

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

**СУЧАСНІ ПРОБЛЕМИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НА ТРАНСПОРТІ**

СПІБТ–2024

МАТЕРІАЛИ

**ХІІ 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

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

УДК 004.056.5

КРИТЕРІЇ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ В МОРСЬКІЙ ГАЛУЗІ

***Автор:** Турти М.Ю., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

У сучасному цифровому світі розвиток морської галузі тісно пов'язаний із впровадженням новітніх цифрових технологій, і, відповідно, успішність функціонування водного транспорту суттєво залежить від здатності критичної морської інформаційної інфраструктури протистояти кіберзагрозам.

Дослідженням практичних і теоретичних аспектів кібербезпеки на морі присвячені праці багатьох українських [1-4] та іноземних [5-11] фахівців, зокрема фахівців Національного університету кораблебудування [1, 3]. Однак, на даний час відсутні затверджені методики управління кіберризиками для критичної морської інформаційної інфраструктури (КМІІ) України.

Метою даної роботи є визначення критеріїв прийняття рішень щодо забезпечення кіберстійкості в морській галузі.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- визначити особливості забезпечення кіберстійкості в морській галузі;
- визначити особливості прийняття рішень в морській галузі;
- сформулювати перелік критеріїв прийняття рішень щодо забезпечення кіберстійкості в морській галузі і визначити принципи їх вибору для вирішення конкретних прикладних задач.

Визначення загального поняття «кіберстійкість» (англ. *Cyber resilience*) наводиться в Стратегії кібербезпеки України [12], згідно з якою кіберстійкість характеризується як здатність:

- до швидкої адаптації до внутрішніх і зовнішніх кіберзагроз;
- до підтримки сталого функціонування національної інформаційної інфраструктури;

– до відновлення сталого функціонування національної інформаційної інфраструктури після кіберінцидентів.

Стратегія кібербезпеки України першочерговою задачею називає забезпечення кіберстійкості об'єктів критичної інформаційної інфраструктури (ОКІІ), до якої відносяться і об'єкти КМІІ. Кіберстійкість має забезпечуватися на всіх рівнях при взаємодії всіх суб'єктів забезпечення кібербезпеки.

Кожна галузь критичної інфраструктури (КІ) і кожен об'єкт КІ (ОКІ) характеризуються виконанням специфічних функцій, наслідки неналежного виконання котрих визначають категорію критичності ОКІ. Тому для кожної галузі КІ поняття кіберстійкості пов'язане із такими функціями. Наприклад, кіберстійкість інформаційної інфраструктури банку – із бізнес-процесами, продуктом яких є банківські та фінансові послуги [13], а кіберстійкість в морській галузі – з операційними технологіями, які використовуються для безпечної експлуатації суден, порушення котрих може призвести до порушення безпеки людей, судна та/або навколишнього середовища [6].

За ступенем впливу на безпеку людини, безпеку судна та навколишнього середовища в Рекомендаціях щодо кіберстійкості [6], розроблених Міжнародною асоціацією класифікаційних товариств у 2020 році (остання редакція – 2022 рік, очікується редакція 2024 року) виділяють (із посиланням на UR E22 IACS, які були розроблені у 2006 році, остання редакція – 2023 рік [7]) системи трьох категорій:

- категорія I – системи, вихід з ладу яких не призведе до небезпечних ситуацій;
- категорія II – системи, вихід з ладу яких міг би призвести до небезпечних ситуацій;
- категорія III – системи, вихід з ладу яких може негайно призвести до небезпечних ситуацій.

Згідно Закону України «Про критичну інфраструктуру» [14] встановлюються 4 категорії критичності ОКІ, які визначаються за ступенем тяжкості наслідків порушення функціонування ОКІ:

- I категорія критичності – виникає кризова ситуація державного значення;

- II категорія критичності – виникає кризова ситуація регіонального значення;
- III категорія критичності – виникає кризова ситуація місцевого значення;
- IV категорія критичності – виникає кризова ситуація локального значення.

