



Менеджмент

УДК 330.656.6

DOI <https://doi.org/10.5281/zenodo.18830456>

**Невизначеність безпеки у стратегічному управлінні розвитком
морської транспортної інфраструктури України**

Сотниченко Людмила Леонідівна,

доктор економічних наук, професор, завідувачка кафедри Менеджменту та економіки морського транспорту, Національний університет «Одеська морська академія», м. Одеса, Україна, <https://orcid.org/0000-0003-4537-1553>

Табенський Сергій Васильович,

аспірант кафедри Менеджменту та економіки морського транспорту,
Національний університет «Одеська морська академія»,
м. Одеса, Україна, <https://orcid.org/0009-0001-5842-5808>

Барінов Дмитро Анатолійович,

аспірант кафедри Менеджменту та економіки морського транспорту,
Національний університет «Одеська морська академія»,
м. Одеса, Україна, <https://orcid.org/0009-0005-4335-3345>

Прийнято: 07.02.2026 | Опубліковано: 26.02.2026

***Анотація.** Актуальність дослідження зумовлена різким зростанням безпекової невизначеності у сфері функціонування та розвитку морської транспортної інфраструктури України після початку повномасштабної військової агресії у 2022 році. Вплив геополітичних, військових, кібернетичних*



загроз суттєво ускладнив процеси стратегічного управління, операційного планування та залучення інвестицій у портову інфраструктуру. **Метою статті** є обґрунтування напрямів подолання безпекової невизначеності в процесі стратегічного управління розвитком морської транспортної інфраструктури України з урахуванням сучасних ризиків та міжнародного досвіду. **Методи дослідження.** Методологічною основою дослідження є системний підхід, методи аналізу та синтезу, порівняльний аналіз, сценарне прогнозування, а також узагальнення міжнародних нормативних та практичних підходів до управління морськими ризиками. У **результаті дослідження** ідентифіковано ключові прояви безпекової невизначеності, що впливають на конкурентоспроможність морської транспортної системи України, зокрема військові загрози, кіберризики, обмеження навігації, трансформацію логістичних ланцюгів та інвестиційні бар'єри. Запропоновано систему адаптивних заходів стратегічного управління, спрямовану на підвищення стійкості портів. **Практична цінність** статті полягає у можливості використання отриманих результатів органами державного управління, портовими адміністраціями та інвесторами при формуванні стратегій розвитку морської транспортної інфраструктури. Зроблено **висновок**, що гнучкість стратегій, інтеграція безпекових принципів та розвиток цифрових компетенцій персоналу є ключовими чинниками відновлення конкурентоспроможності морської транспортної інфраструктури України.

Ключові слова: управління, безпека, порти, судноплавство, персонал, невизначеність, кібербезпека, цифровізація, ризики.



Security Uncertainty in Strategic Management of Ukraine's Maritime Transport Infrastructure

Lyudmila Sotnychenko,

Doctor of Economics, Professor, Head of the Department of Maritime Transport Management and Economics, National University "Odesa Maritime Academy",
Odessa, Ukraine, <https://orcid.org/0000-0003-4537-1553>

Sergiy Tabenskyy,

Postgraduate Student, of the Department of Maritime Transport Management and Economics, National University "Odesa Maritime Academy",
Odessa, Ukraine, <https://orcid.org/0009-0001-5842-5808>

Dmytro Barinov,

Postgraduate Student, of the Department of Maritime Transport Management and Economics, National University "Odesa Maritime Academy",
Odessa, Ukraine, <https://orcid.org/0009-0005-4335-3345>

Abstract. *The relevance of the study is driven by the sharp increase in security uncertainty in the functioning and development of Ukraine's maritime transport infrastructure following the onset of full-scale military aggression in 2022. The impact of geopolitical, military, and cyber threats has significantly complicated strategic management processes, operational planning, and investment attraction in port infrastructure. The purpose of the article is to substantiate directions for overcoming security uncertainty in the process of strategic management of the development of Ukraine's maritime transport infrastructure, taking into account current risks and international experience.*



Research methods. The methodological basis of the study is a systemic approach, methods of analysis and synthesis, comparative analysis, scenario forecasting, as well as generalization of international regulatory and practical approaches to maritime risk management.

