоризація ОКІ проводиться згідно Закону України «Про критичну інфраструктуру» [4] і «Загальних вимоги до кіберзахисту об'єктів КІ» [5] за затвердженою методикою [6, 7]. Розв'язку комплексної проблеми захисту КІ проблеми присвячені роботи багатьох науковців та практиків, документи міжнародних організацій [8-13] тощо, однак на даний час методика визначення категорії [7] ОКІ базується на чітких бальних оцінках, що може привести до похибок категоризації.

Метою даної роботи є розробка пропозицій до удосконалення процедур категоризації об'єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно провести аналіз нормативно-правової бази категоризації, визначити наявні недоліки методики категоризації і розробити прпозиції до її удосконалення.

При оцінюванні критичності ОКІ за методикою, затвердженою постановою Кабінету міністрів України [6], і методичними вказівками,

затвердженими Наказом Адміністрації ДССЗЗІ [7], віднесення ОКІ до певної категорії критичності здійснюється на підставі належності показника нормованої оцінки рівня критичності ОКІ PK_{OKI} до певного інтервалу значень. Показник PK_{OKI} визначається як доля максимально можливого значення $\Sigma PK_{\max}$ для конкретного ОКІ і обчислюється як відношення суми оцінок ОКІ за секторальними і між секторальними критеріями ΣPK_i до $\Sigma PK_{\max}$.

Оцінка за кожним критерієм PK_i згідно [7] визначається експертом як чітке число, хоча для окремих критеріїв підставою для визначення оцінок є належність певного кількісного показника до певного числового діапазону, що за змістом відповідає носію нечіткої множни. Крім того, експерт може не бути впевнений на 100% у належності кількісного показника певного між секторального критерію до конкретного інтервалу.Наприклад, експерт з μ_1=0,8 може відносити значення певного показника до інтервалу 1, а з мірою впевненості μ_2=0,2 – до інтервалу 2. Тоді зважена оцінка за цим показником дорівнюватиме: $\mu_1 \cdot 1+\mu_1 \cdot 2=0{,}8 \cdot 1+0{,}2 \cdot 2=1{,}2$. Відповідно, різниця зваженої оцінки і чіткої оцінки становитиме 0,2, якщо експерт вибрав інтервал 1, і 0,8, якщо експерт вибрав інтервал 2. Такі похибки накопичуватимуться від одного показника до іншого. Оскільки максимально можливого значення є константою для певного ОКІ, то накопичені похибки безпосередньо вплинуть на значення , і відповідно на присвоюваний ОКІ рівень критичності.

Оцінка критичності ОКІ за секторальними критеріями визначається для кожного підсектору залежно від наслідків порушення надання послуг цим підсектором і отримується за 1 або 2 показниками, визначеними [7] окремо для кожного підсектору.

Наприклад, для підсектору річкового та морського транспорту знищення, пошкодження або порушення функціонування ОКІ може привести до катастрофічних наслідків (припинення надання морських послуг у морських портах більш як на 72 години, оцінка 4 бали), критичних наслідків (припинення надання морських послуг у морських портах від 24 до 72 годин, оцінка 3 бали), значних наслідків (припинення надання морських послуг у морських портах до 24 годин, 2 бали). Незначні

наслідки в цьому підскторі не оцінюються. Таким чином, оцінка у підсекторі морського та річного транспорту здійснюється за одним секторальним критерієм з показником «тривалість припинення надання морських послуг у морських портах», визначеним на вісі часу.

Для інформаційного сектору наслідки порушення надання основних послуг ОКІ в разі його знищення, пошкодження або порушення функціонування оцінюються за двома секторальними критеріями, з показниками «час відновлення функціонування у штатному режимі» і «кількість жителів». Оцінки надаються катастрофічним (4 бали), критичним (3 бали), значним (2 бали) і незначним (1 бал) наслідкам.

Таким чином, зважена оцінка за секторальними критеріями може розраховуватися як $\sum_{j=1}^{2}\sum_{i=1}^{4} i\mu_{ij}$, де $\sum_{i=1}^{4}\mu_{ij}=1$; $i=\overline{1,4}$ – номер оцінки, що відповідає кількості балів; $j=\overline{1,2}$ – номер показника. За методикою [7] оцінка за секторальними критеріями дорівнюватиме $\sum_{j=1}^{2} PK_j$, де $PK_j \in \{1,2,3,4\}$. Різниця між чіткими і нечіткими оцінками ОКІ певного підсектору в загальному випадку становитиме $\Delta=\sum_{j=1}^{2}\sum_{i=1}^{4} i\mu_{ij}-\sum_{j=1}^{2} PK_j=\sum_{j=1}^{2}\left(\sum_{i=1}^{4} i\mu_{ij}-PK_j\right)$. Якщо критичність підсектору оцінюється тільки за одним показником, то μ_{i2}=0, PK_2=0.

