



**НАУКОВО-ТЕХНІЧНІ
КОНФЕРЕНЦІЇ**

Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

**XIII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ
КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ**

27-28 листопада 2025 р.

**У двох частинах
Частина 2**



Миколаїв ■ НУК ■ 2025

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова**

**Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова**

**54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
<http://conference.nuos.edu.ua>
e-mail: conference@nuos.edu.ua**

**Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова**

**54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
<http://iae.nuos.edu.ua>
e-mail: university@nuos.edu.ua**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

**СУЧАСНІ ПРОБЛЕМИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НА ТРАНСПОРТІ**

СПІБТ–2025

МАТЕРІАЛИ

**XIII Всеукраїнської науково-технічної конференції
з міжнародною участю**

27–28 листопада 2025 року

**У двох частинах
Частина 2**

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



МИКОЛАЇВ • НУК • 2025

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 XIII Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2025. – Ч. 2. – 100 с.

У збірнику подано матеріали XIII 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, 2025

УДК 004.056.5

ІНФОРМАЦІЙНА МОДЕЛЬ ВИБОРУ ЗАХОДІВ ЗАХИСТУ ЗА НД ТЗІ 3.6-006-24

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

Україна є морською державою з активно працюючою інфраструктурою морської галузі. Безпека річкового і морського транспорту є складовою національної економічної безпеки. Водний транспорт є важливою складовою сучасних логістичних систем і належить до критичної інфраструктури (КІ). На даний час спостерігається тенденція до підвищення кількості кібератак на об'єкти критичної інфраструктури (ОКІ) фактично у всіх секторах – в енергетиці, банківській сфері, на різних видах транспорту тощо. Функціонування водного транспорту суттєво залежить від здатності критичної морської інформаційної інфраструктури, яка включає в себе берегові і суднові компоненти, протистояти кіберзагрозам.

Кібербезпека в галузі річкового і морського транспорту регламентується нормативно-правовими актами [1-11], що видаються організаціями різного підпорядкування і з різними повноваженнями, кількість цих актів і кількість організацій, задіяних у їх розробці, постійно зростає. Крім того, дослідженням проблем захисту інформації в галузі водного транспорту, теоретичним обґрунтуванням ефективних методів вирішення цих займаються вітчизняні і зарубіжні науковці [12-16]. Однак, на даний час в Україні відсутні галузеві профілі безпеки і затверджені методики управління ризиками інформаційної безпеки у галузі водного транспорту.

Метою даної роботи є визначення особливостей проектування суден з врахуванням уніфікованих вимог Міжнародної асоціації класифікаційних товариств (англ. International Association of Classification Societies, IACS) до забезпечення кібербезпеки судових комп'ютеризованих систем (англ. Computer-Based Systems, CBS).

Для досягнення поставленої мети необхідно розв'язати наступні задачі: провести аналіз нормативно-правової бази забезпечення кібербезпеки у галузі водного транспорту і визначити вимоги IACS до CBS та їх узгодженість з вітчизняною нормативно-правовою базою.

Нормативно-правова бази забезпечення кібербезпеки у галузі водного транспорту може бути умовно поділена на два блоки:

- загальні нормативно-правові акти, які стосуються управління якістю товарів і послуг; захисту критичної інфраструктури; організаційного, технічного і криптографічного захисту інформації, розробки комплексних систем захисту інформації / систем безпеки інформації; менеджменту інформаційної безпеки;

- спеціалізовані нормативно-правові акти, які стосуються організації діяльності морського та внутрішнього водного транспорту; безпеки навігації, екіпажу, пасажирів, вантажів, кібербезпеки морської галузі, порту і портових споруд, суден, бортових комп'ютеризованих систем, зокрема кіберстійкості [2, 3, 6].

До нормативно-правової бази забезпечення кібербезпеки у галузі водного транспорту відносяться [16]:

- міжнародні стандарти;
- директиви та регламенти Європейського Союзу захисту критичних інфраструктур, мережевих та інформаційних систем, загального рівня кібербезпеки на території Союзу;
- базові законодавчі акти України і постанови Кабінету Міністрів у галузі кібербезпеки, державні стандарти України, нормативна документація з технічного захисту інформації;
- документи, видані провідними міжнародними організаціями і групами організацій у галузі водного транспорту, одна частина з яких має рекомендаційний характер, а інша є обов'язковою для виконання.