As a result of the research, key manifestations of security uncertainty affecting the competitiveness of Ukraine's maritime transport system have been identified, including military threats, cyber risks, navigation restrictions, transformation of logistics chains, and investment barriers. A system of adaptive strategic management measures aimed at enhancing port resilience is proposed.

The practical value of the article lies in the possibility of using the obtained results by public authorities, port administrations, and investors in the development of strategies for maritime transport infrastructure development. It is concluded that flexibility of strategies, integration of security principles, and development of digital competencies of personnel are key factors in restoring the competitiveness of Ukraine's maritime transport infrastructure.

Keywords: *management, security, ports, shipping, personnel, uncertainty, cybersecurity, digitalization, risks.*

Постановка проблеми. Формування світових практик оновлення компонентів стратегічного управління розвитком морської транспортної інфраструктури відбувається під впливом глобальних трендів, які мають суттєве значення для створення окремих напрямків та компонентів планування організаційно-економічних механізмів, задіяних у процесах розвитку морської транспортної інфраструктури. До глобальних трендів відносяться геоекономіка та міжнародна торгівля, сталий розвиток, цифровізація, логістична інтеграція, безпека та сталість.

Зростання обсягів навантаження на порти та інші компоненти морської транспортної інфраструктури у світовому масштабі призвело до необхідності



підвищення рівня безпеки та стійкості функціонування. Оскільки цифрове управління процесами створює компонент підвищеної небезпеки через потенційну вразливість цифрових засобів, що використовуються в процесі забезпечення управління технологічними процесами, то підвищеної уваги потребує кіберзахист об'єктів морської транспортної інфраструктури.

Це зумовлює необхідність переосмислення визначення безпекової невизначеності в сьогоденних умовах як одного із головних факторів розвитку та стійкості морської транспортної інфраструктури в Україні.

Аналіз останніх досліджень і публікацій.

За останні роки зростання ризиків у морському транспорті привертає дедалі більше уваги наукової спільноти. Сучасні дослідження вказують на необхідність комплексного підходу до безпеки морського транспорту, який охоплює не лише економічні аспекти, але й політичні, технічні, кліматичні та інші фактори. Упродовж останніх років провідне місце в наукових дослідженнях посідає проблематика стійкості портової інфраструктури.

У працях зарубіжних науковців порти розглядаються як складні соціо-еколого-економічні системи, що поєднують інфраструктурну ефективність, екологічну відповідальність та інституційну узгодженість за критеріями безпекоорієнтованості (Notteboom, T., & Haralambides, H. [1], Lam C.N. & Notteboom, T. [2]). Глобальні тренди управління портами та ключові аспекти стійкості портової інфраструктури є важливою складовою сучасних досліджень А. Pallis та J.-P. Rodrigue. [3]. Праця О. Diachenko, О. Gab та Р. Marchuk присвячена адаптивному управлінню портами, ефективності та модернізації інфраструктури [4]. Clavijo Mesa, M.V., Patiño-Rodríguez, C.E., & Guevara Carazas, F.J. [5] у своїх дослідженнях детально проаналізували основні елементи, що сприяють підвищенню портової стійкості - це адаптивне, ефективне управління та інтеграція технологій кіберризиків. Адаптивні моделі управління кіберризиками були представлені в останніх дослідженнях як



перспективні інструменти для кількісної оцінки та мінімізації ризиків кібератак у портах і автономних суднах (автори: Gaiyun Liu, Omar Amri, Ye Liang та ін.) [6].

Окремий напрям наукових дискусії до забезпечення безпеки морського транспорту пов'язаний із цифровою трансформацією портових систем. У роботах Heilig L., Lalla-Ruiz E., Voß S. [7], а також Klar R., Fredriksson A., Angelakis V. [8] обґрунтовано роль Port Community Systems, цифровізації та штучного інтелекту як інструментів адаптивності портів до невизначених ризиків. Водночас автори наголошують, що цифровізація має бути інтегрована в загальну стратегію сталого розвитку.

У контексті стратегічного управління зарубіжні науковці Notteboom, Pallis та Rodrigue [9] підкреслюють, що сучасна портова система повинна ґрунтуватися на взаємодії держави, бізнесу, місцевих громад і міжнародних інституцій, що дозволяє забезпечити баланс між стабілізаційними та інноваційними контурами розвитку. Подібний підхід узгоджується з положеннями європейських стратегічних документів, зокрема EU Green Deal [10], Blue Economy Framework [11] та політикою розвитку мережі TEN-T (European Commission) [12].