Таким чином, поняття «категорія системи» за UR E22 IACS «Computer-based systems» і поняття «категорія критичності» [7] ОКІ і, відповідно, ОКП за Законом України «Про критичну інфраструктуру» [14] та Методикою категоризації об'єктів критичної інфраструктури [15] не є ідентичними.

Особливості прийняття рішень в морській галузі зумовлені необхідністю узгоджувати інтереси багатьох стейкхолдерів (вантажодержавців і вантажовідправників, страхувальників суден і морських агентів, судновласників і екіпажів, портів і постачальників послуг, берегової охорони і лоцманів, докерів і логістичних компаній тощо), пов'язаних із багатьма бізнес-процесами, наслідки порушення котрих асоціюються із різними ризиками. Крім того, вибір процедур обробки цих ризиків має здійснюватися з врахуванням не тільки вітчизняного законодавства, а й з врахуванням міжнародних нормативних актів, вимог наявних договорів і законодавчих вимог інших країн (найчастіше для морських перевезень).

Крім того, кіберстійкість має визначатися на різних рівнях за різними документами:

- для портів і портових споруд – згідно IAPH Cybersecurity Guidelines for Ports and Port Facilities [10];
- для суден – згідно IACS UR E26 Cyber resilience of ships [8];
- для бортових систем – згідно IACS UR E27 Cyber resilience of on-board systems and equipment [9].

Перелічені вище документи мають рекомендаційний характер (однак з липня 2024 року їм мають відповідати всі нові судна) і не застосовуються до комп'ютерних систем, вимоги до яких визначені на законодавчому рівні. Наприклад, Частина X «Комп'ютерні системи» з «Rules for the survey and construction of steel ships» визначає вимоги до проектування, конструювання, тестування та технічного обслуговування комп'ютерних систем, які підпадають під класифікаційні вимоги,

включаючи апаратне та програмне забезпечення, яке становить такі системи, однак не поширюється на навігаційне обладнання, зазначене в Правилах техніки безпеки, радіоустановки, зазначені в Правилах радіоустановок тощо [11]. Крім того, для вирішення проблем, пов'язаних із забезпеченням відповідності новим вимогам з кібербезпеки невеликих і нетрадиційних суден, сфера застосування UR E27 та UR E26 може бути класифікована як обов'язкова та необов'язкова відповідність залежно від типів і розмірів суден.

Слід враховувати також, що на даний час у міжнародному морському праві існують певні прогалини стосовно регулювання питань кібербезпеки, і на думку багатьох дослідників [2] актуальним є прийняття універсального міжнародного договору з кібербезпеки у морській галузі.

Таким чином, прийняття рішень стосовно кіберстійкості морської інфраструктури має здійснюватися поетапно – починаючи з ознайомлення всіх зацікавлених сторін із наявними нормативними вимогами і рекомендаціями та узгодження складу базової документації до визначення кількісних значень і обробки ризиків, асоційованих із різними стейкхолдерами, країнами, інформаційними ресурсами, загрозами, порушеннями властивостей захищеної інформації, критичними інфраструктурами, ОКІ та ОКП різних категорій критичності (як за законодавством України так і за рекомендаціями Міжнародної асоціації класифікаційних товариств). При цьому мають розглядатися ризики для портів і портових споруд, бортових систем і судна в цілому та інтегральні ризики для морської інфраструктури з врахуванням міжнародних зв'язків.

В якості критеріїв оцінювання кіберстійкості можуть бути використані:

- для оцінювання швидкості адаптації до внутрішніх і зовнішніх кіберзагроз – час між виявленням нового типу загроз чи сценаріїв атак і впровадженням засобів протидії;
- для оцінювання сталості функціонування ОКІ, ОКП та морської інформаційної інфраструктури в цілому – співвідношення успішних/неуспішних атак до загальної кількості виявлених атак і тренди у цих співвідношеннях, рівні і тренди у ризиках, рівні і тренди у втратах внаслідок кіберінцидентів;

– для оцінювання здатності відновлення сталого функціонування після кіберінцидентів – час відновлення, витрати на відновлення, співвідношення показників якості функціонування та ризиків до кіберінцидентів і після відновлення, ймовірність успішного відновлення.