Приймемо, що конкуруючими є тільки сусідні терми оцінок [14]. Тоді

– для незначних наслідків

$$\Delta=\sum_{j=1}^{2}\left(\mu_{1j}+2\mu_{2j}-1\right)=\sum_{j=1}^{2}\left(\mu_{1j}+2\left(1-\mu_{1j}\right)-1\right)=\sum_{j=1}^{2}\left(1-\mu_{1j}\right);$$

– для катастрофічних наслідків

$$\Delta=\sum_{j=1}^{2}\left(4\mu_{4j}+3\mu_{3j}-4\right)=\sum_{j=1}^{2}\left(4\mu_{4j}+3\left(1-\mu_{4j}\right)-4\right)=\sum_{j=1}^{2}\left(\mu_{4j}-1\right);$$

– для критичних наслідків

$$\Delta = \sum_{j=1}^{2}\left(\left(4\mu_{4j} + 3\mu_{3j} + 2\mu_{2j}\right) - 3\right) = \sum_{j=1}^{2}\left(\left(4\mu_{4j} + 3\left(1 - \mu_{4j}\right) + 2\mu_{2j}\right) - 3\right) =$$

$$= \sum_{j=1}^{2}\left(\mu_{4j} + 2\mu_{2j}\right);$$

– для значних наслідків

$$\Delta = \sum_{j=1}^{2}\left(\left(3\mu_{3j} + 2\mu_{2j} + \mu_{1j}\right) - 2\right) = \sum_{j=1}^{2}\left(\left(3\mu_{3j} + 2\left(1 - \mu_{3j}\right) + \mu_{1j}\right) - 2\right) =$$

$$= \sum_{j=1}^{2}\left(\mu_{3j} + \mu_{1j}\right).$$

Аналогічно можна визначити різниці між чіткими і нечіткими оцінками ОКІ за міжсекторальнимми критеріями, для яких оцінки отримуються за 16-ма показниками. Якщо міра впевненості експерта в оцінці кожного показника є досить високою, припустимо 90%, а на інші оцінки припадає лише 10%, то накопичена похибка за секторальними і між секторальними критеріями для водного транспорту становитиме 1,7 бали, а нормована оцінка рівня критичності ОКІ буде відрізнятися на 2,5%, що може вплинути на рішення щодо категорії критичності ОКІ. Якщо середня міра впевненості експерта в оцінках буде гранично низькою – 60%, то накопичена похибка становитиме 6,8 балів, що змінить оцінку рівня критичності ОКІ на 10%.

Таким чином, недоліком наявної методики є потенційна наявність похибок внаслідок недостатньої впевненості експертів при оцінюванні критичності наслідків порушення надання ОКІ основних функцій. Для усування цього недоліку рекомендується модифікувати методику [7], додавши до експертних оцінок міру впевненості експертів у цих оцінках. Необхідність застосування модифікованої методики можна визначити шляхом оцінки впливу граничних величин накопиченої похибки на рішення щодо категоризації ОКІ.

Крім того, для морського і річкового транспорту в секторальних критеріях враховується тільки припинення надання морських послуг у морських портах, хоча порушення надання послуг річковими портами

також може мати масштабні наслідки. Внаслідок того, що склад стейкхолдерів в портах постійно змінюється, доцільно переглядати рівень критичності портів кожного разу при плануванні через них масштабних поставок і перевезень небезпечних чи цінних (з точки зору договірних зобов'язань) вантажів.

Висновки

В даній роботі проведено аналіз нормативно-правової бази категоризації, визначені недоліки методики категоризації і розробити прпозиції щодо її удосконалення.

Список літератури:

1. Норвегія, Фінляндія та Швеція створять транскордонний військово-транспортний коридор. URL: https://suspilne.media/773079-norvegia-finlandia-ta-svecia-stvorat-transkordonnij-vijskovo-transportnij-koridor/

2. Шмигаль: у 2024 році морським коридором Україна експортувала 66 мільйонів тонн вантажів. URL: https://suspilne.media/833077-smigal-u-2024-roci-morskim-koridorom-ukraina-eksportuvala-66-miljoniv-tonn-vantaziv/

3. Морська економіка і морська безпека мають розвиватися паралельно – інтерв'ю з Юлією Клименко. URL: https://cfts.org.ua/articles/morska_ekonomika_i_morska_bezpeka_mayut_rozvivatisya_paralelno__intervyu_z_yulieyu_klimenko_1990/137899

4. Закон України "Про критичну інфраструктуру". URL: https://zakon.rada. gov.ua/laws/show/1882-20#Text

5. Загальні вимоги до кіберзахисту об'єктів КІ, затверджені постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada. gov.ua/laws/show/518-2019-%D0%BF#n8

6. Методика категоризації об'єктів КІ, затверджена Постановою Кабінету міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 р. №1109. URL: https://zakon.rada.gov.ua/ rada/show/1109-2020-%D0%BF#Text

7. Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: https://zakon.rada.gov.ua/ rada/show/v0023519-21#Text

8. Cybersecurity in Maritime Critical Infrastructure. Reflection on African Ports. Critical Maritime Routes Programme Monitoring, Support and Evaluation Mechanism (CRIMSON III). (2023) URL: https://rusieurope.eu/wp-content/uploads/2024/02/cybersecurity-in-maritime-critical-infrastructure-crimson-report-english.pdf

9. Osei-Kyei R. et al. Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction. 60 (2021): 102316.

10. Tadas L. et al. Cyber security management model for critical infrastructure. International Journal Entrepreneurship and Sustainability. Issues ISSN 2345-0282 (online). URL: http://jssidoi.org/jesi/ 2017 Volume 4 Number 4 (June) http://doi.org/10.9770/jesi.2017.4.4(12)

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

12. Рогов П.Д., Воровичˇ Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері. Зб. наук. праць Центру воєнно-стратегічних досліджень Нац-го ун-ту оборони України ім. Івана Черняховського. 2017. № 1. С. 64-72. URL: http://znp-cvsd.nuou.org.ua/article/view/125525

13. 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

14. Турти М.В. Теорія однозначних нечітких систем і нейронні мережі. Монографія. В 2-х част. – М.: Миколаївська філія Європейського університету, 2007. – Ч.1. – 140 с.

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