Галина АЛЕКСЕЄВСЬКА[1,2],
доктор філософії, старший науковий співробітник відділу ринку транспортних послуг, доцент кафедри світового господарства, ORCID ID: 0000-0002-6708-0098
Владислав МИХАЙЛЕНКО[1],
доктор філософії, науковий співробітник відділу ринку транспортних послуг, ORCID ID: 0000-0001-6667-2457
Олена БОНДАРЕНКО[1],
кандидат економічних наук, науковий співробітник відділу ринку транспортних послуг, ORCID ID: 0000-0003-2847-3267

[1] *Державна установа «Інститут ринку і економіко-екологічних досліджень НАН України»;*
[2] *Одеський національний університет імені І. І. Мечникова*

Прийняття: 22/07/2025
Рецензія: 28/07/2025
Публікація: 30/09/2025

DOI: https://doi.org/10.53920/ES-2025-3-7

JEL Класифікатор:
L91, L98, O33, H56

ISSN 2786-5339 (print)
ISSN 2786-5347 (online)

КОНЦЕПТУАЛЬНІ ПІДХОДИ ЩОДО УПРАВЛІННЯ КІБЕРРИЗИКАМИ У МОРСЬКІЙ ІНФРАСТРУКТУРІ В УМОВАХ ЦИФРОВІЗАЦІЇ

У статті проаналізовано трансформацію підходів щодо безпеки морської критичної інфраструктури в умовах цифровізації, гібридних загроз та кіберризиків. На підставі порівняльного аналізу законодавства Австралії, Канади, США, країн ЄС і України досліджено усталені підходи шодо визначення критичної інфраструктури та її галузевих компонентів. Виокремлено морський транспорт як особливо уразливу, але стратегічно важливу складову, що потребує оновлення інституційної моделі безпеки. Обґрунтовано необхідність переходу від ризик-орієнтованого управління (Risk-Based Approach) до моделі управління на основі стійкості (Resilience-Based Management), що забезпечує адаптивність і здатність швидко відновлювати функціонування після інцидентів. Наведено приклади міжнародної практики та інструментів цифрової безпеки, таких як цифрові двійники, супутниковий моніторинг, портова система електронної взаємодії «PortNet» та оцінка ризиків у реальному часі. Визначено інституційні бар'єри впровадження управління на основі стійкості в Україні, зокрема фрагментарність міжвідомчої відповідальності, відсутність спеціалізованої команди реагування на комп'ютерні надзвичайні події (CERT) для морських об'єктів та слабку координацію між державою і бізнесом. Отримані результати можуть бути використані для формування

стратегій кіберстійкості портів, розробки нормативної бази та підвищення ефективності міжвідомчої взаємодії.

Ключові слова: *морський транспорт, кібербезпека, судноплавні компанії, порти, інституційна координація, інфраструктура, стійкість, ризик-орієнтований підхід, цифровізація, гібридні загрози, Україна.*

Halyna ALEKSEIEVSKA, Vladyslav MYKHAILENKO, Olena BONDARENKO

CONCEPTUAL APPROACHES TO CYBER RISK MANAGEMENT IN MARITIME INFRASTRUCTURE IN THE CONTEXT OF DIGITALIZATION

The article examines the evolution of security management models for maritime critical infrastructure in the context of increasing digitalization, cyber threats, and hybrid warfare. Drawing on the analysis of legal definitions and strategic documents from Australia, Canada, the United States, the European Union, and Ukraine, the study identifies key commonalities in the treatment of maritime transport as a component of national critical infrastructure. The research focuses on the shift from a traditional risk-based approach (RBA), which emphasizes risk identification and mitigation, to a resilience-based management (RBM) model that integrates adaptive capabilities, system redundancy, and recovery mechanisms. The article analyzes international regulatory frameworks, including the ISPS Code, the U.S. Maritime Transportation Security Act, and the Network and Information Security Directive 2, which require port and shipping operators to implement systematic risk assessments and protective measures. The study also highlights advanced digital tools such as the Port Community System «PortNet», AIS monitoring systems, and digital twins, which are increasingly used to model, predict, and prevent infrastructure disruptions, improve situational awareness, and support rapid response. In addition, recent reports by organizations such as the European Union Agency for Cybersecurity (ENISA) and the Atlantic Council confirm the importance of building cross-sector cooperation and proactive threat intelligence sharing mechanisms. The findings indicate that Ukraine lacks institutional coordination, sector-specific Computer Emergency Response Team (CERT) units for maritime cybersecurity, and a unified interagency strategy for cyber risk management. The fragmentation of responsibilities and the limited integration of ports into national cybersecurity systems create vulnerabilities in the maritime domain. The results can be applicable in policy formulation, institutional reform, regulatory harmonization, capacity-building programs, and the development of national maritime cybersecurity frameworks.

