

УДК: 341.225.5:347.8:349.6

DOI <https://doi.org/10.24144/2307-3322.2025.92.2.38>

ПРАВОВІ ВИКЛИКИ КІБЕРБЕЗПЕКИ ЯК ФАКТОРА ЕКОЛОГІЧНОЇ БЕЗПЕКИ МОРСЬКОГО СЕРЕДОВИЩА

Борщевська О.М.,
*кандидат юридичних наук, доцент,
доцент кафедри національного та міжнародного права
Одеського національного морського університету,
член комітету конституційного правосуддя та прав людини
Ради адвокатів Одеської області
ORCID: 0000-0003-2549-429X*

Борщевська О.М. Правові виклики кібербезпеки як фактора екологічної безпеки морського середовища.

У статті розглянуто проблему забезпечення кібербезпеки у морському судноплаванні як складову системи екологічної безпеки морського середовища, оскільки у контексті зростання складності морських інформаційно-комунікаційних систем особливої ваги набуває питання формування комплексної правової моделі протидії кіберзагрозам, спрямованої на мінімізацію екологічних ризиків. Діюча міжнародна нормативна база не повною мірою враховує специфіку кібератак, які можуть одночасно виступати джерелом техногенної небезпеки та чинником трансграничного забруднення морських акваторій.

Вказується на необхідність подальшої гармонізації правових стандартів, удосконалення механізмів розподілу відповідальності між суб'єктами судноплавства та розроблення ефективних процедур реагування, які б інтегрували технічні, правові та екологічні вимоги в єдину систему управління ризиками.

Аналізуються міжнародно-правові акти, що регулюють управління морськими кіберризиками (Конвенція SOLAS-74, ISM Code, Резолюція MSC.428(98) Міжнародної морської організації), а також питання цивільно-правової відповідальності за шкоду, спричинену кібератаками на судові системи. Визначено методологічні підходи до дослідження явища кіберризиків як фактора екологічної небезпеки, обґрунтовано наявність правової колізії між принципом об'єктивної відповідальності судновласника та презумпцією вини третіх осіб у кіберінцидентах.

Наголошується на необхідності імперативного правового регулювання цифровізації та автоматизації морського судноплавства, що істотно змінює структуру глобальної транспортної системи, оскільки судна дедалі частіше оснащуються автономними системами управління, навігації, баласту, вантажних операцій, а також дистанційного зв'язку з береговими центрами управління.

Досліджується проблема розвитку технологічного прогресу, що супроводжується підвищенням кіберзагроз, здатних порушити роботу цих систем та призвести до масштабних екологічних наслідків.

Окреслюється необхідність впровадження на нормативному рівні систем розширеного виявлення загроз, що надасть змогу оперативно реагувати на аномалії руху судна, несанкціоноване втручання в датчики екологічного моніторингу чи спроби вплинути на системи автоматичного управління, підкреслюючи, що в умовах, коли морське середовище є об'єктом міжнародно-правової охорони, така рання діагностика загроз має важливе регуляторне значення.

Визначається, що кібербезпека судноплавства не лише технічне питання, а й складова міжнародної та екологічної безпеки. В умовах глобальної інтеграції транспортних і логістичних мереж, будь-який кіберінцидент може призвести до забруднення морського середовища, аварійних викидів нафтопродуктів, блокування портової діяльності або втрати контролю над автономним судном.

Ключові слова: кібербезпека у морському середовищі, судноплавство, екологічна безпека, кіберризик, кібератака, цивільно-правова відповідальність судновласника, міжнародне морське право, навколишнє середовище.

Borshchevska O.M. Legal challenges of cybersecurity as a factor in the environmental safety of the marine environment.

The article considers the problem of ensuring cybersecurity in maritime shipping as a component of the environmental safety system of the marine environment, since in the context of the growing complexity of maritime information and communication systems, the issue of forming a comprehensive legal model for countering cyber threats aimed at minimizing environmental risks is of particular importance. The current international regulatory framework does not fully take into account the specifics of cyberattacks, which can simultaneously act as a source of man-made danger and a factor in transboundary pollution of marine waters.

The need for further harmonization of legal standards, improvement of mechanisms for distributing responsibility between shipping entities and development of effective response procedures that would integrate technical, legal and environmental requirements into a single risk management system is indicated.

