

НАПРЯМ 1. ЕКОНОМІКА

Алексєєвська Галина Сергіївна

*доктор філософії, старший науковий співробітник,
Державна установа «Інститут ринку і економіко-екологічних
досліджень Національної академії наук України»;
доцент кафедри світового господарства і міжнародних
економічних відносин,*

Одеський національний університет імені І. І. Мечникова

Михайленко Владислав Іванович

*доктор філософії, науковий співробітник,
Державна установа «Інститут ринку і економіко-екологічних
досліджень Національної академії наук України»*

DOI: <https://doi.org/10.36059/978-966-397-543-6-1>

ЦИФРОВА ТРАНСФОРМАЦІЯ МОРСЬКОЇ ГАЛУЗІ: МОЖЛИВОСТІ ТА КІБЕРРИЗИКИ

Упродовж останнього десятиліття глобальна морська галузь зазнала масштабної цифрової трансформації, яка спричинила глибокі зрушення у структурі логістичних процесів, системах управління суднами, механізмах портової координації та організації ланцюгів постачання. Перехід до цифрових платформ, впровадження Інтернет речей (IoT), штучного інтелекту (ШІ), автономного судноплавства, хмарних технологій та обчислень на периферії (edge computing) створює нову операційну реальність, у якій ефективність тісно переплітається з інформаційною вразливістю [1].

Близько 90% світової торгівлі здійснюється морським транспортом, що обумовлює ключову роль морської інфраструктури у забезпеченні глобальної економічної стабільності. Підвищення

складності та інтенсивності логістичних потоків зумовлює потребу в цифрових рішеннях, які дозволяють автоматизувати управління маршрутами, здійснювати прогнозне технічне обслуговування, моніторити витрати пального, а також гарантувати екологічну безпеку операцій [2; 3].

Однією з найбільш поширених цифрових інновацій у морській галузі є цифрові двійники (digital twins) суден. Вони дозволяють у режимі реального часу моделювати технічний стан судна, взаємодію компонентів, ефективність навігації, зношування систем тощо. Це дає змогу своєчасно виявляти несправності та уникати дорогих зупинок, тим самим компанії можуть скоротити витрати на технічне обслуговування до 30% [4]. Також ще однією важливою інновацією є активне впроваджуються інтелектуальних платформ управління портами (Port Community Systems), які інтегрують митні, логістичні, брокерські та судноплавні сервіси в єдине цифрове середовище [5] PCS дозволяє значно скоротити обсяг паперових документів. Наприклад, у порту Джибуті експедитори тепер витрачають лише 1–2 хвилини на онлайн-бронювання, уникнувши годин очікування та ручних перевірок [6].

Штучний інтелект у морській сфері використовується для автоматизації навігації, оптимізації енергоспоживання, управління логістичними потоками в портах, моделювання цифрових двійників суден, а також для відеоаналітики та підвищення безпеки на борту. Завдяки ШІ судна можуть ухвалювати більш ефективні рішення щодо маршруту, виявляти несправності до їх фактичного виникнення, зменшувати витрати пального і краще координувати дії в межах портових операцій [7].

Попри значні переваги цифрових інновацій у морській галузі їх впровадження підвищує рівень вразливості об'єктів критичної інфраструктури до інформаційних загроз. Зростання ролі даних і мережевої взаємодії між учасниками логістичних процесів трансформує безпекову парадигму морського сектору: ключовим викликом стає не лише технічна ефективність, а насамперед – захист інформаційного простору.

Цифровізація призводить до виникнення нових, раніше нехарактерних ризиків. Йдеться, насамперед, про втрату автономності систем через постійне підключення до глобальних мереж зв'язку. Сьогодні більшість суден оснащені супутниковими системами, які забезпечують високошвидкісну передачу даних, але знищують «повітряний розрив» (air gap), що раніше відокремлював суднову інфраструктуру від загроз ззовні [8].

Крім того, підвищується роль систем обміну даними у ланцюгах постачання. Сучасні морські перевезення залежать від хмарних платформ, які забезпечують управління контейнеризацією, портовим завантаженням, реєстрацією вантажів, клієнтським обслуговуванням. Проте саме такі багаторівневі платформи стають мішенню для кіберзлочинців, які використовують фішинг, програмне забезпечення-вимагачі (ransomware), «бекдори» (backdoors) та інші засоби доступу до конфіденційної інформації [9].