Keywords: *maritime transport, cybersecurity, shipping companies, ports, institutional coordination, infrastructure, resilience, risk-based approach, digitalization, hybrid threats, Ukraine.*

Постановка проблеми. У контексті зростання глобальних викликів – від гібридних загроз до технологічних збурень – питання безпеки критичної інфраструктури набуває нового значення. Особливої актуальності набуває захист морської інфраструктури, яка є ключовим елементом світової логістики, міжнародної торгівлі та економічної стабільності. З урахуванням цифрової трансформації морського транспорту, посилення залежності від інформаційно-комунікаційних систем і зростання кількості кіберінцидентів, з'являється об'єктивна потреба у перегляді підходів щодо управління ризиками та стійкістю об'єктів морської критичної інфраструктури. Водночас, в Україні проблематика кіберзахисту морських об'єктів залишається фрагментарною, з недостатньою міжвідомчою координацією та відсутністю спеціалізованих механізмів реагування. Це ускладнює інтеграцію європейських практик та підвищує уразливість морської галузі в умовах війни й гібридних атак. Тому постає завдання осмислення концепцій Risk-Based Approach (RBA) та Resilience-Based Management (RBM).

Аналіз останніх досліджень. У сучасних дослідженнях все більшу увагу приділяють питанням кібербезпеки та стійкості морської критичної інфраструктури в умовах цифровізації. Проведений аналіз наукових публікацій засвідчує зростаючий інтерес наукової спільноти до проблеми вразливості морського транспорту щодо кіберзагроз та до пошуку ефективних моделей управління ризиками.

У дослідженнях [1 – 4] переважно акцентовано увагу на необхідності впровадження методик управління ризиками на борту суден та розробці моделей оцінки стійкості інфраструктури до збоїв. Особливу увагу приділено інтеграції ризик-орієнтованого підходу і моделі управління на основі стійкості, що передбачає як запобігання загрозам, так і здатність системи до відновлення, з урахуванням міжнародного досвіду та транскордонної співпраці.

Вагомий внесок також роблять і міжнародні організації. Так, ENISA розробила практичні рекомендації щодо оцінки та зниження кіберризиків у портах, які стали основою для впровадження цифрових рішень у європейських «розумних портах». Міжнародна морська організація (IMO) у своїх настановах закликає до інтеграції кіберризик-менеджменту в систему управління безпекою судноплавства (ISM Code). Аналітичний звіт Atlantic Council, у свою чергу, підкреслює масштабне зростання кіберзагроз у морському секторі та наголошує на необхідності консолідації політичних і технічних зусиль для посилення кіберстійкості глобальних логістичних ланцюгів [5 – 7].

Попри помітний прогрес, у науковій літературі залишається низка нерозв'язаних питань. Зокрема, недостатньо дослідженими є механізми адаптації міжнародних практик захисту морської інфраструктури до умов країн з високим рівнем зовнішніх загроз, таких як Україна. Дана стаття спрямована на узагальнення сучасних підходів до розуміння морської критичної інфраструктури та її кіберзахисту, а також на виявлення напрямів, що потребують подальших досліджень в українському контексті.

Метою дослідження є обґрунтування ролі морської інфраструктури як складової критичної інфраструктури в умовах цифровізації, а також аналіз міжнародних підходів щодо її захисту, з урахуванням зростаючих кіберзагроз, ризиків та викликів безпеці.

Виклад основного матеріалу. У сучасному глобалізованому світі морський транспорт виступає ключовим елементом міжнародної торгівлі та логістики, забезпечуючи понад 80% обсягу міжнародних світових перевезень [8]. Проте зростаюча цифровізація галузі, впровадження новітніх технологій, таких як Інтернет речей (IoT), штучний інтелект (AI), цифрові двійники та автоматизовані системи управління, водночас відкривають нові вектори кіберзагроз, які можуть призвести до значних економічних втрат, порушення ланцюгів постачання та загроз національній безпеці.

У сучасних умовах глобальної взаємозалежності та зростаючих викликів, пов'язаних із безпекою, стабільністю та стійкістю суспільства, поняття критичної інфраструктури набуває особливої актуальності. В таблиці 1 наведені визначення поняття «крична інфраструктура» з законодавства різних країн світу.