The international legal acts regulating the management of maritime cyber risks are analyzed (SOLAS-74 Convention, ISM Code, Resolution MSC.428(98) of the International Maritime Organization), as well as the issue of civil liability for damage caused by cyber attacks on ship systems. Methodological approaches to the study of the phenomenon of cyber risk as a factor of environmental danger are determined, and the existence of a legal conflict between the principle of objective liability of the shipowner and the presumption of fault of third parties in cyber incidents is substantiated.

The need for imperative legal regulation of the digitalization and automation of maritime shipping is emphasized, which significantly changes the structure of the global transport system, since ships are increasingly equipped with autonomous systems of control, navigation, ballast, cargo operations, as well as remote communication with shore control centers is emphasized.

The problem of technological progress, accompanied by an increase in cyber threats that can disrupt the operation of these systems and lead to large-scale environmental consequences, is studied.

The need to introduce advanced threat detection systems at the regulatory level is outlined, which will allow for a prompt response to vessel movement anomalies, unauthorized interference with environmental monitoring sensors, or attempts to influence automatic control systems, emphasizing that in conditions where the marine environment is an object of international legal protection, such early threat diagnosis is of important regulatory importance.

It is determined that shipping cybersecurity is not only a technical issue, but also a component of international and environmental security. In conditions of global integration of transport and logistics networks, any cyber incident can lead to pollution of the marine environment, accidental releases of oil products, blocking port activities, or loss of control over an autonomous vessel.

Key words: cybersecurity in the maritime environment, shipping, environmental security, cyber risk, cyber attack, civil liability of the shipowner, international maritime law, environment.

Постановка проблеми. Сучасна цифровізація морського судноплавства створює новий вимір екологічної небезпеки, зумовлений кіберризиками. Попри наявність міжнародних актів низки нормативних актів, їхні норми не забезпечують в повному обсязі інтеграції кібербезпеки до механізмів охорони навколишнього середовища. У цих умовах виникає потреба у комплексному аналізі взаємозв'язку між кібербезпекою та екологічною безпекою морського середовища, а також у виробленні правових механізмів мінімізації кіберзагроз, що мають потенціал спричинити екологічну шкоду. В ракурсі тематики статті необхідно визначити правову природу кіберризиків у контексті їхнього впливу на екологічну безпеку морського середовища; проаналізувати міжнародно-правові акти, що регулюють кібербезпеку судноплавства, на предмет їхньої відповідності вимогам охорони морського середовища; з'ясувати правові колізії між обов'язками судовласника щодо екологічної безпеки та специфікою кібератак як дій третіх осіб; оцінити роль людського фактору та цифрової компетентності персоналу у виникненні кіберінцидентів, що можуть мати екологічні наслідки; дослідити правовий статус планів реагування на кіберінциденти та їхню роль у запобіганні забрудненню моря; визначити місце фізичної безпеки морської інфраструктури у системі правового забезпечення екологічної безпеки; запропонувати модель комплексного кіберзахисту, здатну забезпечити виконання міжнародних екологічних стандартів і мінімізувати ризики шкоди морській екосистемі.

Метою статті є визначення правових викликів кібербезпеки як фактора екологічної безпеки морського середовища при морських перевезеннях з огляду на міжнародний характер таких пере-

везень, а також формулювання пропозицій щодо удосконалення практичного сегменту розвитку кібернетичної та екологічної безпеки саме при морських перевезеннях.

Стан опрацювання проблематики. Дослідження побудовано на міждисциплінарному підході, який поєднує норми міжнародного морського, екологічного та інформаційного права та дозволяє виявити обов'язки судновласників у сфері кіберзахисту, взаємозв'язок між кіберризиками суден і потенційними екологічними наслідками, проводить аналіз положень Резолюції ІМО MSC.428(98) «Maritime cyber risk management in safety management systems» [1] та законодавства про цивільно-правову відповідальність за шкоду від забруднення морського середовища.

Оскільки питаннями кібербезпеки як фактора екологічної безпеки морського середовища майже ніхто ще не займався при дослідженні теми статті опрацьовувалися праці вчених щодо дотримання правил як кібербезпеки, так і екологічної безпеки, на підставі яких можна визначити ступінь готовності суспільства до коректування вектору безпеки суднооплавства з огляду на дотримання кібербезпеки як фактору екологічної безпеки навколишнього середовища.

Виклад основного матеріалу. Підвищення кібербезпеки в сучасних умовах набуває особливого значення для сектору морської діяльності, оскільки саме кіберінциденти можуть стати пусковим механізмом масштабних екологічних катастроф. Вразливість суднових навігаційних систем, автоматизованих платформ, портової інфраструктури та морських енергетичних об'єктів створює новий спектр правових викликів, пов'язаних із забезпеченням екологічної безпеки морського середовища.

