УДК 341.225.5:004.056
DOI https://doi.org/10.32782/2304-1587/2024-26-1(38)-2

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ У МОРСЬКІЙ ГАЛУЗІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Веремчук Владислав Сергійович
викладач кафедри загальноправових дисциплін
та міжнародного права,
Одеський національний університет ім. І. І. Мечникова
ORCID: https://orcid.org/0009-0001-3618-2630

Стаття присвячена дослідженню проблематики міжнародно-правового регулювання захисту інформації у морській сфері. У статті здійснюється огляд існуючих міжнародних правових механізмів, покликаних забезпечувати кібербезпеку морської галузі та торговельного мореплавства. На базі аналізу сучасних праць вчених, фахівців з кібербезпеки та міжнародного морського права виокремлюються виклики та проблеми, пов'язані з кіберзагрозами та кібератаками на автоматизовані системи морських суден, портів, логістичних компаній, які зумовлюють виклик перед міжнародним морським співтовариством для реалізації ефективних заходів захисту від кіберзагроз у морській галузі. З урахуванням стрімкого розвитку інформаційних технологій, що зумовлюють ефективність морських перевезень, стаття сприяє більш глибокому розумінню проблеми кібербезпеки в морській галузі, у тому числі у контексті визначення категорій зловмисників із їх мотивами та крізь призму негативних наслідків успішних кібератак. Приділено увагу ролі міжнародних неурядових організацій, зокрема Міжнародної морської організації (ІМО) у розробці міжнародно-правового регулювання морської кібербезпеки. Визначено роль та значущий вплив міжнародних актів «м'якого права», розроблених під егідою Міжнародної морської організації, асоціацій судновласників, суднобудівельників, перевізників морських вантажів на розробку основних заходів із забезпечення кібербезпеки морського транспорту. У статті робиться висновок про існування прогалин у міжнародному морському праві в частині регулювання морської кібербезпеки та обґрунтовано думку про необхідність розробки та прийняття універсального міжнародного договору з морської кібербезпеки.

Ключові слова: *міжнародно-правове регулювання, морська галузь, морське судно, кібербезпека, морський кіберризик, кіберзагроза, кібератака, управління кіберризиком.*

Veremchuk Vladyslav. International Legal Regulation of Cyber Security in the Maritime Industry: The Current State and Prospects for Development

The article is devoted to the study of the problems of international legal regulation of information protection in the maritime industry. The article reviews existing international legal mechanisms designed to ensure cybersecurity of the maritime industry and merchant shipping. Based on the analysis of modern works of scientists, specialists in cybersecurity and international maritime law, challenges and problems related to cyber threats and cyber-attacks on automated systems of ships, ports, and logistics companies are identified, which cause a challenge to the international maritime community to implement effective protection measures against cyber threats in the maritime industry. Considering the rapid development of information technologies, which determine the efficiency of maritime transportation, the article contributes to a deeper understanding of the problem of cybersecurity in the maritime industry, including in the context of determining the categories of attackers with their motives and through the prism of the negative consequences of successful cyber attacks. The author draws the attention to the role of international non-governmental organizations, in particular the International Maritime Organization (IMO) in the development of international legal regulation of maritime cybersecurity. The role and significant influence of soft law developed under the auspices of the International Maritime Organization, associations of shipowners, shipbuilders on the development of basic measures to ensure cybersecurity of maritime transport are determined.The author comes to the conclusion about the gaps in international maritime law in terms of maritime cyber security regulation and substantiates the opinion regarding the need to develop and adopt a universal international treaty on maritime cyber security.