Вибір критеріїв оцінювання кіберстійкості для вирішення конкретних прикладних задач має здійснюватися за зваженою експертною оцінкою. При цьому вважається доцільним формувати декілька груп експертів, які оцінюватимуть кіберстійкість на різних рівнях (бортові системи, судно, порт, морська критична інформаційна інфраструктура, галузь в цілому). Вагові коефіцієнти експертів при цьому мають залежати від їх кваліфікації в конкретній галузі діяльності і можуть визначатися взаємною оцінкою.

Висновки. В даній роботі на основі аналізу відкритих інформаційних джерел визначені особливості забезпечення кіберстійкості та прийняття рішень в морській галузі, сформовано перелік критеріїв прийняття рішень щодо забезпечення кіберстійкості в морській галузі і визначити принципи їх вибору для вирішення конкретних прикладних задач.

Список літератури:

1. Баронова О., Турти М., Ганчо С. Визначення рівня впливу кіберзагроз на розвиток морської галузі // Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ICT-2020». – Харків: ХНУРЕ, 2020. – С.275-278.

2. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку // Вісник Одеського Національного ун-ту. Серія: Правознавство. – 2024. – Т.26. – Випуск 1(38). – С.112-117. <https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462>

3. Зубков А.П. Критерії прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2023. – С.175-181. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

4. Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. Водний транспорт. No.1 (37). 2023. С. 179–188. URL: <https://vt.duit.in.ua/index.php/home/article/view/267/224>

5. Juan Ignacio Alcaide, Ruth Garcia Llave. Critical infrastructures cybersecurity and the maritime sector. Trans- portation Research Procedia. 2020. Volume 45. Pages 547–554. URL: <https://www.sciencedirect.com/science/article/pii/S2352146520302209>

6. Recommendation on Cyber Resilience No. 166. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf>

7. IACS E22. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf

8. IACS UR E26 Cyber resilience of ships. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf

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. Rules for the survey and construction of steel ships. Part X. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/rules/465_part_x_e_202406.pdf

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

13. Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг Постанова № 4 Правління Національного банку України від 16.01.2021 URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>

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

15. 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>

ЗМІСТ

Секція 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ..... 3

Загрози об'єктам морської критичної інфраструктури України та напрямки досліджень щодо їх нейтралізації <i>Блінцов В.С.; Буруніна Ж.Ю.</i>	3
Аналіз загроз системі інформаційного обміну між постом керування та дроном <i>Гололобов О.В.</i>	5
Оцінка безпеки баз даних NOSQL у системах відстеження та моніторингу транспорту <i>Євдокимов С.О.</i>	8
Перспективи комп'ютерного зору в задачах підводного моніторингу <i>Іванов В.А.</i>	13
Критерії вибору системи виявлення вторгнень для водного транспорту <i>Тотх М.</i>	15
Зважене оцінювання критичності об'єктів морського та річкового транспорту <i>Турти М.В.</i>	22
Критерії прийняття рішень щодо забезпечення кіберстійкості в морській галузі <i>Турти М.Ю.</i>	29

Секція 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ..... 35

Система аналізу методів забезпечення безпеки у бездротових мережах <i>Бердніков В.В.</i>	35
Автоматизована система реєстрації відвідувачів на основі wi-fi підключення <i>Білець О.О.</i>	38
Модель прогнозування кібератак на основі аналізу поведінки <i>Божаткін С.М.; Гусєва-Божаткіна В.А.; Пасюк Б.Б.</i>	42
Дослідження використання прихованих каналів сучасних месенджерів <i>Восков К.П.</i>	46
Аналіз та виявлення мережових атак грубої сили на інтернет-сервіси <i>Десятов А.М.</i>	49

Наукове видання

**СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ НА ТРАНСПОРТІ**

СПІБТ–2024

**ХІІ 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