Перш за все, слід звернутися до самого поняття екологічної безпеки. Згідно з положеннями статей 16 та 17 Конституції України, екологічна безпека є складовою частиною національної безпеки України, рівень її забезпечення співвідноситься з рівнем забезпечення національної безпеки [2]. Так, стаття 50 Закону України «Про охорону навколишнього середовища» зазначає, що екологічна безпека – це такий стан навколишнього природного середовища, за якого забезпечується попередження погіршення екологічної обстановки та виникнення небезпеки для здоров'я людей [3].

Однак більшість науковців погоджуються, що дане визначення не розкриває всю сутність, не враховує основні аспекти та ознаки екологічної безпеки як комплексного поняття.

Одне з найбільш влучних визначень екологічної безпеки дав у своїй роботі В.А. Ліпкан. Він зазначає, що екологічна безпека – це складова національної безпеки, процес управління системою національної безпеки, за якого державними і недержавними інституціями забезпечується екологічна рівновага і гарантується захист середовища проживання населення країни і біосфери в цілому, атмосфери, гідросфери, літосфери і космосфери, видового складу тваринного і рослинного світу, природних ресурсів, збереження здоров'я і життєдіяльності людей і виключаються віддалені наслідки цього впливу для теперішнього і майбутніх поколінь [4, с. 261].

На жаль, дане визначення також не в повному обсязі охоплює комплексність та багаторівневість поняття екологічної безпеки. Окрім цього, слід зазначити, що хоча екологічна безпека частково є складовою частиною національної безпеки, тим не менш, на відміну від неї, наслідки порушення екологічної безпеки зазвичай можуть мати міжнародний характер та впливати на стан навколишнього середовища не лише однієї країни, а інколи й країн цілого регіону, як, наприклад, країн басейну Чорного моря.

Так, в політиці міжнародних морських компаній формується думка, яку висловлюють експерти, зокрема Л.М. Казінс та П.П. Залевський про те, що у контексті сталого розвитку морська кібербезпека відіграє життєво важливу роль у захисті морських екосистем та ресурсів [5]. Дійсно, кібератаки, спрямовані на морську інфраструктуру, можуть призвести до розливів нафти, забруднення та інших екологічних катастроф. І в цьому сенсі необхідно забезпечувати безпеку критично важливих систем, таких як системи навігації та управління, запобігаючи аваріям, які можуть завдати шкоди навколишньому середовищу. Тому значення дотримання кібербезпеки при морських перевезеннях та іншій діяльності в морегосподарському комплексі виходить за межі лише технічного аспекту, оскільки забезпечення належного рівня кіберзахисту є невід'ємною частиною охорони морського середовища і дотримання його екологічної безпеки.

Є.В. Савчук вважає безпеку мореплавства «важливою умовою охорони людського життя на морі, навколишнього середовища і невід'ємною частиною суднооплавства і торговельного мореплавства. Існуюча система її забезпечення пов'язана з міжнародним співробітництвом у цій сфері, встановленням і забезпеченням застосування технічних норм і стандартів» [6, с. 38].

К.Г. Матієнко та В.О. Допілка вказують, що «у поняття безпека мореплавства вкладається більш широкий зміст, ніж безаварійна експлуатація морських суден. Воно охоплює систему захо-

дів, спрямованих на збереження людського життя на морі, захист морських суден від небезпеки на морі, а також захист морського середовища від забруднення з суден» [7, с. 333].

Таким чином, захист морського середовища від забруднення є не лише екологічним імперативом, але й ключовою запорукою безпечного функціонування морського транспорту, запобігання техногенним катастрофам та збереження економічної рентабельності морських перевезень.

На сьогодні діє низка міжнародних договорів, що регулюють різноманітні аспекти забезпечення екологічної безпеки морського середовища – від загальних зобов'язань держав до встановлення відповідальності за спричинене забруднення.

Конвенція ООН з морського права 1982 р. (UNCLOS), в ст. 192 закріплює загальний обов'язок держав захищати та зберігати морське середовище, а у ст. 194 вимагає вживати заходів щодо запобігання, скорочення і контролю забруднення моря з будь-яких джерел [8].