Key words: *international legal regulation, maritime industry, sea vessel cybersecurity, maritime cyber risk, cyber threat, cyber-attack, cyber risk management.*

Вступ. Вислів «моря з'єднують країни, які вони роз'єднують» повною мірою відображає значення торговельного мореплавства у сучасному світі, адже важко уявити собі функціонування світової економіки без морського транспорту, саме за допомогою якого здійснюються перевезення вантажів та пасажирів, промислова, видобувна діяльність тощо. Розвиток інформаційних технологій у морській сфері привносить революційні зміни, підвищуючи ефективність, безпеку та стійкість морських операцій, зокрема, сучасні інформаційні технології дозволяють оптимізувати проектування нового судна, його будівництво, забезпечити безпечну експлуатацію судна, обмін інформацією, пришвидшити процеси перевалки вантажів у портах та терміналах і, як наслідок, зробити морські перевезення дешевшими. Більш того, автоматизація дозволяє реалізувати проекти автономних морських суден (Maritime autonomous surface ship), які не потребують присутності екіпажу на борту та можуть керуватися віддалено з берегових центрів управління.

Разом із очевидними перевагами автоматизації для морської галузі актуальним стає питання захисту інформації (кібербезпеки) зі створенням відповідної міжнародно-правової бази з метою протидії несанкціонованому доступу з боку сторонніх осіб із подальшим завданням шкоди.

Матеріали та методи. До матеріалів дослідження слід віднести теоретичні положення, які визначають актуальні аспекти морської кібербезпеки та надають пропозиції для розвитку правового регулювання вказаних питань; статистичні дані, які відображають випадки морських кібератак, а також положення міжнародних конвенцій та актів «м'якого» права у формі рекомендацій Міжнародної морської організації та асоціацій представників морської галузі.

Дослідженням питань кібербезпеки на морі займаються як іноземні, так і українські фахівці, праці яких присвячені аналізу не тільки викликів і ризиків, що виникають внаслідок кіберзагроз, а й правових проблем, пов'язаних із впровадженням практик з управління морськими кіберризиками у експлуатацію морських суден та портових споруд. Серед них: В. Г. Пядишев, Ю.В. Даус, М.Є. Даус, О.І. Полікаровських, Д.Г. Ларін, А.О. Трофименко, С.Б. Майданевич, Т.О. Войченко, З.Я. Дорофєєва, D. Dimitrios, Juan Ignacio Alcaide, T. Walters, L. Graham та інші.

Методологічна основа дослідження визначається використанням сучасних наукових методів, таких як метод системно-функціонального аналізу, за допомогою якого було визначено основні структурні елементи морської кібербезпеки та охарактеризовано міжнародно-правове регулювання забезпечення кібербезпеки у морській галузі. Герменевтичний метод дозволив охарактеризувати коло потенційних зловмисників, які посягають на морську кібербезпеку, включно з їх мотивами та цілями. Метод аналізу та синтезу сприяв формулюванню висновків на підставі норм міжнародного права, рекомендацій Міжнародної морської організації та доктринальних напрацювань експертів з морської кібербезпеки.

Мета дослідження полягає у виявленні відповідності чинного міжнародно-правового регулювання необхідному рівню захисту інформації у морській галузі, виявленні прогалин та наданні власних пропозицій щодо вдосконалення регулювання питань кібербезпеки міжнародним морським правом.

Результати. Необхідність забезпечення міжнародно-правового регулювання кібербезпеки у морській галузі зумовлена невпинністю процесу автоматизації морських суден, портових споруд та впровадження електронних баз даних, що є потенційно вразливими для кібератак. У цьому контексті слід погодитись із думкою Д. Дімітріоса (D. Dimitrios), який стверджує, що «чим вищим буде ступінь автоматизації морського судна, тим вищим буде й ризик кібератак» [1].

За визначенням Міжнародного союзу телекомунікацій (ITU), кібербезпека – це набір інструментів, політики, концепцій безпеки, гарантій безпеки, рекомендацій, методів управління ризиками, дій, навчання, передового досвіду, страхування та технологій, які можна використовувати для захисту активів організації та користувачів в кіберсередовищі. Інфраструктура кібербезпеки — це підключені обчислювальні пристрої, користувачі, послуги або програми, системи зв'язку, мультимедійні комунікації та інформація у повному обсязі передається або зберігається в кіберсередовищі [2].