З 1 червня 2024 року для проектів суден є обов'язковими уніфіковані вимоги Міжнародної асоціації класифікаційних товариств до суднових комп'ютеризованих систем – IACS UR E22 «Computer-based systems» [1].

IACS UR E22 поширюється на весь життєвий цикл всіх суднових CBS, що використовують програмне забезпечення і мають відповідати класифікаційним вимогам, за виключенням тих систем, вимоги до яких регулюються іншими нормативними актами. Наприклад, вимоги до радіо-комунікаційних і навігаційних систем визначені у IV і V главах

Міжнародної конвенції з охорони людського життя на морі (англ. International Convention for the Safety of Life at Sea, SOLAS) [9].

В IACS UR E22 судно розглядається як сукупність систем, підсистем і окремих програмованих приладів з власним програмним забезпеченням. Вимоги IACS UR E22 до CBS є диференційованими залежно від категорії критичності CBS, яка визначається згідно з [1] ймовірною тяжкістю наслідків виходу CBS з ладу для безпеки людини, судна та/або навколишнього середовища, і оцінюються в контексті (категорії однакових CBS на різних судах можуть бути різними):

- категорія I: небезпечні ситуації не виникнуть. CBS цієї категорії не перевіряються IACS, однак у проекті має бути передбачене можливе надходження запиту щодо підтвердження категорії або щодо надання гарантій відсутності прямого і опосередкованого впливу CBS цієї категорії критичності на роботу інших CBS II і III категорій критичності;
- категорія II: небезпечні ситуації можуть виникнути;
- категорія III: небезпечні ситуації негайно виникнуть і можуть бути катастрофічними.

Уніфіковані вимоги до CBS, поділяються на наступні групи:

- загальні вимоги;
- вимоги до складових системи;
- вимоги до системного інтегратора, яким зазвичай є верф;
- вимоги до обслуговування CBS, що окремо визначені для власника, системного інтегратора і постачальників;
- вимоги до управління змінами;
- технічні вимоги до CBS, які включають вимоги щодо звітності і журналювання інцидентів, підвищені вимоги до систем II і III категорії критичності, вимоги до застосування бездротових мереж (заборонені для CBS III категорії критичності, а для інших – можуть застосовуватися за ряду умов) і вимоги щодо перевірки відповідності технічним вимогам Класифікаційного товариства.

Вимоги IACS UR E22 щодо програмного забезпечення операційного технологічного обладнання та інтегрованих систем в цілому відповідають вимогам ISO 24060:2021 «Ships and marine technology — Ship software logging system for operational technology» [4], згідно з яким воно має бути зареєстроване, і має бути доступною інформація про його поточний робочий стан.

Вимоги IACS щодо кіберстійкості бортових систем і обладнання визначені в окремому документі [3] і згруповані за підцілями досягнення кіберстійкості – ідентифікація (SG1), захист (SG2), виявлення (SG3), реагування (SG4), відновлення (SG5). За змістом ці вимоги поділяються на функціональні вимоги, технічні аспекти і вимоги щодо верифікації і тестування.

Настанови щодо менеджменту морських кіберризиків Міжнародної ідентифікація, захист, виявлення, реагування, відновлення морської організації MSC-FAL.1/Circ.3/Rev.2 [5], як і вимоги IACS щодо кіберстійкості [3], також згруповані по розділах ідентифікація, захист, виявлення, реагування, відновлення.

Мінімальні функціональні вимоги і критерії продуктивності, щоб судно можна було визнати кіберстійким, визначені в IACS UR E26 «Cyber resilience of ships» [2] за цільовим підходом, при якому функціональні/технічні вимоги наведені для досягнення кожної субцілі. Вимоги [2] призначені для того, щоб забезпечити однакову реалізацію всіма зацікавленими сторонами у певних умовах однакових рішень і забезпечити за рахунок цього прийнятний рівень стійкості для всіх класифікованих суден/блоків незалежно від експлуатаційних ризиків і складності систем операційних технологій (ОТ-систем).