Конвенція щодо запобігання забрудненню моря скидами відходів та інших матеріалів 1972 року зобов'язує Договірні сторони вживати ефективні заходи із попередження забрудненню морського середовища, спричиненого навмисним скиданням відходів та інших матеріалів, які можуть мати небезпеку для здоров'я людей, зашкодити живим ресурсам моря тощо. Тим не менш, Лондонська конвенція не поширює свою дію на ненавмисне скидання шкідливих відходів у процесі нормальної експлуатації суден [9].

Важливим міжнародним актом, спрямованим на припинення забруднення морського середовища нафтою та іншими шкідливими речовинами є Міжнародна конвенція по запобіганню забрудненню з суден 1973 року (далі – Конвенція MARPOL-73/78).

Стаття 1 Конвенції MARPOL-73/78 зобов'язує Сторони здійснювати відповідні заходи з метою запобігання забрудненню морського середовища шкідливими речовинами або стоками, що містять такі речовини [ст. 1]. Зокрема, ст. 2 Конвенції забороняє скидання шкідливих речовин з порушенням положень Конвенції, незалежно від причин, якими викликане таке скидання у формі витоків, видалення, розливу, протікання, відкачки, виділення або спорожнювання таких речовин [10].

Але вказані Конвенції виходили з уявлення про запобігання забрудненню моря, що спричинене традиційні загрозами, не враховуючі загрози, що виникають у контексті автоматизації морських суден.

Сучасна система управління морськими кіберризиками формувалася в межах діяльності Міжнародної морської організації (ІМО), яка розробила політичні та технічні стандарти для держав-членів. Поряд із очевидними економічними перевагами, автоматизація вимагає дотримання кібербезпеки – комплексу методів, технологій та політик, спрямованих на захист суден, морської інфраструктури та пов'язаних галузей від кіберзагроз та кібератак. Ефективна кібербезпека має вирішальне значення для попередження кібератак, які можуть завдати шкоди морському середовищу, призвести до економічних втрат та загроз безпеці.

Визначення управління морським кіберризиком подано в документах ІМО як «процес виявлення, аналізу, оцінки та інформування про ризики для морської кібербезпеки, а також їх прийняття, запобігання, передачу або зниження до прийнятного рівня» [11]. Ключовими актами в цьому контексті також є: Резолюція ІМО MSC.428(98) «Maritime Cyber Risk Management in Safety Management Systems» (2017) [12]; Міжнародний кодекс управління безпекою (ISM Code) [13]; Міжнародна конвенція з охорони людського життя на морі (SOLAS-74) [14].

Як вбачається з аналізу цих документів, зокрема, Резолюція MSC.428(98) зобов'язує судновласників інтегрувати управління кіберризиками в системи управління безпекою суден (SMS) відповідно до цілей International Safety Management Code, який встановлює міжнародний стандарт безпечної експлуатації суден, спрямований на запобігання аваріям та забрудненню морського середовища.

Обов'язок судновласників дотримуватись вимог Резолюції MSC.428(98) забезпечується інтегрованістю Міжнародного кодексу управління безпекою до Міжнародної конвенції з охорони людського життя на морі 1974 року (далі – Конвенція SOLAS-74) у якості Розділу IX Конвенції SOLAS-74, яка встановлює комплекс технічних та організаційних вимог щодо безпечної експлуатації суден [14].

Таким чином, вимоги кіберзахисту стають частиною механізму охорони навколишнього середовища, а їхнє недотримання може трактуватися як порушення міжнародних екологічних зобов'язань.

У контексті аналізу впливу кібербезпеки судна на екологічну безпеку моря, слід зазначити дослідження С.В. Засець, в якому вказується, що до основних систем торговельного судна, враз-

ливих до кібератак належать, зокрема, системи управління баластними операціями, вантажними операціями, системи контролю суднової енергетичної установки [15, с. 69].

Кібератака на бортові системи морського торговельного судна може мати наслідком аварійне скидання з борту нафтопродуктів або інших небезпечних для морського середовища речовин. Слід враховувати, що класичні засоби реагування на технічні збої (резервні механізми, ізоляція систем) у разі кібератак виявляються недостатніми, адже зловмисники можуть модифікувати дані датчиків і створити ілюзію нормального функціонування судна. У таких випадках екологічна шкода може виникнути непомітно для екіпажу.

Отже, кібербезпека прямо корелює з екологічною безпекою морського середовища, а її недотримання може бути кваліфіковане як непряма форма екологічного правопорушення.

За цих умов, постає важливе питання визначення суб'єкта відповідальності у ситуації, коли кібератака на судно спричинила екологічну шкоду, навіть за умови вжиття судновласником усіх належних заходів з управління морським кіберризиком та вірних дій екіпажу, спрямованих на уникнення забруднення навколишнього середовища.