Таблиця 1. Національні визначення критичної інфраструктури

Країна	Визначення критичної інфраструктури
Австралія	Критична інфраструктура визначається як фізичні об'єкти, ланцюги постачання, інформаційні технології та мережі зв'язку, які, у разі їх знищення, пошкодження або тривалої недоступності, суттєво вплинуть на соціальне або економічне благополуччя нації чи здатність Австралії здійснювати національну оборону та забезпечувати національну безпеку.
Канада	Критична інфраструктура Канади включає фізичні об'єкти та об'єкти інформаційних технологій, мережі, послуги та активи, які, у разі порушення або знищення, матимуть серйозний вплив на здоров'я, безпеку, захист або економічне благополуччя канадців або на ефективне функціонування уряду Канади.
Німеччина	Критична інфраструктура – це організації та об'єкти, що мають важливе значення для громади, відмова або порушення роботи яких може спричинити тривалий дефіцит постачання, значні порушення громадського порядку або інші серйозні наслідки.

Закінчення таблиці 1

Країна	Визначення критичної інфраструктури
Нідерланди	Критична інфраструктура охоплює продукти, послуги та пов'язані з ними процеси, які, в разі збоїв або відмови, можуть спричинити великі соціальні потрясіння. Це може включати великі людські жертви та серйозну економічну шкоду.
Велика Британія	Критична національна інфраструктура охоплює активи, послуги та системи, що підтримують економічне, політичне та соціальне життя Великої Британії, втрата яких може: 1) спричинити масові людські жертви; 2) серйозно вплинути на національну економіку; 3) мати інші серйозні соціальні наслідки або бути предметом негайної уваги уряду.
США	Загальне визначення критичної інфраструктури в США: «системи та активи, фізичні або віртуальні, настільки важливі для Сполучених Штатів, що їх руйнування чи неспроможність функціонувати матиме руйнівний вплив на безпеку, національну економічну безпеку, національне здоров'я або поєднання цих факторів».
ЄС	Критична інфраструктура – актив, система або їх частина, що розташовані на території держав-членів і є життєво необхідними для підтримання основних суспільних функцій, охорони здоров'я, безпеки, захисту, економічного чи соціального добробуту населення, і порушення або знищення яких матиме суттєвий вплив у державі-члені через неможливість забезпечення цих функцій.
Україна	Об'єкти критичної інфраструктури – об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Джерело: [9 – 16]

Отже, критична інфраструктура (KI) – це сукупність фізичних об'єктів, інформаційно-комунікаційних систем, технологій, мереж, послуг та активів (як матеріальних, так і віртуальних), які мають вирішальне значення для підтримання життєво важливих функцій держави та суспільства. Йдеться, зокрема, про забезпечення безпеки, громадського порядку, економічної стабільності, охорони здоров'я, соціального добробуту та ефективного функціонування органів влади.

Також чітко простежується спільне розуміння ключових галузей, від яких залежить життєздатність держави та суспільства. Більшість країн визнають критичними такі сектори, як енергетика (включаючи ядерну), інформаційно-комунікаційні технології, фінансову систему, охорону здоров'я, харчову та водну безпеку, а також транспорт. Особливе місце в системі критичної інфраструктури посідає саме транспортна галузь, яка виступає основою функціонування логістики, мобільності населення, постачання товарів першої необхідності та екстреного реагування.

Усі країни, подані в таблиці 2, включають транспорт до переліку критичних секторів, а США, Велика Британія й Австралія додатково виділяють служби екстреного реагування, пов'язані з ним. Україна, згідно з національним законодавством, також визнає транспорт невід'ємною частиною критичної інфраструктури. Це свідчить про загальну тенденцію щодо розширення поняття критичності на всі сфери, які мають вирішальне значення для стійкості суспільства.

Таблиця 2. Сектори критичної інфраструктури

Сектор	Австралія	Канада	Нідерланди	Велика Британія	США	ЄС	Україна
Енергетика (включаючи ядерну)	x	x	x	x	x	x	x
ІКТ (інформаційно-комунікаційні технології)	x	x	x	x	x	x	x
Фінанси	x	x	x	x	x	x	x
Охорона здоров'я	x	x	x	x	x	x	x
Харчування	x	x	x	x	x	x	x
Водопостачання	x	x	x	x	x	x	x
Транспорт	x	x	x	x	x	x	x
Безпека	Служби екстреної допомоги			Служби екстреної допомоги	Служби екстреної допомоги		Служби екстреної допомоги
Державне управління		x	x	x	x	x	x
Хімічна промисловість		x	x	x	x	x	x
Оборонно-промислова база	x	x					x
Інші сектори або діяльність	Масові зібрання, національні символи		Правова/				
судова система		Греблі, комерційні об'єкти, національні пам'ятки	Космічні та наукові об'єкти				

Джерело: [17]

У цьому контексті особливої уваги заслуговує морська інфраструктура як складова транспортного сектору. Поняття критичної інфраструктури в морському секторі формується на перетині безпекових, логістичних, інформаційно-комунікаційних та економічних вимірів. За міжнародними стандартами, критичною вважається інфраструктура, порушення функціонування якої може призвести до серйозного негативного впливу на національну безпеку, економіку, здоров'я громадян або навколишнє середовище. Морський транспорт у повному обсязі відповідає цим критеріям.

