ГРЕЗІНА О. М.,
доктор філософії,
доцент кафедри кримінального аналізу
та інформаційних технологій
*(Одеський державний університет
внутрішніх справ)*
ORCID ID: 0000-0002-2491-6529

ФОРОС Г. В.,
кандидат юридичних наук, доцент
завідувачка кафедри кримінального
аналізу та інформаційних технологій
*(Одеський державний університет
внутрішніх справ)*
ORCID ID: 0000-0002-9504-3681

УДК 004.056.5/946.5:656.61
DOI https://doi.org/10.32842/2078-3736/2025.5.2.65

ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ МОРСЬКОЇ БЕЗПЕКИ ТА ПРАВОВОМУ АНАЛІЗІ

У статті досліджується застосування сучасних інформаційних технологій для забезпечення морської безпеки та проведення правового аналізу. Сучасна морська галузь переживає інтенсивну цифрову трансформацію, що включає широке впровадження штучного інтелекту (ШІ), Інтернету речей (IoT) та аналізу великих даних (big data) у суднових, портових та логістичних системах, від яких залежить понад 90% світової торгівлі. Показано, що така цифровізація підвищує вразливість критичної морської інфраструктури до кіберзагроз, таких як Advanced Persistent Threats (APTs), GPS-спуфінг, атаки на операційні технології та хактивізм, що може призводити до порушення безпеки судноплавства, економічних збитків, екологічних катастроф та юридичних спорів.

Проаналізовано міжнародні та національні правові рамки, включно з UNCLOS, рекомендаціями IMO, USCG Final Rule та IACS E26/E27, які частково забезпечують стандартизацію кібербезпеки, але часто носять рекомендаційний характер і відстають від швидкого розвитку технологій. Виявлено прогалини у питаннях юрисдикції, атрибуції відповідальності та примусового виконання норм у разі кіберінцидентів на морі.

Розглянуто технологічні рішення для підвищення кіберстійкості морської інфраструктури: системи моніторингу та виявлення аномалій на базі IoT і ШІ, використання гібридних алгоритмів AE–CNN–LSTM для раннього виявлення загроз, аналіз великих даних для оцінки вразливостей критичних елементів інфраструктури, а також інтеграція концепцій cyber resilience та cyber-worthiness у стандарти ISM та ISPS.

У висновках підкреслено, що комплексне поєднання сучасних інформаційних технологій із удосконаленими та гармонізованими правовими рамками забезпечує ефективний захист морської інфраструктури. Рекомендовано розвиток глобальних реєстрів кіберінцидентів, багатосторонніх протоколів,

інтеграцію автономних систем та підвищення обізнаності екіпажів і операторів портової інфраструктури щодо кіберризиків.

Ключові слова: *морська безпека, кібербезпека, кібербезпека морського транспорту, сучасні інформаційні технології, штучний інтелект, штучний інтелект у морській безпеці, Інтернет речей, аналіз великих даних, IoT у морських системах.*

Hrezina O. M., Foros H. V. The application of modern information technologies in maritime security and legal analysis

The article investigates the application of modern information technologies for ensuring maritime security and conducting legal analysis. The contemporary maritime sector is undergoing intensive digital transformation, which includes the widespread implementation of artificial intelligence (AI), the Internet of Things (IoT), and big data analytics in vessel, port, and logistics systems, which account for over 90% of global trade. It is shown that such digitalization increases the vulnerability of critical maritime infrastructure to cyber threats, such as Advanced Persistent Threats (APTs), GPS spoofing, attacks on operational technologies, and hacktivism, which can lead to disruptions in maritime safety, economic losses, environmental disasters, and legal disputes.

International and national legal frameworks, including UNCLOS, IMO guidelines, the USCG Final Rule, and IACS E26/E27, have been analyzed. While these frameworks partially standardize maritime cybersecurity, they are often advisory in nature and lag behind the rapid development of technology. Gaps were identified in jurisdiction, attribution of responsibility, and enforcement in the case of cyber incidents at sea.

Technological solutions for enhancing the cyber resilience of maritime infrastructure are considered, including anomaly monitoring and detection systems based on IoT and AI, the use of hybrid AE–CNN–LSTM algorithms for early threat detection, big data analytics for assessing vulnerabilities of critical infrastructure elements, and the integration of cyber resilience and cyber-worthiness concepts into ISM and ISPS standards.

The conclusion emphasizes that the comprehensive combination of modern information technologies with improved and harmonized legal frameworks ensures effective protection of maritime infrastructure. Recommendations include the development of global cyber incident registries, multilateral protocols, integration of autonomous systems, and increasing awareness among crews and port operators regarding cyber risks.