В цьому контексті слід звернути увагу на ст.3 Міжнародну конвенцію про цивільну відповідальність за шкоду від забруднення нафтою 1969 року [16], яка встановлює презумпцію відповідальності власника судна за шкоду, спричинену забрудненням нафтопродуктами із можливістю звільнення від відповідальності якщо власник судна доведе, що шкода була повністю спричинена, зокрема, дією або бездіяльністю третіх осіб з наміром завдати шкоду.

З огляду на контекст цього нормативного документу постає певна правова колізія між принципом об'єктивної відповідальності судновласника (як носія екологічного ризику) та принципом вини третіх осіб (кіберзлочинців), які вчинили втручання в судові системи. Вирішення цієї колізії потребує уточнення критеріїв доведення «наміреності» кібератаки та її причинно-наслідкового зв'язку із забрудненням. Проблемним залишається також питання юрисдикції, адже кібератака може бути здійснена з території іншої держави.

Сучасна доктрина пропонує розглядати подібні інциденти як форс-мажорні обставини лише за умови, якщо судновласник доведе наявність сертифікованої системи управління кіберризиками відповідно до Резолюції MSC.428(98) та International Safety Management Code. У протилежному разі його бездіяльність у сфері кіберзахисту може розцінюватися як недбалість.

У цьому контексті сегментація мережі виступає не лише технічним, а й правовим інструментом превенції. Вона дозволяє локалізувати інциденти, що можуть вплинути на управління судном, системи контролю за рухом танкерів із небезпечними вантажами чи платформами видобутку енергоресурсів. Розділення інфраструктури на ізольовані сегменти зменшує ризик екологічних аварій, що в національних та міжнародних правових актах розглядаються як серйозні порушення екологічної безпеки.

Виходячи з вищевказаних нормативних актів слід зазначити, що ефективне управління морськими кіберризиками має включати декілька етапів, а саме: ідентифікацію вразливостей та оцінку систем управління баластом, навігацією, енергетикою; оцінку ризику, як встановлення ймовірності кіберінцидентів і їх можливих наслідків для навколишнього середовища; впровадження заходів контролю, зокрема, застосування технічних і процедурних бар'єрів у вигляді ізоляції мереж, багаторівневої аутентифікації та шифрування; можливості реагування та відновлення при формуванні планів дій у разі кібератаки, включаючи взаємодію з екологічними службами та береговими станціями. International Maritime Organization підкреслює, що управління кіберризиками повинно бути інтегрованим елементом системи управління безпекою суден, втому числі й екологічною безпекою.

Слід зазначити, що кібератаки на морську інфраструктуру мають потенційні ризики порушити міжнародні стандарти охорони довкілля, закріплені в Конвенції ООН з морського права (1982); Міжнародній конвенції з попередження забруднення з суден (MARPOL 73/78); Резолюціях ІМО щодо охорони морського середовища (MEPC). Тому необхідно мати на увазі, що кібератака може призвести до забруднення морського середовища. Водночас держави несуть обов'язок розслідування інциденту, обміну інформацією та відшкодування шкоди відповідно до принципу *polluter pays*.

Отже, можна визначити, що морська кібербезпека виступає профілактичним інструментом запобігання забрудненню морського середовища, а її забезпечення є елементом екологічної політики кожної держави.

Висновки. Отже, кібербезпека у судноплаванні є критичним фактором екологічної безпеки морського середовища в розрізі того, що міжнародні акти формують систему зобов'язань держав і судновласників щодо управління кіберризиками.

Зазначається, що захист морського середовища від забруднення є не лише екологічним імперативом, але й ключовою запорукою безпечного функціонування морського транспорту, запобігання техногенним катастрофам та збереження економічної рентабельності морських перевезень.

Визначається, що кібератаки на суднові системи можуть спричинити екологічну шкоду, яка прямо корелює з екологічною безпекою морського середовища.

Підкреслюється, що вимоги кіберзахисту стають частиною механізму охорони навколишнього середовища, а їхнє недотримання може трактуватися як порушення міжнародних екологічних зобов'язань.

Наголошується, що інтеграція кіберзахисту у стратегії екологічної безпеки має стати пріоритетом для держав, що прагнуть до сталого розвитку морської галузі.