Європейська комісія у Директиві 2008/114/ЕС визначає критичну інфраструктуру як елементи, системи або їх частини, розташовані в державах-членах ЄС, які є важливими для підтримання життєво важливих суспільних функцій. У межах цієї рамки морські порти (особливо трансєвропейського значення) розглядаються як частина Європейської критичної інфраструктури (ECI). В оновленій Директиві NIS2 (2022) встановлено вимоги щодо кіберзахисту таких об'єктів, включаючи системи управління портами, логістичні ланцюги та цифрову комунікаційну інфраструктуру, що пов'язує порти з внутрішніми транспортними системами [18; 19].

Міжнародна морська організація наголошує, що кіберзагрози здатні вивести з ладу критично важливі процеси морських операцій, і що захист критичної інфрастуктури має інтегруватися в систему управління безпекою суден (ISM Code). Міжнародна морська організація визнає, що порти, судна, автоматизовані навігаційні й вантажні системи належать до KI і потребують постійного аналізу ризиків [6].

Таким чином, можна сформувати поняття «морської критичної інфраструктури» як сукупності фізичних, цифрових і організаційних компонентів, від стійкості яких залежать глобальні ланцюги постачання, продовольча та енергетична безпека. Рисунок 1 відображає комплексну систему ключових елементів, від яких залежить безперебійне функціонування морської галузі, зовнішньоекономічна діяльність, енергетична безпека та обороноздатність держави.

До системи об'єктів морської інфраструктури входять морські порти з вантажними, пасажирськими, нафтовими та зерновими терміналами; судноплавні канали та фарватери, що забезпечують рух між портами; морські шляхи та води під юрисдикцією держави; офшорна інфраструктура (платформи, вітрові електростанції, плавучі термінали); підводні об'єкти, зокрема кабелі зв'язку й трубопроводи; системи морської безпеки (радарні станції, навігаційні системи, пункти контролю та охорони), а також об'єкти подвійного призначення, які можуть використовуватись у цивільних і військових цілях. Ці компоненти тісно взаємопов'язані та формують єдину

критичну інфраструктуру, вразливість якої може мати серйозні соціально-економічні та безпекові наслідки як на національному, так і міжнародному рівнях. Україна, враховуючи своє стратегічне розташування й роль у зерновому експорті та транзиті, повинна адаптувати ці підходи, інтегруючи управління ризиками критичної морської інфраструктури у свою транспортну політику, оборонну стратегію та цифрову трансформацію сектору.

Рис. 1. Основні об'єкти морської критичної інфраструктури

Джерело: побудовано автором на основі [1 – 19]

Ці компоненти тісно взаємопов'язані та формують єдину критичну інфраструктуру, вразливість якої може мати серйозні соціально-економічні та безпекові наслідки як на національному, так і міжнародному рівнях. Враховуючи стратегічне розташування України та її ключову роль у глобальних ланцюгах постачання, зокрема у сфері експорту зерна, виникає об'єктивна потреба у впровадженні системного підходу щодо управління безпекою морської інфраструктури. Одним із найефективніших підходів у цьому контексті є концепція ризик-орієнтованого підходу (Risk-Based Approach). Цей підхід ґрунтується на попередній оцінці ймовірності виникнення загроз і вразливостей, що дозволяє своєчасно розробляти механізми запобігання, реагування та відновлення. Його головною перевагою є здатність адаптувати політику безпеки до швидких змін у зовнішньому середовищі. У світлі зростання геополітичної нестабільності, поширення кіберзагроз, морського піратства, терористичних ризиків і наслідків змін

клімату, саме ризик-орієнтований підхід забезпечує необхідну гнучкість і проактивність у захисті морської критичної інфраструктури.