Key words: *maritime security, cybersecurity, maritime transport cybersecurity, modern information technologies, artificial intelligence, artificial intelligence in maritime security, Internet of Things, big data analytics, IoT in maritime systems.*

Постановка проблеми. Сучасна морська галузь зазнає стрімкої цифрової трансформації, що супроводжується широким упровадженням штучного інтелекту, інтернету речей та технологій аналізу великих даних у суднові, портові й логістичні системи, від яких залежить понад 90% світової торгівлі. Така цифровізація істотно підвищує вразливість критичної морської інфраструктури до кіберзагроз, зокрема Advanced Persistent Threats, GPS-спуфінгу, атак на операційні технології та хактивізму, наслідками яких можуть бути порушення безпеки судноплавства, значні економічні збитки, екологічні катастрофи та юридичні спори. Водночас чинні міжнародно-правові механізми, насамперед Конвенція ООН з морського права, не адаптовані до специфіки кіберпростору, що зумовлює прогалини у питаннях юрисдикції, атрибуції відповідальності та примусового виконання норм у разі кіберінцидентів

у морському середовищі. Фрагментарність регуляторних підходів, переважно рекомендаційний характер міжнародних стандартів, нерівномірність їх упровадження на національному рівні та випереджальний розвиток технологій порівняно з правовим регулюванням обумовлюють необхідність комплексного поєднання сучасних інформаційних технологій із удосконаленими та гармонізованими правовими рамками з метою підвищення кіберстійкості та загального рівня морської безпеки.

Мета дослідження. Метою статті є комплексний аналіз застосування сучасних інформаційних технологій, таких як ШІ, IoT та big data, у забезпеченні морської безпеки та кібербезпеки, а також правовий аналіз існуючих міжнародних і національних регуляторних рамок з пропозиціями щодо їх удосконалення.

Аналіз останніх публікацій. Публікації за період 2022–2025 років свідчать про зростання інтердисциплінарного інтересу до морської кібербезпеки, з акцентом на технологічні інновації та правові виклики. Jin Y. et al. (2025) аналізують правові прогалини в UNCLOS щодо морських кібероперацій та пропонують багатосторонній підхід з потенційним протоколом [4]. Melnyk O. et al. (2025) розглядають міжнародні регуляторні рамки кібербезпеки морського транспорту, пропонуючи створення глобального реєстру інцидентів на основі аналізу 112 випадків з Maritime Cyber Attack Database (MCAD) [5]. У роботах 2025 року акцентується увага на нових обов'язкових вимогах США, таких як Final Rule USCG, що встановлює базові стандарти кібербезпеки для суден [6]. Дослідження з ШІ в морській кібербезпеці (2025) систематизують застосування машинного навчання для виявлення загроз, включаючи гібридні моделі AE–CNN–LSTM [7]. Автори з 2024 року вводять концепцію «кібердостойності» як розширення морехідності, інтегруючи кіберризики в ISM та ISPS Codes [8]. Публікації DNV (2024/2025) та IACS (2023–2024) фокусуються на cyber resilience, з уніфікованими вимогами E26/E27 для нових суден [9]. Роботи з IoT та ШІ (2023–2025) підкреслюють роль у моніторингу аномалій, але вказують на брак емпіричних даних та відставання правових інструментів [10, 11]. Бібліометричний аналіз (2025) ілюструє еволюцію фокусу від загроз до рішень, з зростанням публікацій на 15% щорічно [12]. Дослідження з перспективи моряків (2025) розкривають слабкі ланки в практичному впровадженні, такі як низька обізнаність екіпажів [13]. Загальна тенденція — перехід від рекомендацій до обов'язкових стандартів, але з повільним глобальним впровадженням та необхідністю інтеграції з критичною інфраструктурою.

Виклад основного матеріалу. Морські кібератаки додають новий рівень складності до традиційних загроз на морі, таких як піратство, незаконна діяльність, морський тероризм та аварії. Глобальний морський сектор стає дедалі більш цифровим, автоматизованим та взаємопов'язаним, що супроводжується зростанням кількості кіберзагроз. Так, за останні роки кількість кібератак на берегові морські системи збільшилася в дев'ять разів. Україна як потужна морська держава також стикається з цими викликами у повному обсязі [2].