Аналогічним чином в уніфікованих вимогах IACS UR E27 [3] представлені вимоги щодо кіберстійкості бортових систем і обладнання.

Слід зауважити, що вимоги [1-3] є узгодженими і уніфікованими, а порівняно з вітчизняною нормативно-правовою базою, не дивлячись на спорідненість підходів до забезпечення кібербезпеки, спостерігається ряд суттєвих відмінностей, які необхідно нівелювати:

- категорії критичності об'єктів критичної інформаційної інфраструктури визначаються інакше [15];
- при розробці систем безпеки інформації за НД ТЗІ використовується інша класифікація заходів захисту.

Висновки

В даній роботі проведено аналіз нормативно-правової і визначені вимоги до CBS. Обґрунтовано необхідність узгодження нормативних документів, виданих різними відповідальними органами у морській галузі.

Список літератури:

1. 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
2. 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
3. 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>
4. ISO 24060:2021 Ships and marine technology – Ship software logging system for operational technology. URL: <https://www.iso.org/ru/standard/77678.html>
5. MSC-FAL.1/Circ.3/Rev.2 Guidelines on maritime cyber risk management. URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\)%20\(1\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf)
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. 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
8. The Guidelines on Cyber Security Onboard Ships. Version 5 (2024). URL: https://www.maritimeworldsecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_cyber_security-v5-final.pdf
9. Treaties and international agreements registered on 30 June 1980 No. 18961. International Convention for the Safety of Life at Sea, 1974 (with annex and final act of the International Conference on Safety of Life at Sea, 1974). Concluded at London on 1 November 1974. URL: <https://treaties.un.org/doc/Publication/UNTS/Volume%201184/volume-1184-I-18961-English.pdf>
10. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

11. 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>

12. 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>

13. 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. URL: <https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462>

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

15. Турти М.В. Зважене оцінювання критичності об'єктів морського та річкового транспорту //Матеріали XII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2024. – С.22-28.

16. Хван Ю.В. Норматино-правова база кібербезпеки галузі водного транспорту //Матеріали XII Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». Миколаїв: НУК, 2024. С156-162

ЗМІСТ

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

Побудова реляційної моделі взаємовпливу факторів вразливостей на захищеність об'єкту водного транспорту <i>Бондаренко І.Ю.</i>	3
Порівняльний аналіз методів розпізнавання ознак в біометричних системах контролю доступу <i>Гальченко О.Л.</i>	8
Інформаційна модель вибору базового профілю безпеки <i>Ломова О.О.</i>	13
Інформаційна модель вибору альтернативних заходів захисту при створенні системи безпеки інформації <i>Ткаченко Д.О.</i>	19
Інформаційна модель вибору заходів захисту за НД ТЗІ 3.6-006-24 <i>Турти М.В.</i>	27
Інформаційна модель вибору заходів захисту за НД ТЗІ 3.6-006-24 <i>Шаповалова О.П.</i>	33

Секція 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ..... 42

Обґрунтування методики оцінки часової складності алгоритмів на базі кореляційного аналізу <i>Бабенко Н.; Пантелєєв В.; Самойленко Д.М.; Суліма М.М.; Туманов О.А.</i>	42
Проблемні питання використання операційних систем Windows у комплексних системах захисту інформації <i>Васєв В.В.</i>	47
Технології виявлення фальсифікованої інформації для підвищення інформаційної безпеки <i>Кобзєв В.Г.; Ховрат А.В.</i>	51
Використання елементів задачі покриття для програмної реалізації удосконаленого способу симетричного шифрування даних <i>Лученко Я.В., аспірант; Тавдгірідзе Д.Д.</i>	53
Щодо адаптації тонального методу визначення розбірливості мови до задач захисту інформації <i>Лях О.Д.</i>	56
Дослідження особливостей програмування генераторів випадкових чисел <i>Нестерович Е.Р.</i>	59

Наукове видання

**СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ НА ТРАНСПОРТІ**

СПІБТ–2025

**XIII Всеукраїнська науково-технічна конференція
з міжнародною участю**

27–28 листопада 2025 року

*Національний університет кораблебудування
імені адмірала Макарова*

*Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв*

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

**У двох частинах
Частина 2**

(українською мовою)

Відповідальна за випуск В. В. Трибулькевич