У сфері морських перевезень цей підхід був інституціоналізований через запровадження Міжнародного кодексу з охорони суден і портових засобів (ISPS Code), що був ухвалений Міжнародною морською організацією (IMO) у 2002 році як відповідь на нові виклики після терористичних атак 11 вересня 2001 року [20]. Відповідно до цього кодексу, кожне судно та кожен портовий об'єкт повинні здійснювати оцінку загроз безпеці (Security Assessment) та розробляти плани захисту (Security Plan) з урахуванням ризиків. Практика свідчить, що саме орієнтація на ризики дає змогу формувати більш адаптивні й ефективні стратегії захисту в умовах невизначеності. Важливо, що такі оцінки здійснюються не одноразово, а вимагають регулярного оновлення та перегляду, відповідно до нових загроз і змін у середовищі функціонування.

Суттєвими ознаками ризик-орієнтованого підходу є його превентивність, пропорційність заходів безпеки рівню загроз, документованість процедур і наявність чіткої координації між усіма учасниками морської інфраструктури – як державними, так і приватними. У рамках цього підходу формуються й національні політики. Наприклад, у США Maritime Transportation Security Act (MTSA) вимагає від усіх портів і судновласників регулярного здійснення оцінки ризиків, які надалі передаються в систему управління берегової охорони для координації національної морської безпеки [21].

Досвід інших країн також свідчить про ефективність цього підходу. У порту Роттердама функціонує цифрова система, яка щоденно аналізує понад 150 параметрів активності в порту, включаючи переміщення персоналу, транспортних засобів, суден і даних. Це дає можливість своєчасно виявляти аномалії й запобігати потенційним загрозам [22]. У Сінгапурі інтегрована інформаційна система PortNet поєднує цифровий обмін даними та профілювання суден за ризик-орієнтованими критеріями ще до прибуття судна до порту [23].

У рамках Європейської програми захисту критичної інфраструктури (EPCIP) ризик-орієнтований підхід використовується для ідентифікації вразливих елементів у сфері транспорту, зокрема в морській логістиці. Це дозволяє спрямовувати ресурси на захист об'єктів із найвищим рівнем ризику, підвищуючи ефективність державної політики безпеки [24].

Сучасне трактування ризик-орієнтованого підходу також містить інтеграцію цифрових технологій, таких як системи супутникового моніторингу суден (AIS), платформи управління портами (Port Community Systems),

кіберзахист інформаційної інфраструктури, штучний інтелект для прогнозування подій і навіть цифрові двійники (Digital Twins) для моделювання інфраструктурних ризиків. Останні дослідження свідчать про необхідність поєднання ризик-орієнтованих моделей з підходами щодо забезпечення стійкості (resilience), що дозволяє не лише уникати втрат, а й відновлювати транспортні ланцюги після інцидентів [25].

Ризик-орієнтований підхід (RBA) дедалі частіше поєднується з концепціями управління ланцюгом поставок і кібербезпекою. У зв'язку з цим на перший план виходить потреба міжвідомчої та міжнародної співпраці, прозорого обміну інформацією та підвищення компетентності учасників логістичних процесів. Важливо також наголосити, що впровадження RBA у морському секторі не є технічним питанням, а частиною ширшої парадигми управління безпекою, в якій поєднуються інституційні, правові, організаційні й технологічні інструменти [26].

Ще однією актуальною моделлю, є модель управління на основі стійкості, яке передбачає не тільки запобігання загрозам, а й здатність швидко відновлювати функціонування систем після інцидентів. На відміну від традиційного ризик-орієнтованого підходу, який фокусується переважно на запобіганні загрозам і зниженні вразливостей, модель RBM ґрунтується на ідеї, що повністю уникнути загроз неможливо, а тому система повинна бути готовою адаптуватися до збурень і відновлюватися після інцидентів з мінімальними втратами.

Стійкість, у цьому контексті, трактується як здатність морської транспортної системи зберігати функціональність, швидко відновлювати порушені процеси та пристосовуватися до змінних умов. До ключових складових RBM у морському секторі належать: резервні маршрути транспортування, дублювання функцій, гнучкість портової логістики, різноманітність джерел постачання, інформаційна прозорість, інституційна координація та інфраструктурна адаптивність [27].

Перехід до RBM передбачає не лише технічні рішення (резервування, дублювання каналів зв'язку, адаптивні платформи), але й інституційну реорганізацію, мультисекторальну координацію та залучення локальних і міжнародних партнерів до процесу забезпечення стійкості. Крім того, RBM краще відповідає умовам гібридної війни, що є особливо актуальним для України, де загрози поєднують фізичні, цифрові та інформаційні складові.

Таким чином, перехід від RBA до RBM є логічною еволюцією системи управління безпекою морської інфраструктури, яка дозволяє не лише уникати загроз, а й забезпечувати безперервність функціонування та швидке відновлення у кризових ситуаціях.