Сучасна морська галузь переживає інтенсивну цифрову трансформацію, що суттєво підвищує її вразливість до кіберзагроз. Понад 90% глобальної торгівлі здійснюється морським шляхом, а критична інфраструктура, включаючи підводні комунікаційні кабелі, автономні судна та портові системи, дедалі більше залежить від інтернету речей (IoT), штучного інтелекту (ШІ) та аналізу великих даних (big data). Кібератаки можуть спричиняти зупинку логістики, економічні збитки в мільярди доларів та фізичні загрози, як у випадках з порушенням навігації чи екологічними катастрофами [1]. Міжнародне право, зокрема Конвенція ООН з морського права (UNCLOS), не адаптоване до кіберпростору, що створює прогалини в юрисдикції. Відсутність єдиних глобальних стандартів, повільне впровадження обов'язкових вимог у країнах, що розвиваються, та зростання складності загроз, таких як Advanced Persistent Threats (APTs) і хактивізм, посилюють ризики [3].

Сучасні інформаційні технології відіграють ключову роль у посиленні морської безпеки. Штучний інтелект застосовується для аналізу даних AIS (Automatic Identification System), виявлення аномалій та прогнозування загроз, таких як спуфінг GPS чи незаконний вилов риби, з ефективністю до 95% у реальному часі [7]. IoT інтегрується в бортові

системи та портову інфраструктуру для моніторингу, тоді як аналіз великих даних дозволяє оцінювати вразливості критичних елементів, наприклад, підводних кабелів, з використанням моделей на базі MITRE ATT&CK [10]. Гібридні алгоритми, такі як AE–CNN–LSTM, забезпечують end-to-end виявлення вторгнень у кіберфізичних мережах суден, зменшуючи час реагування на 30–40% порівняно з традиційними методами [11].

Правовий аналіз виявляє значні прогалини в регулюванні. UNCLOS (1982) регулює фізичне пошкодження інфраструктури (стаття 113), але не охоплює кібервтручання, що ускладнює атрибуцію на високому морі та в ексклюзивних економічних зонах [4]. Міжнародна морська організація (IMO) через резолюцію MSC.428(98) та оновлені guidelines (2021–2025) інтегрувала кіберризики в ISM Code, але ці заходи залишаються переважно рекомендаційними, з низьким рівнем примусового виконання [14]. Значний прогрес спостерігається в США: Final Rule USCG (ефективний з липня 2025) встановлює обов'язкові вимоги, включаючи призначення Cybersecurity Officer, плани реагування на інциденти, регулярні дрили та звітність про «reportable cyber incidents», базуючись на моделі CIRC [6]. IACS unified requirements E26/E27 (оновлені 2023, обов'язкові з 2024) визначають мінімальні стандарти cyber resilience для нових суден, з акцентом на архітектуру нульової довіри та сегментацію мереж [9].

Серед ключових загроз 2025 року виділяються Advanced Persistent Threats (APTs), хактивізм та вразливості портової інфраструктури. Аналіз 112 інцидентів з MCAD (2020–2025) показує, що APTs становлять 40% атак, з фокусом на стійке проникнення в OT-системи, тоді як хактивізм, часто геополітично мотивований, призводить до DDoS-атак та витоків даних [3]. Перспектива моряків розкриває слабкі ланки: низька обізнаність екіпажів (лише 30% проходять регулярне навчання) та відсутність інтеграції кібербезпеки в повсякденні операції роблять судна вразливими до соціальної інженерії [13].

Для подолання цих викликів пропонуються комплексні рамки, базовані на ISO/IEC 27001 та NIST, з впровадженням Maritime Security Operation Centers (M-SOCs) для реального часу моніторингу [15]. Концепція «кібердостойності» (cyber-worthiness) розширює традиційну морехідність, вимагаючи захисту навігаційного обладнання через файрволи, шифрування та навчання, з інтеграцією в ISM та ISPS [8]. Багатосторонні ініціативи включають оновлення UNCLOS протоколом для визначення кіберзагроз, створення глобального реєстру інцидентів та системи обміну даними [5]. Регіональне співробітництво, як NIS2 Directive в ЄС чи ASEAN-центри кібербезпеки, доповнює глобальні зусилля, але потребує кращої координації [12]. Основні виклики — швидкий розвиток технологій, що випереджає правові відповіді, недостатні інвестиції (лише 20% бюджетів на кібербезпеку в морській галузі) та брак емпіричних даних про інциденти [9].

