

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА МОРСЬКА АКАДЕМІЯ»
Навчально-науковий інститут морського права та менеджменту

Кафедра морського права

Козирева Карина Віталіївна

УДК 347.79:656.615

**ІННОВАЦІЇ В УПРАВЛІННІ МОРСЬКИМИ ПОРТАМИ: ПРАВОВІ
ПИТАННЯ ВПРОВАДЖЕННЯ НОВИХ ТЕХНОЛОГІЙ**

Дипломна робота магістра

Науковий керівник,
PhD, доцент кафедри
морського права НУОМА
Сурілова Анастасія Олегівна

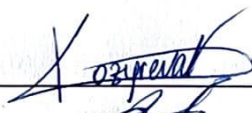
освітньо-професійна програма
«Морське право»
спеціальність 081 «Право»

Здобувач

Науковий керівник

Завідувач кафедри

Нормконтроль






м. Одеса – 2025 р.

АНОТАЦІЯ

Козирева К. В. Інновації в управлінні морськими портами: правові питання впровадження нових технологій. Кваліфікаційна дипломна робота магістра спеціальності 081 “Право”, освітньо-професійна програма “Морське право”. Національний університет “Одеська морська академія”, Одеса, 2025.

Питання впровадження нових технологій в портовій діяльності ґрунтується на комплексному дослідженні юридичних аспектів трансформації морських портів у високотехнологічні «Розумні порти» (Smart Ports), що відбувається в контексті глобального переходу до концепції «Порт 4.0». Важливим аспектом вивчення легалізації штучного інтелекту в роботу морських портів виступає наявність системного юридичного вакууму, який вимагає швидкого врегулювання питань власності на цифрові дані, визначення юридичної відповідальності за збої алгоритмів та забезпечення правової еквівалентності електронних товаророзпорядчих документів. Особливої актуальності тема набуває для держави Україна в умовах повоєнного відновлення та євроінтеграції, оскільки цифровізація є ключем до інтеграції в Транс'європейську транспортну мережу та зміцнення режиму критичної інфраструктури.

Дане дослідження сфокусовано на правовому регулюванні ключових інноваційних технологій, зокрема інтегрованих цифрових платформ Port Community Systems, електронних навігаційних систем та рішень на основі блокчейну. Аналіз національних та міжнародних стандартів, включаючи Міжнародну конвенцію з охорони людського життя на морі 1974 року, Конвенція про полегшення міжнародного морського судноплавства 1965 року та Типовий закон ЮНСІТРАЛ про електронні передавальні документи 2018 року є ключовими у питанні гармонізації українського законодавства. Також критичним є розгляд співвідношення приватного інтересу та публічного інтересу при впровадженні інновацій в портові інфраструктури.

У фокусі роботи — правові виклики та ризики цифрової трансформації. По-перше, є необхідність детального аналізу юридичних ризиків у сфері кібербезпеки та захисту персональних даних, що формують інтегральний характер відповідальності у разі порушень. По-друге, дослідження проблеми правового регулювання трудових відносин, спричинені автоматизацією є нагальним питанням вирішення, оскільки чинний Національний класифікатор професій не відповідає новим технологічним посадам. У зв'язку з зазначеним, можна дійти висновку що ризик, пов'язаний із помилками алгоритмів, повинен нести роботодавець, а не працівник.

У зв'язку з вище викладеним вважаємо, що формулювання низки науково обґрунтованих пропозицій щодо вдосконалення законодавства України визнано за потрібне, внаслідок того, що вони спрямовані на гармонізацію з європейськими стандартами, зокрема, Директивою NIS 2 від 14.12.2022 року, забезпечення правового статусу електронних документів та адаптацію трудового законодавства, зокрема, Кодексу законів про працю України 1971 року та Національного класифікатора України ДК 003:2010, для гарантування соціальної справедливості, цифрової стійкості та прозорості в процесі інноваційного відновлення портової інфраструктури.

Ключові слова: інновації, морські порти, технології, «Розумні порти», цифровізація, правовий режим, критична інфраструктура, інноваційні технології, портова інфраструктура, кібербезпека, інтеграція, правове регулювання, блокчейн, трудові відносини, управління, автоматизація, портова діяльність, цифрова трансформація, e-Navigation, Port Community System.

SUMMARY

Kozyreva A. V. Innovations at Seaport Management: Legal Issues on Introducing New Technologies. Master's thesis in the field of study 081 'Law', educational and professional programme "Maritime Law". National University 'Odessa Maritime Academy', Odesa, 2025.

The issue of introducing new technologies in port activities is based on a comprehensive study of the legal aspects of the transformation of seaports into high-tech "Smart Ports", which takes place in the context of the global transition to the "Port 4.0" concept. An important aspect of studying the legalization of artificial intelligence in the work of seaports is the presence of a systemic legal vacuum, which requires immediate resolution of issues of ownership of digital data, determination of legal liability for algorithm failures and ensuring the legal equivalence of electronic goods management documents. The topic is of particular relevance for the state of Ukraine in the context of post-war reconstruction and European integration, since digitalization is the key to integration into the Trans-European Transport Network and strengthening the critical infrastructure regime.

This study focuses on the legal regulation of key innovative technologies, in particular integrated digital platforms Port Community Systems, electronic navigation systems (e-Navigation) and blockchain-based solutions. Analysis of national and international standards, including the International Convention for the Safety of Life at Sea 1974, the Convention on Facilitation of International Maritime Navigation 1965 and the UNCITRAL Model Law on Electronic Transfer Documents 2018 are key in the issue of harmonization of Ukrainian legislation. Also critical is the consideration of the balance of private interest and public interest when implementing innovations in port infrastructure.

The focus of the work is on the legal challenges and risks of digital transformation. First, there is a need for a detailed analysis of legal risks in the field of cybersecurity and personal data protection, which form the integral nature of liability in case of violations. Secondly, the study of the problem of legal regulation

of labor relations caused by automation is an urgent issue to be resolved, since the current National Classifier of Occupations does not correspond to new technological positions. In connection with the above, it has been proven for the first time that the risk associated with algorithm errors should be borne by the employer (port operator), not the employee. In connection with the above, we believe that the formulation of a number of scientifically based proposals for improving the legislation of Ukraine is recognized as necessary, due to the fact that they are aimed at harmonization with European standards, in particular, the NIS 2 Directive of 14.12.2022, ensuring the legal status of electronic documents and adapting labor legislation, in particular, the Labor Code of Ukraine of 1971 and the National Classifier of Ukraine DK 003:2010, to guarantee social justice, digital sustainability and transparency in the process of innovative restoration of port infrastructure.

Keywords: innovation, seaports, technologies, «Smart Ports», digitalization, legal regime, critical infrastructure, innovative technologies, port infrastructure, cybersecurity, integration, legal regulation, blockchain, labor relations, management, automation, port activities, digital transformation, e-Navigation, Port Community System.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ.....	7
ВСТУП.....	9
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІННОВАЦІЙ В УПРАВЛІННІ МОРСЬКИМИ ПОРТАМИ.....	16
1.1. Поняття та види інноваційних технологій у сфері портового управління.....	16
1.2. Правова природа інновацій у транспортному праві: концептуальні підходи.....	30
1.3. Роль морських портів як об'єктів критичної інфраструктури в умовах війни.....	36
РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ВПРОВАДЖЕННЯ ІННОВАЦІЙ У МОРСЬКИХ ПОРТАХ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ ВИМІРИ.....	43
2.1. Аналіз українського законодавства щодо цифровізації портів.....	43
2.2. Міжнародно-правові акти у сфері цифровізації та безпеки портової діяльності.....	56
2.3. Співвідношення приватного і публічного інтересу при впровадженні технологій в портах.....	65
РОЗДІЛ 3. ПРАВОВІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ІННОВАЦІЙ В УПРАВЛІННІ МОРСЬКИМИ ПОРТАМИ УКРАЇНИ.....	80
3.1. Юридичні ризики цифрової трансформації портів: кібербезпека, відповідальність, захист даних.....	80
3.2. Проблеми правового регулювання трудових відносин в умовах автоматизації портової діяльності.....	87
3.3. Правові пропозиції щодо післявоєнного відновлення портової інфраструктури з використанням інновацій.....	91
ВИСНОВКИ.....	99
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	103

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AES - ADVANCED ENCRYPTION STANDART

AI - ARTIFICIAL INTELLIGENCE

AIS - AUTOMATIC IDENTIFICATION SYSTEM

ARPA - AUTOMATIC RADAR PLOTTING AIDS

CEF - CONNECTION EUROPE FACILITY

CERT-UA – COMPUTER EMERGENCY RESPOMCE TEAM OF
UKRAINE

COPPA - CHILDREN'S ONLINE PRIVACY PROTECTION ACT

DPIA - DATA PROTECTION IMPACT ASSESSMENT

DT - DIGITAL TWIN

EBL – ELECTRONIC BILL OF LADING

ECDIS - ELECTRONIC CHART DISPLAY AND INFORMATION
SYSTEM

EDIFACT - ELECTRONIC DATA INTERCHANGE FOR
ADMINISTRATION, COMMERCE AND TRANSPORT

E-NAVIGATION - ELECTRONIC NAVIGATION CONCEPT

ERP-SYSTEM - ENTERPRISE RESOURCE PLANNING SYSTEM

FAL - CONVENTION ON FACILITATION OF INTERNATIONAL
MARITIME TRAFFIC

GDPR - GENERAL DATA PROTECTION REGULARION

GMDSS - GLOBAL MARITIME DISTRESS AND SAFETY SYSTEM

GNSS - GLOBAL NAVIGATION SATELLITE SYSTEM

HPH TRUST - HUTCHISON PORT HOLDINGS TRUST

IAPH - INTERNATIONAL ASSOCIATION OF PORTS AND HARBORS

ICC - INTERNATIONAL CHAMBER OF COMMERCE

ICS2 - IMPORT CONTROL SYSTEM 2

ILO - INTERNATIONAL LABOUR ORGANIZATION

INS - INERTIAL NAVIGATION SYSTEM

IOT - INTERNET OF THINGS

ITS - INTELLIGENT TRANSPORTATION SYSTEMS

KIDS - KOREAN TRADE AND DISTRIBUTION SYSTEM

MLERT - UNCITRAL MODEL LAW ON ELECTRONIC TRANSFERABLE RECORDS

MSW - MARITIME SINGLE WINDOW

NIS 2 - NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2

PCS - PORT COMMUNITY SYSTEM

PPP - PUBLIC-PRIVATE PARTNERSHIP

SMS - SAFETY MANAGEMENT SYSTEM

SRP - STANDARDS AND RECOMMENDED PRACTICES

TEN-T - TRANS-EUROPEAN TRANSPORT NETWORK

TOS - TERMINAL OPERATING SYSTEM

UN\EDIFACT - UNITED NATIONS/ELECTRONIC DATA INTERCHANGE FOR ADMINISTRATION, COMMERCE AND TRANSPORT

VTMIS – VESSEL TRAFFIC MONITORING & INFORMATION SYSTEMS

VTS - VESSEL TRAFFIC SERVICES

WINWIN - СТРАТЕГІЯ ЦИФРОВОГО РОЗВИТКУ ІННОВАЦІЙ УКРАЇНИ ДО 2030 РОКУ

WCO – WORLD CUSTOMS ORGANIZATION

XML - EXTENSIBLE MARKUP LANGUAGE

АСУ КТ - АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ ТЕРМІНАЛАМИ

ДПП - ДЕРЖАВНО-ПРИВАТНЕ ПІДПРИЄМСТВО

ІСПС - ІНФОРМАЦІЙНА СИСТЕМА ПОРТОВОГО СПІВТОВАРИСТВА

НТС - НАЦІОНАЛЬНА ТРАНСПОРТНА СТРАТЕГІЯ УКРАЇНИ

ПЗ – ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

ВСТУП

Обґрунтування вибору теми та її актуальність. У XXI столітті морські порти переходять до моделі Port 4.0, що передбачає широке використання систем автоматизації, цифрових платформ обміну даними, модулів штучного інтелекту та інших інноваційних рішень. Такі технології впливають на організацію логістичних процесів і формують нові напрями правового регулювання, зокрема у сфері функціонування Port Community Systems, де залишаються не врегульовані питання правового статусу згенерованих даних, визначення режиму доступу до них, вимоги до нейтральності платформ, а також механізми встановлення відповідальності за технічні збої. Важливим елементом є перехід до електронних товаророзпорядчих документів відповідно до положень Типового закону ЮНСІТРАЛ про електронні передавальні документи 2017 року.

Використання автоматизованих технологій та алгоритмічних систем потребує нормативного уточнення, оскільки чинні міжнародні акти, включаючи Конвенцію про охорону людського життя на морі 1974 року, не регламентують специфіку автономних рішень у портах. Це обумовлює необхідність встановлення механізмів розподілу відповідальності за шкоду, спричинену алгоритмічними помилками.

Для України цифрова трансформація портів пов'язана з інтеграцією до Транс'європейської транспортної мережі (TEN-T) та розробленням правового механізму для інтеграції українських портів у європейський цифровий простір. Трансформація виробничих процесів також впливає на трудові відносини, зокрема на перегляд Національного класифікатора процесій 003:2010 та трудового законодавства України з урахуванням появи нових цифрових спеціальностей і потреби в перекваліфікації працівників. У міжнародній практиці оператор портової інфраструктури зазвичай несе відповідальність за технічний збій та ризики, пов'язані з алгоритмічними системами, однак така модель потребує нормативного закріплення в Україні.

Зв'язок теми з науковими програмами/планами: Тема магістерської роботи узгоджується з пріоритетним науковими напрямками розвитку транспортної та цифрової інфраструктури, визначеними у Стратегії розвитку морських портів України та Національної транспортної стратегії України до 2030 року. Вона безпосередньо корелює з програмами гармонізації українського законодавства з правом Європейського Союзу, зокрема у сфері TEN-T, кібербезпеки (NIS2) та цифровізації логістичних процесів. Магістерська робота також відповідає актуальним завданням наукових проектів, спрямованих на удосконалення правового регулювання критичної інфраструктури та впровадження міжнародних стандартів у сфері морського права. Отримані результати можуть бути використані у формуванні рекомендацій для портової галузі в межах державних програм відновлення та модернізації.

Мета та задачі роботи. Метою магістерської роботи є комплексне теоретико-правове обґрунтування особливостей правового регулювання впроваджень інноваційних цифрових технологій в управління морськими портами, а також формування науково-вмотивованих пропозицій щодо вдосконалення національного законодавства України з метою забезпечення належної правової визначеності, прозорості та безпеки портової діяльності.

Для досягнення поставленої мети визначено такі основні задачі роботи:

1. Уточнити та сформулювати юридичне поняття «інноваційні технології у сфері портового управління» та здійснити їх класифікацію з позиції правового регулювання.
2. Проаналізувати міжнародно-правові акти, що регулюють цифрові процеси в морських портах, зокрема Конвенцію SOLAS, Конвенцію FAL, Типовий закон ЮНСІТРАЛ MLERT та Директиву ЄС NIS2, і визначити їх вплив на національне законодавство України.
3. Дослідити правовий режим функціонування ключових інноваційних технологій, включаючи Port Community Systems, електронні навігаційні системи (e-Navigation) та технології розподілених реєстрів (блокчейн).

4. Визначити та проаналізувати юридичні виклики цифрової трансформації морських портів у сферах кібербезпеки, захисту персональних даних та операційних даних, а також відповідальність за алгоритмічні збої.

5. Дослідити особливості правового регулювання трудових відносин в умовах автоматизації портової діяльності та встановити необхідні напрями адаптації трудового законодавства України.

6. Сформулювати науково обґрунтовані пропозиції щодо вдосконалення чинного національного законодавства України з метою його гармонізації з міжнародними стандартами та забезпечення належного правового статусу електронних документів і цифрових платформ у морській логістиці.

Об'єкт і предмет дослідження. Об'єктом дослідження є суспільні відносини, що виникають у процесі впровадження та функціонування інноваційних технологій (цифрових та організаційних) в управлінні морськими портами України.

Предметом дослідження є міжнародно-правові та національні правові норми, які регулюють запровадження, застосування та правові наслідки використання інноваційних технологій (зокрема Port Community Systems, e-Navigation, блокчейн-рішень, Smart Ports, штучного інтелекту, цифрового двійника (Digital Twin), «Інтернет речей» (IoT) та технології 5G) у сфері управління морськими портами, а також вітчизняна та міжнародна практика їх застосування.

Методи дослідження. Для проведення дослідження автор керувався сукупністю загальнонаукових та спеціально-юридичних методів пізнання. Порівняльно-правовий метод використано для аналізу міжнародних актів (SOLAS, FAL Convention) та їх співвідношення з національним законодавством України. Формально-юридичний метод дав змогу дослідити правовий статус електронних документів (коносаментів) та визначенні юридичної відповідальності у сфері кібербезпеки. Аналіз та синтез застосовувано під час опрацювання наукової літератури та практичних прикладів впровадження технологій (TradeLens, Portbase, KIDS) у портах.

Логічні методи використовувались для уточнення понять та формулювання правових висновків.

Аналіз використаних джерел та літератури. У процесі підготовки роботи були використані міжнародні нормативно-правові акти: конвенції Міжнародної морської організації (IMO), зокрема Міжнародна конвенція про охорону людського життя на морі (SOLAS) 1974 року, Конвенція про полегшення міжнародного морського руху (FAL Convention) 1965 року, Типовий закон ЮНСІТРАЛ про електронні передавальні документи (MLETR) 2017 року. Дослідження ґрунтується на національному законодавстві України, включаючи Закон України «Про морські порти України» 2013 року, Закон України «Про електронні документи та електронний документообіг» 2003 року, Кодекс законів про працю України 1971 року (далі за текстом – КЗпП), а також підзаконні акти та нормативні документи, що стосуються кібербезпеки та захисту персональних даних.

Також проаналізовані наукові праці та публікації провідних вітчизняних та зарубіжних фахівців у галузі морського, транспортного, інформаційного та трудового права, а також економіки та управління морським транспортом. Зокрема, правові аспекти забезпечення кібербезпеки критичної інфраструктури досліджено у працях О. В. Ніколюк, яка акцентує увагу на необхідності вдосконалення національного законодавства з урахуванням сучасних кіберзагроз. Питання міжнародно-правового регулювання морської безпеки розкрито у роботі О. М. Котлубая, де обґрунтовано роль міжнародних стандартів у формуванні безпечного морського середовища. Економічні та управлінські аспекти розвитку портової інфраструктури висвітлено у дослідженнях С. В. Онешко та С. В. Ільченка, які розглядають державно-приватне партнерство як ефективний механізм розвитку портів, а також у працях В. В. Шемаєва та Л. М. Шемаєвої, присвячених імплементації моделі управління портами типу «лендлорд» в Україні. Проблеми цифровізації транспортної та морської галузі розкрито у працях М. Т. Примачова та Н. М. Примачової, Н. В. Сментини, Н. Г. Шпак, Л. А. Павловської та О. М.

Коробкової, які аналізують вплив цифрових технологій на ефективність управління портами, зокрема в умовах воєнного стану. У працях М. Acciari, T. Vanelslender, C. Sys, F. Parola, T. Notteboom, A. Pallis, J.-P. Rodrigue та інших авторів обґрунтовується роль інноваційних і цифрових рішень у формуванні сучасних моделей управління портами, розвитку «розумних портів» та оптимізації логістичних процесів. Дослідження Р. К. Bagchi, Н. А. Chun, В. С. Ha, L. Heilig, S. Schwarze, S. Voss, A. Molavi, G. J. Lim, Y. Yang, M. Zhong та їх співавторів зосереджені на впровадженні інформаційних платформ, IoT-технологій, аналізу AIS-даних і цифрових індексів оцінювання рівня розвитку портів, а також на макроекономічному ефекті цифровізації портової галузі, зокрема на прикладі провідних морських держав. Водночас значний масив зарубіжних досліджень присвячений проблемам кібербезпеки морської та портової інфраструктури в умовах зростання цифрових ризиків. У працях F. Akpan, G. Bendiab, S. Shiaeles, H. Boyes, R. Isbell, R. Harris, M. Neo, а також у звітах Allianz Global Corporate & Specialty і University of Cambridge акцентується увага на вразливості портових і суднових інформаційних систем, необхідності управління кіберризиками та впровадження галузевих стандартів кіберзахисту. Окремі дослідження, зокрема V. Carlan, C. Sys, T. Vanelslender, M. P. Nunes, G. B. B. Vieira, A. Q. da Rosa та B. Obrenovic, розглядають інновації й державно-приватне партнерство як інституційну основу цифрового розвитку портів, що дозволяє узагальнити міжнародний досвід для подальшого вдосконалення правового регулювання цифровізації та безпеки портової інфраструктури.

Наукова новизна одержаних результатів:

обґрунтовано доцільність закріплення на нормативному рівні положення про те, що ризики, пов'язані з помилками або збоями алгоритмів та автономних систем, мають покладатися на портового оператора як роботодавця, що потребує уточнення підходів до матеріальної відповідальності у трудовому праві;

удосконалено підхід до визначення поняття «інноваційні технології у сфері портового управління» як сукупності технічних, цифрових та організаційних рішень, спрямованих на оптимізацію управлінських процесів, підвищення прозорості діяльності та узгодження портових процедур з міжнародними стандартами морського права;

визначено особливості правового статусу інтегрованих цифрових платформ (Port Community Systems) як об'єкта самостійного правового регулювання у сфері транспортного права, з урахуванням їхньої ролі у забезпеченні взаємодії учасників логістичних процесів та інтеграції з європейським транспортним середовищем;

запропоновано оновлене бачення комплексного підходу до юридичної відповідальності у сфері цифрової трансформації портів, який охоплює дотримання вимог кібербезпеки, захисту персональних даних та правомірність цифрових операцій;

удосконалено пропозиції щодо врегулювання правових колізій у сфері трудових відносин, пов'язаних із невідповідністю Національного класифікатора професій сучасним технологічним посадам в умовах автоматизації портової діяльності.

Практичне значення одержаних результатів. Викладені у магістерському дослідженні положення, висновки та пропозиції можуть бути використані: а) у науково-дослідницькій сфері – як основа для подальшої теоретичної розробки правових питань про цифрову трансформацію, кібербезпеку, правовий статус електронних документів та адаптацію трудового законодавства у морській галузі; б) у правотворчості – як основа для розробки спеціального нормативно-правового акта, що регулює цифрові процеси у морських портах, та внесення змін до чинного законодавства (зокрема до Кодексу законів про працю України 1971 року та Національного класифікатора професій України 2010 року) з метою гармонізації з європейськими стандартами; в) у правозастосовній діяльності – як практичні рекомендації для портових адміністрацій, операторів та інших суб'єктів

портової діяльності щодо забезпечення правового режиму електронного документообігу, захисту даних та управління юридичними ризиками при впровадженні Port Community Systems, e-Navigation та блокчейн-рішень; г) у навчальному процесі – при викладанні дисциплін «Морське право», «Транспортне право», «Інформаційне право», підготовці підручників, навчальних посібників і методичних вказівок, а також у науково-дослідницькій роботі здобувачів.

Апробація результатів. Основні положення магістерського (дипломного) дослідження розглядались на засіданні кафедри морського права та оприлюднені на таких наукових конференціях: XI Всеукраїнська науково-практична онлайн конференція молодих науковців та здобувачів вищої освіти «Морське право та менеджмент: еволюція та сучасні виклики» та XV Всеукраїнська студентська наукова конференція «Сучасні проблеми морського транспорту та безпека мореплавства».

Обґрунтування структури роботи. Виходячи з мети та основних задач роботи, враховуючи необхідність послідовного дослідження, дипломна робота складається зі вступу, трьох розділів, які поділені на три підрозділи, висновків та списку використаних джерел.

Розділ 1 присвячено теоретико-правовим засадам інновацій в управлінні морськими портами, включаючи поняття, види технологій та їхню правову природу.

Розділ 2 розкриває правове регулювання впровадження ключових інноваційних технологій у морських портах з аналізом міжнародного та національного досвіду.

Розділ 3 зосереджується на правових викликах та перспективах, досліджуючи питання кібербезпеки, захисту даних, а також проблеми трудового права в умовах автоматизації портової діяльності України.

Така структура забезпечує логічну послідовність дослідження від теоретичних основ до практичних викликів і пропозицій.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ІННОВАЦІЙ В УПРАВЛІННІ МОРСЬКИМИ ПОРТАМИ

1.1. Поняття та види інноваційних технологій у сфері портового управління

У сучасному світі інтеграція морських портів у глобальні ланцюги постачання визначає не лише їхню інфраструктурну значимість, а й роль у міжнародному правовому просторі. Порти перетворюються з простих вузлів транзиту на високотехнологічні центри з інтенсифікацією електронного документообігу, застосуванням інтелектуальних систем спостереження, цифровою координацією логістичних ланцюгів та впровадження штучного інтелекту. В цих умовах поняття «інноваційні технології у сфері портового управління» набуває комплексного значення, що виходить далеко за межі просто технічних рішень — аби стати об'єктом системного юридичного аналізу.