Одним із основних напрямів морської кібербезпеки є протидія організованим кібератакам. За визначенням Х. Алкайде (Juan Ignacio Alcaide), «кібератаки є незаконними діями, які здійснюються через комп'ютерні канали або спрямовані на знищення і пошкодження комп'ютерів, Інтернет-мереж, а також системи управління» [3].

Експерти програми Європейського Союзу CyberRoad визначають поширені типи кібератак: розсилка спаму; схема фішингу; шпигунське програмне забезпечення; шкідливе програмне забезпечення (віруси); ботнет; програми-вимагачі; невміла поведінка операторів; фізичне пошкодження систем [4].

Трофименко А.О., Майданевич С.Б наголошують на необхідності « чітко визначити зміст та класифікацію загроз інформаційній безпеці мореплавства. Таке дослідження дозволить на законодавчому рівні розмежувати різні види загроз інформаційної безпеці мореплавства та вдосконалити механізм державної протидії цим викликам» [4, с. 186].

Як зазначає Т. Уолтерс (T. Walters), партнер юридичної компанії HFW, «результати досліджень показують, що хоча морська кібербезпека покращується, галузь залишається легкою мішенню. Судновласники зазнають більшої кількості кібератак, ніж будь-коли, а вартість збитків від атак і вимоги про виплату викупу різко зросли. А оскільки використання технологій продовжує зростати у всіх аспектах судноплавства – від суднових мереж до морських установок та берегових центрів управління – зростає і ймовірність порушень кібербезпеки» [5].

Так, у квітні 2016 року влада Республіки Корея повідомила, що близько 280 торговельних суден були змушені повернутися до портів через кібератаку на навігаційні системи, внаслідок якої спостерігалося переривання GPS-сигналу та отримання недостовірної інформації щодо місцезнаходження цих суден [6].

У грудні 2022 року було зафіксовано кібератаку на автоматизовані системи порту Лісабон, що мало наслідком отримання зловмисниками конфіденційної інформації від адміністрації порту, у тому числі фінансової звітності, контрактів, суднових ролей, судових журналів тощо [7].

У 2023 році класифікаційне товариство DNV заявило про кібератаку, внаслідок якої не функціонували сервери системи «ShipManager», що спричинило перешкоди в управлінні близько тисячею суден по всьому світу, що становить близько 15% флоту компанії [8].

Здається, зазначені вище випадки становлять лише меншу частину з відомих кібератак у морській галузі. При цьому стає очевидним, що кібератаки становлять загрозу як для систем обміну інформацією у портах та компаніях, виходу з ладу інфраструктури портів, так і безпосередньо для систем управління морськими суднами, що може призвести до наслідків у вигляді аварії та загибелі судна із завданням супутньої шкоди іншим суднам та береговим спорудам. Особливим цей ризик вбачається для повністю автономних суден, оскільки відсутність екіпажу унеможливлює перехід на ручне управління судном та оперативне здійснення заходів із рятування судна.

Непрямими наслідками морських кібератак вважаємо затримку доставки вантажів у порт призначення, сповільнення операцій з перевалки у портах, порушення логістичних ланцюгів, здороження вартості страхових та логістичних послуг та підвищення вартості товарів для кінцевого споживача.

Зловмисники можуть намагатися отримати несанкціонований доступ до інформації з метою завдання фізичної шкоди судну та екіпажу, промислового шпигунства, недобросовісної конкуренції, так і з метою отримання матеріальної винагороди за розблокування автоматизованих систем, нерозголошення конфіденційної інформації тощо. Такий висновок можна сформулювати за данними експертів клубу взаємного страхування «The North of England P&I Association», які визначили наступні категорії зловмисників, що здійснюють несанкціонований доступ до інформації у морській галузі, їх мотивацію та цілі:

Категорія	**Мотивація**	**Цілі**
Активісти (у тому числі «ображені» співробітники)	Репутаційна шкода. Порушення операцій.	Знищення даних. Публікація чутливих даних. Розголос у ЗМІ.
Злочинці (у тому числі організована злочинність)	Фінансова вигода. Комерційне та промислове шпигунство.	Продаж вкрадених даних. Викуп викрадених даних. Непрацездатність систем. Організація шахрайських перевезень вантажів.
Опортуністи	Прийняти виклик.	Злам систем кіберзахисту. Фінансова вигода.
Держави та організації, що фінансуються державами. Терористи.	Політична вигода. Шпигунство.	Отримання розвідувальних даних. Завдання економічної шкоди.