Висновок. Застосування ШІ, IoT та big data значно підвищує рівень морської безпеки через автоматизоване виявлення та прогнозування загроз, але вимагає термінового оновлення правових рамок, таких як UNCLOS та IMO, від рекомендацій до обов'язкових стандартів, як у Final Rule USCG та IACS E26/E27. Концепції cyber resilience, cyber-worthiness та моделі T-V-I для оцінки ризиків, разом з глобальним реєстром інцидентів та багатосторонніми протоколами, формують основу комплексного захисту. Майбутні дослідження мають фокусуватися на емпіричних даних з MCAD, інтеграції автономних систем, регіонально-глобальній гармонізації регулювання та ролі моряків у кіберстійкості, з урахуванням зростання APTs та хактивізму.

Список використаних джерел:

1. Badea, M., Bucovețchi, O., Gheorghe, A. V., Hnatiuc, M., Raicu, G. Maritime Industry Cybersecurity Threats in 2025: Advanced Persistent Threats (APTs), Hacktivism and Vulnerabilities. Logistics. 2025. Vol. 9, No. 4, art. 178.DOI: 10.3390/logistics9040178.https://www.mdpi.com/2305-6290/9/4/178

2. Пядишев В.Г. Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. *Морська безпека та оборона*. 2023. №1. С. 78-86. URL: https://doi.org/10.32782/msd/2023.1.10

3. Raymaker A., Kumar A., Wong M. Y., Pickren R., Chhotaray A., Li F., Zonouz S. A., Beyah R. A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. 2025. P. 588–602. DOI: 10.1145/3719027.3744816.

4. Jin Y, Feng Y, Liu C, Li S. Navigating the digital seas: Legal challenges and global governance of maritime cyber operations. *Frontiers in Marine Science*. 2025. URL:https://www.frontiersin.org/journals/marine-science/articles/10.3389/fmars.2025.1616906/full

5. Melnyk O, Drozdov O, Kuznichenko S. Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. *Lex Portus.* 2025.11(1):7–19. https://lexportus.net.ua/vipusk-1-2025/melnyk_1111.pdf

6. Cybersecurity in the Marine Transportation System. *Federal Register.* 2025. https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system

7. Kanwal K., Shi W., Kontovas C., Yang Z., Chang C.-H. Maritime cybersecurity: are onboard systems ready? Maritime Policy & Management. 2024; 51(3): 484–502. DOI: 10.1080/03088839.2022.2124464.

8. Kara Balcı Ö., Varan Samut İ., Ademuni-Odeke X. An evaluation of cyber-worthiness and related factors in maritime safety and maritime security. Journal of International Maritime Safety, Environmental Affairs, and Shipping. 2024; 8(4): 1–17. DOI: 10.1080/25725084.2024.2411180

9. Global maritime industry continues to address cyber risk. Hill Dickinson. 2025. URL: https://www.hilldickinson.com/our-view/articles/global-maritime-industry-continues-to-address-cyber-risk

10. Liu G., Amri O., Liang Y., Zhang Z., Merino Laso P., Bertelle C., Berred A., Lefebvre D. Survey and Future Trends for Cybersecurity in Maritime and Port Sectors: A Discrete Event Systems Perspective. Mathematics. 2025; 13(22): 3650. DOI: https://doi.org/10.3390/math13223650

11. Anuja, R., Annrose, J. End-to-end deep learning for smart maritime threat detection: an AE–CNN–LSTM-based approach. *Sci Rep* **15**, 36316 (2025). https://doi.org/10.1038/s41598-025-19450-4

12. Peng P., Xie X., Claramunt C., Lu F., Gong F., Yan R. Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. Transportation Research Part E: Logistics and Transportation Review. 2025; 195: 103971. DOI: https://doi.org/10.1016/j.tre.2025.103971

13. Raymaker A., Kumar A., Wong M.Y., Pickren R., Chhotaray A., Li F., Zonouz S., Beyah R. A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners. In: Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), Taipei, Taiwan, 13–17 Oct 2025. New York, NY, USA: Association for Computing Machinery (ACM); 2025: 18 pp. DOI: https://doi.org/10.1145/3719027.3744816

14. Paullet K. Strengthening cybersecurity education: The urgent need to integrate maritime cybersecurity into cyber programs. Issues in Information Systems. 2025; 26(3): 377–386. DOI: https://doi.org/10.48009/3_iis_2025_2025_130

15. Zhou J. Maritime Cybersecurity: A Big Change Ahead. IEEE Security & Privacy. 2025; 23(4): 4–7.DOI: https://doi.ieeecomputersociety.org/10.1109/MSEC.2025.3589068

Дата першого надходження рукопису до видання: 20.09.2025
Дата прийнятого до друку рукопису після рецензування: 22.10.2025
Дата публікації: 28.11.2025