У вітчизняній науковій літературі проблеми невизначеності безпеки у стратегічному управлінні розвитком морської транспортної інфраструктури України переважно досліджуються крізь призму інституційних реформ, концесійних механізмів та модернізації інфраструктури (Жихарєва В.В. [13]). Потаповська М. у своїх роботах досліджує стратегії управління розвитком для підвищення конкурентоспроможності портової галузі та визначає основні теоретичні положення і практичні аспекти належного забезпечення стійкості логістичних процесів, які стосуються питань безпеки [14]. В.С. Веремчук досліджує міжнародно-правові аспекти безпеки морської галузі, приділяючи



увагу міжнародним механізмам щодо захисту інформації та мінімізації ризиків кібератак у морському середовищі [15].

Українські дослідники Т.В. Зайцева, О.М. Безбах та Н.Г. Камінська [16] у своїй роботі розглядають управління кіберінцидентами у морській галузі, включаючи розробку стратегій реагування на кіберпорушення та моделі управління таким реагуванням. Дослідження О. Полікаровського, Ю. Дауса, Д. Ларіна та М. Ткаченко [17] класифікують сучасні кіберзагрози у морському транспорті, включаючи аналіз вразливостей у навігаційних системах та потенційних типів атак на портову інфраструктуру. Це підтверджує, що на рівні наукового аналізу зростає увага до систематизації та детального розгляду кіберзагроз саме для морського сектору.

Цифрові технології у світовій практиці управління портами аналізують Русанова С. та Перепічко М., акцентуючи увагу на адаптації моделей управління до сучасних викликів, що дозволить підвищити ефективність логістичних процесів і конкурентоспроможність портів [18].

Виділення невирішених раніше частин загальної проблеми. У сфері логістики та транспорту останні дослідження підкреслюють важливість цифровізації та кіберстійкості, оскільки понад половина організацій у транспортно-логістичному секторі вважає безпеку пріоритетом у своїх ризик-менеджмент стратегіях, але часто стикається з недостатньою готовністю реагувати на сучасні загрози.

Вітчизняні публікації висвітлюють недостатній рівень уваги до невизначеність безпеки у сфері морської транспортної інфраструктури України порівняно із західними країнами, а також необхідність посилення нормативної бази й практичних рішень у цій сфері.

Внесок цієї статті в розв'язання зазначених проблем полягає у формуванні цілісного наукового бачення того, як запропонована система заходів щодо подолання безпекової невизначеності в процесі стратегічного



управління розвитком морської транспортної інфраструктури України впливають на підвищення стійкості портових систем.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є теоретичне обґрунтування та практичне формулювання напрямів подолання безпекової невизначеності в процесі стратегічного управління розвитком морської транспортної інфраструктури України, з урахуванням сучасних безпекових викликів, міжнародних стандартів управління ризиками, а також досвіду розвитку кіберстійкості у портових системах.

Для досягнення поставленої мети передбачається розв'язати наступні наукові й практичні **завдання дослідження**: 1) проаналізувати прояви безпекової невизначеності в морській транспортній галузі України; 2) узагальнити міжнародний досвід і сучасні підходи до стратегічного управління ризиками в морських портах; 3) дослідити вплив безпекової невизначеності на конкурентоспроможність, ефективність операційного планування та інвестиційну привабливість портових систем; 4) визначити ключові складові комплексної стратегії підвищення стійкості морської транспортної інфраструктури в умовах невизначеності безпеки; 5) сформулювати практичні рекомендації та адаптивні заходи щодо покращення стратегічного управління.

Викладання основного матеріалу дослідження.

З лютого 2022 року Україна зіткнулась із системними ризиками, які докорінно змінили умови стратегічного управління розвитком морської транспортної інфраструктури, оскільки на всі компоненти розвитку впливає невизначеність у сфері безпеки. Невизначеність проявляється у неможливості прогнозувати стабільність навігації, рівня збереженості портової інфраструктури, безпеки персоналу та вантажів. Від рівня безпеки залежить обсяг операційних потреб портів, виникають обмеження їх функціонування,



зацікавленості інвесторів та довгострокового планування розвитку. На рисунку 1 наведено загальну схему невизначеності у сфері безпеки та операційних потреб в процесі стратегічного управління та розвитку морської транспортної інфраструктури України.