[9].

Таким чином, наявність широкого кола зловмисників, цілей неправомірного доступу до інформації та обсягу шкоди, завданої таким доступом, зумовлює необхідність розробки міжнародних стандартів захисту інформації на морському транспорті та протидії кіберзлочинності.

Слід зазначити, що більшість чинних «морських» конвенцій, зокрема, Конвенція ООН з морського права (1982) [10], Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки судноплавства (1988) [11] не містять спеціальних положень, які регулюють захист інформації від кіберзагроз на морських суднах, що пояснюється часом їх розробки та прийняття, коли ступінь автоматизації суден був мінімальним.

П. «е» ст. 3 Конвенції про боротьбу з незаконними актами, спрямованими проти безпеки судноплавства (далі – Конвенція) визначає, що «будь-яка особа вчинить злочин, якщо вона незаконно та навмисно руйнує морське навігаційне обладнання, або завдає йому серйозного пошкодження, або створює серйозні перешкоди його експлуатації, якщо будь-який такий акт може загрожувати безпечному плаванню судна» [11, с. 3].

Конвенція не визначає, у якій саме спосіб мають створюватися серйозні перешкоди експлуатації морського навігаційного обладнання, однак, виходячи з того, що кібератаки можуть бути здійснені проти програмного забезпечення суднового навігаційного обладнання, припинення або некоректна робота такого програмного забезпечення може кваліфікуватися як незаконний акт (злочин), спрямований проти безпеки судноплавства шляхом створення серйозних перешкод експлуатації навігаційного обладнання у розумінні Конвенції. Вказана Конвенція регулює питання встановлення юрисдикції держав щодо злочинів проти безпеки судноплавства та надання правової допомоги між державами-учасниками з вказаної категорії злочинів.

Враховуючи специфіку кіберзлочинності, особа, що вчиняє такі правопорушення, може перебувати у будь-якій державі світу, тому правила встановлення юрисдикції держав щодо притягнення до кримінальної відповідальності за вчинення кібератаки на морське судно можуть бути орієнтиром при здійсненні заходів з розшуку та притягнення до відповідальності таких зловмисників.

Міжнародний кодекс з охорони суден і портових засобів (ISPS Code), який є додатком до Конвенції про захист людського життя на морі (SOLAS 1974/1988), встановлює загальні вимоги, пов'язані з безпекою на морі та в портах, яких повинні дотримуватися уряди держав-учасників конвенції SOLAS, представники портової влади та судноплавних компаній, щоб відповідати Кодексу [12].

Кодекс вважається своєрідною відповіддю морської галузі на загрози, що виникли внаслідок терактів 11 вересня 2001 року у США, тому до мети Кодексу ISPS належить, зокрема, забезпечення вжиття адекватних та пропорційних заходів безпеки на морі, на борту суден та в портах.

Кодекс містить положення про рівні безпеки морського судна, обмін інформацією про морську безпеку, встановлення на борту систем сигналізації з метою оголошення тривоги під час виникнення інциденту з безпекою судна, а також містить інші норми, спрямовані на попередження несанкціонованого доступу на борт суден сторонніх осіб, пронесення на борт зброї, запалювальних, вибухових речовин тощо.

Таким чином, Кодекс має дуже опосередковане значення для забезпечення кібербезпеки на морських суднах і у портах лише у частині захисту електронного обладнання від стороннього доступу, пошкодження або знищення [12].