Пропонується підвищувати підготовку персоналу у попередженні кіберінцидентів, оскільки неналежний рівень цифрової обізнаності стає фактором підвищеного правового ризику, адже дії членів екіпажу або працівників портів можуть призвести до порушення екологічних норм MARPOL, Конвенції ООН з морського права чи національного екологічного законодавства у разі інциденту, спричиненого фішингом або шахрайством.

Стверджується, що створення та регулярне оновлення плану реагування на інциденти має не лише технічну, а й правову природу. Такий план визначає порядок взаємодії між судновласником, портовою адміністрацією, контролюючими органами та екологічними службами, забезпечуючи оперативне запобігання шкоді морському середовищу та виконання обов'язків, передбачених міжнародним правом.

Зауважується, що фізична безпека критичної морської інфраструктури (портів, датчиків моніторингу, суднових систем управління тощо) також є важливою складовою правового забезпечення екологічної безпеки. Будь-яке несанкціоноване втручання може кваліфікуватися як порушення екологічного законодавства та міжнародних норм охорони моря.

Рекомендується своєчасна профілактика цифрових застосунків зменшує вразливість перед кібератаками, що можуть стати підставою для юридичної відповідальності судновласника або інфраструктурного оператора в разі виникнення шкоди навколишньому природному середовищу внаслідок кіберінциденту.

Отже, комплексність кіберзахисту стає необхідною умовою реалізації міжнародно-правових зобов'язань щодо охорони морського середовища. Такі заходи мають сформувати не лише технологічно стійку систему, а повинні забезпечити виконання екологічних і правових стандартів, спрямованих на мінімізацію ризиків кіберзагроз для морської екосистеми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Резолюція IMO MSC.428(98) «Maritime cyber risk management in safety management systems URL: <https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428%2898%29.pdf>.
2. Конституція України: Закон України від 28 червня 1996 року. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
3. Про охорону навколишнього середовища : Закон України від 25 червня 1991 року зі змінами та доповненнями. URL: <https://zakon.rada.gov.ua/laws/show/1264-12#Text>.
4. Ліпкан В. А. Національна безпека України : навч. посіб. К.: Кондор, 2008. 552 с.
5. Офіційний сайт компанії Darktrace. URL: <https://pollution.sustainability-directory.com/area/maritime-cybersecurity>.
6. Савчук Є.В. Проблеми забезпечення екологічної безпеки на морському транспорті. *International Scientific and Practical Conference "WORLD SCIENCE"* № 4(20), Vol. 1, April 2017, с. 37-38. URL: <https://journals.indexcopernicus.com/api/file/viewByFileId/418382>.
7. Допілко В.О., Матієнко К.Г. Правове регулювання відповідальності за забруднення навколишнього середовища при перевезенні небезпечних вантажів морем. Науковий вісник Ужгородського Національного Університету, 2021, с. 331–335. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/01/64.pdf>. DOI <https://doi.org/10.24144/2307-3322.2021.67.62>.

8. United Nations Convention on the Law of the Sea. URL: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.
9. Конвенція № 995_127 від 29.12.1972 Конвенція про запобігання забрудненню моря скидами відходів та іншими матеріалами. URL: http://zakon4.rada.gov.ua/laws/show/995_127.
10. Міжнародна конвенція по запобіганню забрудненню з суден 1973 року. URL: https://zakon.rada.gov.ua/laws/show/896_009#Text.
11. International Maritime Organization. Cyber Security. URL: <https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx>.
12. IMO Resolution MSC.428(98) «Maritime Cyber Risk Management in Safety Management Systems», 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).
13. International Safety Management Code (ISM Code). Resolution A. 741(18) adopted 04 November 1993. URL: [https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.741\(18\).pdf](https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.741(18).pdf).
14. International Convention for the Safety of Life at Sea (SOLAS), 1974, adopted 01 November 1974; Entry into force: 25 May 1980. 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).
15. Заєць С.В. Вразливість суднових систем до кібератак // System Genesis of the Economy. 2023. № 16. С. 67–73. URL: <https://desymp.promonograph.org/index.php/sge/article/download/sge16-01-017/781>.
16. International Convention on Civil Liability for Oil Pollution Damage (CLC, 1969), adopted 29 November 1969; entry into force: 19 June 1975; being replaced by 1992 Protocol: adopted: 27 November 1992; entry into force: 30 May 1996. URL: [https://www.imo.org/en/about/conventions/pages/international-convention-on-civil-liability-for-oil-pollution-damage-\(clc\).aspx](https://www.imo.org/en/about/conventions/pages/international-convention-on-civil-liability-for-oil-pollution-damage-(clc).aspx).