У науковій літературі не існує єдиного підходу до визначення поняття «інноваційні технології» в контексті сфери портового управління та морського права загалом. З одного боку, під ними можуть розумітись будь-які нові технічні або програмні рішення, що спрямовані на оптимізацію логістичних процесів. З іншого боку, більш сучасні підходи включають до цього поняття й організаційно-управлінські інновації, які змінюють саму структуру взаємодії між суб'єктами портової діяльності. Таким чином, поєднання та ретельний аналіз наукових робіт дає можливість прийти до припущення, що інноваційні технології можна тлумачити як комплекс технічних, цифрових та управлінських рішень, що спрямовані на автоматизацію, цифровізацію та інтеграцію портових процесів, а також на підвищення прозорості господарських відносин і правової визначеності у сфері портового менеджменту.

Поняття «інноваційні технології» у портовому управлінні включає не лише нові апаратно-програмні рішення, але й організаційно-управлінські моделі, які змінюють взаємодію між суб'єктами ринку. Це відповідає розумінню інновації як «впровадження нового чи суттєво вдосконаленого продукту, процесу, маркетингового чи організаційного методу» [6, с. 244-250].

У контексті морського права і портової діяльності це означає, що інноваційні технології — це технічні, цифрові та організаційні рішення, що спрямовані на автоматизацію, інтеграцію, прозорість та безпеку портових процедур у відповідності з міжнародними стандартами і національним законодавством. Впровадження цифрових платформ, електронних навігаційних систем чи блокчейн-рішень та ШІ неможливе без належного правового врегулювання. Тут мова йдеться не лише про закріплення правового статусу таких систем, але й про визначення відповідальності за наслідки їхнього застосування, порядок обробки та збереження даних, взаємодію з міжнародними нормативно-правовими актами, а також про гармонізацію національного законодавства з нормами міжнародного морського права.

Оскільки єдиного визначеного критерію класифікації запровадження інновацій у портовій діяльності не має, на основі аналізу наукових робіт та офіційно оприлюднених джерел, можна зробити припущення, що систематизація інновацій у портовій діяльності для їх комплексного вивчення та подальшого впровадження здійснюється відповідно до загальноприйнятого науково-правового підходу, що передбачає класифікацію за кількома ключовими критеріями.

Для широкого розуміння впроваджень технологій в портову галузь, вважаємо за доцільним почати з огляду ключового елементу, а саме з сучасного порту – «Розумний Порт». Свою історію термін – «Розумний Порт» веде з ХХІ століття, початком використання якого згаданого на міжнародній арені, коли виникла необхідність у цифровізації операцій між великими контейнерними портами Європи та Азії. Визначення походження терміна «Розумний Порт» є складним і не однозначним. Його поява була пов'язана не

з конкретним першоджерелом, а скоріше з вербальними анонсами масштабних інфраструктурних проєктів, що описували значні ініціативи з цифровізації, автоматизації та роботизації у провідних глобальних хабах, таких як Гамбург, Роттердам та Сінгапур. Ці анонси, які спершу з'явилися у періодичних, а потім і у наукових виданнях, стали підґрунтям для поширення вживаності зазначеного терміну [7, с. 81-87].

Широкого застосування «Розумний Порт» отримав у 2010-х роках завдяки розвитку локальних цифрових рішень і автоматизованих систем, що підкреслює еволюційний характер його формування, а не виникнення у конкретному джерелі. Цей термін розвинувся як прямий наслідок загальносвітового тренду на технологічну модернізацію транспортної інфраструктури та процесів у портах. Незважаючи на широке використання та актуальність «Розумного Порту», на сьогодні відсутнє єдине, універсально прийняте та формально закріплене визначення терміна, оскільки кожен представник наукової і професійної спільноти пропонує власне тлумачення, що відображає багатогранність підходів до концепії «Smart Port».

У науковій літературі поняття «Smart Port» досліджується як високотехнологічний, автономний портовий комплекс, що має на меті об'єднання сучасних цифрових рішень та інфраструктуру. Так, Чо С.В. та Вон С.Х. у своїй науковій роботі зазначили, що «Розумний Порт» є таким, що має повну автоматизацію, високу продуктивність та розвинену систему портових операцій. У той же час, автори Кі Джун В., Лі М.К. та Янг Чо Дж. підкреслили орієнтацію таких портів на підвищення ефективності завдяки використанню технологій IoT, Big Data та екологічно чистих рішень. Такої самої позиції дотримуються Ян Ю., Чжун М., Яо Х., Ю Ф., Фу Х. та Постолаче О., які у своїх наукових роботах описують Smart Port як повністю автоматизований порт, робота якого забезпечується мережею датчиків та систем IoT, що дозволяє здійснювати управління процесами в режимі реального часу [54, pp. 205-236; 68, pp. 480-493; 87, pp. 34-43; 7, с. 81-87].

Розумні порти загалом охоплюють низку інформаційно-комунікаційних технологій, до яких входять, на сам перед: Port Community System, електронні навігаційні системи, технологія великих даних, штучний інтелект, «Інтернет речі», технологія «Цифровий двійник (близнюк)», технологія блокчейн, а також технологія 5G.

Port Community System (далі за текстом - PCS) — це інтегрована електронна платформа, що забезпечує ефективний та безпечний обмін інформацією між усіма учасниками портової спільноти, включаючи адміністрації портів, митні органи, портових операторів, судновласників, вантажовласників, експедиторів та інших зацікавлених осіб. Основною метою PCS є спрощення та автоматизація обміну даними, оптимізація процедур обробки вантажів, підвищення ефективності портових операцій та забезпечення прозорості взаємодії між учасниками, що сприяє підвищенню конкурентоспроможності портів на міжнародному ринку. З юридичної точки зору, PCS виступає як інструмент управління електронними документами та даними, передбачає встановлення правового режиму електронного документообігу, забезпечення захисту комерційної таємниці та персональних даних, визначення відповідальності за порушення обробки інформації та регламентує правила взаємодії між суб'єктами портової діяльності [8, с. 21-23].

Історія PCS бере свій початок з 1980–1990-х років у Європі як відповідь на потребу уніфікації документообігу та пришвидшення обробки вантажів. Первинно ці системи лише передавали митні та судові документи, але згодом еволюціонували до другого покоління, залучаючи більше учасників портового ланцюга та використовуючи стандартні формати EDIFACT та XML. Сучасні PCS поєднують в собі логічні цифрові платформи, блокчейн та аналітичні інструменти, що забезпечують автоматичне відстеження вантажів, аналітичними інструментами, що забезпечують автоматичне відстеження вантажів, документообіг та підтримку при мультимодальному ланцюгу постачання [9, с. 72-76].

Міжнародне правове регулювання впровадження PCS здійснюється через стандарти та рекомендації Міжнародної морської організації (ІМО), зокрема через e-Navigation та MSC.1/Circ.1634, а також через директиви Європейського Союзу, зокрема Directive 2010/65/EU, що забезпечує гармонізацію електронного документообігу та інтеграцію PCS у єдину цифрову транспортну систему. Рекомендації UN/CEFACT та WCO визначають стандарти для електронного обміну митними та логістичними документами. На національному рівні законодавство України забезпечує нормативну основу для впровадження PCS. Так, Закон України «Про морські порти України» від 2012 року встановлює загальні принципи діяльності портів і їх адміністрацій, включаючи координацію інформаційного обміну між учасниками. Митний кодекс України 2012 року та підзаконні акти регламентують електронне декларування вантажів, що є складовою частиною PCS, а законодавство про електронні довірчі послуги визначає правові рамки для документів, що передаються через PCS [7, с. 81-87].

Приклади ефективного використання PCS спостерігаються у різних регіонах світу. У Європі порти Роттердама та Антверпена використовують системи Portbase та KIDS, які інтегровані з митницею та портовими операторами, забезпечуючи відстеження вантажів, обробку документів і оптимізацію логістичних ланцюгів. В Азії порт Сінгапуру впровадив National Single Window, інтегрований із PCS, що дозволяє відстежувати вантажі і забезпечувати ефективну взаємодію між державними органами та портовими операторами. В Україні порти Одеси та Чорноморська запровадили експериментальні PCS-платформи, що інтегрують митницю, порти та логістичних операторів, хоча їхній функціонал поки обмежений і потребує законодавчого закріплення стандартів.

Підсистема Portbase, що обслуговує порти Нідерландів, працює на основі договірних відносин з своїми клієнтами. Її юридична відповідальність зазвичай обмежується наданням послуг з належною обачністю, забезпеченням стабільності та безпеки системи. Ключовим моментом тут є розмежування

власності та відповідальності за дані. Тобто, згідно з умовами «Клієнт залишається власником своїх даних та несе повну відповідальність за їхній зміст і законність обробки», тоді як Portbase використовує їх лише для надання послуг [24, с. 35-44].

Вище зазначена система оперує в чітко визначеному європейському правовому полі, що гарантує суворе дотримання General Data Protection Regulation (далі за текстом – GDPR) щодо обробки персональних даних. Окрім того, її діяльність нерозривно пов'язана з митним законодавством Європейського Союзу, оскільки система забезпечує цифрову взаємодію з митними органами, наприклад, для систем ICS2 чи AES. Дана підсистема також має визначену модель Data Governance, яка допомагає зберігти право власності на дані, які генеруються платформою. Такі процеси супроводжуються на самперед організаційними та технічними заходами, які у свою чергу спрямовані на дотримання конфіденційності та безпеки, що є основою функціонування портової спільноти.

Інша підсистема, Korean Trade and Distribution System (далі за текстом – KIDS), має на меті встановлення високого рівня відповідальності, яка покладається на портових операторів. Оскільки дана система є дитиноцентричною, у зв'язку з тим, що діти повною мірою не мають змоги усвідомлювати ризики, компанії-оператори, за умовою цієї підсистеми, несуть відповідальність за забезпечення найкращих інтересів дітей. Це включає необхідність отримання дійсної згоди від батьків (або опікунів) до встановленого законом віку та уникнення використання даних, яке може призвести до шкоди чи експлуатації.

Правове регулювання KIDS визначається передусім такими актами, як Регламентом (ЄС) 2016/679 Європейського Парламенту і Ради від 27.04.2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС» (далі за текстом – GDPR) та спеціальними законами (наприклад, COPPA у США). Регуляторні вимоги наголошують на принципі: дизайн, відповідний віку, який

змушує розробників сервісів закладати захист приватності та безпеку як налаштування за замовчуванням.

Загалом, юридичні аспекти впровадження PCS включають в себе правовий режим електронних документів, що визнається юридично значимим відповідно до міжнародних та національних стандартів, таких як UNCITRAL Model Law on Electronic Commerce 1996 року та Закон України «Про електронні документи та електронний документообіг» 2003 року. Важливим аспектом є захист персональних даних та комерційної інформації, адже учасники PCS обмінюються великою кількістю чутливої інформації, що регулюється GDPR. Додатково виникають питання відповідальності та страхування ризиків, пов'язані з помилками системи, неправильним декларуванням або затримками вантажів, а також юрисдикційні питання щодо визначення компетентного суду та застосовного права у міжнародних портах [40].

Отже, Port Community Systems є ключовим елементом цифровізації портового управління, що забезпечує оптимізацію обробки вантажів, прозорість і ефективність портових операцій, інтеграцію різних учасників ланцюга постачання та відповідність міжнародним і національним правовим стандартам. Водночас впровадження PCS створює нові юридичні виклики, зокрема у сфері захисту даних, визначення відповідальності та гармонізації нормативно-правових актів, що потребує постійного удосконалення законодавчої бази та розробки спеціальних регламентів для цифрових портових платформ.

Також, важливою інновацією є електронні навігаційні системи (далі за текстом - e-Navigation), які визначаються інтегрованим підходом до збору, обробки, обміну та подання навігаційної інформації як на борту судна, так і на березі, з метою підвищення безпеки, ефективності та екологічної безпеки мореплавства. Ці системи передбачають використання сучасних інформаційно-комунікаційних технологій для забезпечення надійної та своєчасної навігаційної підтримки, зокрема через інтеграцію даних з різних

джерел, таких як автоматичні ідентифікаційні системи (далі за текстом - AIS), радарні системи, електронні навігаційно-інформаційні системи (далі за текстом - ECDIS), інтегровані навігаційні системи, радіолокаційні станції, засоби автоматичної радіолокаційної прокладки, глобальні навігаційні супутникові системи, глобальна морська система зв'язку та інші.

ІМО визнала необхідність інтеграції існуючих та нових навігаційних засобів у єдину систему для покращення безпеки та ефективності мореплавства. У 2008 році було затверджено Стратегію впровадження e-Navigation, яка визначила основні напрямки розвитку та впровадження цієї концепції. З того часу відбулося кілька етапів оновлення стратегії, зокрема у 2018 році було ухвалено оновлену версію, що враховує новітні технології та потреби користувачів [58].

Основним міжнародним нормативно-правовим актом, що регулює питання e-Navigation, є Конвенція про охорону людського життя на морі (SOLAS) 1974 року (далі за текстом - SOLAS), зокрема її Розділ V, що стосується безпеки навігації. У 2018 році були ухвалені поправки до Розділу V, які зобов'язують судна оснащуватися електронними навігаційно-інформаційними системами (далі за текстом - ECDIS) та передбачають використання інших електронних засобів для забезпечення безпеки навігації[64].

На національному рівні впровадження e-Navigation в Україні регулюється низкою нормативно-правових актів, зокрема Законом України «Про морські порти України» 2012 року, який визначає загальні принципи діяльності морських портів, включаючи впровадження сучасних технологій для забезпечення безпеки та ефективності портових операцій, Митним кодексом України 2012 року, що регламентує електронне декларування вантажів, та Законом України «Про електронні документи та електронний документообіг» 2003 року, який встановлює правовий режим електронних документів, що використовуються в рамках e-Navigation.

Практичне застосування e-Navigation можна побачити в порту Сінгапуру, в якому інтегрована система забезпечує ефективну взаємодію між суднами, портовими операторами та береговими службами, що сприяє зменшенню часу обробки вантажів та підвищенню безпеки операцій. Також в порту Роттердама використання e-Navigation дозволило інтегрувати дані з різних джерел, таких як AIS, ECDIS та метеорологічні станції, що забезпечило покращену ситуаційну обізнаність та ефективне управління портовими операціями. У порту Осака впровадження e-Navigation дозволило автоматизувати процеси обробки судових повідомлень та зменшити адміністративне навантаження на персонал порту [58].

Впровадження e-Navigation також пов'язане з низкою юридичних аспектів. По-перше, правовий статус електронних документів, що використовуються у системі, визнається юридично значущим відповідно до міжнародних та національних стандартів, таких як UNCITRAL Model Law on Electronic Commerce 1996 року та Закон України «Про електронні документи та електронний документообіг» 2003 року. По-друге, забезпечується захист персональних даних учасників системи відповідно до міжнародних стандартів, таких як Загальний регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, що скасовує Директиву 95/46/ЄС, та національних законів про захист даних. По-третє, встановлюються чіткі правила визначення відповідальності за помилки системи, неправильне декларування або затримки вантажів. Нарешті, гармонізація національних нормативно-правових актів із міжнародними стандартами є необхідною для ефективного функціонування e-Navigation та інтеграції з міжнародними портовими системами [1].

Таким чином, електронні навігаційні системи є невід'ємним інструментом сучасного портового управління та морського транспорту, що дозволяє підвищити безпеку мореплавства, забезпечити ефективну

координацію між суднами та портовими організаціями, оптимізувати процеси обробки вантажів та інтегрувати різні інформаційні джерела.

Важливого значення при аналізі інновацій набуває блокчейн, який трансформує процеси обміну інформацією, управління контрактами та відстеження вантажів, дозволяючи зменшити адміністративні витрати та підвищити ефективність портових операцій. Дана інновація передбачає створення цифрових платформ, які об'єднують усіх учасників ланцюга постачання — судновласників, портових операторів, експедиторів, митні органи та інших суб'єктів господарювання, забезпечуючи їм доступ до достовірної та актуальної інформації у режимі реального часу.

Блокчейн бере свій початок з 2010-х років, коли з'явилися перші дослідження та пілотні проекти, спрямовані на підвищення прозорості ланцюгів постачання та автоматизацію документообігу. Значним кроком розвитку блокчейну стало створення платформи TradeLens у 2018 році компаніями IBM та Maersk, яка використовує блокчейн для відстеження руху вантажів та супровідних документів у реальному часі, інтегруючи інформацію від усіх учасників логістичного ланцюга, що сприяє швидшій обробці вантажів, зменшенню ризику шахрайства та підвищенню ефективності портових операцій [7, с. 81-87].

На міжнародному рівні правове регулювання блокчейн-технологій у морській логістиці здійснюється через Типовий закон ЮНСІТРАЛ про електронні передавальні документи (UNCITRAL Model Law on Electronic Transferable Records) 2017 року (далі за текстом - MLETR), який визначає юридичну силу електронних документів, зокрема електронних коносаментів, що є ключовими у морських перевезеннях. Це створює правове підґрунтя для інтеграції блокчейн-рішень у міжнародну торгівлю та морську логістику [3].

В Україні впровадження блокчейну у сфері морського права не має спеціальної нормативної регламентації. Проте у контексті глобальної цифровізації портових систем та ланцюгів постачання очікується, що в майбутньому будуть розроблені законодавчі ініціативи, що дозволять

законодавчо закріпити використання блокчейну, електронних коносаментів та інших цифрових платформ у морських портах.

Практичні приклади використання блокчейн-технологій у портовій логістиці демонструють їхню ефективність. Так, платформа TradeLens дозволяє всім учасникам процесу отримувати доступ до єдиного джерела достовірної інформації про рух вантажів і документи, що забезпечує прозорість і безпеку операцій. Використання Smart Bills of Lading на базі блокчейн-технологій автоматизує процес передачі прав власності на вантаж, зменшує паперовий документообіг та прискорює обробку вантажів [10, с. 62-74].

З юридичної точки зору, використання блокчейну потребує забезпечення захисту персональних даних і комерційної інформації, що обробляється на платформі, відповідно до міжнародних стандартів, таких як GDPR, та національних законів про захист даних, щоб забезпечити ефективне функціонування блокчейн-рішень у глобальних ланцюгах постачання.

Із наведеного вище можна зробити висновок, що блокчейн та цифрові платформи в морській галузі виступають як сучасні інструменти цифровізації портового управління, забезпечуючи прозорість, безпеку та ефективність морських перевезень, оптимізацію документообігу та сприяють інтеграції учасників логістичного ланцюга. Водночас їх впровадження створює нові юридичні виклики, зокрема у сфері правового статусу електронних документів, захисту даних та визначення відповідальності, що потребує постійного удосконалення законодавчої бази та адаптації національних нормативно-правових актів до міжнародних стандартів.

Для повного та всебічного огляду впровадження інновацій у портові системи здійснимо розгляд тих інновацій, які відіграють важливу роль у модернізації портового управління. До таких інновацій можна віднести наступні: Big Data, штучний інтелект, система «Інтернет речей», технологія 5G.

Big Data технологія, за своєю суттю, надає компаніям можливість ефективно працювати з великими обсягами даних, отриманих з нетрадиційних джерел у формі оперативних і чутливих до часу потоків інформації. Розумне застосування цих даних сприяє вдосконаленню прогнозування, зокрема таких систем, як технології передбачення та розрахунків очікуваного часу прибуття суден і транспортних засобів. Наприклад, датчики, встановлені на суднах, передають інформацію в режимі реального часу, а системи Big Data аналізують її, включаючи текстові, аудіо- та відеодані. Точність вхідної інформації забезпечує максимальну продуктивність та ефективність роботи сучасних портових комплексів [7, с. 81-87].

Штучний інтелект (далі за текстом - ШІ) — це комп'ютерні системи, здатні імітувати процеси людського розуму за допомогою машинного навчання, обробки природної мови, робототехніки та інших технологій. Основою розвитку ШІ є машинне навчання, яке виступає «рушійною силою» цієї галузі. Головна мета ШІ — створення рішень, що дозволяють вирішувати завдання, які зазвичай вимагають людського інтелекту. ШІ автоматизує рутинні процеси, значно підвищуючи загальну ефективність бізнесу, зокрема у портовій сфері.

ШІ використовується як інструмент підтримки прийняття рішень, надаючи управлінцям точні прогнози та рекомендації. Завдяки обробці великих даних, ця система може передбачати тренди в глобальних ланцюгах постачання, а також сприяти покращенню безпеки робочого середовища шляхом запобігання аваріям і зменшення кількості помилок працівників.

Портова екосистема, що базується на технологіях штучного інтелекту через системи типу PCS, суттєво покращує співпрацю між усіма учасниками ринку. Це дозволяє ефективніше координувати цифрові дорожні карти окремих суб'єктів, створюючи нові взаємовигідні можливості для підвищення продуктивності. Водночас застосування ШІ вимагає чіткого розуміння портами та терміналами власних потреб, оскільки уніфікованого підходу до інтеграції цієї технології не існує. Провідні порти світу, такі як Сінгапур,

Роттердам і Гамбург, активно використовують інструменти штучного інтелекту для створення прогнозованих моделей поведінки й підтримки управлінських рішень [7, с. 81-87].

Система «Інтернет речей» (далі за текстом - IoT) являє собою інтегровану платформу, що об'єднує різноманітні технології, зокрема датчики. Ці датчики розташовані на судах так, щоб забезпечити моніторинг у режимі реального часу, дозволяючи відстежувати рух і ефективно управляти ризиками. Вони здатні контролювати ключові робочі параметри, зокрема продуктивність двигуна, витрати пального, температуру та стан корпусу. Передача цієї інформації на берег дає змогу судноплавним компаніям віддалено спостерігати за станом флоту та здійснювати прогнозне технічне обслуговування, що суттєво скорочує фінансові витрати та час простоїв [8, с. 21-23].

Окрім цього, IoT детально ідентифікує вантажі, які транспортуються, що дозволяє портовим адміністраціям у реальному часі відстежувати як вантажі, так і судна, що сприяє покращенню роботи порту, підвищенню загальної ефективності та зменшенню заторів, а також за її допомогою контролюється рух активів на території порту, що підвищує рівень безпеки та знижує ризики крадіжок вантажів.

Цифровий двійник (далі за текстом — DT) являє собою технологію віртуального моделювання фізичних об'єктів, систем або процесів, що дозволяє імітувати поведінку та характеристики, і надає можливість операторам здійснювати моніторинг, тестування і глибинний аналіз фізичної системи, спрямований на оптимізацію її продуктивності. Транспортні компанії використовують ці дані за-для прогнозування потреб у технічному обслуговуванні, ефективного планування операцій, зниження витрат палива та скорочення викидів.

Наприклад, порт Тяньцзінь у Китаї у співпраці з Huawei створює цифровий двійник порту для модернізації традиційних терміналів. У цьому проєкті застосовуються технології автономного водіння 5G і L4, а також

роботи, керовані супутниковою системою Beidou. Проект представляє собою нову модель для глобальної трансформації портової інфраструктури [30, с. 81-87].

Технологія 5G є п'ятим поколінням бездротового зв'язку та гарантує покращену швидкість передачі даних. Ця технологія відіграє ключову роль у розвитку Smart Ports, сприяючи переходу до інтелектуальних систем управління. 5G дозволяє портам працювати з більшою кількістю даних при зниженому енергоспоживанні, забезпечувати передачу інформації в реальному часі і оперативно використовувати дані, отримані від систем IoT.

До впровадження 5G порти часто стикалися з проблемою втрати сигналу через велику кількість металевих поверхонь. Однак технологія формування променя, інтегрована в систему 5G, забезпечує цілеспрямоване бездротове передавання сигналу у заданому напрямку. Наприклад, оператори терміналів Santos Port і Brasil Terminal Portuário активно адаптують технологію 5G до своїх потреб. Наприкінці 2022 року ці компанії розпочали співпрацю з телекомунікаційними провайдерами TIM та Nokia для створення приватної мережі 5G в порту. Це партнерство стало основою першої приватної портової мережі 5G у Латинській Америці.

У 2023 році глобальний портовий оператор Hutchison Port Holdings Trust (далі за текстом - НРН Trust) також повідомив про інтеграцію технології 5G на контейнерних терміналах у Гонконзі. Крім того, порт Гамбург проводить тестування цієї системи, готуючись до перетворення в центр передового промислового мобільного зв'язку. В порту вже протестовано застосування 5G для підтримки роботи інженерів на місцевості, моніторингу, а також оптимізації планування розвитку та будівництва портової інфраструктури [68, pp. 480-493].

Проведений аналіз інноваційних технологій у сфері портового управління дозволяє зробити висновок про їхню ключову роль у модернізації морської галузі та підвищенні ефективності діяльності портових операторів. Водночас, виникає потреба у нормативному підґрунті використання таких технологій,

що дасть змогу розмежування відповідальності між суб'єктами використання новітніх технологій, та забезпечення рівності у впровадженні в морські порти.

1.2. Правова природа інновацій у транспортному праві: концептуальні підходи.

Інновації в морських перевезеннях та управлінні портами, є складною категорією, що поєднує технічні, організаційні та нормативно-правові аспекти, визначає правовий статус учасників перевізного процесу, формує систему відповідальності і юридичної сили документів, а також впливає на ефективність, прозорість та безпеку перевезень. У сучасних умовах глобалізації та цифровізації інтеграція інновацій у транспортну сферу є ключовим чинником розвитку національної та міжнародної логістики. З точки зору правової доктрини, інновації є комплексним механізмом, що охоплює організаційні зміни, впровадження новітніх технологій і формування правового режиму їх використання. В Україні, згідно з Законом України «Про інноваційну діяльність» 2002 року, інновації визначаються як новостворені або вдосконалені технології, продукція та організаційно-технічні рішення, що суттєво покращують процеси виробництва та управління. У контексті морських перевезень правова значущість інновацій виникає лише при наявності нормативно-правового забезпечення, що встановлює їх легітимність та визначає правові наслідки використання [29].