Кіберзахист портів виражається у комплексному впровадженні заходів кібербезпеки та розвитку кіберстійкості для захисту критичної інфраструктури, операцій та даних від зростаючих цифрових загроз. Порти обробляють 80% світової торгівлі, тому атака може спричинити значні фінансові втрати та порушення ланцюга поставок, як приклад, атака на дунайський судноплавний гігант A.P. Moller-Maersk у 2017 році стала серйозним сигналом тривоги для галузі. Кібератаки можуть поставити під загрозу системи операційних технологій, що контролюють рух суден, обробку вантажів та навігацію, створюючи ризики для життя, вантажу та навколишнього середовища.

Порти керують конфіденційними даними, включаючи інформацію про клієнтів, деталі вантажу та фінансові записи, які необхідно захистити від порушень. Порти є критично важливою інфраструктурою та потенційними цілями для пов'язаних з державою порушників, що робить їхню безпеку головним пріоритетом [3].

Багаторівнева стратегія кібербезпеки об'єктів морської транспортної інфраструктури має декілька напрямків розвитку. Кібербезпека потребує формування структури управління ризиками, які представлені у світовому досвіді такими заходами, як контрольні принципи NIST 800-171 у США або рекомендації Міжнародної морської організації [19] щодо управління морськими кіберризиками, допомагає виявляти та пом'якшувати ризики.



Рис. 1. Невизначеність безпеки та вплив на операційні потреби морської транспортної інфраструктури України

Джерело: побудовано авторами

Особливо важливим при формуванні стратегічного управління розвитком морської транспортної інфраструктури є сегментація мережі та створення спеціалізованих брандмауерів, що допомагає контролювати трафік, здійснювати моніторингові операції діяльності окремих підрозділів у портах та запобігати несанкціонованому доступу.

В процесі формування стратегії розвитку об'єктів морської транспортної інфраструктури має бути заздалегідь створена концепція обмеження доступу



до певних систем та даних за допомогою надійних механізмів автентифікації зменшує внутрішні загрози та несанкціонований доступ. Розробка та регулярне тестування планів реагування на інциденти забезпечує швидку та ефективну реакцію на будь-яку кібератаку, мінімізуючи вплив. Оновлення програмного забезпечення та систем є важливим для усунення відомих вразливостей, якими часто користуються зловмисники.

Важливе значення в процесі стратегічного планування розвитку морської транспортної інфраструктури у світовому досвіді приділяється навчанню та підвищенню обізнаності співробітників, оскільки загальна безпека об'єктів морської транспортної інфраструктури залежить від культури кібербезпеки співробітників. Постійний моніторинг та аудит усіх активів морської транспортної інфраструктури допомагає виявляти підозрілу активність та перевіряти ефективність заходів безпеки. Співпраця та обмін інформацією з партнерами, урядовими установами (такими як НАТО та Агентство ЄС з кібербезпеки ENISA [20]) та галузевими організаціями має вирішальне значення для того, щоб підтримувати постійний рівень освіченості у питаннях змін загроз у інформаційному просторі, що є невід'ємною складовою морської транспортної інфраструктури.

Для визначення головних проявів змін у безпековій ситуації потрібно обрати первинний рівень, відносно якого будуть формуватися компоненти невизначеності. Оскільки більшість з компонентів невизначеності безпеки для морської транспортної інфраструктури були сформовані з початком бойових дій 24 лютого 2022 року, то в якості первинного рівня можна взяти попередній період. Невизначеність у сфері безпеки є одним з головних чинників впливу на конкурентоздатність всієї системи морського транспорту як України, так й чорноморського регіону в цілому.

Прояви невизначеності безпеки мають різний характер та джерело походження, однак, всі ці прояви мають негативний вплив на розвиток



морської транспортної інфраструктури України. За останні роки значної шкоди було нанесено військовими загрозами, через що виникли значні ушкодження портів Маріуполь, Бердянськ, Одеса, Південний, Миколаїв. Існує мінна загроза в акваторії Чорного моря, що також обмежує розвиток морської транспортної інфраструктури України. Значного впливу на конкурентоздатність також зазнали традиційні ланцюги поставок, які виникли внаслідок блокування морських шляхів, залежності від тимчасових зернових коридорів та альтернативних маршрутів через Дунай [20].