Впровадженню моделі управління на основі стійкості (RBM) в Україні заважає низка інституційних чинників. По-перше, спостерігається фрагментарність відповідальності між відомствами, що відповідають за кібербезпеку – Держслужба спеціального зв'язку (CERT-UA), НЦЗК при РНБО, Служба морського та річкового транспорту, Міністерство цифрової трансформації – без єдиного координаційного механізму. Відсутність такого механізму значно ускладнює узгоджену реалізацію RBM у морських портах і транспортній інфраструктурі.

По-друге, в Україні відсутній спеціалізований підрозділ CERT, який би займався кібербезпекою об'єктів морської інфраструктури. Хоча урядова команда реагування на комп'ютерні надзвичайні події CERT-UA активно працює у сфері кіберзахисту критичної інфраструктури загалом, специфічні ризики та вразливості морського сектору залишаються поза її фокусом. Це створює прогалини в системі моніторингу, попередження та реагування на кіберінциденти в морській галузі [28].

По-третє, низька координація між державним та приватним секторами, а також недостатній обмін інформацією про кіберзагрози, створюють уразливості, особливо в контексті стійкості проти геополітичних викликів і гібридних загроз [29].

Разом ці чинники знижують ефективність запровадження RBM у морській сфері. Для їх подолання необхідні законодавчі зміни, створення міжвідомчого операційного штабу та формування спеціалізованих CERT-механізмів саме для портів і морської логістики.

Висновки. Морська інфраструктура є невід'ємною складовою критичної інфраструктури, від якої залежить не лише логістична ефективність, але й економічна, продовольча та національна безпека держав. В умовах цифрової трансформації та зростаючих геополітичних ризиків, традиційні підходи щодо безпеки, зокрема Risk-Based Approach (RBA), потребують розширення та доповнення моделлю управління на основі стійкості (Resilience-Based Management – RBM).

Впровадження RBM дозволяє не лише оцінювати та зменшувати ризики, а й забезпечити безперервність функціонування морської транспортної системи в умовах кризи або після інцидентів. Такий підхід охоплює інфраструктурну, цифрову, організаційну та інституційну компоненти безпеки, інтегруючи сучасні цифрові технології, системи моніторингу, прогнозування та аналітики.

Застосування RBM є особливо актуальним для України з огляду на тривалу війну, уразливість портової інфраструктури, її важливу роль у глобальних ланцюгах постачання, а також необхідність адаптації до гібрид-

них загроз. Водночас впровадженню цього підходу перешкоджає низка інституційних бар'єрів – фрагментарність відповідальності між органами влади, відсутність спеціалізованого CERT для морського сектору, недостатня взаємодія державних і приватних структур.

Для реалізації RBM у морському секторі України необхідне: створення міжвідомчого координаційного механізму з питань кіберзахисту морської інфраструктури; формування спеціалізованих CERT-підрозділів для портів; законодавча адаптація принципів стійкості; стимулювання обміну інформацією між усіма учасниками морської логістики.

Всі ці дії сприятимуть формуванню гнучкої, адаптивної та стійкої системи безпеки в морському секторі, що відповідатиме сучасним викликам і європейським стандартам управління критичною інфраструктурою.

Перспективи подальших досліджень у даному напрямі пов'язані з необхідністю глибшого аналізу цифрових аспектів захисту морської інфраструктури, зокрема розробки моделей вразливості на основі технологій цифрових двійників. Особливої уваги потребує вивчення міжнародного досвіду реагування на кіберзагрози в портах країн ЄС, з метою адаптації успішних практик до українських реалій. Перспективним напрямом також є аналіз потенціалу українських дунайських портів як бази для впровадження інноваційних моделей управління на основі стійкості. Крім того, важливим завданням є оцінка економічної доцільності впровадження заходів кіберзахисту в морській логістиці як для держави, так і для приватного сектору.

ЛІТЕРАТУРА

1. Alcaide J. I., Llave R. G. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. 2020. Vol. 45. Pp. 547–554. URL: https://www.sciencedirect.com/science/article/pii/S2352146520302209 (дата звернення: 10.07.25).

2. 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. 2025. URL: https://arxiv.org/abs/2506.15842 (дата звернення: 10.07.25).

3. Li M., Zhou J., Chattopadhyay S., Goh M. Maritime Cybersecurity: A Comprehensive Review. 2024. URL: https://arxiv.org/abs/2409.11417 (дата звернення: 10.07.25).

4. Dui H., Zheng X., Wu S. Resilience analysis of maritime transportation systems based on importance measures. *Reliability Engineering & System Safety*. 2021. Vol. 214. URL: https://www.sciencedirect.com/science/article/abs/pii/S0951832021000296 (дата звернення: 10.07.25).