Міжнародна практика визначає інновації як інструмент уніфікації та стандартизації, що забезпечує правову визначеність у перевезеннях. Одним із основних міжнародних інструментів є MLETR 2017 року, який встановлює юридичну силу електронних транспортних документів, таких як коносаменти, чеки та векселі. Цей Типовий закон визначає електронний документ як такий, що може виконувати всі функції паперового аналога, зокрема підтверджувати права власності, забезпечувати цілісність і контроль над документом протягом його життєвого циклу [41].

Законодавча нейтральність технологій дозволяє використовувати різні цифрові механізми, включаючи блокчейн та розподілені реєстри, при цьому міжнародне визнання таких документів забезпечує їх застосування у глобальній торгівлі. Юридична значущість електронного документообігу полягає в тому, що він забезпечує рівень правової захищеності, аналогічний традиційним паперовим документам, зменшує ризики шахрайства та підвищує ефективність перевезень.

ІМО у 2019 році внесла зміни до Конвенції про полегшення міжнародного морського руху 1965 року (далі за текстом - FAL Convention), які впроваджують обов'язковий обмін електронними деклараціями та концепцію «Єдиного вікна», що дозволяє скоротити час обробки вантажів та забезпечити прозорість процедур. Ця концепція є прикладом впровадження інноваційного підходу до управління портовими процесами, оскільки інтегрує взаємодію митних органів, портових адміністрацій і перевізників у єдину цифрову платформу.

У Європейському Союзі інновації розглядаються як ключовий чинник розвитку внутрішнього ринку та цифрової інтеграції. White Paper on Transport 2011 року підкреслює необхідність створення інтелектуальних транспортних систем, цифрових платформ для управління перевезеннями, блокчейн-технологій та систем моніторингу вантажів. Судова практика ЄС, включно з рішенням C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain*, демонструє важливість визначення правового статусу цифрових платформ, їх відповідальності та контролю за безпекою перевезень [20, с. 67-75].

Серед ключових інновацій, які впроваджуються у транспортному праві та морських портах, варто виділити: Port Community Systems, електронні навігаційні системи, блокчейн-технології та цифрові платформи логістики. Кожна з цих технологій має власну історію, правову природу та приклади використання, що дозволяє розглянути їх окремо та в контексті національної і міжнародної правової системи.

Port Community Systems є комплексними електронними платформами, що інтегрують усіх учасників портової діяльності: вантажовласників, перевізників, митні органи, портові адміністрації та логістичні компанії. Правова база PCS ґрунтується на міжнародних стандартах електронного документообігу, таких як MLETR, а також на національних законах про морські порти та електронні послуги. PCS забезпечує автоматизовану взаємодію всіх учасників ланцюга постачання, скорочує час обробки вантажів, зменшує адміністративні ризики та забезпечує прозорість процедур. Прикладом української адаптації PCS є Інформаційна система портового співтовариства (далі за текстом - ІСПС) у Чорноморських портах, що демонструє успішну інтеграцію міжнародних стандартів і національного законодавства.

Електронні навігаційні системи включають автоматизовані системи суднового контролю, зокрема AIS, ECDIS, GPS-моніторинг та системи управління трафіком суден. Правова основа використання електронних навігаційних систем встановлюється міжнародним правом, зокрема Конвенцією SOLAS, а також національними законами про морське судноплавство та безпеку руху. Міжнародна та національна судова практика у справах про зіткнення суден на морі та порушення правил безпеки судноплавства свідчить, що недотримання правил електронного моніторингу може мати юридичні наслідки, включаючи відповідальність капітана та судновласника за порушення правил безпеки. В Україні використання таких систем регламентується наказами Міністерства інфраструктури та законодавством про морське судноплавство, що дозволяє інтегрувати сучасні технології у портову та судову діяльність.

Блокчейн-технології у транспорті та морських перевезеннях використовуються для забезпечення прозорості, безпеки та автоматизації ланцюгів постачання. Історично застосування блокчейну почалося у фінансовій сфері, але вже у 2017–2018 роках великі порти та логістичні оператори, такі як Maersk та IBM, почали використовувати його для обміну

електронними коносаментами та контролю за переміщенням вантажів. Правова природа блокчейн-технологій регулюється стандартами UNCITRAL та законодавством про електронні документи, оскільки блокчейн є засобом забезпечення цілісності та достовірності електронних записів. Арбітражна практика Лондонського морського арбітражу свідчить про визнання юридичної сили електронних коносаментів, у тому числі виданих за допомогою блокчейн-платформ, за умов дотримання міжнародних стандартів, сформульованих MLETR.

Цифрові платформи логістики інтегрують різні елементи транспортного процесу: бронювання суден, оформлення вантажів, взаємодію між учасниками ланцюга постачання та моніторинг доставки. Вони дозволяють автоматизувати управління ризиками, платежами та контролем вантажів. Правова база таких платформ формується через поєднання національного законодавства про електронні документи, морські порти та міжнародних стандартів, таких як EU Digital Transport and Services Infrastructure та MLETR. Практика морських арбітражів GAFTA та FOSFA, а також рішення судів Англії та Уельсу у спраху щодо електронного укладення договорів і цифрових транспортних документів *Golden Ocean Group Ltd v Salgaocar Mining Industries Pvt Ltd* 2012 року, свідчить про відсутність чіткого розмежування відповідальності між оператором платформи та сторонами договору може призвести до покладення договірної відповідальності за збої електронних систем, а також неналежного виконання покладених зобов'язань.

Попри очевидні переваги, існують виклики впровадження інновацій у транспортному праві. По-перше, правова невизначеність щодо електронних документів та цифрових платформ може призвести до колізій, суперечок та невизначеності правового режиму. По-друге, необхідність міжнародної гармонізації стандартів UNCITRAL, IMO та ЄС є ключовою для інтеграції національної системи у глобальний ланцюг поставок. По-третє, технічні та фінансові бар'єри, включно з інвестиціями у цифрову інфраструктуру та підвищенням кваліфікації персоналу, визначають темпи та масштаби

впровадження інновацій. Ці бар'єри стають особливо відчутними у країнах з недостатньо розвиненою цифровою інфраструктурою, включаючи Україну, де модернізація портових систем та інтеграція міжнародних стандартів потребує значних інвестицій, перегляду нормативно-правових актів та підготовки кваліфікованих кадрів. Водночас досвід провідних європейських та азійських портів демонструє, що ефективне впровадження інновацій можливе за умови комплексного підходу, що поєднує технологічне вдосконалення, нормативне забезпечення та навчання персоналу.

Окрему увагу слід приділити юридичним аспектам використання Port Community Systems. Такі системи не лише автоматизують документообіг і взаємодію учасників портового процесу, а й створюють правові передумови для електронного підпису, електронного обміну коносаментами та контролю дотримання митних процедур. Наприклад, в портах Роттердама та Антверпена PCS стали основою для регулювання електронного обміну інформацією між державними органами та приватними операторами, що значно скоротило час простою суден і ризики порушень митного законодавства. Українська система ІСПС інтегрує ці міжнародні стандарти, однак правове регулювання електронних підписів, цифрових коносаментів та блокчейн-записів поки що потребує уточнення у законодавстві. Важливим є питання відповідальності учасників цифрового обміну: хто несе відповідальність у разі помилки у системі, втрати вантажу чи некоректної інформації, оскільки традиційні норми Кодекс законів про працю України 1971 року та Цивільного кодексу України 2003 року не завжди прямо поширюються на цифрові платформи.

Електронні навігаційні системи та автоматизовані системи управління рухом суден також мають важливий правовий аспект. Міжнародна конвенція SOLAS 1974 року передбачає обов'язкове обладнання суден сучасними навігаційними системами, а порушення цих норм тягне цивільну, адміністративну та кримінальну відповідальність. У практиці суддів Англії та Уельсу у справах про зіткнення суден неодноразово підкреслювалось, що відсутність чи неналежне використання даних AIS або ECDISB є доказом

порушення обов'язку належної навігації та може впливати на розподіл відповідальності між судновласниками. В Україні законодавчо закріплені вимоги до навігаційних систем, проте впровадження електронного моніторингу руху вантажів та суден ще потребує розвитку нормативної бази, що включає стандарти електронного документообігу та механізми захисту даних.

Блокчейн-технології, інтегровані у морське право через електронні коносаменти, забезпечують незмінність записів, прозорість та можливість швидкої перевірки прав власності. Юридична складова блокчейну полягає у визнанні електронних записів юридично значущими документами. Наприклад, компанія Maersk у співпраці з IBM розробила платформу TradeLens, яка дозволяє учасникам перевізного процесу вести електронний документообіг, контролювати переміщення вантажів у реальному часі та підтверджувати юридичні права власності на товари. Арбітражні рішення Лондонського морського арбітражу демонструють, що електронні коносаменти, видані через блокчейн, можуть визнаватися юридично значущими, якщо вони відповідають стандартам UNCITRAL MLETR та національному законодавству.

Цифрові платформи логістики, такі як CargoX або Bolero, інтегрують функції бронювання суден, оформлення вантажів, обміну електронними документами та моніторингу поставок. З правової точки зору ключовими є питання: визначення юридичної сили електронного документообігу, відповідальності операторів платформ та захисту прав користувачів. Судова практика Європейського Союзу, зокрема рішення Суду ЄС у справі C-390/18 *Airbnb Ireland UC v ANTOP*, підтверджує, що оператори цифрових платформ зобов'язані забезпечувати безпечний обмін інформацією, прозорість умов користування та наявність ефективних механізмів відповідальності у разі порушень або технічних збоїв, що дозволяє знизити ризики спорів між учасниками транспортних і логістичних правовідносин.

Загалом, в Україні процес гармонізації ще триває, і правова база потребує уточнення щодо статусу електронних документів, цифрових коносаментів та механізмів відповідальності. Верховний Суд України у ряді рішень визнавав електронні документи, видані через цифрові платформи, такими, що підтверджують право власності на вантаж, якщо вони відповідають законодавству про електронні документи та електронний підпис. Водночас суди наголошують на необхідності забезпечення цілісності даних та відповідності міжнародним стандартам, що підкреслює важливість гармонізації українського законодавства з UNCITRAL, ІМО та нормами ЄС.

Таким чином, правова природа інновацій у транспортному праві є багатогранною і динамічною категорією, яка поєднує технічні, організаційні та нормативно-правові елементи. Інновації визначають правовий статус учасників перевізного процесу, юридичну силу електронних документів та систему відповідальності у цифрових транспортних системах. Для ефективної інтеграції інновацій необхідна гармонізація національного законодавства з міжнародними стандартами UNCITRAL та ІМО, чітке визначення правового статусу цифрових платформ і електронних документів, а також інвестиції у розвиток цифрової інфраструктури та підвищення кваліфікації кадрів. Лише за умов комплексного підходу можна забезпечити ефективний розвиток транспортного права та інтеграцію України у глобальну транспортну систему.

1.3 Роль морських портів як об'єктів критичної інфраструктури в умовах війни

Морські порти України відіграють стратегічну роль у забезпеченні економічної стабільності та національної безпеки країни. Найбільш значущими з них є порти Одеса, Чорноморськ, Миколаїв та Херсон, які забезпечують значну частину зовнішньої торгівлі та є критично важливими для логістики країни. Згідно із Законом України «Про критичну інфраструктуру» №1650-IX від 2021 року об'єктами критичної інфраструктури визнаються ті, що гарантують життєдіяльність населення,

функціонування держави та обороноздатність, до яких віднесені й морські порти, оскільки вони забезпечують транспортування стратегічних вантажів, економічну стабільність та обороноздатність. Статус портів як об'єктів критичної інфраструктури зумовлює потребу у комплексному підході до їхнього управління, охорони та модернізації, особливо в умовах воєнного конфлікту [15, с. 48-62].

Повномасштабне вторгнення Російської Федерації у лютому 2022 року спричинило значні руйнування українських портів. Згідно з даними Державної служби морського та річкового транспорту України, станом на липень 2024 року внаслідок бойових дій було пошкоджено понад двісті шістдесят об'єктів портової інфраструктури та сімнадцять цивільних суден, що значно обмежило пропускну спроможність портів. Найбільш постраждали порти, розташовані в зоні активних бойових дій або під тимчасовою окупацією, зокрема порти Херсона та Миколаєва. Одеський порт, який є найбільшим в Україні за обсягом перевалки вантажів, зазнав пошкоджень причалів, складів та обладнання через ракетні та дроніві атаки, що призвело до зниження ефективності обробки вантажів та ускладнило логістичні операції. Водночас порти, розташовані на контрольованих територіях, таких як Чорноморськ, зазнавали обмежених руйнувань, проте їхня діяльність також ускладнена ризиками ракетних атак та морських мін.

Історія та сучасний досвід портів демонструють, що навіть у складних умовах війни забезпечення їхньої діяльності є можливим за умови комплексного підходу, який поєднує технологічні інновації та правове регулювання. Наприклад, під час окупації Херсонського порту працівники та волонтери забезпечували збереження документації вантажів та оперативне відновлення роботи порту після звільнення території. Цей випадок ілюструє необхідність чіткого правового регулювання доступу до об'єктів критичної інфраструктури, а також роль людського фактору у підтриманні функціонування стратегічних об'єктів у кризових умовах.

В умовах активних бойових дій морські порти стикнулися з реальними загрозами для своєї інфраструктури. Одеський порт, який є найбільшим в Україні за обсягом перевалки вантажів, постраждав від ракетних та дронівих атак, що призвело до пошкодження причалів, складів і суден. Проте, завдяки використанню сучасних технологій, таких як автоматизовані системи управління вантажопотоками, оперативно вдається координувати судна, моніторити стан причалів та планувати ремонтні роботи. Аналогічна ситуація відбулася в порту Чорноморськ, де впровадження цифрових платформ дозволило не лише оптимізувати логістичні процеси, але й забезпечити безпеку вантажів у режимі воєнного стану.

Для забезпечення функціонування портів у таких умовах Україна запровадила комплекс заходів щодо їхнього захисту та відновлення. До них належать обмеження доступу до стратегічно важливих об'єктів, посилений контроль за переміщенням вантажів та осіб, а також постійний моніторинг стану інфраструктури за допомогою сучасних технологій. Значна увага приділяється відновленню пошкоджених причалів, складів, енергетичних та водопостачальних систем, а також модернізації портового обладнання, що дозволяє підвищити ефективність обробки вантажів і зменшити залежність від обмежених маршрутів постачання. Особливо важливим є впровадження диверсифікації логістичних маршрутів, що дозволяє забезпечити безперервність функціонування портів навіть за умов часткової блокади або обмеження доступу до окремих об'єктів.

Згідно з даними Державної служби морського та річкового транспорту України, понад 400 об'єктів портової інфраструктури було пошкоджено внаслідок ракетних та дронівих атак Російської Федерації. Це включає причали, склади, енергетичні та водопостачальні системи, що суттєво обмежило пропускну спроможність портів і створило додаткові ризики для перевалки вантажів. Наприклад, порти Одеси та Чорноморська зазнали значних пошкоджень, що призвело до затримок у вантажо перевалці та ускладнило логістичні операції [21, с. 10-15].

Одним із ключових інноваційних рішень стало застосування підводного картографування та дронів для моніторингу підхідних каналів і морського дна. Ці технології дозволяють виявляти затонулі судна та морські міни, мінімізуючи ризики для комерційних та гуманітарних суден. Прикладом є роботи українських інженерів у Чорному морі, де завдяки дронам вдалося забезпечити безпечний прохід суден через мінні поля та пошкоджені ділянки. Такий підхід демонструє, як технологічні інновації та правове регулювання безпеки портів взаємодіють для підтримання критичної інфраструктури у кризових умовах.

Варто також зазначити вплив війни на соціально-економічну складову функціонування портів. Блокування Херсонського порту призвело до затримки експорту зернових культур, що безпосередньо вплинуло на аграрний сектор та міжнародні торговельні відносини України. Одночасно порти Одеси та Чорноморська забезпечили часткову компенсацію цих втрат, що підтверджує стратегічне значення морських портів для національної економіки та продовольчої безпеки [37, с. 248-256].

Міжнародний досвід підтверджує ефективність технологічних рішень та правового регулювання у захисті портової інфраструктури під час конфліктів. Наприклад, порти Лівану після вибуху у 2020 році використовували мобільні склади, автономні крани та дрони для оцінки пошкоджень і швидкого відновлення логістики. Україна адаптувала ці практики до власних умов, інтегруючи їх у національну транспортну стратегію та модернізацію портів [44, с. 389-394].

Не менш важливим аспектом є застосування блокчейну для забезпечення прозорості та легальності вантажів під час обмеженого доступу до портів. Тестування таких систем в портах України показало, що цифрові платформи дозволяють уникнути шахрайства та забезпечити безперервність логістичних процесів навіть у разі часткової зупинки державних органів. Це підкреслює інтеграцію технологій у правове поле управління портовою інфраструктурою та підвищення її стійкості у кризових умовах.

Сучасні інноваційні технології відіграють критичну роль у забезпеченні стійкості портів. Автоматизовані системи управління портами (Port Community Systems) дозволяють інтегрувати всі логістичні та адміністративні процеси в єдину цифрову платформу, підвищуючи прозорість та ефективність обробки вантажів. Використання безпілотних літальних апаратів та дронів для моніторингу стану інфраструктури дозволяє оперативно виявляти пошкодження та планувати ремонтні роботи. Впровадження систем управління безперервністю бізнесу ISO 22301, дозволяє прогнозувати ризики та мінімізувати наслідки від зовнішніх загроз. Прикладом ефективного застосування таких технологій є порт Чорноморськ, де автоматизована система управління вантажопотоками скоротила час обробки вантажів і підвищила контроль за переміщенням товарів, а використання дронів дозволяє моніторити стан причалів та складських приміщень у режимі реального часу [37, с. 248-256].

Міжнародний досвід свідчить про ефективність впровадження технологій та нормативно-правових механізмів для захисту портової інфраструктури. Так, країни, які стикалися з воєнними конфліктами або терористичними загрозами, зокрема Сирія та Ірак, застосовують комплексні системи моніторингу та управління критичною інфраструктурою, що включають цифрові платформи, автоматизовані системи контролю доступу, а також державний нагляд за безпекою стратегічних об'єктів. Україна активно співпрацює з міжнародними партнерами, зокрема країнами НАТО, у питаннях посилення безпеки портів, обміну досвідом, надання технічної допомоги та впровадження сучасних технологій управління ризиками. Однією з таких ініціатив є Мережа критичної підводної інфраструктури НАТО, що сприяє координації дій щодо захисту підводних об'єктів та обміну інформацією між державами-членами.

Державне регулювання та міжнародні стандарти також відіграють ключову роль у захисті та розвитку морських портів. Крім національного законодавства, до уваги беруться міжнародні стандарти ISO та директиви ЄС,

зокрема Директива Ради 2008/114/ЄС від 8 грудня 2008 року «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту», що забезпечують інтегрований підхід до охорони стратегічних об'єктів. На рівні національної політики важливу роль відіграє Національна транспортна стратегія до 2030 року, яка передбачає модернізацію морських портів, розвиток річкових перевезень, диверсифікацію логістичних маршрутів та впровадження інноваційних технологій для підвищення стійкості портів у кризових умовах.

Міжнародний досвід свідчить про ефективність застосування інноваційних технологій та комплексного підходу до відновлення портової інфраструктури. Наприклад, після вибуху в порту Бейрута у 2020 році було використано дрони та фотограмметричні методи для створення детальних 3D-моделей пошкодженої території, що дозволило оперативно оцінити масштаби руйнувань та спланувати відновлювальні роботи. Україна адаптувала цей досвід, впровадивши подібні технології у процес відновлення своїх портів [33, с. 62-74].

Наразі немає усталеної судової практики щодо захисту критичної інфраструктури в умовах війни в Україні, однак вже є приклади розгляду спорів, пов'язаних із доступом до портових об'єктів, відшкодуванням збитків від бойових дій та забезпеченням охорони стратегічних вантажів. Так, Господарський суд Одеської області у ряді справ розглядав питання відшкодування збитків портовими операторами, зокрема щодо пошкодження складів та причалів внаслідок ракетних атак, що створює прецеденти для подальшого правового регулювання у сфері захисту портової інфраструктури [44, с. 389-394].

Соціально-економічний вплив пошкодження портів є значним. Порушення функціонування портів впливає на внутрішній ринок, експортно-імпорتنі операції та забезпечення продовольчої безпеки. Наприклад, блокування Херсонського порту призвело до затримки експорту зернових

культур, що безпосередньо вплинуло на аграрний сектор та зовнішньоекономічні зв'язки країни. Водночас функціонування портів Одеси та Чорноморська дозволило частково компенсувати ці втрати та забезпечити безперервність поставок критичних ресурсів.

Перспективи розвитку морських портів України у наступні роки пов'язані з комплексною модернізацією інфраструктури, впровадженням інноваційних технологій та міжнародною співпрацею. Стратегія передбачає розширення контейнерних терміналів, розвиток річкових перевезень, впровадження цифрових платформ управління вантажопотоками та посилення заходів безпеки. Це дозволить зменшити залежність від окремих маршрутів постачання, підвищити прозорість та ефективність портових операцій і забезпечити стійкість інфраструктури у разі нових загроз.

Таким чином, морські порти України є критично важливими об'єктами інфраструктури, які виконують стратегічну роль у забезпеченні економічної стабільності, обороноздатності та соціального добробуту країни. Їхнє функціонування в умовах війни вимагає комплексного підходу, що включає модернізацію інфраструктури, застосування інноваційних технологій, міжнародну співпрацю та ефективне державне регулювання. Забезпечення стійкості та безпеки портів є ключовим фактором для відновлення економіки та зміцнення національної безпеки України. Морські порти України є критично важливими об'єктами, функціонування яких забезпечує економічну стабільність, національну безпеку та безпеку логістичних ланцюгів. Забезпечення їхньої стійкості та ефективності потребує комплексного підходу, що поєднує модернізацію інфраструктури, впровадження інноваційних технологій, міжнародне співробітництво та відповідне правове регулювання.

У майбутньому морські порти України мають стати не лише центрами перевалки вантажів, але й хабами для розвитку інноваційних технологій та міжнародної співпраці, що сприятиме зміцненню національної безпеки та економічної стабільності.

РОЗДІЛ 2

ПРАВОВЕ РЕГУЛЮВАННЯ ВПРОВАДЖЕННЯ ІННОВАЦІЙ У МОРСЬКИХ ПОРТАХ: НАЦІОНАЛЬНИЙ ТА МІЖНАРОДНИЙ ВИМІРИ

2.1. Аналіз українського законодавства щодо цифровізації портів

Цифровізація морських портів в Україні є одним із ключових напрямів модернізації національної транспортної системи та підвищення її конкурентоспроможності у світовому економічному просторі. У сучасних умовах глобального розвитку логістичних ланцюгів, коли швидкість, безпека та прозорість операцій стають визначальними факторами економічної ефективності, цифрові інструменти у портовій сфері перетворюються на необхідний елемент забезпечення інтеграції України до міжнародних ринків. Додаткового значення процес цифровізації набув після 2022 року, коли функціонування морських портів було поставлено в умови воєнного ризику, обмеженої пропускну здатності та потреби забезпечення стійкості критичної інфраструктури. Таким чином, перехід до сучасних цифрових моделей управління портовою діяльністю розглядається не лише як економічний та логістичний чинник, але і як елемент збереження обороноздатності держави та забезпечення безперервності товаропотоків у кризових ситуаціях [41, с. 248-256].

Цифровізація морської галузі України є невід’ємною складовою державного курсу на цифрову трансформацію та модернізацію транспортної інфраструктури. Вона передбачає впровадження електронного документообігу, цифрових платформ для управління перевезеннями, автоматизацію логістичних процесів, моніторинг вантажів у реальному часі, а також застосування аналітики великих даних і штучного інтелекту для прогнозування попиту та оптимізації маршрутів. Такі технології дозволяють скоротити час обробки вантажів, підвищити ефективність і безпеку портових

операцій, а також забезпечити прозорість і контроль логістичних процесів на всіх етапах.

На законодавчому рівні розвиток цифровізації морської галузі підтримується рядом нормативних актів. Зокрема, Закон України «Про Національну програму інформатизації», грудень 2022 року, заклав основу для розвитку інформаційного суспільства та цифрової економіки шляхом ефективного використання державних ресурсів, створення інформаційних систем та забезпечення рівного доступу до цифрових послуг. Закон передбачає розвиток електронного урядування та координацію дій органів державної влади і місцевого самоврядування, що безпосередньо впливає на оптимізацію логістичних процесів і управління портовою інфраструктурою.

Особливе значення має Стратегія цифрового розвитку інновацій до 2030 року, відома під назвою WINWIN (далі за текстом - WINWIN), затверджена у січні 2025 року. Цей документ передбачає створення сприятливого середовища для бізнесу, стартапів і науковців, визначає пріоритетні напрями розвитку технологій та інновацій, серед яких DefenseTech, MedTech, EdTech, Agritech і штучний інтелект. Основна мета документа — сприяти впровадженню передових цифрових рішень у логістику, транспорт, навігацію та безпеку, забезпечуючи ефективність, прозорість і інтеграцію українських портів до міжнародних цифрових логістичних мереж [44, с. 389-394].