Ризики для судноплавства виражаються шляхом невизначеності навігаційної безпеки та ускладнень у страхуванні вантажів через обмеження діяльності багатьох страхових компаній, які традиційно працювали з вантажами у цьому економічному регіоні. На конкурентоздатність портів та на можливість залучення інвесторів до проєктів оновлення морської транспортної інфраструктури впливає технологічна нестабільність через кіберзагрози, оскільки високою є ймовірність втрати контролю над логістичними процесами внаслідок атак на інформаційні системи портів [17].

Окремого розгляду потребують проблеми у сфері операційних потреб та стратегічного управління. Через суттєвий вплив поточних загроз стратегічні плани розвитку дуже часто переглядаються, що призводить до зниження ефективності операційного планування. Зростання експлуатаційних витрат об'єктів морської транспортної інфраструктури пов'язано з необхідністю посилення охоронних заходів, протимінних та інших превентивних безпекових заходів, особливих умов страхування, розробки та технологічного підтримання альтернативних маршрутів. Підвищення рівня безпеки об'єктів морської транспортної інфраструктури має сприяти поверненню довіри іноземних інвесторів, оскільки через падіння інвестиційної привабливості деякі проєкти з оновлення морської транспортної інфраструктури не можуть бути вчасно завершені [13].



Морська інфраструктура має пряму залежність від політичної стабільності та безпеки пересування морськими шляхами. Локальні військові конфлікти, дії піратів та санкції порушують транспортні ланцюги, що має отримати відображення у стратегічних планах розвитку морської транспортної інфраструктури інших країн світу, через виникнення необхідності пошуку можливостей інфраструктурного забезпечення оновлених ланцюгів поставок. Наприклад, блокування маршрутів у Червоному морі та Суецькому каналі у 2021-2024 роках призвели до необхідності пошуку нових маршрутів у світовій логістиці. Через збройний конфлікт в Україні у загальносвітовому масштабі було змінено ставлення до стратегічного планування експортних потоків. Через тривалу бездіяльність влади у Ємені та Сомалі до піратства підвищуються страхові видатки власників судів суден, які здійснюють перевезення через маршрути, що проходять повз нейтральні води, які межують з акваторією цих країн. Геополітичні та логістичні ризики призводять до росту транспортних видатків, скорочення міжнародного трафіка та зниження інвестиційної привабливості портів.

Однією з важливих проблем стратегічного планування діяльності у сфері модернізації морської транспортної інфраструктури України є необхідність гнучкості та адаптивності стратегій, оскільки на теперішній час існуюча система стратегічного управління дуже повільно реагує на зміни в умовах безпеки, що додатково призводить до втрати конкурентоздатності. Ці проблеми виникають через проблеми з координацією між різними державними структурами, які беруть участь як в управлінні об'єктами морської транспортної інфраструктури, таких як, наприклад, Адміністрація морських портів України та Міністерства внутрішніх справ. Створення системних комунікаційних каналів допоможе у формуванні оперативних рішень відповідно до безпекової ситуації у портах України.



Для подолання безпекової невизначеності в процесі стратегічного управління розвитком морської транспортної інфраструктури України, можна запропонувати систему заходів, яка відображена у таблиці 1.

Таблиця 1

Система заходів щодо подолання безпекової невизначеності у сфері морської транспортної інфраструктури України

Захід	Короткий зміст	Потенційні виконавці
1. Розробка адаптивних стратегій управління	Вироблення сценарних планів, які враховують різні рівні загроз	Національна академія наук України, Адміністрація морських портів України
2. Інтеграція принципів безпеки	Перегляд вимог до інфраструктурних проєктів з метою інтеграції принципів стійкості та безпеки	Міністерство розвитку громад та територій
3. Міжнародне співробітництво	Участь міжнародних організацій для створення безпечних транспортних коридорів	Міністерство закордонних справ, Міністерство розвитку громад та територій
4. Розвиток альтернативних маршрутів	Розвиток альтернативних маршрутів і портів Дунайського кластера (Ізмаїл, Рені, Усть-Дунайськ) не тільки як тимчасового, але й як стратегічного рішення	Міністерство розвитку громад та територій, Адміністрація морських портів України
5. Система оперативного моніторингу ризиків	Створення системи оперативного моніторингу ризиків шляхом інтеграції використання різноманітних супутникових технологій та аналітичних систем	Міністерство розвитку громад та територій, Міністерство внутрішніх справ, Міністерство цифрової трансформації, Адміністрація морських портів України
6. Поліпшення фінансового становища портів	Залучення додаткових страхових та фінансових інструментів	Міністерство закордонних справ, Міністерство економіки, довкілля та сільського господарства