Окрему загрозу становить відсутність уніфікованих стандартів безпеки для суднового обладнання. Відомо, що багато постачальників зберігають віддалений доступ до суднових систем навіть після інсталяції обладнання, що у разі недбалого захисту може бути використано зловмисниками. Наприклад, у 2023 році уряд США повідомив, що понад 80% портових кранів були вироблені китайськими компаніями, які не гарантують закриття бекдорів у своєму програмному забезпеченні.

Паралельно, компанії стикаються з проблемою сумісності нових технологій із застарілою інфраструктурою. Більшість суден мають термін експлуатації понад 25 років і не були спроектовані з урахуванням цифрових вимог. Їх модернізація вимагає значних фінансових і технічних ресурсів, що не завжди доступні для середніх і малих операторів.

Цифрові системи, що керують суднами, портами, вантажними потоками та митними процедурами, створюють нові точки входу для потенційних кібератак. Особливо критичними є сценарії, коли дані, що аналізуються штучним інтелектом, змінюються або підміняються. Неправильні висновки щодо технічного стану судна,

помилкові маршрути, невірна класифікація вантажу – усе це може мати катастрофічні наслідки для безпеки судноплавства і міжнародної торгівлі. Як зауважують Мауро Ф. і Кана А.А., відсутність комплексного захисту на рівні інфраструктури відкриває можливості для компрометації критичних даних і порушення цілісності рішень, що приймаються автоматизованими системами [7].

Ключова проблема полягає в тому, що наразі у більшості країн, включно з Україною, інформаційна безпека об'єктів морської інфраструктури ще не розглядається як частина загальної стратегії національної кіберстійкості. У той час як морська галузь дедалі більше інтегрується в цифрові екосистеми, відсутність централізованих політик, обов'язкових стандартів і наглядових органів із кіберзахисту критичних морських об'єктів створює системну загрозу.

Література:

1. UNCTAD. Review of Maritime Transport 2023. URL: <https://unctad.org/publication/review-maritime-transport-2023> (дата звернення: 25.03.2025).
2. Meade R. Ten trends that will shape the shipping industry in 2025 and beyond. Lloyd's List : веб-сайт. URL: <https://www.lloydslist.com/LL1151828/Ten-trends-that-will-shape-the-shipping-industry-in-2025-and-beyond> (дата звернення: 25.02.2025).
3. Raza Z., Woxenius J., Altuntas Vural C., Lind M. Digital transformation of maritime logistics: Exploring trends in the liner shipping segment. *Computers in Industry*. 2023. Vol. 145. Article 103811. DOI: <https://doi.org/10.1016/j.compind.2022.103811>. URL: <https://www.sciencedirect.com/science/article/pii/S016636152200207X> (дата звернення: 25.02.2025).
4. Digital twins in the shipping industry. Hapag-Lloyd : веб-сайт. URL: <https://www.hapag-lloyd.com/en/online-business/digital-insights-dock/insights/2024/03/digital-twins-in-the-shipping-industry.html> (дата звернення: 25.03.2025).
5. DNV. Maritime Cyber Priority 2024/25: Managing cyber risk to enable innovation. URL: <https://www.dnv.com/cyber/insights/publications/maritime-cyber-priority-2024/> (дата звернення: 21.05.2025).

6. World Bank. Port Community Systems: Lessons from Global Experience. Washington, D.C., 2024. P. 72. URL: <https://documents1.worldbank.org/curated/en/099092624152038561/pdf/P176587-54dd3e7b-e083-43cc-9df3-10b441697c0d.pdf> (дата звернення: 25.03.2025).
7. Mauro F., Kana A.A. Digital twin for ship life-cycle: A critical systematic review. *Ocean Engineering*. 2023. Vol. 269. Article 113479. DOI: <https://doi.org/10.1016/j.oceaneng.2022.113479>. URL: <https://www.sciencedirect.com/science/article/pii/S0029801822027627> (дата звернення: 25.03.2025).
8. CyberOwl. Maritime Cybersecurity Conference 2024 Hamburg. CyberOwl : веб-сайт. URL: <https://cyberowl.io/resources/cyberowl-maritime-cybersecurity-conference-2024-hamburg/> (дата звернення: 25.03.2025).
9. Wärtsilä. Cyber security at Wärtsilä. Wärtsilä : веб-сайт. URL: <https://www.wartsila.com/about/cyber-security> (дата звернення: 25.03.2025).