

МІЖНАРОДНЕ ПРАВО; ПОРІВНЯЛЬНЕ ПРАВОЗНАВСТВО

Веремчук В.С.,

*аспірант кафедри цивільно-правових дисциплін
Одеського національного університету імені І.І. Мечникова*УДК 341.225.5:351.862.4:007]:347.79(477)
DOI 10.32782/2663-5666.2025.2.10ПРОБЛЕМАТИКА ІМПЛЕМЕНТАЦІЇ МІЖНАРОДНО-ПРАВОВИХ СТАНДАРТІВ
МОРСЬКОЇ КІБЕРБЕЗПЕКИ У НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО УКРАЇНИ

Вступ. Автоматизація торговельного мореплавства, широке впровадження інформаційно-комунікаційних систем, а також використання штучного інтелекту на морському транспорті зумовили появу нових викликів, серед яких особливої актуальності набуває проблема забезпечення кібербезпеки морських суден і портової інфраструктури. Кібератаки, несанкціонований доступ до систем управління судном та портовою інфраструктурою, втрата конфіденційних даних можуть мати катастрофічні наслідки не лише для конкретного судна, компанії чи портового терміналу, але й для безпеки судноплавства в цілому, довкілля та людського життя.

Детермінантами морських кіберзагроз у сучасному світі виступають комплексні геополітичні та економічні чинники, серед яких ключову роль відіграють збройні конфлікти, у тому числі гібридного характеру, у яких здійснюються спрямовані кібератаки з боку держав або за їх підтримки. Зокрема, збройний конфлікт міжнародного характеру на території України завдає істотного впливу на кібербезпеку транспортної інфраструктури держави, що вимагає впровадження адекватних механізмів протидії кіберзагрозам.

Згідно Базис даних морських кібератак Нідерландського університету прикладних наук, у період з вересня 2001 року по травень 2025 року відомо про 384 кібератаки на морський транспорт у всьому світі, кількість яких неухильно зростає протягом останніх десяти років. Зокрема, у серпні 2024 року повідомлялось про кібератаку на порт Рієка (Хорватія) із метою крадіжки даних та вимоги сплати викупу, що спричинило порушення роботи порту та затримку обробки вантажів. У травні 2025 року контейнеровоз MSC Antonia сів на мілину поблизу берегів Саудівської Аравії у наслідок підміни інформації про місцезнаходження судна [1]. Вказана статистика вказує на нагальну

необхідність розробки механізмів забезпечення кібербезпеки із подальшим їх закріпленням на у правових нормах.

Особливу увагу у цьому контексті слід приділити міжнародній кібербезпеці, оскільки торговельне судноплавство є міжнародною діяльністю, а кіберпростір не має чітких державних кордонів. Таким чином, наслідки кібератак на морський транспорт можуть мати транснаціональний характер, порушуючи нормальне функціонування світової економіки. Відтак, з огляду на неможливість ефективного реагування на морські кіберзагрози виключно на національному рівні, виникає необхідність у гармонізації національного законодавства із міжнародними правовими механізмами забезпечення морської кібербезпеки.

Питання міжнародно-правового регулювання морської кібербезпеки та його імплементації у національне право України залишається недостатньо дослідженим. Окремим аспектам цього питання присвячені праці В. В. Куща, В. Г. Пядишева. Разом із тим, імплементація міжнародних стандартів морської кібербезпеки у національне законодавство України потребує ґрунтовного дослідження, оскільки стикається з низкою проблем нормативного, інституційного та технічного характеру. Українське морське законодавство досі не містить системної регламентації питань кібербезпеки в морській сфері.

Виклад основного матеріалу. Морську кібербезпеку доцільно вважати відносно новою підгалуззю міжнародного морського права, яка набуває все більшого значення у зв'язку із безперервною цифровізацією морської галузі, широким використанням автоматизованих систем управління на борту суден та зростаючою кількістю кіберзагроз.

Агенція з кібербезпеки та захисту інфраструктури Сполучених Штатів Америки, визначає кібербезпеку як «заходи із захисту електронних мереж, пристроїв і даних від несанкціонованого

доступу чи злочинного використання, а також практика забезпечення конфіденційності, цілісності та доступності інформації» [2]. Таким чином, завданням морської кібербезпеки є захист автоматизованих систем та даних, що використовуються у морській галузі від несанкціонованого доступу, знищення, зміни або витоку, а також забезпечення безперервності їх роботи. У цьому контексті однією з основних проблем на шляху імплементації міжнародних стандартів морської кібербезпеки є відсутність відповідного міжнародного договору.

У процесі розробки та впровадження міжнародних стандартів з кібербезпеки помітну роль відіграє Організація Об'єднаних Націй (далі – ООН). Резолюція Генеральної Асамблеї ООН № 64/211 від 21 грудня 2009 року «Створення глобальної культури кібербезпеки та оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур» позиціонує кібербезпеку як стратегічно важливий напрямок розвитку держав, закликаючи до розробки національних стратегій з кібербезпеки, включаючи розширення взаємодії між державою та приватним сектором, підкреслює важливість впровадження практик реагування на кіберзагрози та наголошує на необхідності створення ефективної системи державних органів, уповноважених здійснювати захист інформації та здійснювати розслідування кіберзлочинів [3].

Конвенції, які регулюють безпеку судноплавства, зокрема, Конвенція з охорони людського життя на морі 1974 року (SOLAS), включно із Міжнародним кодексом з охорони суден та портових споруд 2004 року (ISPS Code), містять лише норми загального характеру, спрямовані на оцінку ризиків, розробку планів безпеки суден та портових споруд, призначення уповноважених офіцерів з безпеки [4]. Ці положення вбачаються позитивними з точки зору фізичного недопущення сторонніх осіб до обладнання автоматизованих систем, проте вони не містять інструкцій для екіпажів та співробітників щодо безпечної роботи із автоматизованими системами та їх дій у випадку кібератаки. Міжнародна конвенція про підготовку і дипломування моряків та несення вахти 1978 року (SCTW) не закріплює вимоги щодо наявності компетенцій з кібербезпеки у членів екіпажу судна, які відносяться до капітана-палубної команди, машинної команди та радіотехнічної служби [5].

Помітну роль у розвитку права морської кібербезпеки відіграє Міжнародна морська організація (далі – ІМО). Вказана організація своєю

метою має «забезпечувати механізм співробітництва урядів у галузі урядового регулювання та практики в технічних питаннях будь-якого роду, що стосуються міжнародного торговельного судноплавства; заохочувати та сприяти загальному прийняттю практично можливих максимальних норм у питаннях, що стосуються безпеки на морі, ефективності судноплавства, запобігання забрудненню моря з суден та боротьби з ним, а також розглядати адміністративні та правові питання, пов'язані з цілями, викладеними в цій статті» [6].

Міжнародний кодекс з управління безпекою (МКУБ) встановлює міжнародний стандарт безпечного управління та експлуатації суден, а також запобігання забрудненню моря. Прийнятий ІМО у 1993 році резолюцією А.741 (18), Кодекс став обов'язковим із набранням чинності 1 липня 1998 року поправками 1994 року до Конвенції SOLAS, які ввели до Конвенції новий розділ IX [7].

Циркуляр ІМО MSC-FAL.1/Circ.3 «Рекомендації щодо кібербезпеки в морській сфері» є ключовим документом, який містить рекомендації високого рівня щодо управління морськими кіберризиками, визначає вразливі до кібератак бортові системи судна та рекомендує кращі практики управління морським кіберризиком [8].

Резолюція ІМО MSC.428 (98) «Управління морськими кіберризиками в системах управління безпекою» 2017 року передбачає інтеграцію управління кіберризиками, включаючи положення Цирюляру MSC-FAL.1/Circ.3 у системи управління безпекою відповідно до цілей та функціональних вимог Кодексу ISM [9].

Оскільки Кодекс ISM є невід'ємною складовою Конвенції SOLAS-74, учасницею якої є Україна [4], можемо зробити висновок, що ухвалені ІМО міжнародні стандарти морської кібербезпеки є частиною національного законодавства України у силу положень ст. 9 Конституції України [10].

Виконання зазначених вище положень в Україні, станом на 2025 рік, регулює Наказ Міністерства транспорту України «Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті» від 20.11.2003 № 904. Вказаний Наказ зобов'язує судовласників запроваджувати систему управління безпекою згідно вимог МКУБ та надає повноваження класифікаційним товариствам, визначеним Кабінетом Міністрів України здійснювати контроль за дотриманням

вимог безпеки судноплавства із подальшою видачою свідоцтво про управління безпекою [11].