Джерело: сформульовано та систематизовано авторами

Не зважаючи на декларування Україною інтеграції з транспортною системою Європи (TEN-T), не всі нормативні акти приведені у відповідність



до стандартів, за якими працює ця інтегрована система, що створює штучні бар'єри для роботи окремих перевізників та прийомі вантажів у морських портах як України, так й Європи. Така ж ситуація складається з директивами Міжнародної морської організації у сфері безпеки, упровадження цифрових інструментів сталому розвитку морських портів, що створює штучні перепони щодо ефективної інтеграції морської транспортної інфраструктури України до світових систем.

Поліпшення цифрових компетенцій персоналу полегшить функціонування систем безпеки, у тому числі кібербезпеки. Для виконання умов якісної охорони даних потрібно уводити спеціалізовані освітні модулі у програми підвищення кваліфікації як керівного складу, так й фахівців сфери морської транспортної інфраструктури. Ці компоненти мають супроводжуватись реальними прикладами попередніх кібератак на різноманітні об'єкти морської транспортної інфраструктури у світі та вивченням організаційних та цифрових заходів, що були впроваджені після цих атак.

Висновки. Отже, невизначеність у сфері безпеки та пов'язані з нею операційні потреби створюють ключовий бар'єр стратегічного розвитку морської транспортної інфраструктури України. Подолання цього бар'єру визначає гостру необхідність у зміні технологій управління від традиційного до динамічного, яке сприятиме стійкості у сфері морської транспортної інфраструктури, міжнародної координації та диверсифікації логістичних маршрутів. Аналіз проблем стратегічного управління розвитком морської транспортної інфраструктури України визначив основні групи проблем, серед яких ризики та руйнування інфраструктури, безпекова невизначеність та операційні потреби, подолання яких найчастіше знаходиться поза межами морської транспортної інфраструктури.



У ході дослідження встановлено, що безпекова невизначеність є визначальним чинником, який суттєво впливає на процеси стратегічного управління розвитком морської транспортної інфраструктури України в сучасних умовах. Повномасштабна військова агресія, обмеження навігаційної безпеки, зростання кіберзагроз та трансформація глобальних логістичних ланцюгів призвели до порушення стабільності функціонування портів, ускладнення операційного планування та зниження інвестиційної привабливості галузі.

Доведено, що традиційні підходи до стратегічного управління морською транспортною інфраструктурою є недостатньо ефективними в умовах високої динаміки безпекових загроз і потребують трансформації у напрямі гнучких, адаптивних і сценарно орієнтованих моделей управління. Застосування міжнародних стандартів управління кіберризиками, розвиток систем моніторингу, сегментація мереж та підвищення цифрових компетенцій персоналу визначено як ключові напрями підвищення стійкості портів систем. Запропонована система заходів щодо подолання безпекової невизначеності, що включає розробку адаптивних стратегій управління, розвиток альтернативних транспортних маршрутів, посилення міжвідомчої координації та міжнародного співробітництва, може бути використана як практичний інструмент для формування державної політики у сфері розвитку морської транспортної інфраструктури України. Реалізація цих заходів сприятиме відновленню довіри інвесторів, підвищенню конкурентоспроможності портів та інтеграції України до європейської та світової транспортної системи.

Подальші дослідження доцільно спрямувати на розробку кількісних моделей оцінювання рівня безпекової невизначеності, обґрунтування показників кіберстійкості портів та формування інструментів підтримки



прийняття стратегічних рішень у сфері управління морською транспортною інфраструктурою в умовах довготривалих кризових викликів.

Список використаних джерел

1. Notteboom, T., & Haralambides, H. Notteboom, T., & Haralambides, H. (2020). Port management and governance in a post-COVID-19 era: Quo vadis? *Maritime Economics & Logistics*, 22(3), 329–352. DOI: <https://doi.org/10.1057/s41278-020-00162-7>
2. Lam C. N. & Notteboom, T. Lam Canh Nguyen & Theo Notteboom, 2019. "The relations between dry port characteristics and regional port-hinterland settings: findings for a global sample of dry ports," *Maritime Policy & Management, Taylor & Francis Journals*, vol. 46(1), pages 24-42, January. DOI: <https://doi.org/10.1080/03088839.2018.1448478>
3. Notteboom T., Pallis A., Rodrigue J.-P. Port economics, management and policy. London : Routledge, 2022. 690 p. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9780429318184O>.
Diachenko, O. Gab та P. Marchuk
4. Clavijo Mesa, M. V., Patiño-Rodríguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity risks in maritime supply chains: A systematic literature review. *Information*, 15(11), 710. DOI: <https://doi.org/10.3390/info15110710>
5. Liu, G., Amri, O., Liang, Y., & Chen, Z. (2025). A multi-criteria cyber risk assessment framework for maritime and port systems. *Mathematics*, 13(22), 3650. DOI: <https://doi.org/10.3390/math13223650>
6. Heilig L., Lalla-Ruiz E., Voß S. Digital transformation in maritime ports: analysis and a game theoretic framework. *Netnomics* 18, 227–254 (2017). DOI: <https://doi.org/10.1007/s11066-017-9122-x>
7. Klar R., Fredriksson A., Angelakis V. Klar R., Fredriksson A., Angelakis V. Digital twins for ports: Derived from smart city and supply chain



twinning experience. IEEE Access: *Practical Innovations, Open Solutions. Sustainability*. 2021. 13 (5). 71777–71799. DOI: <https://doi.org/10.1109/access.2023.3295495>

8. Notteboom T., Pallis A., Rodrigue J.-P. Port economics, management and policy. London : Routledge, 2022. 690 p. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9780429318184>

9. European Commission. (2020). The European Green Deal. Brussels. https://www.esdn.eu/fileadmin/ESDN_Reports/ESDN_Report_2_2020.pdf

10. Blue Economy Framework <https://medblueeconomyplatform.org/blue-economy-framework>

11. Progress on TEN-T network - Mobility and Transport <https://transport.ec.europa.eu/news-events/news/progress-ten-t-network>

12. Економіка судноплавства і сервісної діяльності: глобальні тренди й трансформація : монографія / В. В. Жихарєва, Р. А. Бундюк, О. С. Власенко, М. С. Соколова ; Одес. нац. морський ун-т ; за заг. ред. В. В. Жихарєва. Одеса : ОНМУ, 2023. 352 с. DOI: <https://doi.org/10.47049/978-966-7716-91-2>

13. Потаповська М. Формування організаційного механізму управління портовим кластером. Адаптивне управління: теорія і практика. Серія Економіка. 2023. Вип. 17. №. 34. DOI: [https://doi.org/10.33296/2707-0654-17\(34\)-05](https://doi.org/10.33296/2707-0654-17(34)-05)

14. Veremchuk, V. S. (2022). International legal aspects of cybersecurity in maritime transport. *Visnyk of Odesa National University. Law Series*, 27(2). DOI: [https://doi.org/10.32782/2304-1587/2024-26-1\(38\)-2](https://doi.org/10.32782/2304-1587/2024-26-1(38)-2)

15. Zaitseva, T.V., Bezbakh, O.M., & Kaminska, N.H. (2023). Management of cyber incidents in the maritime industry. *Problems of Port and Marine Management*, 1, 33–41. DOI: <https://doi.org/10.32782/mathematical-modelling/2025-8-1-6>



16. О. Полікаровських, Ю. Даус, Д. Ларін та М. Ткаченко, «Систематизація кіберзагроз на морському транспорті», SISIOT, т. 1, № 1, с. 01008, 2023 р., DOI: <https://doi.org/10.31861/sisiot2023.1.01008>.
17. Русанова С., Перепічко М. Моделі управління морськими портами: світові практики. *Економіка та суспільство*. 2024. № 61. <https://doi.org/10.32782/2524-0072/2024-61-102>
18. International Maritime Organization (IMO): *вебсайт.URL*: <https://www.imo.org/>
19. European Union Agency for Network and Information Security, ENISA. *вебсайт.URL*: <https://www.enisa.europa.eu/>
20. Щербина І. С., Батракова Т. І. Адаптація експорту в умовах війни. «Молодий вчений», *Економічні науки*. № 3 (134), 2025 р. DOI: <https://doi.org/10.32839/2304-5809/2025-3-134-23>