Тим не менш, некоректно було б стверджувати, що конкретні заходи щодо захисту інформації на морському транспорті залишаються поза межею міжнародно-правового регулювання і застосовуються виключно на розсуд судновласників або портової влади.

Помітну роль у регулюванні діяльності морської галузі відіграє Міжнародна морська організація (ІМО), яка є спеціалізованою установою ООН та відповідає за безпеку судноплавства та запобігання забрудненню моря та атмосфери суднами. Зазначається, що ІМО «є глобальним органом, що встановлює стандарти безпеки, захищеності та екологічних показників міжнародного судноплавства. Основна роль полягає у створенні нормативної бази для судноплавної галузі, яка була б справедливою та ефективною, універсально прийнятою та повсюдно реалізованою» [13].

Відповідно до п. «а» ст. 29 Конвенції про Міжнародну морську організацію 1948 року, «до обов'язків Комітету з безпеки на морі належить розгляд питань, що мають відношення до навігаційних засобів, конструкції та обладнання суден, укомплектування суден екіпажами з точки зору безпеки, правил щодо запобігання зіткненню суден, поводження з небезпечними вантажами, заходів та вимог безпеки на морі» [14, с. 29].

Важливим етапом у запровадженні регулювання захисту інформації у морській галузі стало ухвалення 7 липня 2022 року Комітетом з безпеки на морі ІМО Керівництва з управління морськими кіберризиками (MSC-FAL.1/Circ.3/Rev.2). У Керівництві представлені «рекомендації високого рівня для управління морськими кіберризиками для захисту судноплавства від поточних та нових кіберзагроз та вразливостей» [15].

Керівництво визначає морський кіберризик як міру, до якої технологічний актив може бути під загрозою через потенційну обставину чи подію, яка може призвести до збоїв у роботі судна, безпеці судноплавства внаслідок пошкодження та втрати інформації або систем управління судном [15].

Згідно з п. 2.1. Керівництва, вразливими до кіберризику є системи управління ходового містка, системи обробки і управління вантажем; системи управління рухом судна та силовою установкою; системи контролю доступу на судно; електронні системи обслуговування пасажирів [15].

До інфраструктури управління морськими кіберризиками (Розділ ІІІ Керівництва) віднесено виявлення, аналіз, оцінку та інформування про кіберризики, а також прийняття, запобігання, перенесення або пом'якшення їх до прийнятного рівня, враховуючи витрати та вигоди від дій, вжитих зацікавленими сторонами з метою підтримки безпечного та надійного судноплавства, стійкого до кіберризиків [15].

До загальних заходів забезпечення морської кібербезпеки віднесено:

- навчання та інформування екіпажу управлінню кіберризиками, визначення систем, активів, даних, які, у разі збою, створюють ризики для безпечної роботи судна;
- запровадження контролю кіберризиків та планування дій на випадок кіберзагрози для забезпечення безперервної роботи судна;
- своєчасне виявлення несанкціонованого доступу;
- запровадження заходів для забезпечення стійкості та відновлення систем управління судном, що є порушеними у наслідок кібератаки;
- резервне копіювання даних для швидкого відновлення роботи автоматизованих систем, що постраждали внаслідок кібератаки [15].

Наступним актом, покликаним захистити інформацію на морському транспорті, є Керівництво (Рекомендації) з кібербезпеки на борту суден (2021), видане ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC та SYBAss – міжнародними неурядовими організаціями- асоціаціями представників морської галузі [16], метою якого є покращення безпеки моряків, довкілля, вантажів та суден. Рекомендації спрямовані на допомогу в розробці належної стратегії управління морським кіберризиком згідно з відповідними правилами та передовою практикою на борту судна, акцентуючись на робочих

процесах, обладнанні, навчанні, реагуванні на кіберзагрози та управлінні відновленням пошкоджених систем [16].