5. European Union Agency for Cybersecurity (ENISA). Port Cybersecurity – Good practices for cybersecurity in the maritime sector. URL: https://www.enisa.europa.eu/publications/port-cybersecurity (дата звернення: 10.07.25).

6. International Maritime Organization. Maritime Cyber Risk Management. URL: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (дата звернення: 25.03.25).

7. Atlantic Council. Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity. 2021. URL: https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Cyber-Maritime-Final-Report.pdf (дата звернення: 10.07.25).

8. NCTAD. Shipping data: UNCTAD releases new seaborne trade statistics. https://unctad.org/news/shipping-data-unctad-releases-new-seaborne-trade-statistics (дата звернення: 25.03.25).

9. Australian National Security. What is critical infrastructure? URL: https://www.ag.gov.au/agd (дата звернення: 25.03.25).

10. Public Safety Canada. About Critical Infrastructure. URL: https://www.ps-sp.gc.ca (дата звернення: 25.03.25).

11. Federal Office for Information Security. Critical Infrastructure Protection in Germany. URL: https://www.bsi.de/english/topics/kritis/KRITIS_in_Germany.pdf (дата звернення: 25.03.25).

12. UK Home Office. Counter Terrorism Strategy: Protecting the Critical National Infrastructure. URL: https://www.security.homeoffice.gov.uk (дата звернення: 25.03.25).

13. Ministry of the Interior of the Netherlands. Report on Critical Infrastructure Protection. 2005.

14. United States Department of Homeland Security. National Infrastructure Protection Plan. 2006. URL: https://www.dhs.gov (дата звернення: 25.03.25).

15. European Union. Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114 (дата звернення: 25.03.25).

16. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 06.05.25).

17. OECD. Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security. 2008. URL: https://www.oecd.org/en/publications/protection-of-critical-infrastructure-and-the-role-of-investment-policies-relating-to-national-security_7d159744-en.html (дата звернення: 25.03.25).

18. ENISA. NIS2 Directive. URL: https://www.enisa.europa.eu/topics/csirt-cert-services/nis-directive (дата звернення: 25.03.25).

19. European Commission. NIS2 Directive. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (дата звернення: 25.03.25).

20. International Maritime Organization. The International Ship and Port Facility Security Code (ISPS Code). URL: https://www.imo.org/en/OurWork/Security/Pages/ISPSCode.aspx (дата звернення: 08.03.25).

21. United States Congress. Maritime Transportation Security Act of 2002. Public Law. 107 — 295. URL: https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf (дата звернення: 25.03.25).

22. Port of Rotterdam Authority. Smart infrastructure URL: https://www.portofrotterdam.com/en/port-future/smart-infrastructure (дата звернення: 20.03.25).

23. Maritime and Port Authority of Singapore. Media Centre. URL: https://www.mpa.gov.sg/media-centre?page=1&year=All&type=acde700a-7731-4738-902e-9513d5fac394 (дата звернення: 20.03.25).

24. European Commission. Protecting European critical infrastructures. URL: https://ec.europa.eu/home-affairs/policies/internal-security/critical-infrastructure_en (дата звернення: 08.03.25).

25. UNDRR. 2023 Progress Report: Implementation of the UN Plan of Action on Disaster Risk Reduction for Resilience. URL: https://www.undrr.org/media/103580/download?startDownload=20250508 (дата звернення: 20.03.25).

26. Bueger C., Edmunds T., Ryan B. J. Maritime security: The uncharted politics of the global sea. *International Affairs*. 2019. Vol. 95. No 5. Pp. 971 — 978. DOI: https://doi.org/10.1093/ia/iiz145.

27. OECD. Building resilience: New strategies for strengthening infrastructure resilience and maintenance. *OECD Public Governance Policy Papers*. 2021. No 05. Paris: OECD Publishing. DOI: http://dx.doi.org/10.1787/354aa2aa-en.

28. CERT UA. Сайт Урядової команди реагування на комп'ютерні надзвичайні події України. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cert.gov.ua (дата звернення: 15.07.25).

29. Melnyk O., Drozdov O., Kuznichenko S. Cybersecurity in maritime transport: an international perspective on regulatory frameworks and countermeasures. *Lex Portus*. 2025. Vol. 11. Iss. 1. DOI: https://doi.org/10.62821/lp11101.

REFERENCES

1. Alcaide J. I., Llave R. G. (2020) Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, Vol. 45. Pp. 547–554. https://www.sciencedirect.com/science/article/pii/S2352146520302209.

2. Raymaker A., Kumar A., Wong M. Y., Pickren R., Chhotaray A., Li F., Zonouz S., Beyah R. (2025) A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners. https://arxiv.org/abs/2506.15842.

3. Li M., Zhou J., Chattopadhyay S., Goh M. (2024) Maritime Cybersecurity: A Comprehensive Review. https://arxiv.org/abs/2409.11417.

4. Dui H., Zheng X., Wu S. (2021) Resilience analysis of maritime transportation systems based on importance measures. *Reliability Engineering & System Safety*, Vol. 214. https://www.sciencedirect.com/science/article/abs/pii/S0951832021000296.

5. European Union Agency for Cybersecurity (ENISA) (2020) Port Cybersecurity: Good practices for cybersecurity in the maritime sector. https://www.enisa.europa.eu/publications/port-cybersecurity.

6. International Maritime Organization (IMO) (2020) Maritime Cyber Risk Management. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

7. Atlantic Council (2021) Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity. https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Cyber-Maritime-Final-Report.pdf.

8. NCTAD (2025). Shipping data: UNCTAD releases new seaborne trade statistics. https://unctad.org/news/shipping-data-unctad-releases-new-seaborne-trade-statistics .

9. Australian National Security (2021) What is critical infrastructure? https://www.ag.gov.au/agd.

10. Public Safety Canada (2021) About Critical Infrastructure. https://www.ps-sp.gc.ca.

11. Federal Office for Information Security (Germany) (2021) Critical Infrastructure Protection in Germany. https://www.bsi.de/english/topics/kritis/KRITIS_in_Germany.pdf.

12. UK Home Office (2010) Counter Terrorism Strategy: Protecting the Critical National Infrastructure. https://www.security.homeoffice.gov.uk.

13. Ministry of the Interior of the Netherlands (2005) Report on Critical Infrastructure Protection.

14. United States Department of Homeland Security (2006) National Infrastructure Protection Plan. https://www.dhs.gov.

15. European Union (2008) Directive 2008/114/EC on the identification and designation of European critical infrastructures. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114.

16. Verkhovna Rada of Ukraine (2021) Zakon Ukrainy «Pro krytychnu infrastrukturu» [Law of Ukraine «On Critical Infrastructure»]. No 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20#Text.

17. Organisation for Economic Co-operation and Development (OECD) (2008) Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security. https://www.oecd.org/en/publications/protection-of-critical-infrastructure-and-the-role-of-investment-policies-relating-to-national-security_7d159744-en.html.

18. ENISA (2023) NIS2 Directive. https://www.enisa.europa.eu/topics/csirt-cert-services/nis-directive.

19. European Commission (2023) NIS2 Directive. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

20. IMO (2002) The International Ship and Port Facility Security Code (ISPS Code). https://www.imo.org/en/OurWork/Security/Pages/ISPSCode.aspx.

21. United States Congress (2002) Maritime Transportation Security Act of 2002. Public Law. 107 – 295. https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf.

22. Port of Rotterdam Authority (2025) Smart infrastructure URL: https://www.portofrotterdam.com/en/port-future/smart-infrastructure.

23. Maritime and Port Authority of Singapore (2023) Media Centre. https://www.mpa.gov.sg/media-centre?page=1&year=All&type=acde700a-7731-4738-902e-9513d5fac394.

24. European Commission (2023) Protecting European Critical Infrastructures. https://ec.europa.eu/home-affairs/policies/internal-security/critical-infrastructure_en.

25. United Nations Office for Disaster Risk Reduction (UNDRR) (2023) Progress Report: Implementation of the UN Plan of Action on Disaster Risk Reduction for Resilience. https://www.undrr.org/media/103580/download?startDownload=20250508.

26. Bueger C., Edmunds T., Ryan B. J. (2019) Maritime security: The uncharted politics of the global sea. *International Affairs*, Vol. 95. No 5. Pp. 971 – 978. https://doi.org/10.1093/ia/iiz145.

27. OECD (2021) Building resilience: New strategies for strengthening infrastructure resilience and maintenance. *OECD Public Governance Policy Papers*, No 05. https://doi.org/10.1787/354aa2aa-en.

28. CERT-UA (2025) Uriadova komanda reahuvannia na kompiuterni nadzvychaini podii v Ukraini [The Government Computer Emergency Response Team of Ukraine]. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. https://cert.gov.ua.

29. Melnyk O., Drozdov O., Kuznichenko S. (2025) Cybersecurity in maritime transport: An international perspective on regulatory frameworks and countermeasures. Lex Portus. Vol. 11. Iss. 1. https://doi.org/10.62821/lp11101.