В рамках WINWIN реалізуються конкретні проєкти цифровізації морської галузі, які спрямовані на підвищення ефективності та конкурентоспроможності портів. Серед них — проєкт DocPort, що автоматизує процес заїзду вантажного транспорту до портів, зменшуючи час очікування та черги, і модуль «Морське вікно», який переводить оформлення приходу та відходу суден у електронну форму відповідно до стандартів Міжнародної морської організації. Крім того, планується запуск ERP-системи для Адміністрації морських портів України (далі за текстом - АМПУ), яка об'єднує всі учасники логістичного ланцюга — портових операторів,

митницю, перевізників — у єдину цифрову платформу, що забезпечує прозорість, швидкість та синхронізацію операцій [37, с. 248-256].

WINWIN не лише спрямована на підвищення ефективності поточних процесів, але й формує стратегічну основу для розвитку «розумних портів» (Smart Ports), які інтегруються у глобальні логістичні мережі, забезпечують кібербезпеку та контроль екологічних параметрів діяльності портів і суден. Реалізація стратегії передбачає також гармонізацію з європейськими цифровими транспортними платформами, включно з TEN-T, Port Community System і Maritime Single Window, що створює передумови для міжнародної сумісності українських портів та залучення інвестицій [37, с. 389-294].

Таким чином, українське законодавство і стратегічні документи, зокрема WINWIN, формують нормативно-правову та організаційну базу для цифровізації морської галузі. Вони спрямовані на підвищення ефективності, прозорості та безпеки портових операцій, розвиток інноваційних технологій і інтеграцію українських портів у європейські та глобальні транспортні мережі. Цифровізація морської інфраструктури стає ключовим фактором підвищення конкурентоспроможності України та забезпечення сталого розвитку логістичних і економічних систем держави.

Нормативно-правові засади цифрової трансформації морських портів в Україні формуються під впливом як внутрішніх стратегічних документів, так і міжнародно-правових зобов'язань. Основою правового регулювання є Національна транспортна стратегія України до 2030 року, яка визначає цифровізацію портової системи одним із ключових напрямів державної політики у сфері транспорту, Національна транспортна стратегія України до 2030 року, 2018. У ній підкреслюється, що ефективність функціонування портів та їх інтеграція у глобальні логістичні ланцюги є неможливими без впровадження автоматизованих систем управління вантажопотоками, електронного документообігу та інтелектуальних засобів моніторингу операцій. Стратегія передбачає створення єдиної цифрової інфраструктури транспортного сектору, яка мала би поєднати всі види транспорту, включно з

морським, у єдині інформаційні логістичні платформи. При цьому наголос робиться на необхідності розвитку таких напрямів, як автоматизоване управління рухом суден, інтеграція стандартів електронного документообігу до митних та прикордонних процедур, а також цифровий обмін даними між портовими адміністраціями, судновласниками та вантажовласниками [34].

Національна транспортна стратегія України на період до 2030 року закладає важливу основу для розвитку інноваційних та цифрових технологій у транспортній сфері, зокрема у морських портах. У документі підкреслюється, що сучасна транспортна система потребує інтеграції новітніх технологій для підвищення ефективності управління та забезпечення безперервного розвитку галузі. Цифровізація розглядається як ключовий фактор модернізації, що сприяє спрощенню логістичних процесів, підвищенню прозорості та гармонізації з європейськими стандартами, зокрема з вимогами мереж TENT та міжнародних правил морського перевезення. Стратегія встановлює чіткий вектор розвитку, який передбачає реформування процедур у портах, оптимізацію тарифної політики та створення сучасної цифрової інфраструктури, що дозволяє забезпечити більш ефективне управління портовими ресурсами та інтеграцію з міжнародними транспортними системами.

Водночас аналіз українського законодавства свідчить, що чинні нормативні акти забезпечують лише часткову основу для цифровізації портової діяльності. Основним документом залишається Закон України «Про морські порти України», який регулює загальні питання функціонування портів, однак не містить спеціальних положень щодо впровадження цифрових технологій, електронного документообігу та автоматизації процесів. Стратегія розвитку морських портів України на період до 2038 року визначає модель реформування управління портами та оптимізації процедур, однак правове регулювання цифровізації залишається фрагментарним. У цьому контексті окремі нормативні ініціативи, такі як розробка електронних систем обміну інформацією та проєкт DocPort, свідчать про практичний початок

цифровізації, проте законодавча база поки що не забезпечує комплексного підходу.

Серед головних викликів, що визначають сучасний стан правового регулювання, можна виділити відсутність спеціального закону, який би регламентував цифрові процеси у портах, недостатню гармонізацію національного законодавства з європейським та міжнародним, а також відсутність єдиних стандартів для електронних систем. Крім того, умови воєнного стану та часткового пошкодження портової інфраструктури роблять питання цифровізації особливо актуальним, оскільки електронні системи та автоматизовані платформи можуть стати критично важливими для швидкого відновлення роботи портів та ефективного управління логістикою.

У міжнародному контексті цифровізація морських портів України безпосередньо пов'язана з імплементацією європейських стандартів та інтеграцією з міжнародними системами обміну інформацією, такими як SafeSeaNet. Це вимагає не лише технічної модернізації, а й адаптації національних норм до стандартів ЄС та міжнародних конвенцій, що регулюють безпеку морських перевезень, електронний документообіг та інформаційний обмін. Таким чином, цифровізація морських портів є одночасно стратегічним завданням на національному рівні та важливим елементом євроінтеграційного курсу України.

Підсумовуючи, можна стверджувати, що національна транспортна стратегія створює загальні рамки для цифровізації портової діяльності, забезпечуючи стратегічний напрям розвитку інновацій та підвищення ефективності. Однак чинне законодавство потребує суттєвого доопрацювання для формування комплексної нормативної бази, яка регламентувала б впровадження цифрових технологій, електронного документообігу та взаємодію з міжнародними системами. Тільки у поєднанні стратегічної підтримки, законодавчого регулювання та практичних ініціатив цифровізація морських портів зможе стати реальним інструментом модернізації та інтеграції України у європейський транспортний простір [34].

Стратегія розвитку морських портів України на період до 2038 р. від 23.12.2020 № 1634-р - Документ регулює та встановлює основні стратегічні напрями і пріоритети України для розвитку морських портів до 2038 р. Зазначено перелік морських портів та наведено їх основну характеристику. У стратегії визначено основні цілі, завдання, напрями для реформування портової галузі України, вказано існуючі проблеми у портовій галузі та наведено кроки і шляхи щодо забезпечення реалізації даної стратегії і підвищення рівня конкурентоспроможності морських портів.

Затвердження цієї Стратегії свідчить про прагнення держави створити сучасну та ефективну систему управління морськими портами, здатну забезпечити зростання вантажообігу, залучення приватних інвестицій і розвиток нових робочих місць. Одним із ключових аспектів документу є впровадження моделі управління «портлендлорд», за якою державна адміністрація порту надає інвесторам майно та земельні ділянки для будівництва та експлуатації терміналів. Така модель передбачає більшу роль приватного капіталу в управлінні портовими активами, що, у свою чергу, потребує створення належної законодавчої бази та вдосконалення процедур концесії, оренди та тарифного регулювання.

Особливу увагу в Стратегії приділено цифровізації та впровадженню сучасних інформаційних технологій. Серед зазначених ініціатив виділяються розвиток електронних сервісів, створення інформаційної системи «Морське вікно» та формування смартінфраструктури портів. Ці заходи мають на меті спростити документообіг, підвищити прозорість і ефективність управління, а також інтегрувати українські порти в міжнародні інформаційні системи, зокрема SafeSeaNet, що відповідає європейським стандартам. Водночас, хоч стратегія і визначає напрямок цифровізації, правове регулювання цієї сфери поки що є неповним. Чинне законодавство не містить спеціальних норм, які б комплексно регламентували цифрові процеси в портах, електронний документообіг та взаємодію з контролюючими органами, що створює певні прогалини для практичної реалізації стратегічних намірів держави.

Оновлена Стратегія також звертає увагу на модернізацію інфраструктури та екологічну безпеку портів, включно з розвитком альтернативних джерел енергії. Ці напрями вимагають від законодавства створення додаткових механізмів регулювання, які б забезпечили поєднання технологічного розвитку, екологічних стандартів і правових норм управління портами. Особливо актуальним це стає в умовах сучасних викликів, пов'язаних з воєнним станом та пошкодженням інфраструктури, коли цифрові системи та автоматизовані платформи здатні забезпечити швидке відновлення діяльності портів та ефективний контроль логістики.

Таким чином, оновлена Стратегія розвитку морських портів України формує чіткий стратегічний контекст для цифровізації та впровадження інновацій, встановлюючи пріоритети модернізації, інвестицій та управлінських моделей. Водночас існує потреба у вдосконаленні законодавчого забезпечення цих процесів. Створення спеціальних нормативних актів, які регламентували б електронний документообіг, інформаційну взаємодію, цифрові сервіси та управлінські моделі «портлендлорд», є важливою умовою для реалізації стратегічних завдань. Поєднання державної політики, правової бази та практичних ініціатив у сфері цифровізації дозволить підвищити ефективність морських портів України, забезпечити їх інтеграцію в європейський транспортний простір та створити передумови для сталого розвитку транспортної галузі в цілому [3].

Також, як інструмент реалізації стратегічних положень було розроблено Дорожню карту цифрової трансформації морської галузі, ухвалену Міністерством інфраструктури України у співпраці з ДП «Адміністрація морських портів України» та представниками портового бізнесу. Дорожня карта деталізує механізми модернізації портів на основі цифрових технологій та визначає конкретні технічні рішення, які мають бути впроваджені для оптимізації робочих процесів. Зокрема, документ передбачає поступове впровадження системи Port Community System, яка має забезпечити електронний обмін інформацією між усіма учасниками портових операцій —

від адміністрацій портів і митних органів до перевізників та експедиторів. PCS розглядається як основа створення цифрового порту, у якому інформаційні потоки стають наскрізними, а всі операції — прозорими, стандартизованими та контрольованими в режимі реального часу. Дорожня карта також передбачає впровадження механізму «єдиного вікна» для процедур, пов'язаних зі заходом судна до порту, оформленням вантажів, перевантажувальними процесами та відправленням вантажів у подальший обіг. Це дозволяє суттєво зменшити час оформлення документів, мінімізувати ризики корупційних зловживань та усунути дублювання адміністративних процедур [7, С. 62-74]

Окреме значення у процесі цифровізації портів має Закон України «Про національну інфраструктуру геопросторових даних» №554-IX, ухвалений у 2020 році. Даний закон створює правову базу для розвитку систем електронного просторового картографування об'єктів транспортної інфраструктури, включаючи морські порти, причали, термінали, підхідні канали та акваторії. Його впровадження дозволяє формувати єдині стандарти геопросторових даних, необхідних для управління рухом суден, гідрографічної розвідки дна, моніторингу стану гідротехнічних споруд та прогнозування аварійних ситуацій. Особливо важливим цей закон став у контексті воєнних дій, оскільки точне та оперативне оновлення інформації про навігаційні ризики, мінні загрози та структурні пошкодження портової інфраструктури є критично необхідним для забезпечення безпеки морських перевезень. Використання цифрових геопросторових карт дозволяє уникати навігаційних інцидентів, оптимізувати маршрути суден та планувати реконструкцію пошкоджених портових об'єктів [4].

Цифровізація портів в Україні також має чітко окреслену інституційну структуру. Формування політики у сфері цифрової трансформації транспортної галузі здійснює Міністерство розвитку громад, територій та інфраструктури України, тоді як технічна реалізація цифрових проєктів у портах віднесена до компетенції ДП «Адміністрація морських портів

України». Контроль за дотриманням норм у сфері безпеки судноплавства та експлуатації морської інфраструктури здійснює Морська адміністрація України. Своєю чергою, Державна митна служба відіграє ключову роль у впровадженні механізму «єдиного вікна» та переході до електронного документообігу у сфері переміщення товарів. Усі ці інституції мають функціонувати у єдиному цифровому середовищі, яке має забезпечувати узгодженість дій, оперативність реакції та доступність даних у режимі реального часу [43, С. 19-30].

Важливо, що цифровізація портової інфраструктури все більше пов'язується з поняттям національної безпеки. Морські порти є об'єктами критичної інфраструктури, значення яких зростає в умовах воєнного стану. Цифрові системи контролю руху суден, управління вантажами, комунікації між службами порту та державними органами можуть стати об'єктом кібератак або спеціальних інформаційно-диверсійних операцій. Саме тому цифровізація передбачає створення надійних систем кіберзахисту, резервного зберігання даних, автономних каналів зв'язку та комплексів технологічної стійкості, здатних забезпечити продовження операцій навіть у разі загрози фізичного пошкодження обладнання або втручання у цифрову інфраструктуру [42, С. 389-394].

Таким чином, нормативно-правова база цифровізації українських морських портів формується на комплексних засадах, які поєднують стратегічне бачення модернізації галузі, технічні рішення щодо автоматизації операцій та безпекові вимоги до стійкості критичної інфраструктури. Національна транспортна стратегія України до 2030 року визначає стратегічні орієнтири, Дорожня карта цифрової трансформації морської галузі — інструменти і механізми реалізації, а Закон України «Про національну інфраструктуру геопросторових даних» формує технічну основу просторового управління портовою системою. У сукупності ці нормативні документи створюють передумови для поступового формування в Україні сучасної моделі «смарт-порту», яка відповідає міжнародним стандартам, забезпечує

прозорість операцій, стійкість логістичних ланцюгів та інтеграцію до європейського транспортного простору.

Попри наявність стратегічних документів, зокрема Стратегії WINWIN та Дорожньої карти цифрової трансформації, правове регулювання впровадження інноваційних технологій у сфері морської логістики України залишається неповним. Існуючі нормативно-правові акти не забезпечують комплексного правового механізму для впровадження цифрових систем, що ускладнює реалізацію завдань цифровізації на галузевому рівні. У зв'язку з цим доцільним є проведення системного аналізу чинного законодавства, зокрема в аспектах, які стосуються цифрових активів, електронного документообігу та кібербезпеки у сфері морських портів.

Аналіз положень Закону України «Про морські порти України» дозволяє встановити, що його регуляторна конструкція орієнтована переважно на фізичну інфраструктуру портів. У тексті Закону відсутнє нормативне визначення та правовий режим цифрових систем, таких як Port Community System та автоматизовані системи управління терміналами (далі за текстом - АСУ КТ). Це, зокрема, ускладнює визначення статусу зазначених цифрових систем як об'єктів права власності або як стратегічних активів, що підлягають концесії чи охороні. Відповідно, у статтях 15 та 18 цього Закону, які регулюють питання майнових прав та стратегічної інфраструктури, не передбачено програмного забезпечення або баз даних у складі портового майна, що створює нормативну невизначеність при реалізації інвестиційних проєктів у сфері цифрових технологій [30].

Також варто звернути увагу на статтю 21 вказаного Закону, яка визначає підходи до тарифного регулювання у портах. Ця норма не містить чіткого розмежування між адміністративними та комерційними послугами у контексті цифрових сервісів, зокрема таких, як доступ до електронних документів або використання цифрових платформ. Така невизначеність може спричинити різночитання при практичному застосуванні. У контексті аналізу правового регулювання цифровізації портової інфраструктури України важливим є

звернення до відповідної судової практики, яка демонструє наявні прогалини у законодавстві та їх вплив на учасників логістичного процесу. Показовою в цьому аспекті є справа № 916/3658/23, розглянута Господарським судом Одеської області у 2023 році [22].

Предметом спору у зазначеній справі став договір між ТОВ «Зерновий термінал Кілія», який діє як позивач, та ДП «Морський торговельний порт Усть-Дунайськ», який є відповідачем, відповідно до якого відповідач надавав послуги з оформлення перепусток для доступу на територію порту. Позивач оскаржував чинність цього договору, стверджуючи, що відповідач не мав повноважень на надання таких послуг та отримання плати, а також що особа, яка підписувала договір від імені відповідача, не була належним чином уповноваженою. Крім того, позивач наголошував, що зазначені послуги не передбачені Законом України «Про морські порти України» як обов'язкові або як такі, що можуть бути предметом плати. На підставі цього позивач вимагав визнання договору недійсним та повернення раніше сплачених коштів у розмірі 390 592,36 грн.

Розглянувши матеріали справи, Господарський суд Одеської області встановив, що підписання договору було здійснене уповноваженою особою, а відповідач мав юридичні та фактичні підстави для надання спірної послуги. Суд дійшов висновку, що позивач добровільно скористався відповідними послугами та здійснив оплату, отже підстав для визнання правочину недійсним немає. Таким чином, у задоволенні позову було відмовлено.

З правової точки зору справа № 916/3658/23 є релевантною для розділу, присвяченого аналізу національного законодавства щодо цифровізації портів. Вона ілюструє низку системних проблем, пов'язаних із правовим регулюванням інноваційних послуг у морській логістиці. Зокрема, справа виявляє невизначеність правового статусу нових сервісів, які не прямо передбачені законом, але фактично здійснюються в межах портової інфраструктури. Це стосується і цифрових сервісів — наприклад, оформлення

перепусток через електронні системи, управління даними доступу та автоматизованих процедур [22].

Справу можна розглядати як приклад, що демонструє наслідки відсутності нормативного визначення та правового режиму цифрових послуг у межах морських портів. Зокрема, Законом України «Про морські порти України» не передбачено спеціальної класифікації або порядку затвердження цифрових сервісів, у результаті чого кожна нова ініціатива може бути оскаржена як така, що не має правової основи. Це створює суттєві юридичні ризики для інвесторів, операторів та інших суб'єктів, які зацікавлені у впровадженні інноваційних підходів, зокрема у форматі Port Community System або автоматизованих систем управління терміналами.

Таким чином, справа № 916/3658/23 підтверджує доцільність удосконалення законодавчої бази, спрямованої на цифровізацію портів. Зокрема, необхідним є запровадження чіткої класифікації цифрових послуг, визначення їх правового статусу, порядку надання, оплати та оскарження, а також інституалізація механізмів управління цифровими активами через моделі державно-приватного партнерства. Такий підхід дозволить мінімізувати правові колізії, подібні до розглянутої справи, і забезпечити правову визначеність для суб'єктів портової діяльності в умовах цифрової трансформації [22].

Закон України «Про електронні документи та електронний документообіг» визначає загальні засади обігу електронних документів в Україні. Водночас, він не містить спеціальних положень щодо електронних товаророзпорядчих документів, зокрема електронного коносаменту (далі за текстом - eBL). Цей вид документа виконує функцію посвідчення права власності на вантаж і передбачає можливість передачі цього права іншим суб'єктам, що вимагає окремого правового механізму. Відсутність такого регулювання унеможливорює повноцінне впровадження paperless trade у морських перевезеннях і обмежує використання цифрових платформ, які передбачають автоматизовану взаємодію з документами подібного типу.

У контексті розвитку цифрових технологій у морській галузі актуальним є також питання правового регулювання автономних рішень, прийнятих на основі алгоритмів, штучного інтелекту та smart contracts. У чинному законодавстві України спеціальні норми, які б визначали правовий статус таких технологій, відповідальність за їх використання або допустимість застосування в автоматизованих управлінських процесах у портах, наразі відсутні.

Питання кібербезпеки регулюється Законом України «Про основні засади забезпечення кібербезпеки». Відповідно до статті 8, морські порти віднесено до об'єктів критичної інфраструктури. Водночас на рівні підзаконних актів не встановлено спеціалізованих вимог щодо управління кіберризиками у сфері морських перевезень. Зокрема, не реалізовано вимоги Резолюції ІМО MSC.428(98), яка передбачає інтеграцію управління кіберризиками до Системи управління безпекою портових об'єктів. Відсутність такої гармонізації може призводити до невідповідності міжнародним стандартам і створювати додаткові юридичні ризики для операторів та органів управління портами [32].

Аналіз підзаконного нормативного регулювання також вказує на наявність колізій. Зокрема, накази Міністерства інфраструктури та обов'язкові постанови АМПУ і ДП «МТП» не завжди забезпечують узгодженість у регулюванні платних цифрових послуг, оскільки формально не врегульовані на рівні базового закону. Крім того, чинна судова практика щодо відшкодування шкоди, завданої портовій інфраструктурі в умовах воєнного стану, демонструє відсутність правових інструментів для врахування втрат, пов'язаних із цифровими системами, такими як PCS та АСУ КТ. Суди переважно оперують поняттями фізичних активів, що унеможлиблює належну правову оцінку втрати функціональності ІТ-інфраструктури.

З огляду на міжнародний досвід, можливими для запозичення є кілька моделей правового оформлення PCS. Перша — модель державно-приватного партнерства, що реалізована у порту Роттердам. У цій моделі PCS функціонує

як неприбуткова юридична особа, створена за участі державної адміністрації порту та приватних операторів. Такий формат забезпечує баланс інтересів сторін, дозволяє врегулювати права на дані через договірні механізми та знижує ризик монополізації.

Інша модель, представлена портом Сінгапур, передбачає централізоване державне управління PCS через єдиного оператора. Цей підхід забезпечує високу швидкість впровадження рішень, однак з точки зору правового регулювання передбачає домінування адміністративного елементу, що може обмежувати конкуренцію.

Третя модель, реалізована у Гамбурзі, базується на приватному управлінні PCS. Правові відносини у цій системі регулюються виключно комерційними договорами. Такий підхід забезпечує гнучкість, однак може створювати правові ризики щодо власності на дані та відповідності антимонопольному законодавству.

Ураховуючи правову структуру та стан нормативного середовища в Україні, найбільш доцільною для реалізації видається модель державно-приватного партнерства з чітким нормативним закріпленням правового статусу PCS як окремого об'єкта права. Це передбачає потребу у внесенні змін до чинного законодавства, зокрема до Закону України «Про морські порти України», а також розробку спеціалізованих підзаконних актів, що регулюватимуть цифрові активи, обіг електронних товаророзпорядчих документів і застосування інтелектуальних цифрових систем у портовій діяльності [30].

2.2. Міжнародно-правові акти у сфері цифровізації та безпеки портової діяльності

Протягом останніх десятиліть порти світу перебувають у стані безперервної цифрової трансформації, що обумовлено необхідністю оптимізації традиційних процесів та інтеграції новітніх технологічних рішень. Ця трансформація спрямована на забезпечення більш широких можливостей

для морської галузі, підвищення продуктивності та ефективності транспортних операцій. Сучасні досягнення у сфері інформаційних технологій, зокрема використання хмарних обчислень, аналізу великих даних та IoT, відкривають нові горизонти для портової інфраструктури, дозволяючи підключати широкий спектр автономних пристроїв, датчиків та лічильників до цифрових мереж зв'язку.

Разом із тим, впровадження цифрових технологій у діяльність портів ставить перед ними низку проблем, пов'язаних з інформаційною та кібернетичною безпекою. Успішна реалізація потенціалу нових технологій можлива лише за умови системного управління цими ризиками. Водночас варто зазначити, що цифровізація завжди супроводжується певними витратами та ризиками: централізовані системи портів можуть стати мішенню для кіберзлочинців, які здатні отримати доступ до конфіденційної інформації та завдати значної шкоди функціонуванню інфраструктури.

Існує чітка тенденція зростання кіберінцидентів у портовій сфері. Так, у 2011 році бельгійський порт Антверпен зазнав багатоступеневої кібератаки, організованої наркоторговцями для отримання контролю над системами управління контейнерами з метою перехоплення контрабанди наркотиків. Аналогічно, у 2017 році компанія Maersk постраждала від атаки вірус-зидирника NotPetya, що призвело до зараження понад 50 тисяч кінцевих точок, тисяч серверів і додатків на 600 сайтах у 130 країнах. На щорічній конференції Асоціації операторів балкерних терміналів 2019 року було наголошено на особливій вразливості портів у точках взаємодії судна та берега, що підкреслює нагальність підвищення рівня кіберзахисту [47].

Сьогодні порти все частіше розглядаються як об'єкти критичної інфраструктури та ключові цілі для злочинних або терористичних угруповань. Незважаючи на це, значна частина портових операторів демонструє недостатню готовність до протидії кіберзагрозам. Серед основних проблем, що перешкоджають забезпеченню ефективної кібербезпеки, можна виділити відсутність цифрової культури, низький рівень обізнаності та підготовки

персоналу, відсутність кваліфікованих ІТ-спеціалістів, дефіцит ресурсів для протидії загрозам, а також недостатнє розуміння необхідного часу та бюджету для заходів кіберзахисту. Крім того, порти стикаються з проблемами ланцюга постачання та високою взаємозалежністю систем, що створює додаткові вразливості.

Кібербезпека стала пріоритетним напрямком у системі безпеки портів поряд із забезпеченням комерційної конкурентоспроможності. Характер діяльності портів, що включає одночасне виконання великої кількості процесів із залученням наземного та морського персоналу, робить їх особливо вразливими до кібератак. Незважаючи на використання сучасних захисних систем та технологій, порти залишаються об'єктами потенційного злочинного втручання, оскільки велика кількість даних, що передаються і зберігаються в інфраструктурі, є привабливою для кіберзлочинців.

Серед основних загроз для портів слід виділити крадіжку критично важливої інформації, перехоплення зв'язку між портом та зацікавленими сторонами, незаконне сканування систем з метою корпоративного чи державного шпигунства, викрадення сеансів доступу, мережеву розвідку, фішингові атаки, контрабанду та можливість повного відключення систем порту. Ці ризики підтверджують, що цифровізація не усуває загрози злочинності, а лише змінює її характер, переводячи фокус на цифрові процеси та дані.

Для ефективного управління кіберризиками порти мають застосовувати комплексний підхід, що включає визначення стратегічних цілей і керівних принципів кібербезпеки, ідентифікацію внутрішніх та зовнішніх загроз, залучення всіх зацікавлених сторін до безпечного процесу взаємодії, підвищення обізнаності персоналу, регулярне оновлення аналізу ризиків, забезпечення швидкого реагування на інциденти та контроль доступу третіх осіб. Необхідним є також запровадження обов'язкових навчальних курсів з кібербезпеки та впровадження ризик-орієнтованих стратегій управління.

Висновком є те, що глобальна цифрова трансформація та зростання залежності від ефективних систем комунікації зробили кібербезпеку ключовим пріоритетом для портів. Підвищення рівня обізнаності про кіберзагрози, розвиток культури кібербезпеки та інтеграція кіберзахисту в глобальну стратегію безпеки портів є необхідними заходами для збереження стабільності, конкурентоспроможності та безпечного функціонування морської галузі у сучасних умовах.

Цифровізація та кібербезпека стають дедалі визначальними у функціонуванні морських портів і логістичних ланцюгів міжнародного судноплавства, що створило необхідність створення й розвитку міжнародноправових конструкцій, які б забезпечували правову рамку, стандартизацію та координацію дій держав, портових адміністрацій і операторів. У цьому контексті Міжнародна морська організація - спеціалізована установа ООН, що відповідальна за безпеку та захист судноплавства, а також запобігання забрудненню моря з суден, як провідна міжурядова організація у сфері морського транспорту, посіла центральне місце: від класичних конвенцій до нових резолюцій та стратегій вона формує основу для регулювання цифрових процесів, у тому числі на стику порту–судно–логістика. Паралельно з цим, промислові об'єднання, такі як Міжнародна асоціація портів і гаваней (далі за текстом - IAPH), відіграють роль каталізаторів впровадження цифрових підходів, ініціюючи типові рішення, рекомендації і кооперацію між зацікавленими сторонами. Далі розглянемо ключові міжнародноправові акти і ініціативи, які мають прямий стосунок до цифровізації та безпеки портової діяльності, а також проаналізуємо, які з них мають практичне значення для портової сфери України [63].

Одним із базових міжнародних документів, що стосуються обміну інформацією у судноплавстві та портовій діяльності, є Конвенція про полегшення міжнародного морського судноплавства «Convention on Facilitation of International Maritime Traffic». Ця конвенція набрала чинності у

1967 році і спрямована на спрощення формальностей, документальних вимог та процедур, що стосуються прибуття, перебування й відбуття судна в порту. В Додатку до цієї Конвенції містяться Стандарти та рекомендовані практики для державучасниць щодо процедур з деклараціями, маніфестами, вантажами, пасажирями, екіпажем тощо [13].

У сучасному цифровому середовищі важливим стало те, що Конвенція FAL була суттєво оновлена саме з метою впровадження електронного обміну даними та «Єдиного вікна» (далі за текстом - MSW) для обміну інформацією між судном, портом та державними органами. Із 1 січня 2024 року застосування MSW стало обов'язковим за амандментами до Конвенції, ухваленими у 2022 році. Таким чином, державиучасниці повинні забезпечити, щоб інформація, що подається про прибуття, перебування та відбуття судна, а також дані про екіпаж, вантажі, маніфести, подавалась через єдину цифрову точку взаємодії з компетентними органами.

Ця зміна має значення й для портової діяльності: порти, як складова логістичного та судноплавного ланцюга, опиняються в центрі процесу цифрового обміну даними, організаційної інтеграції та взаємодії з державними органами. ІМО у пояснювальних матеріалах зазначає, що MSW дозволяє електронно уніфікувати і пришвидшити процедури прибуття/відбуття, зменшити паперову навантажку, підвищити прозорість та знизити ризики корупції [66].

З 10 по 14 березня 2025 року представники Адміністрації морського судноплавства брали участь у 49-й сесії Комітету сприяння Міжнародної морської організації. Під час сесії розглядалися пропозиції щодо внесення змін до Конвенції FAL, зокрема стосовно визнання моряків ключовими працівниками та налагодження обміну даними про пасажирів круїзних суден і інших морських транспортних засобів.

Учасники також обговорювали питання морської кібербезпеки, впровадження електронних судноплавних документів, ефективну

експлуатацію національних систем «Єдиного вікна» та заходи щодо припинення контрабанди на суднах, що здійснюють міжнародні перевезення.

Українські делегації взяли активну участь у формуванні комплексної стратегії морської цифровізації та висловили підтримку розширеному залученню держави прапора для запобігання ризикам небезпечної морської міграції та мінімізації її гуманітарних наслідків. Крім того, Комітет був поінформований про атаку балістичною ракетою на портову інфраструктуру Одеси, що відбулася 11 березня 2025 року, яка є явним порушенням Російською Федерацією положень Конвенції FAL. Делегації Австралії, Канади, Японії, Норвегії, Польщі та Сполученого Королівства Великої Британії і Північної Ірландії висловили підтримку Україні, водночас усі російські контраргументи були відхилені державами-членами ІМО [45].

У сфері кібербезпеки судноплавства та портів ІМО також визначило ключові документи. Наприклад, резолюція MSC.428(98) «Maritime Cyber Risk Management in Safety Management Systems», ухвалена у червні 2021 року, встановлює, що ризики кібернетичних атак мають враховуватись у SMS судноплавного підприємства не пізніше першої верифікації після 1 січня 2021 року. Разом із цим, існують «Guidelines on Maritime Cyber Risk Management» - документ, що розробляється й удосконалюється з метою надання рекомендацій з управління кіберризиками на морі, також очікується схвалення ФАЛКомітетом [70].

Таким чином, міжнародноправові акти ІМО охоплюють як функціональний аспект так і аспект безпеки морської та портової діяльності. Для портів це означає, що юридична база все більше орієнтована не лише на традиційні процедури обробки вантажів, але й на цифрові взаємодії, стандарти даних, сумісність систем, кіберзахист, а також інтеграцію в глобальні цифрові мережі.

Паралельно з міждержавними документами розвиваються і промислові ініціативи, які створюють додатковий, але не менш важливий, шар регулювання та стандартизації. Зокрема, ІАРН активно просуває цифровізацію

портів. Наприклад, IAPH разом із партнерами реалізує проєкт з розробки «common understanding on critical components of digital port infrastructure», що передбачає гармонізацію даних, стандартизацію термінології, синхронізацію інформаційних потоків між лініями контейнерних перевезень, портовими системами та логістичною мережею. У 2025 році IAPH представила також нові керівні принципи кібербезпеки для портів, які адресують виклики, пов'язані з IoT, 5G, дроном, штучним інтелектом, квантовими технологіями — «cybersecurity by design». Ці ініціативи IAPH не мають статусу міжурядового договору, але виконують важливу роль «м'якої регуляції» та підсилюють міжнародноправовий контекст, сприяючи практичній імплементації стандартів у портах [63].

З точки зору портової діяльності важливим є те, що міжнародноправові акти та промислові ініціативи мають взаємодоповнювальний характер. Наприклад, згідно з Конвенцією FAL та її останніми амандментами, державиучасниці зобов'язані забезпечити створення MSW, що автоматизує взаємодію між судном, портом і держорганами. Це створює технічну й організаційну основу для порту і його інформаційних систем. Натомість IAPH та подібні структури пропонують стандарти, кращі практики та допоміжні документи, які допомагають портам виконати ці зобов'язання, подолати технічні бар'єри та впровадити цифрові рішення. Водночас ІМО продовжує працювати над стратегічним документом — Strategy on Maritime Digitalization — який має задати загальну логіку, архітектуру і ключові етапи цифровізації морського сектору, включно з портами, до кінця 2027 року [63].

У контексті безпеки портів, кіберризики стають важливою категорією. Порти як критична інфраструктура і як вузлові елементи глобальних логістичних ланцюгів піддаються ризикам як фізичних, так і цифрових атак — від переривання інформаційних потоків до шкідливого впливу на системи управління перевантаженням або контролю руху суден. Юридично це означає, що порти і портові оператори повинні враховувати не лише традиційні норми безпеки, але й стандарти кібербезпеки, відповідно до резолюцій ІМО, а також

враховувати промислові рекомендації ІАРН. У міжнародноправовому сенсі це створює вимоги: інтеграція кіберризиків у системи безпеки, застосування електронних сертифікатів, забезпечення цілісності, конфіденційності, достовірності даних, розмежування прав доступу, захист інформаційних систем порту та взаємодія з державними органами відповідно до стандартів.

Для України, з огляду на її портову інфраструктуру, яка переживає виклики через війну, обмеження й відновлення, міжнародноправові акти мають особливе значення. Законодавство та правове регулювання мають враховувати зобов'язання під конвенціями ІМО (наприклад, імплементацію MSW), а також враховувати стандарти кібербезпеки та цифрові платформи, що виходять із ініціатив ІАРН. З огляду на це доцільно відзначити кілька аспектів: поперше, національне законодавство має забезпечити інтеграцію вимог FAL у внутрішні норми щодо портів, логістики, митниці, безпеки; подруге, має бути створена нормативна база для кібербезпеки портів відповідно до міжнародних стандартів, зокрема тих, що розроблені ІМО та ІАРН; потретє, порти повинні бути готові до практичної імплементації стандартів, що існують у промислових ініціативах — тобто створення цифрової платформи, системи управління даними, інтегрованої логістичної інформаційної системи, спільної з державними органами.

Проведений аналіз міжнародно-правових актів дає змогу виявити низку критичних розбіжностей між міжнародними стандартами у сфері цифрової морської логістики та чинним національним законодавством України. Порівняльна оцінка норм дозволяє виокремити декілька ключових напрямів, де спостерігається нормативна невідповідність або відсутність гармонізації з вимогами міжнародного права.

Існує невідповідність між загальним характером регулювання у Законі України «Про основні засади забезпечення кібербезпеки» та вимогами Резолюції ІМО MSC.428(98), яка встановлює обов'язковість інтеграції управління кіберризиками в систему управління безпекою морських портів. Українські нормативні акти не передбачають спеціальних механізмів оцінки,

моніторингу та реагування на кіберінциденти у сфері портової інфраструктури, а також не встановлюють цивільно-правову відповідальність портового оператора за збитки, спричинені порушеннями функціонування цифрових систем, зокрема автоматизованих систем управління терміналами

Ілюстративним у цьому контексті є випадок кібератаки на порт Антверпен 2013 року, в результаті якої зловмисники отримали доступ до термінальної системи з метою забезпечення незаконного переміщення вантажів. Цей випадок продемонстрував, що кіберінцидент може мати не лише інформаційні, але й матеріальні наслідки, що потребує нормативної класифікації таких порушень як комплексних загроз безпеці. Відсутність відповідного національного регулювання ускладнює правову кваліфікацію подібних ситуацій в українських умовах.

Чинне законодавство України, зокрема Закон «Про електронні документи та електронний документообіг», не містить спеціальних положень щодо електронних коносаментів. Ця прогалина унеможливорює ефективне регулювання електронного товаророзпорядчого документообігу. На практиці це призводить до ситуацій, коли спори, що виникають під час використання електронних коносаментів у межах платформ TradeLens або аналогічних систем, наприклад, KIDS, розглядаються не національними судами, а у міжнародному арбітражі, зокрема під егідою LMAA.

Відсутність національного правового режиму для eBL призводить до того, що українські учасники змушені діяти на основі іноземного права, що обмежує їх процесуальні гарантії та доступ до ефективного правового захисту. Крім того, така ситуація не узгоджується із загальними рекомендаціями ІМО, ІСС та ІЛО, які підтримують правове визнання цифрових документів у морських перевезеннях.

У контексті розвитку цифрової портової інфраструктури актуальним є питання регулювання відносин, пов'язаних із обробкою, обміном та зберіганням даних в межах функціонування PCS. Ініціативи IAPH, спрямовані на розробку стандартів управління даними, передбачають необхідність чіткого

визначення правового режиму власності на дані, обов'язків щодо збереження конфіденційності, а також процедур відповідальності за порушення під час обміну інформацією.

Водночас чинне українське законодавство, включаючи Закон України «Про морські порти України», не містить норм, які б визначали статус даних як об'єкта права або врегульовували обов'язки учасників PCS у сфері обміну цифровою інформацією. Відсутність правового регулювання у цій сфері може ускладнити реалізацію проектів цифровізації портів, створити ризики у сфері антимонопольного контролю, а також вплинути на правову визначеність у питаннях контролю та доступу до критичної цифрової інфраструктури.

Отже, можна зробити висновок, що Україна має забезпечити своєчасну імплементацію положень FAL у законодавство і практику, розробити національні керівні принципи кібербезпеки для портової галузі на основі резолюції MSC.428(98) «Про управління кіберризиками в морській галузі в рамках системи управління безпекою» 2017 року та відповідних документів, а також співпрацювати із ІАРН типовими ініціативами та враховувати їхні рекомендації як частину національної політики цифровізації портів, за-для розвинення внутрішньої системи цифрової взаємодії, стандартних даних, інтегрованих інформаційних платформ та забезпечити узгодженість із міжнародними стандартами.

2.3. Співвідношення приватного і публічного інтересу при впровадженні технологій у портах

Співвідношення приватного та публічного інтересів у процесі цифровізації портової інфраструктури становить ключовий правовий виклик, який потребує належного нормативного врегулювання. З одного боку, приватний інтерес охоплює питання комерціалізації цифрових сервісів, захисту інвестицій, управління інтелектуальною власністю та даними. З іншого боку, публічний інтерес охоплює забезпечення національної безпеки, дотримання вимог кібербезпеки, захист критичної інфраструктури та

здійснення державного контролю. Вирішення цього балансу вимагає впровадження чітко визначених моделей правового управління системами типу PCS, з урахуванням як міжнародного досвіду, так і специфіки національного правового порядку.

Порівняльно-правовий аналіз моделей управління PCS, реалізованих у провідних європейських та азійських портах, свідчить про існування трьох основних концепцій. Перша модель, що функціонує у порту Роттердам - Portbase, ґрунтується на принципах державно-приватного партнерства (далі за текстом ДПП/РПП). PCS юридично оформлено як неприбуткову організацію-фонд, створену за участю державної адміністрації порту та приватних операторів. Правовий режим управління ґрунтується на договорі між учасниками, який визначає порядок розподілу відповідальності, режим доступу до даних та принципи спільної участі у прийнятті рішень. Така модель дозволяє забезпечити баланс між публічним і приватним інтересом: державні органи зберігають контроль за дотриманням стандартів, тоді як приватні учасники отримують гарантований доступ до цифрової інфраструктури та можливість впливати на її розвиток. Додатковою перевагою є мінімізація антимонопольних ризиків завдяки розподілу прав власності на дані.

Друга модель реалізована у порту Сінгапур (Portnet) і базується на централізованому державному або напівдержавному управлінні PCS, яке здійснюється через одного сильного оператора — PSA International. Участь у системі для операторів є обов'язковою де-факто, що забезпечує її ефективність і високий рівень уніфікації процедур. Водночас, з огляду на принципи правового регулювання в Україні, подібна модель може бути обмежено застосовною через концентрацію контролю та потенційні суперечності з нормами антимонопольного законодавства і концепцією вільного ринку.

Третя модель представлена прикладом порту Гамбург (Hamburg SmartPORT), де PCS управляється приватною компанією Dakosy AG. Правові відносини між суб'єктами регулюються виключно на основі комерційних договорів, у межах загального права та положень GDPR. Така модель

забезпечує високу гнучкість та орієнтованість на потреби бізнесу, однак створює низку правових ризиків. Зокрема, відсутність участі державних структур у процесі управління може призводити до невизначеності у питаннях власності на дані, а також до можливих конфліктів інтересів і ускладнень в антимонопольному регулюванні.

Міжнародний досвід свідчить, що ефективне врегулювання конфлікту між публічним і приватним інтересом у процесі цифровізації логістичної інфраструктури потребує впровадження нормативно визначеної моделі управління PCS. З огляду на порівняльно-правовий аналіз, модель, застосована у порту Роттердам, є найбільш збалансованою з правової точки зору, оскільки вона поєднує державний нагляд із договірною участю приватного сектору, а також передбачає чіткі механізми управління даними.

У контексті українського законодавства така модель може бути адаптована шляхом внесення змін до Закону України «Про морські порти України», зокрема шляхом запровадження окремих положень, що визначають правовий статус PCS як об'єкта інфраструктури, модель державно-приватного партнерства для її управління, та основи правового режиму даних, оброблюваних в межах PCS. Такі зміни можуть забезпечити нормативну передбачуваність, правову визначеність та відповідність національного регулювання міжнародним стандартам.

Загалом, можна стверджувати, що ДПП в портах - це форма взаємодії державного сектору з приватними інвесторами, спрямована на реалізацію технологічних та інфраструктурних проєктів на умовах довгострокового партнерства, що передбачає спільне використання ресурсів та розподіл ризиків і відповідальності. Такий підхід дає можливість поєднати державні активи із приватними інвестиціями, управлінським досвідом та інноваційними технологічними рішеннями, що сприяє модернізації портових об'єктів, підвищенню ефективності їх функціонування та зміцненню конкурентоспроможності національних морських портів у глобальній логістичній системі [11, С. 438].

У сучасній глобальній економіці морські порти відіграють фундаментальну роль у забезпеченні міжнародної торгівлі. Оскільки переважна більшість світового товарообігу здійснюється морським транспортом, порти виступають ключовою ланкою у глобальних ланцюгах постачання. Вони функціонують як «логістичні шлюзи», що забезпечують інтеграцію національних ринків з міжнародними торговельними потоками та пов'язують морські перевезення з внутрішніми видами транспорту — автомобільними, залізничними та внутрішніми водними шляхами. Саме тому розвиток ефективної та технологічно розвиненої портової інфраструктури є вирішальним чинником економічного зростання, особливо для країн, які прагнуть розширити свою присутність на світових ринках.

В умовах зростання конкуренції між портами, необхідності модернізації інфраструктури та впровадження цифрових технологій, значного поширення набули моделі ДПП. Таке партнерство передбачає взаємодію держави та приватного сектору з метою спільної реалізації проєктів розвитку та управління портовими активами. Історично інфраструктура портів, зокрема гідротехнічні споруди та навігаційні системи, відносилася до виключної сфери державного управління. Проте сучасні виклики — зростання обсягів перевезень, автоматизація портових операцій, потреба у цифрових системах управління логістикою — сприяли тому, що приватні оператори почали відігравати дедалі більшу роль у розвитку та експлуатації портів [11, С. 438].

Структурування ДПП у портовій сфері вимагає врахування ряду ключових факторів. Насамперед це стосується розподілу ризиків, пов'язаних із доходністю портової діяльності. Основні доходи порту формуються зі зборів із судновласників, стивідорів та інших користувачів інфраструктури, тому їх величина прямо залежить від фактичного обсягу вантажопотоків. Зазвичай у рамках концесійної моделі саме приватний оператор бере на себе ризик попиту, сплачуючи державі концесійну плату та отримуючи дохід від надання портових послуг. Разом з тим, щоб зробити інвестиційний проєкт привабливим, держава іноді може надавати гарантії щодо мінімального рівня

доходів або застосовувати механізми розподілу прибутку між сторонами. Такий розподіл ризиків потребує ретельного аналізу можливостей та економічних цілей обох сторін.

Іншим важливим аспектом є питання конкуренції в портовому секторі. Оскільки порт є природною монополією у межах певної географічної зони, держава має забезпечити рівний доступ для різних операторів та запобігти ситуаціям, коли приватна компанія, отримавши контроль над портовою інфраструктурою, обмежує доступ конкурентів або створює бар'єри для інших учасників ринку. Це особливо актуально у випадках, коли приватний партнер одночасно володіє активами у суміжних ланках логістичного ланцюга, загалом судноплавство, термінальні послуги, експедирування, що може призвести до зловживання ринковим становищем.

Третім ключовим компонентом є забезпечення наявності та якості допоміжної інфраструктури — автомобільних доріг, залізничних під'їздів, систем внутрішнього та зовнішнього логістичного зв'язку. Навіть високотехнологічний порт з великим потенціалом пропускної спроможності не здатний функціонувати ефективно, якщо вантажопотоки обмежені слабо розвиненою транспортною інфраструктурою за межами порту. Тому координація між портовими проектами та національними транспортними стратегіями є необхідною умовою реалізації ефективного ДПП.

Запровадження державно-приватного партнерства у портовій сфері може реалізовуватися за різними організаційними моделями, вибір яких залежить від міри залучення державного та приватного секторів. Ключовою ідеєю ДПП є поступове перенесення частини відповідальності та пов'язаних із фінансуванням і подальшою експлуатацією ризиків від держави до приватного партнера. Оскільки ступінь розподілу ризиків може суттєво різнитися, у практиці виокремлюють чотири основні моделі співпраці, що визначають характер взаємодії між державними органами та приватними інвесторами [34, С. 438].

Модель порту громадських послуг передбачає, що держава зберігає право власності як на інфраструктуру, так і на обладнання, а також самостійно здійснює основні портові операції. Приватні компанії в такій системі залучаються лише до виконання другорядних функцій та допоміжних послуг. Управління портом і прийняття ключових рішень зосереджені в руках державного органу. Попри високий рівень контролю з боку держави, така модель часто характеризується низькою операційною ефективністю та нестачею спеціалізованої експертизи, що може уповільнювати розвиток порту.

Модель порту-інструменталу є проміжним варіантом між системою повністю державного управління та моделлю орендодавця. У цьому випадку держава також володіє інфраструктурою та здійснює капітальні інвестиції, проте частина операційних функцій, насамперед вантажно-розвантажувальні роботи, передається приватним компаніям. Така форма співпраці дозволяє поєднати державний контроль над стратегічними активами з використанням практичного досвіду приватного сектора. Приватні оператори беруть участь у технологічній організації роботи терміналів, що сприяє підвищенню ефективності обробки вантажів і частковій модернізації портових процесів.

У підсумку, відмінність між двома моделями полягає у рівні залучення приватного сектору: у першій він виконує допоміжні функції, тоді як у другій бере участь у ключових операційних процесах. Це визначає різний ступінь розподілу відповідальності та управлінських ризиків між державою та приватними операторами.

У світовій практиці провідною моделлю організації портового управління є модель «порту-орендодавця» (Landlord Port). У цій моделі держава зберігає право власності на земельні ділянки та об'єкти базової інфраструктури, тоді як операційна діяльність передається приватним компаніям через механізми концесії, оренди або довгострокових договорів управління. Така система дозволяє поєднати стратегічний контроль держави з ефективністю та гнучкістю приватного управління. Держава визначає загальну політику розвитку порту, встановлює правила доступу та нормативи безпеки, тоді як

приватні оператори інвестують у технології, оптимізують операційні процеси та підвищують конкурентоспроможність порту [44, С. 19-30].

Ця модель зазвичай використовується в державно-приватному партнерстві, весь термінал у цьому випадку здається в оренду в концесію організаціям приватного сектору. Орган державного сектору зберігає лише право власності на землю. З іншого боку, приватний сектор зберігає право власності на операції. Модель орендодавця є найпоширенішою моделлю, що використовується в портовому секторі, відповідальність за розвиток чітко розподілена між державним та приватним секторами. Такий підхід надає приватним інвесторам свободу задовольняти потреби клієнтів та балансувати дефіцит ресурсів з поверненням інвестицій. Однак, оскільки державна структура має управлінську роль в порту, це може створювати певний тиск та обмежувати амбітність планів приватного сектору щодо порту [80].

Модель приватного сервісного порту передбачає фактичну повну приватизацію портового комплексу, коли всі функції управління, експлуатації та розвитку інфраструктури переходять до приватного оператора. Держава в такому випадку зберігає за собою лише роль регулятора та контролює дотримання законодавчих і безпекових вимог. Іноді держава може виступати міноритарним акціонером, однак її вплив на оперативну діяльність залишається обмеженим. Ця модель у портовому секторі використовується порівняно рідко, оскільки передбачає передачу стратегічно важливих об'єктів у повне управління приватному бізнесу. Водночас вона надає приватному інвестору значну свободу щодо фінансування розвитку порту, модернізації інфраструктури та впровадження нових технологічних рішень без прямого втручання державних органів.

Таким чином, ефективне державно-приватне партнерство в портовій галузі є важливою умовою модернізації національної морської інфраструктури. Воно забезпечує баланс між публічним інтересом — збереженням стратегічного контролю та економічної безпеки — та приватним інтересом у підвищенні ефективності, впровадженні інновацій та отриманні

прибутку. Успішність таких проєктів значною мірою залежить від належного правового регулювання, прозорості процедур і здатності держави забезпечити рівні правила гри для всіх учасників ринку.

У сучасній глобальній економіці морські порти відіграють фундаментальну роль у забезпеченні міжнародної торгівлі. Оскільки переважна більшість світового товарообігу здійснюється морським транспортом, порти виступають ключовою ланкою у глобальних ланцюгах постачання. Вони функціонують як «логістичні шлюзи», що забезпечують інтеграцію національних ринків з міжнародними торговельними потоками та пов'язують морські перевезення з внутрішніми видами транспорту — автомобільними, залізничними та внутрішніми водними шляхами. Саме тому розвиток ефективної та технологічно розвиненої портової інфраструктури є вирішальним чинником економічного зростання, особливо для країн, які прагнуть розширити свою присутність на світових ринках.

В умовах зростання конкуренції між портами, необхідності модернізації інфраструктури та впровадження цифрових технологій, значного поширення набули моделі державно-приватного партнерства. Таке партнерство передбачає взаємодію держави та приватного сектору з метою спільної реалізації проєктів розвитку та управління портовими активами. Історично інфраструктура портів, зокрема гідротехнічні споруди та навігаційні системи, відносилася до виключної сфери державного управління. Проте сучасні виклики — зростання обсягів перевезень, автоматизація портових операцій, потреба у цифрових системах управління логістикою — сприяли тому, що приватні оператори почали відігравати дедалі більшу роль у розвитку та експлуатації портів.

Структурування ДПП у портовій сфері вимагає врахування ряду ключових факторів. Насамперед це стосується розподілу ризиків, пов'язаних із дохідністю портової діяльності. Основні доходи порту формуються зі зборів із судновласників, стивідорів та інших користувачів інфраструктури, тому їх величина прямо залежить від фактичного обсягу вантажопотоків. Зазвичай у

рамках концесійної моделі саме приватний оператор бере на себе ризик попиту, сплачуючи державі концесійну плату та отримуючи дохід від надання портових послуг. Разом з тим, щоб зробити інвестиційний проєкт привабливим, держава іноді може надавати гарантії щодо мінімального рівня доходів або застосовувати механізми розподілу прибутку між сторонами. Такий розподіл ризиків потребує ретельного аналізу можливостей та економічних цілей обох сторін [34, С. 438].

Іншим важливим аспектом є питання конкуренції в портовому секторі. Оскільки порт є природною монополією в межах певної географічної зони, держава має забезпечити рівний доступ для різних операторів та запобігти ситуаціям, коли приватна компанія, отримавши контроль над портовою інфраструктурою, обмежує доступ конкурентів або створює бар'єри для інших учасників ринку. Це особливо актуально у випадках, коли приватний партнер одночасно володіє активами у суміжних ланках логістичного ланцюга, що може призвести до зловживання ринковим становищем.

Третім ключовим компонентом є забезпечення наявності та якості допоміжної інфраструктури — автомобільних доріг, залізничних під'їздів, систем внутрішнього та зовнішнього логістичного зв'язку. Навіть високотехнологічний порт з великим потенціалом пропускної спроможності не здатний функціонувати ефективно, якщо вантажопотоки обмежені слабо розвиненою транспортною інфраструктурою за межами порту. Тому координація між портовими проєктами та національними транспортними стратегіями є необхідною умовою реалізації ефективного ДПП.

У світовій практиці провідною моделлю організації портового управління є модель «Landlord Port». У цій моделі держава зберігає право власності на земельні ділянки та об'єкти базової інфраструктури, тоді як операційна діяльність передається приватним компаніям через механізми концесії, оренди або довгострокових договорів управління. Така система дозволяє поєднати стратегічний контроль держави з ефективністю та гнучкістю приватного управління. Держава визначає загальну політику розвитку порту, встановлює

правила доступу та нормативи безпеки, тоді як приватні оператори інвестують у технології, оптимізують операційні процеси та підвищують конкурентоспроможність порту.

Таким чином, ефективне державно-приватне партнерство в портовій галузі є важливою умовою модернізації національної морської інфраструктури. Воно забезпечує баланс між публічним інтересом — збереженням стратегічного контролю та економічної безпеки — та приватним інтересом у підвищенні ефективності, впровадженні інновацій та отриманні прибутку. Успішність таких проєктів значною мірою залежить від належного правового регулювання, прозорості процедур і здатності держави забезпечити рівні правила гри для всіх учасників ринку [44].

Для більш глибокого розуміння даного питання проведемо розгляд практичних кейсів, в яких чітко вбачається співвідношення приватного і публічного інтересу при впровадженні технологій в портах.

Порт Роттердам є одним із провідних прикладів успішної інтеграції інноваційних технологій у портову інфраструктуру в рамках збалансованого співвідношення приватного та публічного інтересів. Розвиток глибоководної зони Maasvlakte 2 продемонстрував можливість повної автоматизації портових операцій за умов активної участі приватних операторів. Такі компанії як Rotterdam World Gateway та APM Terminals здійснили масштабні інвестиції у впровадження безпілотних транспортних засобів, дистанційно керованих перевантажувальних кранів, систем штучного інтелекту та автоматизованих логістичних алгоритмів. Це дозволило забезпечити високу ефективність обробки вантажів, зменшити експлуатаційні витрати та підвищити конкурентоспроможність порту на глобальному ринку, що відповідає приватному комерційному інтересу щодо максимізації прибутковості [35, С. 78-86].

Водночас у цьому кейсі чітко простежується роль держави як гаранта стратегічних та соціальних інтересів. Адміністрація порту Роттердам, яка залишається державним суб'єктом, закріплює в концесійних договорах

вимоги щодо підтримання певної пропускнуєї спроможності та стабільності логістичних потоків, що відповідає загальнонаціональному економічному інтересу Нідерландів як ключового європейського транспортного вузла. Важливою складовою цього балансу є також соціальна політика: з огляду на ризики втрати робочих місць унаслідок автоматизації, у стратегію розвитку порту були включені програми професійної перекваліфікації та створення спеціального фонду соціальної адаптації. Таким чином, Роттердам демонструє модель, у якій державне регулювання забезпечує соціальну стабільність та захист зайнятості, тоді як приватні партнери зосереджуються на технологічному розвитку та операційній ефективності [73].

Іншим показовим прикладом є Порт Сінгапур, управління яким здійснює PSA International — компанія, що формально працює як комерційний оператор, однак належить державі. Така організаційна модель мінімізує потенційний конфлікт між економічною вигодою та стратегічними публічними цілями. Сінгапур інтенсивно впроваджує системи штучного інтелекту, аналітики великих даних та інтернету речей у моніторинг судноплавства та управління контейнерними потоками. Кульмінацією цифрової трансформації є проєкт Tuas Mega Port — повністю автоматизований термінальний комплекс, який об'єднає всі портові потужності країни в єдину інтелектуальну логістичну систему. Державна централізація управління дозволяє підтримувати високий рівень кібербезпеки та повну сумісність інформаційних систем, що є критично важливим для захисту об'єктів стратегічної інфраструктури [7, С. 81-85].

Досвід України у впровадженні інновацій через механізми державно-приватного партнерства почав активно формуватися після прийняття законів «Про морські порти України» та «Про концесію». Одним із найбільш значущих прикладів є концесія порту Ольвія катарській компанії QTerminals. У межах концесійного договору приватний партнер зобов'язався інвестувати значні кошти у модернізацію інфраструктури та впровадження сучасних цифрових систем управління портовими операціями. Держава, у свою чергу,

захищає публічний інтерес через чітке юридичне закріплення обсягів інвестицій, строків їх реалізації та відповідальності за невиконання. Проте вже на цьому етапі виявлено потенційну проблему: недостатня деталізація технологічних стандартів може призвести до несумісності приватних систем із майбутньою національною платформою електронної взаємодії [37, С. 248-256]

Подібна проблема більш очевидно проявляється в українських портах Одеса та Чорноморськ, де іноземні стивідорні компанії, наприклад, DP World, HPS Ukraine, впроваджують власні закриті інформаційні системи TOS для управління терміналами. Такі рішення оптимізують їхню діяльність, оскільки вона задовольняє їх приватний інтерес у комерційній оптимізації та є захистом комерційної таємниці, проте це створює перешкоди для державного контролю за кібербезпекою, прозорістю митних процесів і транспортною координацією. Отже, даний кейс демонструє необхідність законодавчого закріплення уніфікованої цифрової платформи портової спільноти як обов'язкового інструменту координації між приватними та державними операторами.

Узагальнюючи розглянуті приклади, можна дійти висновку, що ефективність упровадження інновацій у портах залежить не лише від обсягу приватних інвестицій, але й від здатності держави забезпечити стратегічний контроль, соціальний баланс та єдині цифрові стандарти. Публічний і приватний інтереси не протиставляються, а можуть бути взаємодоповнюючими за умови правильно структурованого правового та інституційного механізму партнерства.

З огляду на вищевикладене, можна дійти висновку, що співвідношення приватного та публічного інтересу при впровадженні технологій у морських портах є ключовим чинником ефективного розвитку портової інфраструктури та логістичних систем. З одного боку, держава має забезпечити стратегічний контроль над портами як об'єктами критичної інфраструктури та гарантувати безпечні, прозорі та економічно вигідні умови функціонування. З іншого — ефективне управління, інноваційні рішення, технологічна модернізація та

залучення фінансових ресурсів значною мірою залежать від приватного сектору.

Запровадження моделей державно-приватного партнерства дає можливість оптимально поєднати державний контроль із гнучкістю, ефективністю та інвестиційним потенціалом приватних операторів. Вибір конкретної моделі організації портового управління визначається ступенем розподілу ризиків, повноважень та відповідальності між сторонами. Моделі варіюються від повного домінування держави у портовому управлінні до майже повної приватизації портових активів, що свідчить про високий рівень адаптивності ДПП до економічних та стратегічних умов кожної держави.

Найбільш поширеною у світовій практиці є модель порту-орендодавця, яка забезпечує збалансований розподіл відповідальності: держава зберігає стратегічні активи та регуляторні функції, тоді як приватні партнери відповідають за операційну діяльність, інвестування та впровадження інновацій. Такий підхід сприяє підвищенню конкурентоспроможності портів, розширенню їх логістичних можливостей та залученню міжнародних перевізників.

Водночас ефективність державно-приватного партнерства безпосередньо залежить від прозорості процедур відбору інвесторів, справедливого розподілу ризиків, наявності конкурентного середовища та розвитку суміжної транспортної інфраструктури. Лише за умови належного правового регулювання та державного контролю за дотриманням конкуренції можливо забезпечити реальний баланс суспільних та приватних інтересів, уникнути монополізації та гарантувати економічну безпеку держави.

Отже, впровадження технологій у портах на засадах державно-приватного партнерства є необхідною умовою модернізації національної портової системи, її інтеграції у світові транспортно-логістичні мережі та зміцнення позицій України на міжнародному ринку морських перевезень.

РОЗДІЛ 3

ПРАВОВІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ІННОВАЦІЙ В УПРАВЛІННІ МОРСЬКИМИ ПОРТАМИ УКРАЇНИ

3.1. Юридичні ризики цифрової трансформації портів: кібербезпека, відповідальність, захист даних

Морські порти є критичними вузлами глобальної торгівлі та елементами національної безпеки. Сучасна цифрова трансформація, що охоплює впровадження TOS, PCS та автоматизованих систем, створює фундаментальну дилему: як узгодити прагнення приватного капіталу до максимальної ефективності з публічним інтересом у стратегічному контролі, безпеці та соціальній стійкості? Правове вирішення цього конфлікту є ключовим завданням для забезпечення «Розумних Портів» та їхньої стійкості, особливо в умовах геополітичної напруги та підвищених кіберризиків.

Оскільки портова інфраструктура України є об'єктом критичної інфраструктури, доцільним є огляд Закону України «Про основні засади забезпечення кібербезпеки України» 2017 року. Отже, Закон України «Про основні засади забезпечення кібербезпеки України» 2017 року є ключовим нормативним актом, що визначає правові засади цифрової трансформації морських портів та встановлює обов'язкові вимоги до захисту їхніх інформаційних систем. Відповідно до нього порти визнаються об'єктами критичної інфраструктури, що означає перехід питань кіберзахисту з рівня технічної підтримки у площину чітко визначених юридичних зобов'язань та контролю з боку держави. Дія Закону узгоджується з положеннями Стратегії кібербезпеки України та світовими регуляторними підходами, зокрема вимогами NIS 2, що потребує від портових адміністрацій підвищення рівня відповідності міжнародним стандартам.

Віднесення морських портів до об'єктів критичної інфраструктури накладає на їхні адміністрації юридичний обов'язок здійснювати

ідентифікацію та категоризацію критичних цифрових систем – таких як автоматизовані системи управління терміналами та портові інформаційні платформи. Дані системи мають бути включені до Державного реєстру критичних об'єктів, а їхній кіберзахист повинен бути забезпечений через впровадження сертифікованих засобів безпеки та створення системи управління кібербезпекою. Невиконання цих вимог є правопорушенням і може спричинити припис контролюючих органів або обмеження експлуатації цифрових систем порту.

Закон також встановлює чітку відповідальність за реагування на кіберінциденти. Обов'язковим є невідкладне повідомлення про інциденти до CERT-UA та забезпечення функціонування механізмів оперативного реагування. Особливістю даного Закону є персональна відповідальність керівництва суб'єкта критичної інфраструктури за організацію належного рівня кіберзахисту. Таким чином, у разі значного інциденту юридичні наслідки можуть наставати не для технічного персоналу, а для управлінського складу, що підсилює вимоги до корпоративного контролю.

Окреме значення має взаємозв'язок даного Закону із Законом України «Про захист персональних даних». Хоча Закон України «Про основні засади забезпечення кібербезпеки України» 2017 року не регулює безпосередньо порядок обробки персональних даних, він визначає технічні та організаційні заходи, необхідні для забезпечення їх конфіденційності та цілісності. У випадку витоку даних через неналежний кіберзахист виникає подвоєна юридична відповідальність – за порушення обов'язків щодо захисту критичної інфраструктури та за захист персональних даних. Це стимулює порти впроваджувати практики, сумісні з європейським підходом GDPR, особливо в умовах міжнародних логістичних операцій.

Таким чином, Закон України «Про основні засади забезпечення кібербезпеки України» формує правове середовище, у межах якого цифрова модернізація портової інфраструктури повинна розглядатися як складова системи управління ризиками, юридичної відповідальності та економічної

безпеки. Кібербезпека постає не як суто технічне завдання, а як елемент державної безпеки та корпоративного управління.

Також, вище вже було згадано про Закон України «Про захист персональних даних» 2010 року. Закон України «Про захист персональних даних» є ключовим нормативним актом, що формує правові зобов'язання морських портів щодо обробки та зберігання інформації, пов'язаної з фізичними особами. У процесі цифрової трансформації портів, що передбачає впровадження Port Community Systems, систем автоматизованого доступу, Інтернету речей та інших цифрових рішень, значно зростають обсяги персональних даних, які обробляються в реальному часі. Це зумовлює підвищення юридичних ризиків, пов'язаних із забезпеченням законності та безпеки такої обробки.

У межах своєї діяльності порт виступає володільцем або розпорядником персональних даних, що накладає на нього обов'язок дотримання фундаментальних принципів їх обробки. Порушення принципу законної підстави створює один із найбільш поширених ризиків: дані можуть збиратися без чітко визначеної мети або в обсязі, що перевищує необхідний для логістичних операцій. Наприклад, збирання біометричних даних водіїв чи детальної інформації про екіпаж може виходити за межі встановлених законом цілей. Водночас порти повинні забезпечити можливість реалізації фізичними особами своїх прав, зокрема права на доступ, виправлення або видалення даних. Якщо цифрові системи порту не забезпечують ефективних механізмів реалізації таких прав, це є прямим порушенням закону. Додатковим ризиком є транскордонна передача даних, оскільки порти є складовою міжнародних логістичних мереж. Передача інформації до країн, що не забезпечують належний рівень захисту, можлива лише за наявності спеціальних юридичних гарантій; їх відсутність створює підстави для відповідальності.

Закон України «Про захист персональних даних» тісно взаємодіє із Законом України «Про основні засади забезпечення кібербезпеки України». Перший визначає юридичний обов'язок забезпечення конфіденційності та

цілісності даних, тоді як другий встановлює технічні та організаційні механізми реалізації цього обов'язку. Стаття 24 закону прямо вимагає вживати адекватних заходів захисту від несанкціонованого доступу, знищення, блокування або модифікації персональних даних. У разі кібератаки, що призвела до витоку даних із портових інформаційних систем, відповідальність виникає одночасно за порушення вимог обох законів: щодо належного захисту об'єктів критичної інфраструктури та щодо забезпечення захисту персональних даних. Така ситуація створює кумулятивний юридичний ризик та підвищує імовірність застосування санкцій [28].

Подальше посилення вимог до морських портів впливає із міжнародних нормативних тенденцій. Оскільки значна частина портових операцій пов'язана з обробкою інформації про екіпажі, пасажирів і логістичних партнерів держав-членів ЄС, порти фактично підпадають під екстериторіальну дію Регламенту GDPR. Це зумовлює необхідність застосування підходів оцінки впливу на захист даних, ведення реєстру операцій обробки та забезпечення підвищених стандартів прозорості. Імплементация Директиви Європейського Парламенту та Ради (ЄС) 2022/2555 (далі за текстом - NIS 2), у свою чергу, посилює вимоги до кіберстійкості портової інфраструктури, що одночасно підвищує вимоги до технічних засобів захисту персональних даних.

Таким чином, Закон України «Про захист персональних даних» визначає юридичну рамку захисту прав фізичних осіб у процесі цифрової діяльності морського порту. Його виконання є неможливим без належного впровадження систем кібербезпеки та управління інформаційними ризиками, передбачених Законом України «Про основні засади забезпечення кібербезпеки України». Обидва акти мають аналізуватися у комплексі, оскільки порушення одного неминуче спричиняє порушення іншого, що формує інтегральний характер юридичної відповідальності у сфері цифрової трансформації портів.

Розширений аналіз юридичних ризиків цифрової трансформації морських портів показує, що Рішення РНБОУ від 30 грудня 2021 року, яке затвердило

План реалізації Стратегії кібербезпеки України, є каталізатором для трансформації загальних технічних рекомендацій у конкретні юридичні зобов'язання. Морські порти, визнані критичною інфраструктурою, опиняються під пильною увагою держави, що створює перший і найважливіший юридичний виклик: невідповідність стандартів кіберзахисту. Порти мають привести свої інформаційні системи, включаючи Port Community Systems та IoT-обладнання, у відповідність до жорстких національних вимог, використовуючи лише сертифіковані засоби. Відступ від цих норм формує прямий юридичний ризик — можливість притягнення посадових осіб до адміністративної чи кримінальної відповідальності.

Крім того, план посилює обов'язок оперативного повідомлення про кіберінциденти, перетворюючи будь-яку затримку чи приховування інформації на окреме правопорушення. Другий, і найбільш складний, виклик лежить у сфері відповідальності за автономні системи.

Цифровізація впроваджує AI-керовані крани та інші автоматизовані механізми, розмиваючи традиційні принципи морського права, засновані на вині людини. У разі збою, спричиненого алгоритмом, чинне українське законодавство не дає чіткої відповіді, хто нестиме відповідальність за завдану шкоду: власник порту, розробник ПЗ чи оператор, створюючи правовий вакуум та значні фінансові ризики, які порти намагаються лише частково мінімізувати через складні договори про рівень SLA.

Нарешті, третій блок ризиків пов'язаний із захистом даних. Як міжнародні хаби, порти обробляють величезні масиви комерційної таємниці та персональних даних. Кібератаки, протидію яким передбачає План, безпосередньо загрожують цій інформації. Водночас, необхідність міжнародної співпраці змушує порти фактично дотримуватися принципів GDPR, навіть за відсутності повної імплементації цих норм у національному законодавстві, що створює репутаційні ризики та юридичні проблеми у міжнародному полі.

Таким чином, План реалізації Стратегії кібербезпеки є необхідним, але недостатнім інструментом: для забезпечення стійкої та безпечної цифрової трансформації морських портів України потрібна гармонізація законодавства у сферах відповідальності за АІ та захисту даних [39].

Наступний нормативно-правовий акт, який безпосередньо висвітлює наслідки впровадження цифровізації морських портів є NIS 2, є ключовим регуляторним актом Європейського Союзу, який кардинально посилює вимоги до кібербезпеки у критичних секторах, зокрема у транспортній галузі, що безпосередньо стосується морських портів. Хоча Україна ще не імплементувала цю Директиву, вона вже формує регуляторний тиск і визначає майбутні юридичні ризики та виклики для портів у контексті євроінтеграції. Головний виклик для українських портів полягає у необхідності гармонізації національного законодавства про кібербезпеку, оскільки портова інфраструктура, як критичний вузол міжнародної логістики, де-факто має відповідати європейським стандартам для збереження довіри та безперебійності співпраці з партнерами з ЄС.

NIS 2 встановлює обов'язок впровадження комплексних заходів з управління кіберризиками, включаючи безпеку ланцюга постачання, що є критично важливим для портів, які значною мірою залежать від зовнішніх ІТ-провайдерів та операторів. Це створює юридичний ризик – порт може бути притягнутий до відповідальності за інцидент, спричинений слабкою ланкою у ланцюгу постачання, якщо не будуть належним чином аудитовані та договірно закріплені вимоги кібербезпеки з контрагентами.

Ключовий елемент Директиви – це значне посилення відповідальності керівництва та режиму звітності. NIS 2 передбачає, що керівні органи несуть пряму відповідальність за недотримання вимог кібербезпеки. Це перекладає проблему кібербезпеки з технічного рівня на рівень корпоративного управління, змушуючи адміністрації портів юридично оформити внутрішні політики та забезпечити їх виконання. Крім того, Директива встановлює жорсткий режим звітності про інциденти, вимагаючи початкового

повідомлення протягом 24 годин. Цей прискорений термін створює юридичний виклик для українських портів щодо необхідності перегляду та прискорення власних протоколів реагування, щоб уникнути юридичної відповідальності за неналежне чи запізніле інформування.

Хоча NIS 2 не замінює GDPR, вона тісно пов'язана із захистом даних, оскільки вимагає посилення технічних та організаційних заходів для запобігання кібератакам, які є головною причиною витоків даних. Для українських портів, які вже обробляють персональні дані громадян ЄС, гармонізація з NIS 2 є додатковою запорукою дотримання GDPR. Отже, Директива NIS 2 є потужним орієнтиром для правової реформи в Україні і вимагає від морських портів проактивного впровадження європейських стандартів для мінімізації фінансових та репутаційних юридичних ризиків, що виникнуть після неминучої інтеграції українського правового поля у спільний кібербезпековий простір Європейського Союзу.

Отже, аналізуючи вищезазначене можна дійти висновку, що цифрова трансформація морських портів, яка охоплює впровадження автоматизованих систем управління, платформ обміну даними та технологій штучного інтелекту, супроводжується комплексом юридичних ризиків, що прямо впливають на безпеку, ефективність та легітимність портової діяльності. Віднесення портів до об'єктів критичної інфраструктури означає, що питання кіберзахисту та управління інформаційними потоками набувають статусу не технічної, а правової та управлінської відповідальності. Закон України «Про основні засади забезпечення кібербезпеки України» формує обов'язок впровадження систем управління кібербезпекою, забезпечення належних засобів захисту інформаційних систем та оперативного реагування на кіберінциденти, що у свою чергу покладає персональну відповідальність на керівництво портів.

Паралельно, Закон України «Про захист персональних даних» визначає правові рамки обробки та захисту інформації, пов'язаної з фізичними особами, а його порушення у контексті кібератаки створює подвійну юридичну

відповідальність. Міжнародні нормативні стандарти, зокрема GDPR та Директива NIS 2, посилюють регуляторний тиск, вимагаючи від портів гармонізації внутрішніх політик безпеки з європейськими моделями управління ризиками.

3.2. Проблеми правового регулювання трудових відносин в умовах автоматизації портової діяльності

Автоматизація морських портів, впровадження систем штучного інтелекту та робототехніки, є не лише технологічною, але й глибокою соціально-правовою трансформацією. Цей процес докорінно змінює саму природу праці — від фізичного управління обладнанням до інтелектуального контролю складних цифрових систем. Відповідно, чинне українське трудове законодавство, центральним елементом якого є Кодекс законів про працю України 1971 року (далі за текстом – КЗпП), виявляється недостатньо гнучким для швидкої адаптації до нових реалій. Аналіз виявляє критичні юридичні ризики, пов'язані з невідповідністю кваліфікаційних вимог, проблемами захисту зайнятості та складністю визначення матеріальної відповідальності працівника за дії алгоритму, що підштовхує ревізії правових механізмів.

Кодекс законів про працю України є базовим нормативним актом, що регулює трудові відносини між адміністрацією морського порту та його працівниками. Проте в умовах цифрової трансформації портової діяльності, впровадження автоматизованих систем управління, роботизованих механізмів та технологій штучного інтелекту традиційні норми КЗпП виявляються недостатньо адаптованими до нових реалій. Це породжує низку юридичних викликів, пов'язаних зі зміною трудових функцій, забезпеченням зайнятості та визначенням меж відповідальності.

Перший блок викликів стосується трансформації трудової функції працівників порту. Перехід від фізичної операційної праці до діяльності з контролю та управління автоматизованими системами потребує зміни умов праці та підвищення кваліфікації працівників. Відповідно до статті 32 КЗпП,

зміна істотних умов праці допускається лише у разі змін в організації виробництва, однак роботодавець зобов'язаний завчасно попередити працівника про такі зміни не пізніше ніж за два місяці. Порушення цієї процедури може стати підставою для судового визнання переведення незаконним. Крім того, стаття 97 КЗпП передбачає обов'язок забезпечення справедливої оплати праці, яка повинна відповідати складності виконуваних функцій. У ситуації, коли кваліфікаційні довідники професій застарілі, зростає ризик зниження оплати праці операторів сучасних систем управління. Водночас статті 77 та 78 КЗпП покладають на роботодавця обов'язок створювати умови для перенавчання та підвищення кваліфікації працівників, що набуває особливої актуальності в умовах автоматизації виробничих процесів.

Другий важливий аспект пов'язаний із забезпеченням зайнятості та соціального діалогу. Скорочення чисельності персоналу у зв'язку з автоматизацією регулюється статтею 40 КЗпП, яка вимагає чіткого обґрунтування змін в організації виробництва і праці. Судова практика демонструє, що будь-яке скорочення повинно супроводжуватися дотриманням права працівника на переважне залишення на роботі - стаття 42 КЗпП. У цьому контексті особливого значення набуває колективний договір, передбачений статтею 7 КЗпП, який може встановлювати додаткові соціальні гарантії, зокрема фінансування програм перекваліфікації, мораторій на звільнення або підвищену вихідну допомогу. Невиконання таких умов створює підстави для юридичної відповідальності роботодавця [9].

Третій блок ризиків стосується проблеми визначення матеріальної відповідальності та використання цифрових систем моніторингу. Згідно зі статтями 130 та 131 КЗпП, працівник не може бути притягнутий до матеріальної відповідальності за збитки, спричинені технічним збоєм або помилкою алгоритму, якщо його вина не доведена. Це ставить питання: хто несе відповідальність у разі інциденту, викликаного системами штучного інтелекту — оператор, розробник обладнання чи адміністрація порту як

організатор виробничого процесу. Додатково застосування систем цифрового спостереження повинно відповідати вимогам Закону України «Про захист персональних даних», зокрема принципам законності та інформованої згоди працівників. Порухення цих вимог створює ризик притягнення до юридичної відповідальності за незаконне втручання у приватне життя працівників [28].

Таким чином, цифрова трансформація морських портів вимагає не лише модернізації технологічних процесів, але й адаптації трудового законодавства та підсилення ролі колективних договорів як інструменту балансування інтересів роботодавця та працівників. КЗпП залишається дієвим правовим фундаментом, однак його норми потребують сучасного переосмислення для забезпечення справедливих, безпечних та стійких трудових відносин у цифрову епоху [12].

Незважаючи на те, що Кодекс законів про працю України 1971 року встановлює рамкові юридичні процедури для регулювання зайнятості та зміни умов праці, впровадження інновацій у морських портах виявляє гостру проблему відсутності адекватних інструментів для імплементації цих норм. Ключовим регуляторним гальмом у сфері трудових відносин є Національний класифікатор України ДК 003:2010 «Класифікатор професій». Будучи обов'язковим для оформлення штатного розпису та кадрової документації, цей документ, розроблений для індустріального типу економіки, не містить професійних назв, адекватних новим, високотехнологічним ролям. Ця інертність Класифікатора безпосередньо ускладнює законне застосування статей 32 та 97 КЗпП, перетворюючи проблему визначення нової посади на юридичний ризик неправильної тарифікації праці та потенційних трудових спорів.

Національний класифікатор України ДК 003:2010 «Класифікатор професій» має ключове значення для правового регулювання трудових відносин у морських портах, оскільки саме він визначає юридично коректні назви посад, які можуть бути внесені до штатного розпису, трудових договорів та інших кадрових документів. Однак у контексті цифрової трансформації

портової діяльності Класифікатор професій виступає суттєвим інституційним бар'єром для належного оформлення нових технологічних спеціальностей, пов'язаних з автоматизацією, управлінням штучним інтелектом та кіберзахистом.

Головна проблема полягає у тому, що Класифікатор професій є продуктом індустріальної економіки і не відповідає потребам сучасної цифрової логістики. Він не містить назв посад, які відображають компетенції, необхідні для роботи зі Smart Port технологіями, такими як автоматизовані системи управління терміналами, платформи цифрової логістики, системи аналізу даних та кібербезпеки критичної інфраструктури. Внаслідок цього актуальні спеціальності, такі як «оператор-контролер систем штучного інтелекту порту» або «інженер цифрових логістичних платформ», юридично відсутні. Адміністрація порту змушена використовувати узагальнені або застарілі назви професій на зразок «інженер-програміст» чи «оператор ЕОМ», що спотворює зміст виконуваної роботи.

Ця невідповідність безпосередньо впливає на застосування норм Кодексу законів про працю України. По-перше, виникає проблема з визначенням оплати праці згідно зі статтею 97 КЗпП, яка передбачає, що рівень оплати повинен враховувати складність і відповідальність роботи. Оскільки штатна посада формально не відображає фактичний рівень кваліфікації та відповідальності, виникають підстави для індивідуальних і колективних трудових спорів щодо несправедливої оплати. По-друге, ускладнюється реалізація статті 32 КЗпП про зміну істотних умов праці. Переведення працівника з традиційної посади на нову, цифрову роботу без офіційного визнання такої посади у Класифікаторі може бути юридично оскаржено як неправомірне.

Формально Класифікатор передбачає механізм певної гнучкості через Додаток Б, який дозволяє утворювати похідні назви на кшталт «провідний» чи «старший». Проте цей механізм не вирішує головної проблеми: він не створює нових класифікаційних груп і не дозволяє юридично закріпити спеціалізації,

пов'язані з технологіями штучного інтелекту та Інтернету речей. Таким чином, Класифікатор професій фактично стримує формалізацію нових компетенцій і заважає формуванню справедливих, прозорих та сучасних умов оплати праці.

Отже, Національний класифікатор ДК 003:2010 у його чинному вигляді є регуляторним гальмом для розвитку сучасних професій у морських портах. Його оновлення або доповнення є необхідною умовою адаптації трудового законодавства до викликів автоматизації та цифрової логістики, забезпечення справедливої оплати праці та мінімізації юридичних ризиків у сфері трудових відносин [19].

Впровадження роботизованих перевантажувальних комплексів, систем штучного інтелекту та технологій Інтернету речей докорінно змінює характер праці у морському порту. Традиційна функція оператора портового обладнання трансформується у функцію контролера-аналітика, який здійснює нагляд за цифровими системами та приймає рішення на основі даних. Така зміна трудової функції є зміною істотних умов праці, що потребує суворого дотримання вимог статті 32 Кодексу законів про працю України: роботодавець має письмово попередити працівника не пізніше ніж за два місяці. Порушення цієї процедури створює ризик визнання переведення незаконним та можливість поновлення працівника на попередній посаді в судовому порядку.

Зміна змісту трудової діяльності супроводжується зростанням її складності. Відповідно до статті 97 КЗпП оплата праці повинна відповідати рівню кваліфікації та відповідальності. Праця контролера цифрових систем є більш складною та вимагає нових компетентностей, однак інертність Національного класифікатора професій ДК 003:2010 не дозволяє коректно зафіксувати нові технологічні посади. Це змушує адміністрацію використовувати застарілі посадові назви, що призводить до заниження тарифікації і створює передумови для індивідуальних та колективних спорів щодо справедливої оплати.

Особливо важливим є питання матеріальної відповідальності працівника. У випадках, коли інцидент відбувається внаслідок технологічного збою або

помилки алгоритму, застосування статей 130–131 КЗпП, які передбачають відповідальність працівника за заподіяну шкоду, є проблематичним. Неможливість чітко відмежувати помилку працівника від системного технологічного ризику створює правовий вакуум і вказує на необхідність законодавчого визначення, що ризик, пов'язаний із роботою алгоритмів та автономних систем, має нести роботодавець [12].

Масштабна автоматизація також зумовлює необхідність перекваліфікації персоналу. Статті 77 та 78 КЗпП покладають на роботодавця обов'язок забезпечувати умови для професійного розвитку та перенавчання працівників, що є ключовою соціальною гарантією в умовах трансформації. Однак ефективність таких програм часто знижується через ту ж проблему класифікації посад: навіть після успішного освоєння нових компетенцій працівник не може бути юридично оформлений на нову технологічну посаду через її відсутність у Класифікаторі. Крім того, статті 40 та 42 КЗпП, що регулюють порядок скорочення штату та переважне право на залишення на роботі, в умовах цифровізації стикаються зі складністю об'єктивної оцінки кваліфікації працівників, що може призвести до судових спорів та поновлення звільнених осіб [12].

У цих умовах зростає роль соціального діалогу та колективного договору як основного юридичного механізму збереження балансу між інтересами адміністрації та працівників. Колективний договір може закріплювати мораторій на звільнення на період перекваліфікації, гарантії підвищеної вихідної допомоги та обов'язковість консультацій щодо впровадження автоматизованих систем. Невиконання цих зобов'язань створює підстави для колективного трудового спору, що здатне вплинути на безперервність операційної діяльності порту.

Отже, цифрова трансформація портової діяльності виявляє суттєві обмеження чинного трудового законодавства, яке було сформоване для індустріальної моделі праці. Для забезпечення правової визначеності та соціальної стійкості портів необхідним є оновлення КЗпП та Національного

класифікатора професій, а також розширення ролі колективного договірної регулювання як гнучкого інструменту адаптації трудових відносин до умов автоматизованого виробництва.

Узагальнюючи наведене можна зробити висновок, що проблеми правового регулювання трудових відносин в умовах автоматизації портової діяльності свідчать про те, що чинне трудове законодавство України та Національний класифікатор професій не встигають за технологічними змінами у сфері морської логістики. Зміна трудових функцій, потреба у перекваліфікації та визначенні справедливої оплати праці створюють правові ризики як для роботодавця, так і для працівників. Відсутність сучасних професійних назв у Класифікаторі ускладнює коректне оформлення трудових відносин і може стати джерелом трудових спорів. Неврегульованим залишається й питання матеріальної відповідальності в умовах роботи із системами штучного інтелекту, що потребує нормативного уточнення. Отже, забезпечення ефективної цифрової трансформації портової галузі вимагає оновлення правових механізмів та посилення ролі колективного договору як інструменту соціального балансу.

3.3. Правові пропозиції щодо післявоєнного відновлення портової інфраструктури з використанням інновацій

Інтенсивна автоматизація портової діяльності, що є невід'ємною складовою концепції «смарт-порт» та Стратегії розвитку морських портів України, створює низку гострих правових проблем у сфері трудових відносин, які потребують не відкладного вирішення та стануть основою для глибокого аналізу у дипломній роботі. Насамперед, ці процеси ставлять під загрозу стабільність зайнятості великої кількості працівників, вимагаючи радикального перегляду підходів до скорочення штату та зміни істотних умов праці. Чинний Кодекс законів про працю України 1971 року виявляється недостатньо гнучким для регулювання масштабної технологічної трансформації, що підтверджується міжнародним досвідом, де в портах

Роттердама чи Західного узбережжя США для пом'якшення соціальних наслідків були необхідні спеціальні Колективні угоди та створення Фондів Механізації та Автоматизації.

Головною проблемою є правове забезпечення перекваліфікації: автоматизація швидко призводить до невідповідності працівника займаній посаді через застарілість кваліфікації - п. 2 ст. 40 КЗпП, тоді як законодавство не містить чітких гарантій збереження робочого місця або компенсації витрат на перенавчання за рахунок роботодавця. Крім того, впровадження дистанційного керування обладнанням та Port Community System ставить питання про регулювання нових форм зайнятості – дистанційної та надомної праці, а також потребує перегляду норм про матеріальну відповідальність у разі збою автоматизованих систем. Таким чином, дипломна робота має зосередитися на розробці механізмів, які б забезпечили соціальний діалог між адміністрацією та профспілками, та адаптували українське трудове право до реалій цифрової економіки, забезпечуючи баланс між інноваційним розвитком морської галузі та захистом трудових прав українських портовиків [12].

Післявоєнне відновлення портової галузі має бути не просто реконструкцією, а стратегічною та інноваційною трансформацією, юридично закріпленою в контексті європейської інтеграції та підвищення безпеки. Відновлення портів повинно поєднувати модернізацію інфраструктури, інтеграцію в європейські транспортні мережі та управління юридичними ризиками, створюючи правові гарантії для розвитку, інвестицій та цифрової трансформації.

22 грудня між Україною та Європейським Союзом було підписано Порозуміння високого рівня, яке фіксує взаємну згоду щодо оновлених індикативних мап Транс'європейської транспортної мережі (далі за текстом - TEN-T) для автомобільних та залізничних шляхів. Остаточне затвердження цих мап ЄС планує здійснити у квітні 2024 року одночасно з оновленням відповідного Регламенту. Це рішення є стратегічним кроком у процесі інтеграції України в європейську транспортну систему та створює логістичну

основу для ініціатив «Шляхи солідарності», що спрямовані на експорт української аграрної продукції та доставку гуманітарної допомоги.

Відтепер на індикативних мапах TEN-T з'являться українські судноплавні ділянки р. Дніпро, від Дніпровського лиману до гирла р. Прип'ять, та р. Південний Буг, від Дніпровського лиману до м. Вознесенська.

Проекти транспортної мережі мають пріоритет у справах фінансування та модернізації, відтак у майбутньому Україна зможе претендувати на допомогу ЄС в розбудові внутрішніх водних шляхів своєї частини TEN-T.

Оновлення мап TEN-T передбачає включення нових маршрутів до кордону з Польщею та Молдовою, визначених пріоритетними для розвитку залізничного сполучення з ЄС із використанням колії європейського стандарту 1435 мм, зокрема ділянка Львів – Рава-Руська – Люблін. Крім того, оновлені мапи охоплюють маршрути Одеса – Березино – Басарабська, Житомир – Вінниця – Ямпіль, Чоп – Ужгород – Самбір – Львів, а також внутрішні сполучення Красноград – Полтава, Красноград – Харків, Красноград – Дніпро, що забезпечують покращення транспортної мережі між ключовими українськими містами.

Пониження статусу маршрутів, що ведуть до кордонів із країнами-агресорами, відображає актуальні геополітичні реалії та забезпечує безпечну інтеграцію української транспортної мережі в європейську систему.

Приєднання нових українських маршрутів до TEN-T створює можливості для залучення фінансування з боку ЄС, зокрема через гранти у рамках CEF. Це дозволяє реалізовувати інфраструктурні проекти, які відповідають критеріям TEN-T, підвищують ефективність транспортної логістики та сприяють економічній інтеграції України з ЄС. У цілому, оновлення мап TEN-T підкреслює стратегічну роль України як логістичного хаба в європейській транспортній мережі та значення правового закріплення таких змін на національному рівні для подальшого розвитку інфраструктури.

Інтеграція українських портів у Транс'європейську транспортну мережу є ключовим стратегічним вектором відновлення. Це забезпечує не лише

юридичну та фінансову основу для модернізації, а й можливість уніфікації з європейськими стандартами, включно з технічними характеристиками об'єктів, вимогами безпеки та цифровими системами управління транспортом. Відновлена інфраструктура, включно з причалами, під'їзними шляхами та перевантажувальними терміналами, має відповідати європейським нормам щодо габаритів, навантажень та пропускної спроможності, що забезпечить сумісність українських логістичних ланцюгів з європейськими. Обов'язкова інтеграція цифрових систем управління створює основу для реалізації концепції «Smart Port», підвищує ефективність операцій та дозволяє здійснювати моніторинг у режимі реального часу.

Водночас відновлення портів має враховувати військову мобільність та стійкість критичної інфраструктури. Портові об'єкти повинні мати подвійне призначення, що передбачає можливість обробки великогабаритної військової техніки та стратегічних вантажів відповідно до Плану дій ЄС з військової мобільності. Цифрові системи управління порту мають бути інтегровані у єдину європейську мережу стратегічного реагування, що забезпечує безперебійність логістики та цифрову стійкість в умовах відновлення.

Разом із цифровізацією виникають високі юридичні ризики у сфері обробки персональних даних та кібербезпеки, оскільки порти володіють великим масивом інформації про працівників, екіпажі та вантажоодержувачів. Кібератака, яка призведе до витоку цих даних, може одночасно порушити Закон України «Про кібербезпеку» та Закон України «Про захист персональних даних», створюючи подвійний юридичний ризик. Будь-яка обробка даних, включно з відеоспостереженням, GPS-трекерами та лог-файлами, має відповідати принципу цільового використання та передбачати обов'язок інформування суб'єктів про мету, склад і умови обробки. Недотримання цих вимог може призвести до адміністративної відповідальності, що підкреслює необхідність збалансованого підходу між безпекою, ефективністю та правомірністю.

Таким чином, післявоєнне відновлення портової інфраструктури повинно бути комплексним і юридично збалансованим: інтеграція в TEN-T забезпечує стратегічні імпульси, фінансові гарантії та інноваційний розвиток, а внутрішні правові стандарти захисту персональних даних і кібербезпеки гарантують ефективну, безпечну та правомірну цифровізацію портів.

Інноваційне відновлення морських портів потребує комплексного юридичного закріплення як стратегічної інтеграції України в європейський транспортний простір. Постанова Кабінету Міністрів України про Національну транспортну стратегію України на період до 2030 року (далі за текстом - НТС) виступає ключовим правовим документом, який визначає основні напрямки модернізації портової інфраструктури та створює правову основу для реалізації інноваційних проєктів. Використання НТС дозволяє поєднати стратегічні пріоритети України з європейськими стандартами та забезпечити юридичну легітимність впроваджуваних змін [34].

Одним із головних напрямів відновлення є інтеграція українських портів у Транс'європейську транспортну мережу. Це передбачає імплементацію Регламентів ЄС щодо технічних характеристик, безпеки та цифрових систем управління, що забезпечує сумісність інфраструктури з європейськими нормами. Всі проєкти відновлення мають відповідати цим стандартам, а включення заходів із цифрової уніфікації, таких як Port Community System та VTMISS, до Операційного плану НТС на 2025–2027 роки дозволяє реалізувати концепцію Smart Port. Одночасно закріплюється пріоритет розвитку залізничних під'їзних шляхів із колією європейського стандарту 1435 мм, що забезпечує інтермодальність і сприяє стратегічному переорієнтуванню транспортних маршрутів на кордони з ЄС та Молдовою.

НТС також формує правові механізми для залучення фінансової підтримки та інвестицій. Визначення об'єктів TEN-T як пріоритетних у законодавстві про державно-приватне партнерство та концесії відкриває можливості для залучення міжнародного фінансування, включно з грантами Connecting Europe Facility. Водночас для державних проєктів передбачено

розробку критеріїв пріоритезації, що враховують інноваційність та відповідність стандартам Smart Port. Це дозволяє ефективно спрямовувати ресурси на модернізацію портової інфраструктури, а не лише на її відновлення після руйнувань.

Безпека та стійкість портової інфраструктури є невід’ємними складовими юридичного забезпечення інноваційного розвитку. НТС передбачає закріплення вимог щодо подвійного призначення портових об’єктів у Законі України «Про критичну інфраструктуру» та відповідних заходах стратегії, що дозволяє обробляти великогабаритну військову техніку та інтегрувати цифрові системи у загальноєвропейську мережу стратегічного реагування відповідно до вимог безпекового фронту TEN-T. Крім того, у стратегії закріплюється необхідність забезпечення високих стандартів кібербезпеки, що мінімізує юридичні ризики у сфері захисту персональних даних та забезпечує стійкість портових цифрових систем.

Таким чином, Національна транспортна стратегія України виступає комплексним юридичним механізмом, який забезпечує перехід від традиційного ремонту до інноваційного відновлення портової інфраструктури. Поєднання стандартів TEN-T, цифрових технологій та вимог безпеки створює умови для сталого розвитку українських портів та їх ефективної інтеграції в європейський транспортний простір [34].

Також, 19.08.2025 року Представники України та Республіки Корея підписали протокол щодо спільної роботи з відновлення портової інфраструктури. У Варшаві відбулася ключова робоча зустріч, що засвідчила поглиблення співпраці в рамках Меморандуму про взаєморозуміння між Міністерством розвитку громад та територій України та Міністерством океанів і рибальства Республіки Корея. Головною метою заходу стало визначення стратегічних напрямів для забезпечення сталого розвитку портової інфраструктури України. Центральною подією зустрічі була презентація детального «Генерального плану та техніко-економічного обґрунтування реконструкції портів України». Реалізація цього масштабного плану

покликана не лише підтримати український морський сектор, а й сприяти інтеграції національних портів у європейські транспортні ланцюги, що має зміцнити роль України як провідного транспортного хабу Чорноморського регіону. Участь у переговорах взяв начальник відділу міжнародних відносин ДП «Адміністрація морських портів України» Олексій Панасюк. Під час конструктивної дискусії учасники приділили особливу увагу трьом пріоритетним напрямам: по-перше, відновити пошкоджену інфраструктуру українських морських портів; по-друге, модернізувати спеціалізований флот, а також запровадити сучасні електронні системи портового управління [4].

За результатами зустрічі сторони підписали протокол, яким офіційно підтвердили свою спільну зацікавленість у втіленні окреслених проєктів. Цей документ є основою для координації зусиль у пошуку необхідних джерел фінансування та визначенні конкретних практичних кроків для швидкої та ефективної реалізації плану реконструкції. Таким чином, українсько-кореєське партнерство набуває практичної форми, що є критично важливим для повоєнного відновлення морської галузі України.

Враховуючи вищевикладене можна дійти висновку про те, що інноваційне відновлення портової інфраструктури України, стратегічно закріплене у Національній транспортній стратегії та Генеральному плані реконструкції портів, а також підкріплене міжнародним партнерством з Республікою Корея та інтеграцією до мережі TEN-T, є багатоаспектним процесом, що породжує низку гострих правових викликів. Ця трансформація, спрямована на створення концепції «Розумний порт» та зміцнення ролі України як логістичного хабу Чорноморського регіону, вимагає не просто фізичної відбудови, а й радикальної адаптації національного законодавства.

Насамперед, правове регулювання трудових відносин виявляється критично відсталим. Інтенсивна автоматизація ставить під загрозу стабільність зайнятості великої кількості портовиків, вимагаючи радикального перегляду механізмів скорочення штату - п. 1 ст. 40 КЗпП, та зміни істотних умов праці. Головною проблемою є недостатнє правове забезпечення

перекваліфікації: КЗпП не містить чітких гарантій збереження робочого місця або компенсації витрат на перенавчання, що у світлі застарілості кваліфікації - п. 2 ст. 40 КЗпП, створює високий ризик соціальних конфліктів. Міжнародний досвід вказує на необхідність обов'язкового запровадження Соціальних планів та Фондів Механізації через колективні угоди. Крім того, впровадження дистанційного керування та електронних систем портового управління актуалізує питання регулювання нових форм зайнятості та потребує перегляду норм матеріальної відповідальності у випадку збоїв [12].

Одночасно, стратегічна інтеграція в TEN-T, що передбачає включення нових річкових та залізничних маршрутів, забезпечує фінансові гарантії через механізми ЄС, зокрема через гранти CEF, та вимагає уніфікації інфраструктури з європейськими стандартами. Юридичне закріплення цієї інтеграції у НТС дозволяє пріоритезувати проекти, зокрема розвиток залізничних під'їзних шляхів європейського стандарту.

Проте, цифрова трансформація та безпековий компонент створюють додаткові юридичні ризики. Необхідність подвійного призначення портових об'єктів для військової мобільності та стійкість критичної інфраструктури вимагають інтеграції в європейську мережу стратегічного реагування. Водночас, масове впровадження цифрових систем підвищує юридичні ризики у сфері кібербезпеки та захисту персональних даних, вимагаючи суворого дотримання українських законів про кібербезпеку та захист даних, а також принципу цільового використання інформації.

Таким чином, інноваційне відновлення портів України має бути комплексним і юридично збалансованим. Успіх трансформації залежить від здатності держави не лише залучити міжнародне фінансування та імплементувати стандарти TEN-T, але й адаптувати національне трудове та інформаційне законодавство для забезпечення соціальної справедливості, цифрової стійкості та правомірності в умовах невідворотної автоматизації.

ВИСНОВКИ

1. Інноваційні технології в управлінні морськими портами формують цілісну систему технічних, цифрових, організаційних і управлінських рішень, що трансформують традиційні логістичні процеси. Ці технології виходять за межі модернізації обладнання і передбачають впровадження концепції «Порт 4.0», яка ґрунтується на повній цифровізації, використанні автономних систем і алгоритмічного управління. Ключовою відмінністю таких інновацій є їх здатність змінювати правові взаємовідносини між суб'єктами господарювання, трудові функції та підстави відповідальності. У роботі обґрунтовано, що саме такі наслідки, а не сама технологія, мають бути об'єктом правового регулювання. Проведений поділ інновацій за функціональними ознаками (операційні, безпекові, адміністративно-регуляторні) дозволяє ідентифікувати, які саме юридичні питання вони порушують. У свою чергу, класифікація за технологічною базою дозволяє сформулювати підходи до правового регулювання. Так, цифрові платформи потребують унормування доступу та обміну інформацією, автоматизовані системи – нових норм відповідальності, а технології обробки даних – законодавства про прозорість алгоритмів і захист даних. Встановлено, що відсутність цільових норм щодо інновацій створює правовий вакуум, що стримує розвиток портового сектора. Це зумовлює необхідність формування комплексного підходу до правового супроводу впровадження інновацій. Таким чином, правове регулювання має бути спрямоване не на технологію як таку, а на юридичні наслідки її впливу на правову систему.

2. Аналіз міжнародного та національного законодавства виявив істотну асинхронність між темпами впровадження інноваційних технологій у морській логістиці та здатністю правових систем адекватно на них реагувати. Найбільш актуальні проблеми виникають щодо функціонування Port Community Systems, електронних навігаційних систем і технологій розподілених реєстрів, зокрема, блокчейн. У сфері PCS з'ясовано, що міжнародне регулювання є фрагментарним, а національне — відсутнє, що

унеможливиює врегулювання таких питань, як нейтральність платформи, власність на дані та відповідальність за збої. Електронні навігаційні системи поступово визнаються на міжнародному рівні, але національна база не забезпечує повноцінну сертифікацію продуктів і гарантії їх правового статусу. Відсутність внутрішніх стандартів ускладнює розслідування морських інцидентів та впровадження e-Navigation. У випадку блокчейну головною перешкодою є орієнтація законодавства на паперові документи, що блокує комерційне використання eBL. Виявлена правова прогалина унеможливиює реалізацію потенціалу цифрової логістики та знижує конкурентоспроможність українських портів. Встановлено, що лише імплементація MLETR та розробка спеціалізованих норм щодо цифрових платформ здатні усунути ці правові бар'єри. Це дозволить забезпечити юридичну визначеність і стале функціонування інновацій у портовому секторі.

3. У результаті дослідження обґрунтовано доцільність імплементації положень Типового закону ЮНСІТРАЛ про електронні товаророзпорядчі документи у національне законодавство України. MLETR встановлює принцип функціональної еквівалентності між паперовими та електронними документами, що є необхідним для легалізації eBL, транспортних накладних та інших цифрових документів. Ключовим є запровадження поняття «контролю» над електронним записом як юридичного еквіваленту володіння. Це дозволяє визнати за цифровим документом ті самі юридичні функції, що й за фізичним. Крім того, закон передбачає механізми передачі, модифікації та міжнародного визнання електронних записів. Важливою умовою є закріплення принципу технологічної нейтральності, що дозволяє використовувати будь-яку надійну ІТ-технологію без обмежень. Ці положення мають бути інтегровані до закону «Про електронні документи та електронний документообіг», Цивільного кодексу та інших актів. Імплементація MLETR сприятиме визнанню електронних документів у міжнародному обігу. Вона також надасть правову базу для розвитку цифрових платформ типу PCS.

Таким чином, впровадження MLETR стане важливим кроком на шляху до цифрової трансформації логістики.

4. Встановлено, що цифрова трансформація портів створює нові юридичні ризики в сферах кібербезпеки, захисту даних та правової відповідальності за функціонування автономних систем. Широке використання цифрових інструментів, віддаленого управління та штучного інтелекту підвищує вразливість інфраструктури до кіберзагроз. У зв'язку з цим обґрунтовано необхідність гармонізації законодавства з Директивою ЄС NIS 2, що встановлює жорсткі стандарти кіберстійкості. Чинна українська модель кібербезпеки є фрагментарною і не охоплює усі аспекти захисту критичних об'єктів. У сфері обробки даних доведено потребу імплементації принципів GDPR, зокрема Privacy by Design та Data Minimization. Це зменшить ризики порушення прав суб'єктів даних і полегшить транскордонний обіг інформації. Окрему складність становить юридична відповідальність за збитки від алгоритмічних збоїв, оскільки класична конструкція вини не діє в умовах автономного управління. Запропоновано створити інститут об'єктивної відповідальності за алгоритм, аналогічно до відповідальності за джерело підвищеної небезпеки. Такий підхід відображає реальний розподіл ризиків і вигод та сприяє правовій визначеності. Це дозволить гарантувати безпеку та довіру у цифровому середовищі портової діяльності.

5. Аналіз чинного трудового законодавства виявив його неспроможність ефективно реагувати на виклики цифрової трансформації у портовому секторі. Насамперед, Національний класифікатор професій не включає актуальні цифрові спеціальності, що унеможлиблює їх легалізацію. Водночас нові ролі, пов'язані з аналітикою даних, автоматизованими системами та кібербезпекою, вже стали невід'ємною частиною портової діяльності. У зв'язку з цим обґрунтовано необхідність регулярного оновлення класифікатора професій та визнання нових посад. Окрему правову проблему становить матеріальна відповідальність працівників за збої цифрових систем. Оскільки в умовах алгоритмічного управління встановити вини складно, запропоновано ввести у

КЗпП нову статтю 132-1, що покладає відповідальність на роботодавця, якщо інше не доведено. Такий підхід є виправданим, адже саме роботодавець є ініціатором цифровізації і головним вигодонабувачем. Крім того, працівник повинен мати право на безкоштовну перекваліфікацію у разі втрати професії через автоматизацію. Запровадження таких норм сприятиме соціальній стійкості в умовах технологічного переходу. Це дозволить поєднати інтереси ефективності бізнесу з гарантіями для працівників.

6. В рамках дослідження розроблено комплексну стратегію правової трансформації, спрямовану на адаптацію національного законодавства до вимог цифрової економіки та міжнародних стандартів. Основними напрямками є: імплементація MLETR для легалізації е-документів, створення правового режиму для PCS, гармонізація Закону про кібербезпеку з NIS 2, а також модернізація трудового законодавства. Кожен із цих напрямів має конкретне правове підґрунтя та практичну значущість для стабільності функціонування портів. Запропоновані кроки враховують як міжнародну практику, так і особливості українського правового простору. Їх реалізація дозволить сформувати цілісне нормативне середовище для цифрових платформ, захисту даних, управління ризиками та регулювання трудових відносин. Це сприятиме міжнародній інтеграції України, підвищенню її транспортної привабливості та інвестиційного потенціалу. Правова визначеність сприятиме довірі з боку учасників ринку. У підсумку, запропонована модель може слугувати основою для національної доктрини цифрового права у сфері транспорту. Таким чином, правові зміни стають ключовим елементом модернізації портової галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Директива 2010/65/ЄС Європейського Парламенту та Ради від 20 жовтня 2010 року «Про формальності звітності для суден, що прибувають до портів держав-членів та/або відправляються з них, та про скасування Директиви 2002/6/ЄС». URL: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:283:0001:0010:EN:PDF> (дата звернення 24.09.2025 року).

2. Директива Європейського Парламенту та Ради (ЄС) 2022/2555 від 14 грудня 2022 року «Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) №910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2)». URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 20.10.2025 року).

3. Державна служба морського та річкового транспорту України. Звіт про роботу морських портів України за 2023 рік. Київ, 2024.

4. Кабінет Міністрів України. Реалізація проєктів ДПП у морських портах дозволить покращити стан галузі та залучити нові інвестиції для розвитку. 2020. URL: <https://www.kmu.gov.ua/news/realizaciya-proyektiv-dpp-u-morskih-portah-dozvolit-pokrashchiti-stan-galuzi-ta-zaluchiti-novi-investiciyi-dlya-rozvitku-vladislav-kriklij> (дата звернення: 23.10.2025).

5. Кабінет Міністрів України. Схвалено оновлену Стратегію розвитку морських портів до 2038 року: офіційний сайт. 2020. URL: <https://www.kmu.gov.ua/news/shvaleno-onovlenu-strategiyu-rozvitku-morskih-portiv-do-2038-roku-mininfrastrukturi> (дата звернення: 23.11.2025).

6. Кириллова В.Ю., Кириллова О.В. Основні технологічні тренди у сфері інформаційного забезпечення систем доставки вантажів у діяльності транспортно-експедиторських компаній. Вчені записки ТНУ ім. В.І. Вернадського. Серія: Технічні науки. 2023. Том 34 (73) № 6. Видавничий дім «Гельветика». С. 244-250. URL: <https://doi.org/10.32782/2663-5941/2023.6/36>.

7. Кириллова О. В., Кириллова В. Ю., Магамадов О. Р. Поняття «Smart Port» у контексті глобальних тенденцій інтеграції інтелектуальних транспортних та інформаційних технологій у портовій індустрії. Вчені записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки. 2024. Т. 35 (74), № 5. С. 81-87.

8. Кириллова О.В., Кириллова В.Ю. Діджиталізація як шлях до забезпечення екологічності, безпеки і сталого функціонування морської галузі. Інтелектуальні транспортні технології: праці 2 міжнар. наук. техн. конф. (Харків, 27-29 квітня 2021 р.). Харків: УкрДУЗТ, 2021. С. 21-23. URL: <http://itt.kart.edu.ua/images/Tezu2021/TezuITT2021.pdf>.

9. Кириллова О.В., Кириллова В.Ю. Інноваційні робототехнічні технології для морської індустрії. Інтелектуальні транспортні системи: екологія, безпека, якість, комфорт: праці міжнародної конференції (Київ, 29-30 листопада 2022 р.). Київ: НТУ, 2022. С. 72-76. URL: <https://drive.google.com/file/d/1n5wjnM0O7g8CvkCQwvqmjvHVDFs6Gtk/view>.

10. Кириллова О.В., Кириллова В.Ю., Магамадов О.Р., Ромах В.Л. Smart Port: новітні технології і міжнародний досвід їх упровадження. Розвиток транспорту. 2024. № 2(21). С. 62–74. DOI: <https://doi.org/10.33082/td.2024.2-21.06>.

11. Кириллова О. В., Пітерська В. М., Магамадов О. Р., Решетков Д. М., Корнієць Т. Є. Проблеми функціонування та розвитку портів : монографія. Т. 7 / за ред. О. В. Кириллової, І. М. Іванова. Львів-Торунь : Ліга-Прес, 2022. С. 438. DOI: <https://doi.org/10.36059/978-966-397-289-3>.

12. Кодекс законів про працю України: Закон від 10.12.1971 № 322-VIII. URL: <https://zakon.rada.gov.ua/laws/show/322-08> (дата звернення: 10.11.2025).

13. Конвенція про полегшення міжнародного морського судноплавства 1965 року (FAL Convention). URL: <https://ips.ligazakon.net/document/MU65K04U?an=489> (дата звернення: 15.10.2025 року).

14. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки: схвалено розпорядженням Кабінету Міністрів України від 17.01.2018 № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80> (дата звернення: 15.11.2025).

15. Котлубай О. М. Міжнародно-правове регулювання морської безпеки: сучасний стан та перспективи. Актуальні проблеми міжнародних відносин. 2019. Вип. 141. С. 48-62.

16. Митний кодекс України: Закон від 13.03.2012 № 4495-VI. URL: <https://zakon.rada.gov.ua/laws/show/4495-17> (дата звернення: 07.11.2025).

17. Міжнародна конвенція про охорону людського життя на морі 1974 року (SOLAS). URL: [\[https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-\(solas\),-1974.aspx\]](https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx) (дата звернення: 10.10.2025 року).

18. Морська доктрина України на період до 2035 року: затверджена постановою Кабінету Міністрів України від 07.10.2009 № 1307 (у редакції постанови КМУ від 18.12.2018 № 1108). URL: <https://zakon.rada.gov.ua/laws/show/1307-2009-%D0%BF> (дата звернення: 20.11.2025).

19. Національний класифікатор України. Класифікатор професій ДК 003:2010: затв. наказом Держспоживстандарту України від 28.07.2010 № 327. Київ: Держспоживстандарт України, 2010. URL: <https://zakon.rada.gov.ua/rada/show/va327609-10> (дата звернення: 07.11.2025).

20. Ніколюк О. В. Правові аспекти кібербезпеки критичної інфраструктури України. Інформація і право. 2022. № 2(41). С. 67-75.

21. Онешко С. В., Ільченко С. В. Державно-приватне партнерство як механізм розвитку морських портів України. Економіка та держава. 2020. № 1. С. 10-15.

22. Постанова Південно-західного апеляційного господарського суду м. Одеси від 18.06.2024 року у справі №916/3658/23 URL: <https://reyestr.court.gov.ua/Review/119894864> (дата звернення: 06.12.2025 року).

23. Представлено спільний звіт IAPH-World Bank. PPL 33-35. 2021. URL: <https://www.ppl33-35.com/tpost/hua0763pf1-predstavleno-splnii-zvt-iaph-world-bank> (дата звернення: 12.10.2025).

24. Примачов М. Т., Примачова Н. М. Цифрова трансформація транспортної галузі: виклики та можливості. Економіка та управління на транспорті. 2021. Вип. 13. С. 35-44.

25. Про електронні довірчі послуги : Закон від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 11.11.2025).

26. Про електронні документи та електронний документообіг: Закон від 22.05.2003 № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15> (дата звернення: 15.11.2025).

27. Про затвердження Положення про Адміністрацію морських портів України : Наказ Міністерства транспорту та зв'язку України від 19.05.2010 № 327. Верховна Рада України. 2010. URL: <https://zakon.rada.gov.ua/rada/show/va327609-10#n5> (дата звернення: 23.10.2025).

28. Про захист персональних даних: Закон від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 12.11.2025).

29. Про інноваційну діяльність: Закон від 04.07.2002 № 40-IV. URL: <https://zakon.rada.gov.ua/laws/show/40-15> (дата звернення: 28.11.2025).

30. Про морські порти України: Закон від 17.05.2012 № 4709-VI. URL: <https://zakon.rada.gov.ua/laws/show/4709-17> (дата звернення: 10.11.2025).

31. Про національну інфраструктуру геопросторових даних : Закон від 13.04.2020 № 554-IX. Відомості Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/554-20#Text> (дата звернення: 28.10.2025).

32. Про основні засади забезпечення кібербезпеки України : Закон від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 10.11.2025).

33. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021> (дата звернення: 08.11.2025).

34. Про схвалення Національної транспортної стратегії України на період до 2030 року: Розпорядження Кабінету Міністрів України від 30.05.2018 № 430-р. URL: [[\(https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80\(дата\)](https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80(дата))] ([\(https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80\(дата\)](https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80(дата))) звернення: 09.11.2025).

35. Пядишев В. Г. Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. Морська безпека та оборона. 2023. № 1. С. 78–86. DOI: <https://doi.org/10.32782/msd/2023.1.10>.

36. Регламент Європейського Парламенту та Ради (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» (GDPR). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 01.09.2025 року).

37. Сментина Н. В. Цифровізація морської галузі України: економічні ефекти та стратегічні пріоритети конкурентоспроможності. Київський економічний науковий журнал. 2025. № 9. С. 248–256. URL: 10.32782/2786-765X/2025-9-33.

38. Стратегія кібербезпеки України: затверджена Указом Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 08.11.2025).

39. Стратегія розвитку морських портів України на період до 2038 року:
схвалено розпорядженням Кабінету Міністрів України від 23.08.2023 № 1579-

р. URL: <https://zakon.rada.gov.ua/laws/show/1579-2023-%D1%80> (дата звернення: 09.11.2025).

40. Типовий закон 72/114 ЮНСІТРАЛ від 7 грудня 2017 року «Про електронні передавальні документи» (MLETR). URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ru/mletr_ebook_r.pdf (дата звернення: 10.10.2025 року).

41. Типовий закон ЮНСІТРАЛ про електронну торгівлю з Керівництвом для прийняття, 1996 рік: Резолюція Генеральної Асамблеї ООН A/RES/51/162 від 16.12.1996. Комісія Організації Об'єднаних Націй з права міжнародної торгівлі (ЮНСІТРАЛ). Відень: ООН, 1996. URL: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce (дата звернення: 10.10.2025).

42. Уніфіковані тлумачення Глави II-2 Конвенції про охорону людського життя на морі 1974 року (SOLAS) – MSC.1/Circular.1634 від 04 грудня 2020 року. URL: <https://www.imorules.com/GUID-43A9E1E7-C0B6-4846-B182-9E6B58B2D57F.html> (дата звернення: 14.10.2025 року).

43. Шемаєв В. В., Шемаєва Л. М. Наближення до моделі управління портлендлорд: український контекст. Розвиток методів управління та господарювання на транспорті. 2020. № 4 (73). С. 19–30. URL: 10.31375/2226-1915-2020-4-19-30.

44. Шпак Н. Г., Павловська Л. А., Коробкова О. М. Цифрова трансформація системи управління морським портом: новітні можливості та виклики в умовах воєнного стану. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. 2025. Т. 36 (75), № 1. С. 389-394. URL: <https://doi.org/10.32782/2663-5941/2025.1.1/56>.

45. 49th Session IMO Facilitation Committee. Морська адміністрація України. URL: <https://marad.gov.ua/en/news/49th-session-imo-facilitation-committee> (дата звернення: 23.05.2025).

46. Acciaro M., Vanelslender T., Sys C., Ferrari C., Roumboutsos A., Giuliano G., Lam J.S.L., Kapros S. Environmental sustainability in seaports: a framework for

successful innovation. *Maritime Policy & Management*. 2014. Vol. 41, №. 5. pp. 480-500.

47. Akpan F., Bendiab G., Shiaeles S., Karamperidis S., Michaloliakos M. *Cybersecurity Challenges in the Maritime Sector*. MDPI. 2022. 7 March. URL: <https://www.mdpi.com/2673-8732/2/1/9> (дата звернення: 26.09.2025).

48. Allianz Risk Barometer. Top Business Risks for 2019. Allianz Global Corporate & Specialty. 2019. URL: <https://www.assiteca.it/wp-content/uploads/2019/10/Allianz-Risk-Barometer-2019-1.pdf> (дата звернення: 25.09.2025).

49. A Comprehensive Guide to Maritime Cybersecurity. MissionSecure. URL: <https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach> (дата звернення: 25.09.2025).

50. Bagchi P. K., Chun H. A., Ha B. C. (eds.) *Smart Ports and Logistics Competence*. Palgrave Macmillan, 2021.

51. Boyes H., Isbell R. *Code of Practice. Cyber Security for Ships*. London: Institution of Engineering and Technology, 2017. 73 p..

52. Carlan V., Sys C., Vanelslander T. *Innovation in the Maritime Cluster: A Knowledge Transfer Perspective*. Springer, 2019.

53. Chen J., Xue K., Ye J., Huang T., Tian Y., Hua C., Zhu Y. Simplified neutrosophic exponential similarity measures for evaluation of smart port development. *Symmetry*. 2019. 11(4). URL: <https://doi:10.3390/sym11040485>.

54. Cho S.W., Won S.H. A study on the future development plan of container in Korea by analysing the cases of automated container terminals in Europe. *J. Eur. Union Stud*. 2014. 38. pp. 205-236.

55. Coburn A. W., Daffron J., Smith A., Bordeau J., Leverett É., Sweeney S., Harvey T. *Cyber Risk Outlook*. Cambridge: Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc., 2018. 33 p. URL: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2018.pdf> (дата звернення: 25.09.2025).

56. Cybercrime. What does the most damage, losing data or trust? Ernst & Young. URL: https://www.ey.com/en_gl/financial-services/cybercrime-what-does-the-most-damage-losing-data-or-trust (дата звернення: 23.10.2025).

57. Cybersecurity and Disaster Recovery Plan by Marine Digital. Marine Digital. URL: https://marine-digital.com/article_cybersecurity (дата звернення: 23.10.2025).

58. E-Navigation Strategy Implementation Plan – Update 1: MSC.1/Circ.1595. International Maritime Organization. London: IMO, 2021. URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC.1-Circ.1595%20-%20E-Navigation%20Strategy%20Implementation%20Plan%20-%20Update%201%20\(Secretariat\)%20\(2\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC.1-Circ.1595%20-%20E-Navigation%20Strategy%20Implementation%20Plan%20-%20Update%201%20(Secretariat)%20(2).pdf) (дата звернення: 11.11.2025).

59. European Commission (2021). Sustainable and Smart Mobility Strategy. Brussels. URL: https://transport.ec.europa.eu/transport-themes/mobility-strategy_en.

60. Harris R. How Big a Problem is Maritime Cyber Security? Ocean Technology Group. URL: <https://oceantg.com/blog/the-problem-of-maritime-cyber-security/> (дата звернення: 25.09.2025).

61. Heikkilä M., Saarni J., Saurama A. Innovation in Smart Ports: Future Directions of Digitalization in Container Ports. Journal of Marine Science and Engineering. 2022. Vol. 10, No. 12. DOI: <https://doi.org/10.3390/jmse10121925>.

62. Heilig L., Schwarze S., Voss S. An Analysis of Digital Transformation in the History and Future of Modern Ports. 50th Hawaii International Conference on System Sciences (HICSS), 2017. pp. 1341-1350.

63. IAPH – International Association of Ports and Harbours (Міжнародна асоціація портів і гаваней). Порти України. URL: <http://порти.com.ua/info/29-iaph-international-association-of-ports-and-harbours-mezhdunarodnaya-associaciya-portov-i-gavaney-maspog.html> (дата звернення: 23.05.2025).

64. IMO (2021). Guidelines on Maritime Cyber Risk Management: MSC-FAL.1/Circ.3. London: International Maritime Organization.

65. International Chamber of Shipping. The Principal Regulations Governing Maritime Safety. URL: <https://www.ics-shipping.org/shipping-fact/safety-and-regulation-the-principal-regulations-governing-maritime-safety/> (дата звернення: 23.09.2025).

66. International Maritime Organization (IMO). Maritime Single Window: офіційний сайт IMO. 2024. URL: <https://www.imo.org/en/ourwork/facilitation/pages/maritimesinglewindow-default.aspx> (дата звернення: 23.11.2025).

67. International Maritime Organization. Maritime Cyber Risk Management in Safety Management Systems: Resolution MSC.428(98) Annex 10 (adopted on 16 June 2017). URL: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf) (дата звернення: 23.09.2025).

68. Ki Jun W., Lee M.K, Young Cho J. Impact of the smart port industry on the Korean national economy using input-output analysis. Transportation Research Part A: Policy and Practice. 2018. Vol. 118. pp. 480-493. URL: <https://doi.org/10.1016/j.tra.2018.10.004>.

69. Kosse I. From Paper to Data at Ukraine's Seaports: What's Changing and What Still Drags. Ukrainian Maritime Analytics. 2024. URL: <https://medium.com/@iryna.kosse/from-paper-to-data-at-ukraines-seaports-f0d17ab0e385> (дата звернення: 28.10.2025).

70. Maritime Cyber Risk Management in Safety Management Systems : Resolution MSC.428(98) (adopted on 16 June 2017). International Maritime Organization. URL: <https://www.dohle-yachts.com/wp-content/uploads/2021/05/MSC.42898-2.pdf> (дата звернення: 23.05.2025).

71. Molavi A., Lim G. J., Race B. A framework for building a smart port and smart port index. International Journal of Sustainable Transportation. 2020. Vol. 14, No. 9. pp. 686-703. DOI: <https://doi.org/10.1080/15568318.2019.1610919>.

72. Neo M. The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore. Royal

Australian Navy Sea Power. 2021. Issue 42. P. 38. URL: https://www.navy.gov.au/sites/default/files/documents/Soundings_Papers_42_2021.pdf (дата звернення: 26.09.2025).

73. Notteboom T., Pallis A., Rodrigue J.-P. Port Economics, Management and Policy. Routledge, 2022.

74. Nunes M. P., Vieira G. B. B., da Rosa A. Q. Innovation in ports – a systematic literature review. International Journal of Logistics Systems and Management. 2024. Vol. 49, No. 1. URL: <https://www.researchgate.net/publication/384304419> (дата звернення: 23.09.2025).

75. Obrenovic B. The Role of the Public-Private Partnership (PPP) in Achieving the Optimal Economic and Social Benefits Through the Port Sector. 2022. URL: https://www.researchgate.net/profile/Bojan-Obrenovic/publication/363801158_The_Role_of_the_Public-Private_Partnership_PPP_in_Achieving_the_Optimal_Economic_and_Social_Benefits_Through_the_Port_Sector.pdf (дата звернення: 29.10.2025).

76. OECD (2022). Port Infrastructure Financing and Port Governance: OECD Policy Responses. Paris: OECD Publishing.

77. Parola F., Risitano M., Ferretti M., Panetti E. The drivers of port competitiveness: a critical review. Transport Reviews. 2017. Vol. 37, No. 1. pp. 116-138.

78. Rajabi A., Saryazdi A., Belfkih A., Duvallet C. Towards Smart Port: An application of AIS Data. IEEE. 2018. pp. 1414-1421. URL: <https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00234>.

79. Riedl J., Delecencios F.X., Rasmussen A. To Get smarts, Ports go to Digital. Boston Consulting Group, 2018.

80. Sys C., Vanelslander T., Adriaenssens M., Van Rillaer I. International benchmarking of container port performance: An application to the top-20 ports. International Journal of Transport Economics. 2016. Vol. 43, No. 1. pp. 75-101.

81. The Government launches new Digitalisation Strategy. Ministry of Foreign Affairs of Denmark. InvestInDK. 2022. 05 May. URL: <https://investindk.com/insights/digitization-strategy> (дата звернення: 23.08.2025).

82. The Guidelines on Cyber Security onboard Ships. Version 4. BIMCO. URL: <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships> (дата звернення: 24.08.2025).

83. UNCTAD (2023). Review of Maritime Transport 2023. United Nations Conference on Trade and Development. Geneva. URL: <https://unctad.org/rmt2023>.

84. UN/CEFACT (Центр Організації Об'єднаних Націй із спрощення процедур торгівлі та електронних ділових операцій). Рекомендації. Женева: UNECE. URL: <https://unece.org/trade/uncefact/cl-recommendations> (дата звернення: 11.11.2025).

85. WCO (Всесвітня митна організація). Рекомендації. Брюссель: WCO, 2025. URL: <https://www.wcoomd.org/en/about-us/legal-instruments/recommendations.aspx> (дата звернення: 18.11.2025).

86. World Bank, IAPH (2021). The Container Port Performance Index 2021. Washington, DC: World Bank Group. URL: <https://www.worldbank.org/en/topic/transport/publication/container-port-performance-index-2021>.

87. Yang Y., Zhong M., Yao H., Yu F., Fu X., Postolache O. Internet of things for smart ports: Technologies and challenges. IEEE Instrumentation & Measurement Magazine. 2018. 21(1). pp. 34-43. URL: <https://doi.org/10.1109/MIM.2018.8278808>.