Рекомендації представлені у вигляді 64-сторінкового документа, що певною мірою конкретизує положення Керівництва з управління морськими кіберризиками. Рекомендації пояснюють, чому та як слід керувати кіберризиками в контексті судноплавства; містять супровідну документацію, необхідну для проведення оцінки ризику, пояснюється роль кожного компонента кіберризику, опис усіх автоматизованих систем судна, які є потенційно вразливими до кіберризику. Додатково Рекомендації містять поради щодо реагування на кібератаки та як відновлюватися після них [16].

Висновки. Можна констатувати, що міжнародно-правове регулювання кібербезпеки у морській галузі станом на початок 2024 рік перебуває у стадії активного розвитку. Чинні міжнародні договори, які покликані забезпечити безпеку світового судноплавства, мають досить опосередковане відношення до захисту інформації на морському транспорті. Натомість, інші міжнародні акти, які регулюють захист інформації та персональних даних, не є застосовними у контексті міжнародного морського права з огляду на те, що, хоча існують подібності в питаннях морської кібербезпеки з кібербезпекою в цілому, коло суб'єктів, загрози і наслідки кібератак значно відрізняються через унікальну природу морської галузі.

Значний вплив на розвиток міжнародного регулювання морської кібербезпеки належить Міжнародній морській організації (IMO), яка ухвалює відповідні резолюції, та міжнародним неурядовим організаціям, які представляють інтереси судновласників та інших представників морської галузі, ухвалюючи відповідні рекомендаційні акти. Такі акти мають характер м'якого права, проте, вони можуть слугувати орієнтиром, моделлю для подальшої розробки міжнародних договорів. За таких умов слід вважати за доцільне активізацію співпраці держав під егідою ООН з метою розробки змін та доповнень до міжнародних договорів, які будуть покликані запровадити загальнообов'язкові міжнародні стандарти кібербезпеки у морській галузі задля забезпечення сталого розвитку морського транспорту та світової економіки.

Література:

1. Dimitrios D. Exploring the Issue of Technology Trends in the «Era of Digitalisation». *World Maritime Day Parallel Event*. At: Szczecin-Poland, 2018. URL:https://www.researchgate.net/publication/325877588_Exploring_the_Issue_of_Technology_Trends_in_the_Era_of_Digitalisation (дата звернення: 10.01.2024).

2. Definition of cybersecurity. *International Telecommunication Union (ITU).* URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (дата звернення: 12.01.2024).

3. Juan Ignacio Alcaide, Ruth Garcia Llave. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. 2020. Volume 45. Pages 547–554. URL: https://www.sciencedirect.com/science/article/pii/S2352146520302209 (дата звернення: 12.01.2024).

4. Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. *Водний транспорт*. № 1 (37). 2023. С. 179–188. URL: https://vt.duit.in.ua/index.php/home/article/view/267/224 (дата звернення: 12.01.2024).

5. Maritime Cyber Risk Report: Shipping industry remains «Easy target», pays average US $ 3.2. M in cyber-attacks. *HFW*. URL: https://www.hfw.com/Maritime-Cyber-Risk-Report-Shipping-Industry-Remains-Easy-Target (дата звернення: 12.01.2024).

6. Shipping industry vulnerable to cyber attacks and GPS jamming. *CNBS*. URL: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html (дата звернення: 12.01.2024).

7. Cyberattack Threatens Release of Port of Lisbon Data. *The Maritime Executive.* URL: https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data (дата звернення: 12.01.2024).

8. Cyber-attack on ShipManager servers – update. *DNV*. URL: https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931 (дата звернення: 12.01.2024).

9. Cyber Risk in Shipping: Loss Prevention Briefing for North Members Ships. July 2017. *North P&I Club*. URL: https://www.nepia.com/cyber-risks-in-shipping-lp-briefing (дата звернення: 12.01.2024).

10. United Nations Convention on the Law of the Sea (10 December 1982). *United Nations Organization*. *Treaty Series*. URL: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (дата звернення: 12.01.2024).

11. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (10 March 1988). *United Nations Organization*. *Treaty Series*. URL: https://treaties.un.org/doc/db/terrorism/conv8-english.pdf (дата звернення: 12.01.2024).