Тим не менш, положення Кодексу торговельного мореплавства України (далі – КТМ України) [12], Закону України «Про морські порти України» [13], а також інших спеціальних нормативно-правових актів з морського права України, не враховують аспектів кібербезпеки судноплавства. Серед проблемних питань можна виокремити відсутність правового регулювання взаємодії між морською адміністрацією, портами, прикордонними та правоохоронними органами, що ускладнює формування єдиного підходу до реагування на морські кіберзагрози; відсутність законодавчих вимог щодо підготовки персоналу в галузі морської кібербезпеки, що суперечить рекомендаціям ІМО та призводить до низької обізнаності екіпажів суден та працівників морської інфраструктури протидії потенційним кіберзагрозам.

У цьому контексті варто наголосити на необхідності імплементації Директиви Європейського парламенту та Ради № 2022/2555 про заходи для високого загального рівня кібербезпеки 2022 року (директива NIS-2), яка зобов'язує компанії підтримувати безперебійну роботу своїх інформаційних систем, впроваджувати систему управління кіберризиками, повідомляти уповноважені національні органи про будь-які проблеми із кібербезпекою та проводити навчання персоналу з кібербезпеки [14].

При характеристиці проблем на шляху імплементації стандартів морської кібербезпеки слід погодитись із думкою В. В. Зуй про наявність недосконалостей правового регулювання кібербезпеки в Україні, для подолання яких «по-перше, необхідно формування уніфікованого понятійно-термінологічного апарату у сфері кібербезпеки (оборони), по-друге, погодження з термінологією чинного українського законодавства та міжнародних актів (можливо ухвалення кодифіковано акту). По-третє, має місце недостатній рівень санкцій за інформаційні правопорушення» [15, с. 235].

На шляху імплементації загальних стандартів кібербезпеки у 2017 році набрав чинності Закон України «Про основні засади забезпечення кібербезпеки України». Вказаний Закон «визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження

державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки». Закон має опосередковане значення саме для морської кібербезпеки, проте передбачає створення національної системи кібербезпеки, запровадження стандартів кіберзахисту критичної інфраструктури, до якої належать морські порти, обмін інформацією про кіберзагрози на міжнародному рівні та співпрацю з іноземними партнерами, що сприяє гармонізації національних підходів із глобальними практиками у сфері кіберзахисту [16].

Станом на 2025 рік в Україні діє затверджена у 2021 році Президентом України Стратегія кібербезпеки України, одним з пріоритетів якої визначено європейську і євроатлантичну інтеграцію у сфері кібербезпеки та прагматичне міжнародне співробітництво (ціль В.3) з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками [17].

Важливим міжнародним актом «м'якого права» морської кібербезпеки є Рекомендації з кібербезпеки на борту суден, розроблені міжнародними неурядовими організаціями ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss у 2021 році. Як важливий інструмент для формування стратегії захисту морського транспорту від кіберзагроз документ містить низку практичних рекомендацій, спрямованих на підвищення рівня кіберстійкості торговельних морських суден. Основною метою Рекомендацій є допомога судовласникам, операторам суден та екіпажам у забезпеченні цілісності, конфіденційності та доступності даних, а також безперервності функціонування судових систем у цифровому середовищі. Імплементація положень Рекомендацій сприятиме підвищенню стійкості морського торгового флоту до кіберзагроз, забезпечить безпеку життєдіяльності екіпажу, захист навколишнього середовища та безперервність логістичних процесів [18].

Висновки. Кібербезпека торговельного мореплавства поступово перетворюється на важливу складову міжнародного морського права, однак ця підгалузь ще не має чітко структурованої правової бази.

Незважаючи на відсутність універсального міжнародного договору з ключову роль у розробці міжнародного права морської кібербезпеки відіграє Міжнародна морська організація. Зокрема, основу для інтеграції управління кіберризиками у систему безпеки судноплавства становлять положення Циркуляру MSC-FAL.1/Circ.3 та Резолюції MSC.428(98), які є інкорпорованими до Міжнародного кодексу управління безпекою – невід’ємної частини Міжнародної конвенції про охорону людського життя на морі 1974 року (SOLAS).

Україна як держава-учасниця вказаної Конвенції формально зобов’язана імплементувати відповідні міжнародні стандарти морської кібербезпеки у національне законодавство, проте національне правове регулювання у цій сфері залишається фрагментарним. Наказ Міністерства транспорту України «Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті» та Закон України «Про основні

засади забезпечення кібербезпеки України», хоча і містять окремі положення, релевантні для морської галузі, не забезпечують комплексного підходу до протидії кіберзагрозам у морському секторі.

Для подолання окреслених викликів доцільно вжити таких заходів:

1. Імплементувати у національне законодавство вимоги Директиви Європейського парламенту та Ради № 2022/2555 (NIS-2), які стосуються вжиття заходів з управління кіберризиком, повідомлення правоохоронних органів про наявність загроз кібербезпеці.

2. Розробити та прийняти окремий нормативно-правовий акт (або внести відповідні зміни до КТМ України та Закону України «Про морські порти України»), що регламентуватиме питання морської кібербезпеки відповідно до міжнародно-правових стандартів.

3. Забезпечити гармонізацію термінологічного апарату у сфері морської кібербезпеки із міжнародними стандартами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. MCAD Maritime Cyber Attack Database. *NHL Stenden*. URL: <https://maritimecybersecurity.nl/listview>
2. What is Cybersecurity? *U.S. Department of Homeland Security*. URL: <https://www.cisa.gov/news-events/news/what-cybersecurity>
3. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures: resolution. UN General Assembly. 21 December 2009, A/RES/64/211. *UN Digital Library*. URL: <https://docs.un.org/en/A/RES/64/211>
4. International Convention for the Safety of Life at Sea, 1974. *United Nations Treaty Collection*. URL: <https://surl.li/liymfm>
5. Міжнародна конвенція про підготовку і дипломування моряків та несення вахти 1978 року : Міжнародна морська організація; Конвенція, Міжнародний документ від 07.07.1978. URL: https://zakon.rada.gov.ua/laws/show/995_053#Text
6. Convention on International Maritime Organization (1948). *United Nations Treaty Collection*. URL: <https://surl.li/dsjpqy>
7. International Safety Management (ISM) Code. *International Maritime Organization*. URL: <https://surl.li/ttkajb>
8. Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3/Rev.3 (4 April 2025). *International Maritime Organization*. URL: <https://surl.li/cnovmz>
9. Maritime cyber risk management in safety management systems. RESOLUTION MSC.428 (98) (16 June 2017). URL: <https://surl.li/yudhwd>
10. Конституція України : Конституція, Закон від 28.06.1996 № 254к/96-ВР. URL: <https://surli.cc/ckmopo>
11. Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті : Мінтранс України; Наказ, Положення від 20.11.2003 № 904. URL: <https://zakon.rada.gov.ua/laws/show/z1193-03#Text>
12. Кодекс торговельного мореплавства України : Кодекс України; Закон, Кодекс від 23.05.1995 № 176/95-ВР. URL: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>
13. Про морські порти України : Закон України від 17.05.2012 № 4709-VI. URL: <https://zakon.rada.gov.ua/laws/show/4709-17#Text>
14. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng>
15. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. *Правове забезпечення адміністративної реформи*. 2022. № 4. С. 231–235.
16. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
17. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

18. The Guidelines on Cyber Security Onboard Ships. Version 4 (2019). Produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss. BIMCO. URL: <https://surl.lu/bnktre>

Веремчук В.С. ПРОБЛЕМАТИКА ІМПЛЕМЕНТАЦІЇ МІЖНАРОДНО-ПРАВОВИХ СТАНДАРТІВ МОРСЬКОЇ КІБЕРБЕЗПЕКИ У НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО УКРАЇНИ

У статті досліджується проблема імплементції міжнародних стандартів морської кібербезпеки у національне законодавство України в умовах стрімкої автоматизації морської галузі. Автор звертає увагу на зростання кіберзагроз у сфері морського транспорту, які можуть спричинити серйозні наслідки для безпеки судноплавства, довкілля, економіки та людського життя.

Визначено, що забезпечення кібербезпеки у морській сфері неможливе виключно на національному рівні, що вимагає гармонізації вітчизняного правового регулювання з міжнародними нормами.

Проаналізовано основні міжнародні акти, які мають значення для формування правових засад морської кібербезпеки, зокрема Міжнародну конвенцію з охорони людського життя на морі 1974 року (SOLAS), акти Міжнародної морської організації (IMO) – Міжнародний кодекс управління безпекою, циркуляри MSC-FAL.1/Circ.3, резолюцію MSC.428(98), а також Рекомендації з кібербезпеки на борту суден, розроблені міжнародними неурядовими організаціями ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC та SYBAss.

Встановлено, що хоча Україна є учасницею Міжнародної Конвенції з охорони людського життя на морі 1974 року (SOLAS), національне законодавство, зокрема Кодекс торговельного мореплавства України, Закон України «Про морські порти України» та інші акти національного морського права, не враховують аспектів морської кібербезпеки. Проаналізовано чинні нормативно-правові акти, які частково регламентують відповідні питання, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», Наказ Міністерства транспорту України «Про затвердження Положення про систему управління безпекою судноплавства на морському і річковому транспорті».

Автор підкреслює наявність нормативних прогалин, інституційної фрагментації та відсутності системної підготовки персоналу у сфері морської кібербезпеки. Запропоновано імплементцію положень Директиви Європейського парламенту та Ради № 2022/2555 про заходи для високого загального рівня кібербезпеки (Директива NIS-2), а також розробку уніфікованого правового інструменту, який би забезпечив комплексне регулювання питань морської кібербезпеки на національному рівні з урахуванням міжнародних стандартів.

Ключові слова: кібербезпека, кіберзагрози, імплементція, морське право.

Veremchuk V.S. THE ISSUE OF IMPLEMENTING INTERNATIONAL LEGAL STANDARDS OF MARITIME CYBERSECURITY INTO THE NATIONAL LEGISLATION OF UKRAINE

The article addresses the increasingly urgent issue of maritime cybersecurity in the context of global digitalization, automation, and the integration of information and communication technologies and artificial intelligence in the maritime transport sector. These technological advancements, while offering operational efficiencies, have also exposed maritime infrastructure – including vessels and port facilities – to significant cyber threats. Cyberattacks, unauthorized access to navigation and control systems, and breaches of confidential data may lead to critical consequences for safety of navigation, environmental protection, and human life.

Given the inherently international nature of merchant shipping and the borderless characteristics of cyberspace, the article highlights the need for transnational legal responses and stresses the importance of harmonizing Ukraine's domestic maritime legislation with international cybersecurity frameworks. The article notes that the current Ukrainian maritime legal system lacks comprehensive regulation in this area, making the process of implementing international maritime cybersecurity standards both complex and pressing.

The study defines maritime cybersecurity as an emerging subfield of international maritime law that is rapidly gaining prominence. It surveys the absence of a binding universal treaty on maritime cybersecurity and analyzes the role of key international actors, particularly the United Nations (UN) and the International Maritime Organization (IMO), in developing normative frameworks. Reference is made to UN General Assembly Resolution 64/211 (2009), which emphasizes the strategic importance of cybersecurity and urges states to adopt national cybersecurity strategies.

The article critically assesses the limitations of existing international legal instruments, such as the SOLAS Convention (1974), the ISPS Code, and the STCW Convention (1978), which provide only general security guidelines without addressing cybersecurity in a systematic manner. The ISM Code, made mandatory under SOLAS Chapter IX, together with IMO Circular MSC-FAL.1/Circ.3 and Resolution MSC.428(98), is presented as a legal foundation for integrating cybersecurity risk management into safety management systems.

While these instruments are considered part of Ukrainian law by virtue of Article 9 of the Constitution of Ukraine and Ukraine's accession to SOLAS, national implementation remains fragmented. Ukraine's Ministry of Transport Order No. 904 (2003) mandates safety management systems on vessels but does not explicitly address cyber risk. Moreover, key legislative acts such as the Merchant Shipping Code of Ukraine and the Law of Ukraine On Seaports of Ukraine remain silent on cybersecurity issues.

The article identifies several core challenges: the absence of legal provisions regulating interagency cooperation in the event of maritime cyber incidents; lack of mandatory cybersecurity training for seafarers; and the insufficient integration of international cybersecurity principles into Ukrainian maritime law. It argues for the urgent

implementation of the EU's NIS-2 Directive (2022/2555), which establishes a high common level of cybersecurity across critical infrastructure sectors, including maritime transport.

The author supports the opinion that Ukraine must adopt a unified legal terminology in the field of cybersecurity, align national terminology with international standards, and increase legal sanctions for cyber offenses. The adoption of the Law of Ukraine On the Basic Principles of Ensuring Cybersecurity of Ukraine (2017) and the Cybersecurity Strategy of Ukraine (2021) are recognized as positive steps toward establishing a national cybersecurity architecture that facilitates international cooperation and resilience against cyber threats.

Finally, the article underscores the importance of non-binding yet influential international instruments, such as the Guidelines on Cyber Security Onboard Ships (2021), developed by a coalition of maritime NGOs. These guidelines offer practical tools to improve cyber resilience of commercial vessels and support continuous operations in the digital maritime environment.

Key words: cybersecurity, cyber threats, implementation, maritime law.