12. SOLAS XI-2 and the ISPS Code. *International Maritime Organization.* URL: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI 2%20ISPS%20Code.aspx (дата звернення: 12.01.2024).

13. Introduction to IMO. *International Maritime Organization*. URL: https://www.imo.org/en/About6/Pages/Default.aspx (дата звернення: 12.01.2024).

14. Convention on the International Maritime Organization (6 March 1948). *International Maritime Organization*. URL: https://www.imo.org/en/About/Conventions/Pages/Convention-on-the-International-Maritime-Organization.aspx (дата звернення: 12.01.2024).

15. Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3/Rev.2 (7 June 2022). *International Maritime Organization* URL: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (дата звернення: 12.01.2024).

16. The Guidelines on Cyber Security Onboard Ships. Version 4 (2019). Produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss. *Intermational Chamber of Shipping*. URL: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (дата звернення: 12.01.2024).

References:

1. Dimitrios D. Exploring the Issue of Technology Trends in the «Era of Digitalisation» (2018). *World Maritime Day Parallel Event*. At: Szczecin-Poland. Retrieved from: https://www.researchgate.net/publication/325877588_Exploring_the_Issue_of_Technology_Trends_in_the_Era_of_Digitalisation_

2. *Definition of cybersecurity*. (2020). International Telecommunication Union (ITU). Retrieved from: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

3. Juan Ignacio Alcaide, & Ruth Garcia Llave (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. Volume 45, pp. 547–554. Retrieved from: https://www.sciencedirect.com/science/article/pii/S2352146520302209.

4. Trofymenko, A.O., Maydanevych, S.B., Voychenko, T.O., & Dorofeyeva, Z. (2023). Deyaki problemni pytannya vprovadzhennia standartiv kiberbezpeky na mors`komy transporti [Some problematic issues of implementation of cyber security standards in maritime transport]. *Vodnyi transport*. № 1 (37), p. 179–188. Retrieved from: https://vt.duit.in.ua/index.php/home/article/view/267/224 [in Ukrainian].

5. *Maritime Cyber Risk Report: Shipping industry remains «Easy target», pays average US $ 3.2. M in cyber-attacks.* (2023). HFW. Retrieved from: https://www.hfw.com/Maritime-Cyber-Risk-Report-Shipping-Industry-Remains-Easy-Target.

6. *Shipping industry vulnerable to cyber attacks and GPS jamming*. (2017). CNBS. Retrieved from: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html.

7. *Cyberattack Threatens Release of Port of Lisbon Data*. (2022). The Maritime Executive. Retrieved from: https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data.

8. *Cyber-attack on ShipManager servers – update*. (2023). DNV. Retrieved from: https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931.

9. *Cyber Risk in Shipping: Loss Prevention Briefing for North Members Ships*. (2017). North P&I Club. Retrieved from: https://www.nepia.com/cyber-risks-in-shipping-lp-briefing.

10. United Nations Convention on the Law of the Sea (10 December 1982). *United Nations Organization*. *Treaty Series*. Retrieved from: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

11. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (10 March 1988) *United Nations Organization*. *Treaty Series*. Retrieved from: https://treaties.un.org/doc/db/terrorism/conv8-english.pdf.

12. SOLAS XI-2 and the ISPS Code (2002). *International Maritime Organization.* Retrieved from: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI 2%20ISPS%20Code.aspx.

13. *Introduction to IMO.* (2022). International Maritime Organization. Retrieved from: https://www.imo.org/en/About/Pages/Default.aspx.

14. Convention on the International Maritime Organization (6 March 1948). *International Maritime Organization*. Retrieved from: https://www.imo.org/en/About/Conventions/Pages/Convention-on-the-International-Maritime-Organization.aspx.

15. Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3/Rev.2 (7 June 2022). *International Maritime Organization* Retrieved from: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

16. *The Guidelines on Cyber Security Onboard Ships. Produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss*. (2019). Intermational Chamber of Shipping. Retrieved from: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf.