

МІЖНАРОДНЕ МОРСЬКЕ ПРАВО

УДК 341:347.8

DOI <https://doi.org/10.32782/ILA.2025.34.03>

БОРЩЕВСЬКА О. М.

кандидат юридичних наук, доцент,

доцент кафедри національного та міжнародного права

Одеського національного морського університету

ORCID: 0000-0003-2549-429X

КІБЕРНЕТИЧНА БЕЗПЕКА СУДНОПЛАВСТВА: МІЖНАРОДНО-ПРАВОВИЙ ТА НАЦІОНАЛЬНО-ПРАВОВИЙ АСПЕКТИ

Анотація. Актуалізація тематики кібернетичної безпеки судноплавства в її міжнародно-правовому та національно-правовому аспектах обумовлюється прогресом цифровізації майже всіх галузей життя людства. Цифровізація життя, в тому числі і судноплавства, створила певні прогресивні можливості з одного боку, а з іншого боку спровокувала певний ризик кіберризиків. Морські судна як автономні так і з екіпажем курсують як окремі кіберматеріальні системи, які є дуже вразливими як до зовнішніх матеріальних факторів, так і до нематеріальних факторів, зокрема, кібератак. Особливу значущість це питання набуває на сучасному етапі не тільки в умовах глобальної торгівлі, а й в умовах війни в Україні та інших світових збройних конфліктах, як елемент міжнародної та національної безпеки, яка включає повний перелік від воєнної та державної безпеки до екологічної безпеки, в тому числі на глобальному рівні.

Всеохоплююче впровадження діджитал технологій зумовлює виникнення відповідних відносин, які мають регулюватися правовими нормами, оскільки неврегульованість законодавством такого глобального сегменту технологій може мати тенденцію до вчинення дій, які будуть навмисно чи через недбалість порушувати права інших осіб.

Сучасні приклади кібератак ставлять під загрозу функціонування багатьох електронних реєстрів, доступу до баз даних, дистанційне управління процесами, зокрема повітряними та морськими суднами. Особливо це стосується забезпечення діяльності автономних суден.

У статті розглядається позиція міжнародної спільноти щодо забезпечення кібербезпеки у судноплаванні. Проаналізовано міжнародно-правову базу, стандарти та керівні документи, що регулюють кіберризик на морі. Наведено огляд національного нормативно-правового матеріалу, який імплементує або має імплементувати відповідні міжнародні норми. Порушено питання доцільності надання таким нормам імперативного (обов'язкового) характеру з метою досягнення регуляторної ефективності. Визначено, що впровадження міжнародних стандартів та норм з кібербезпеки у судноплавному секторі є критично важливим стратегічним

елементом інтеграції України у міжнародну спільноту. Запропоновано розробку та прийняття систематизованого національного нормативно-правового акта, який би забезпечив комплексне дотримання вимог кібербезпеки у судноплаванні.

Виокремлене питання дотримання національної, в тому числі, й екологічної безпеки через дотримання правил кібербезпеки. Оцінено необхідність створення спеціальної програми підготовки фахівців з кібербезпеки саме для судноплавства у вищих навчальних закладах.

Ключові слова: національна безпека, безпека судноплавства, кібербезпека, кіберінцидент, кібератака, кіберризик, судно, порти, екологічна безпека.

Постановка проблеми. Наразі через важелі економічної вигоди та подекуди, безпеки членів екіпажу, якщо йдеться про прохід судна через небезпечні ділянки морів та океанів, дуже активно розвивається електронавігація, технології щодо безпеки та зв'язку на судні, автоматизація процесів керування судном.

Слід зазначити, що судові системи та програми оновлюються під час здійснення рейсу судна через відкритий доступ до мережі Інтернету і це викликає ряд питань щодо забезпечення безпечної експлуатації судна.

Стан дослідження. Оскільки тематика досить нова то інноваційними дослідженнями в правовому полі з питань кібербезпеки займалося не таке велике коло вчених, але серед небагатьох слід зазначити наукові напрацювання В.Г. Пядишева, В.С. Веремчука, Б.М. Орловського, які аналізують міжнародний досвід організації кібербезпеки на борту суден в розрізі міжнародно-правових механізмів, які стосуються кібербезпеки мореплавства, але на жаль, не надають певних правових рекомендацій щодо закріплення технічних норм щодо кібербезпеки як загальнообов'язкового правила поведінки, що має певний механізм державного примусу та відповідно переведення таких норм у нормативно-правове закріплення з відповідними імперативами виконання.

Мета статті – дослідити позицію міжнародної спільноти щодо забезпечення кібербезпеки в судноплаванні та привести національний нормативно-правовий матеріал з цієї тематики у відповідність до міжнародних норм. При цьому визначити доцільність надання таким нормам імперативного характеру.

Визначити необхідність імплементації міжнародних норм та стандартів щодо кібербезпеки у судноплаванні як важливий стратегічний елемент інтеграції України в міжнародне співтовариство.

Надати пропозиції щодо розробки та прийняття систематизованого національного нормативно-правового акту щодо дотримання кібернетичної безпеки в судноплаванні.

Оцінити необхідність спеціальної підготовки фахівців з кібернетичної безпеки саме у судноплаванні в закладах вищої освіти.

Виклад основного матеріалу. Загальновідомо, що будь-які відносини для ефективного їх здійснення мають бути врегульовані на рівні законодавства з раціональним механізмом правового регулювання. Тому, метою статті є аналіз міжнародного законодавства у порівнянні з законодавством

України для визначення шляхів унормування існуючих рекомендаційних та технічних норм в систему імперативних нормативних актів, а також визначення кола відносин, які мають бути закріплені на рівні законодавства щодо кібербезпеки, зокрема в судноплаванні, з подальшим формуванням відповідної підгалузі морського права.

В цьому зв'язку слід звернути увагу, що дуже слушно зазначає В.М. Веремчук про те, що 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 [1, с.61]

Поряд з цим слід зауважити, що кібербезпека судна має визначатися як сукупність правових, організаційних, технічних та операційно-програмних заходів, що спрямовані на забезпечення стійкого, безпечного та безперервного функціонування всіх систем судна, що повинно включати запобігання несанкціонованому доступу до інформації, її знищенню, спотворенню тощо.

Кібербезпека на теперішній час стала невід'ємним елементом загальної системи забезпечення безпеки судна, зокрема, та судноплавання взагалі. Від забезпечення належного рівня кібербезпеки залежить недопущення чи вчасне виявлення кіберінцидентів, що можуть спричинити загрозу життю та здоров'ю екіпажу, безпеці судна, вантажу, в окремих випадках господарській діяльності власника судна, а також екологічній безпеці на морі.

З огляду на певне перспективне бачення кіберзагроз можна визначити окремі інциденти, які з розвитком глобалізації цифрових технологій, можуть, на жаль, розширяти коло таких правопорушень, а саме:

- фальсифікація чи інше втручання в картографічну інформацію, яка знаходиться в електронному вигляді;
- несанкціоноване оновлення програмного забезпечення через втручання кіберпіратів, що призводить до збоїв у процесі технічного обслуговування;
- знищення або спотворення даних з систем глобального навігаційного супутникового зв'язку.

Але, виходячи з того, що ІМО (Міжнародна морська організація) відносить лише наступні системи судна до найбільш вразливих судових систем, з боку суб'єктів кібератак, зокрема, системи ходового містка; системи обробки та управління вантажем; системи управління двигунами, машинами та енергоживленням; системи контролю доступу на судно; системи обслуговування пасажирів та екіпажу; публічні інтернет-мережі судна, призначені для використання пасажирями; адміністративні системи та мережі; системи зв'язку [2], можна говорити про те, що поза увагою залишаються певні опції щодо логістичних систем та портів.

Тому, з огляду на вищезазначене слід визнати, що кібербезпека судноплавання має становити вже не лише комплексний правовий інститут,

а виділятися в окрему підгалузь права, яка буде охоплювати регламентацію заходів із виявлення, попередження, реагування та усунення наслідків кіберзагроз, які спрямовуються на суднові інформаційні та навігаційні системи через інциденти, що впливають на доступність, цілісність або достовірність даних необхідних для повноцінного функціонування та життєдіяльності судна та екіпажу.

Через вищезазначене предмет правового регулювання підгалузі кібербезпеки судноплавства можна визначити як сукупність суспільних відносин, що пов'язані із правовим, організаційним, технічним та операційно-програмним заходами захисту суден, портів, логістичних та навігаційних шляхів та систем від кіберзагроз, які встановлюють відповідальність за кіберінциденти у судноплавстві через нанесення шкоди чи загрозу життю та здоров'ю екіпажу, безпеці судна, вантажу, в окремих випадках господарській діяльності власника судна, а також екологічній безпеці на морі.

Слід зазначити, що в міжнародній правовій практиці вже напрацьовано ряд документів, які регламентують в правовому полі такі відносини, але такі нормативні акти зазвичай носять рекомендаційний чи описово-правовий характер і не відбивають всіх необхідних заходів, правового регулювання, які необхідні для унеможливлення, недопущення чи перешкоджання кіберінцидентів, які мають носити імперативний характер та мати відповідні санкції.

Наприклад, Резолюція MSC.428(98) «Управління кіберризиками в морській галузі у межах систем управління безпекою»[3], яка ухвалена Міжнародною морською організацією (ІМО), визначає необхідність інтеграції управління кіберризиками до існуючих систем управління безпекою суден відповідно до вимог Міжнародного кодексу управління безпекою [4]. В ній також наголошується на необхідності підвищенні рівня обізнаності персоналу судноплавних компаній і членів екіпажу щодо актуальних кіберзагроз з метою забезпечення безпеки судна та захисту морського судноплавства загалом. Членів екіпажу просто інформують про можливі загрози, але не прописують належним чином інструментарій протидії.

У межах цієї Резолюції державам-членам ІМО рекомендується після 01 січня 2021 року забезпечувати врахування кіберзагроз у системах управління безпекою суден під час першої щорічної перевірки відповідності вимогам Міжнародного кодексу управління безпекою. Можна припустити, що кібербезпека визначається дійсно як невід'ємна частина загальної безпеки судноплавства, але питання щодо подальших річних перевірок залишається відкритим, бо кіберзагрози не мають прив'язки до календарного року.

З зазначеної вище дати управління кіберризиками стало обов'язковим елементом систем управління безпекою суден через що відсутність інформації про кіберризика в документації може бути визначена як порушення вимог Міжнародного кодексу управління безпекою, що тягне адміністративну відповідальність, яка передбачає навіть заборону виходу судна з порту.

ІМО рекомендує Посібник з кібербезпеки на борту суден [5], в якому визначається коло потенційних суб'єктів кібератак, а саме, активісти, включаючи незадоволених працівників; злочинні угруповання; опортуністи; держави та державні утворення; терористичні організації. Як бачиться з контексту цієї рекомендації, це мають бути потенційні суб'єкти, на яких слід звертати увагу, бо коло суб'єктів, які можуть спричинити кіберінциденти має бути визначено більш ширшим, оскільки це можуть бути будь-які особи, які є незадоволеним працівником, опортуністом тощо, а також можуть бути найманою особою, яка працює за гроші чи за іншу користь.

Цікавими є циркуляри MSC.1/Circ.1639 від 14 червня 2021 та MSC-FAL.1/Circ.3/Rev.3 від 04 квітня 2025 року Комітету з безпеки на морі Міжнародної морської організації, які носять також лише рекомендаційний характер, де державам-членам пропонується взяти до уваги рекомендації, що містяться у четвертій версії «Керівництва з кібербезпеки на суднах», яка підготовлена галузевими асоціаціями. В ньому рекомендується відповідним заінтересованим сторонам, включаючи судновласників, операторів та менеджерів, враховувати при необхідності цей посібник при розгляді кіберризиків на суднах відповідно до цілей та функціональних вимог Міжнародного кодексу управління безпекою, як це рекомендовано Резолюцією MSC.428(98) [6]. Наразі, в сучасних умовах, які існують у світі необхідно визначити імперативний характер таких норм, тобто не рекомендувати, а запровадити на нормативному рівні оцінку відповідності системи управління безпекою судноплавства вимогам кібербезпеки.

Попри наявність на міжнародному рівні ще певної кількості нормативних актів щодо кібернетичної безпеки в судноплавстві проблема ефективного врегулювання таких правовідносин все ще залишається досить важливою. Це відбувається через, як зазначалося, по-перше, рекомендаційний характер таких нормативних актів. По-друге, можна відмітити відсутність уніфікованої Конвенції з кібербезпеки в мореплавстві, а також певну сегментарність у регулюванні цих відносин між різними міжнародними морськими організаціями. По-третє, і це може виглядати основною перешкодою, неготовність держав, логістичних компаній та судновласників до практичного впровадження імперативних вимог щодо нівелювання кіберризиків в судноплавстві, а також складнощів з обміном інформацією про кіберінциденти на міжнародному рівні.

Незважаючи на ці недоліки, система міжнародних актів створює те загальне нормативне поле, у межах якого держави можуть формувати власну політику у сфері кібербезпеки у судноплавстві.

В національному законодавстві України також існують деякі нормативні акти про кібербезпеку та кіберризики, але ці норми, по-перше, не уніфіковані, а, по-друге, не мають саме цільового спрямування щодо судноплавства.

Так, профільний закон щодо кібербезпеки Закон України «Про основні засади забезпечення кібербезпеки України» [7] окреслює лише

основні принципи, термінологію та коло державних органів, що стосується цієї галузі, але не надає ані поняття кібербезпеки, у судноплаванні як галузі національного господарства, ані окремих вимог щодо кібербезпеки для судноплавання, логістичних компаній та портів.

Якщо говорити про ширше поняття безпеки, таке як національна безпека, то в Законі України «Про національну безпеку України» [8] кібербезпеку включено в перелік складових національної безпеки, але саме в сфері судноплавання прямо не визначено. Аналогічна ситуація з законами України «Про транспорт» [9] та «Про морські порти» [10], які спрямовані лише на управління транспортною інфраструктурою та інфраструктурою портів, але про регулювання питань пов'язаних з кібербезпекою в них не йдеться.

Щодо Кодексу торговельного мореплавання України [11], то він більш орієнтований на питання безпеки навігації, охорони без врахування киберризиків та закріплює безпеку судноплавання у векторі організації морських перевезень.

Навіть Стратегія кібербезпеки України на 2021-2025 роки [12] лише визначає морську інфраструктуру критичною, містить окремі загальні позиції щодо захисту критичної інфраструктури, але будь-які спеціальні вимоги щодо кібербезпеки у судноплаванні відсутні.

З огляду на такі прогалини в законодавстві щодо неврегульованості на достатньому законодавчому рівні правовідносин з дотримання кібернетичної безпеки в судноплаванні можна констатувати відсутність і правового зобов'язання ефективно реалізовувати політику кібербезпеки в системах управління безпекою суден, зокрема, і судноплавання взагалі.

Досі залишається повністю невирішеним питання створення та функціонування Єдиного органу національної кібербезпеки судноплавання в Україні, який би консолідував моніторинг кіберінцидентів в судноплаванні та проводив політику щодо дотримання кібербезпеки саме у судноплаванні і відповідно координував би свою діяльність з Центральними органами влади України.

Так, вважається за необхідне на рівні міжнародного законодавства, яке в подальшому має бути імплементоване в українське законодавство [13] підготувати нормативний акт, який би містив методологію оцінки кіберризиків. Такі технічні норми мають бути закріплені на міжнародному рівні, а в подальшому на рівні законодавства України як загальнообов'язкове правило поведінки, що має певний механізм державного примусу.

Тобто такі рекомендації та стандарти, що розроблені профільними фахівцями з кібербезпеки мають бути включені до складу нормативно-правових актів та мати структуру норми права: гіпотезу, диспозицію та санкцію з обов'язковим підкріпленням можливості застосування державного примусу для її дотримання.

Схематично можна навести приклад структури такого нормативно-правового акту щодо дотримання кібернетичної безпеки в судноплаванні.

Розділ перший присвятити загальним вимогам організаційного управління згідно рекомендаціям MSC.428 (98), що буде закріплювати поняття кібербезпеки у судноплаванні, необхідність наявності політики компанії з кібербезпеки, яка затверджена на рівні порту приписки судна чи судноплавної компанії; включення управління кіберризиками до документованої системи управління безпекою; визначення відповідальної особи, яка має право підпису і відповідні повноваження в порту (компанії, на судні); наявність реєстрів (інвентаризації) ІТ та ОТ-систем судна з позначенням відповідної критичності та контроль за оновленням цих реєстрів, відповідний періодичний аналіз кіберризиків.

Другий розділ може закріплювати дотримання технічних аспектів ІТ та ОТ-інфраструктури, які втілюють рекомендації IACS Rec, 166 IMO Guidelines v4 [14] такі як, наявність фізичної та логічної сегментації офісної та операційної мережі; обов'язкового контролю відділеного доступу з документацією сесій; зобов'язання щодо регулярного оновлення ПЗ з фіксацією часу; запровадження резервного копіювання критичних даних на ізольованих носіях; ведення журналу безпеки із моніторингом подій кіберінцидентів; постійна перевірка антивірусного ПЗ та відповідних систем; можливість процедури фізичного контролю доступу до ІТ-обладнання серверів та мережевих шаф; наявність окремої мережі для систем навігації, енергетики та камер безпеки.

Третій розділ може містити інструкцію-план реагування на кіберінциденти з певним нормативним описом процедур ідентифікації, реагування, відновлення систем та подальшого звітування; закріплення обов'язку кожного члену екіпажу знати порядок дій у разі кібератаки; вимоги проводити навчання та моделювання вправ з реагування на кібератаки; обізнаність щодо можливості звернення до відповідного органу, якій опікується кібернетичною безпекою в судноплаванні в даному регіоні, в даній компанії чи порту приписки судна.

Четвертий розділ має регламентувати питання підготовки та обізнаності екіпажу з обов'язковою наявністю не тільки підтверджуючих документів з зовнішніх навчань, а безпосередньо ознайомлення під особисте зобов'язання з системами реагування на кіберінциденти в безпосередній зоні роботи, а також дозволи щодо користування персональними пристроями з інтернет-підключенням.

В п'ятому розділі, серед іншого, необхідно зазначити питання сертифікації та документування розслідування кіберінцидентів та аналізу їх причин, визначення суб'єктів та рівнів відповідальності за правопорушення в галузі кібербезпеки судноплавання.

А шостий розділ присвятити безпосередньо заходам правового реагування на невиконання, неналежне виконання закріплених вище вимог чи дії, які мають прямий чи непрямий умисел на настання кіберінциденту, зокрема, чи спричинення ситуації яка загрожує настанням кібернебезпеки в цілому.

І ще одну велику проблему, яка не прямо залежить від поля правового регулювання, але, на яку також слід звернути увагу для розв'язання в подальшому це відсутність українського програмного забезпечення та відповідного обладнання для розвитку захисту кіберпростору.

В зв'язку з цим, як один з напрямків розвитку та посилення кібербезпеки в судноплаванні, є досить перспективним впровадження в закладах вищої освіти освітніх програм, які б поєднували та формували спеціальні компетенції здобувачів вищої освіти для отримання ними таких результатів навчання, які б дозволили випускниками бути конкурентноспроможними на ринку професій які стосуються поглибленої спеціалізації кіберзахисту, кібербезпеки та її нормативно-правового наповнення.

Висновки. Отже, підсумовуючи вищевикладене, можна констатувати, що кібербезпека у судноплаванні є дуже важливим напрямком для розвитку і розширення, в тому числі, й в ракурсі нормативно-правового регулювання.

Якщо міжнародне законодавство, як зазначалося, перебуває в стадії бурхливого розвитку, але все одно носить рекомендаційний характер, залишаючись при цьому базою для управління кіберризиками в судноплаванні для добросовісних користувачів, то для потенційних порушників таке законодавство має носити імперативний характер.

Для нашої держави імплементація міжнародних норм та стандартів щодо кібербезпеки у судноплаванні є, поміж іншого, важливим стратегічним елементом інтеграції України в міжнародне співтовариство, що буде сприяти забезпеченню усталеності процесів як в морегосподарському комплексі в цілому, так і в судноплаванні, зокрема.

Вдається раціональною пропозиція розробки та прийняття систематизованого національного нормативно-правового акту щодо дотримання кібернетичної безпеки в судноплаванні.

Розширити коло потенційних суб'єктів кібератак, на яких слід звертати увагу, порівняно з колом, що рекомендує Посібник з кібербезпеки на борту суден, оскільки це може бути по суті будь-яка особа, яка працює за гроші чи за іншу користь.

Ініціювати створення Єдиного органу національної кібербезпеки судноплавання в Україні, який би консолідував моніторинг кіберінцидентів в судноплаванні та проводив політику щодо дотримання кібербезпеки саме у судноплаванні і відповідно координував би свою діяльність з Центральними органами влади України.

Розглянути можливість впровадження в закладах вищої освіти освітніх програм, які б поєднували та формували спеціальні компетенції здобувачів вищої освіти для отримання ними таких результатів навчання, які б дозволили випускниками бути конкурентноспроможними на ринку професій які стосуються поглибленої спеціалізації кіберзахисту, кібербезпеки та її нормативно-правового наповнення.

Література:

1. Веремчук В.С. Проблематика імплементації міжнародно-правових стандартів морської кібербезпеки у національне законодавство України. *Приватне та публічне право*. 2025. № 2. С. 61–66. URL: <https://dspace.onu.edu.ua/server/api/core/bitstreams/5ecc31a9-8525-4e3f-a8d9-fe12349a3c32/content>
2. Міжнародна морська організація. URL: <http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL41-17>.
3. Резолюція MSC.428(98) «Управління кіберризиками в морській галузі у межах систем управління безпекою» від 16 липня 2017 року. URL: <https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428%2898%29.pdf>
4. Міжнародний кодекс управління безпекою, прийнятий Асамблеєю ІМО від 04.11.1993 № А.741(18), імплементований в рамках регламенту Європейського Парламенту і Ради (ЄС) № 336/2006 від 15 лютого 2006 року. URL: <https://zakon.rada.gov.ua/rada/term/en-lt/15561>
5. Посібник з кібербезпеки на борту суден підготовлений галузевими організаціями, та зведеною Рекомендацією Міжнародної асоціації класифікаційних товариств (МАКО) з кіберзахисту № 166. URL: <http://www.iacs.org.uk>
6. Циркуляри MSC.1/Circ.1639 від 14 червня 2021 та MSC-FAL.1/Circ.3/Rev.3 від 04 квітня 2025 року Комітету з безпеки на морі Міжнародної морської організації. URL: <https://www.imo.org/enghttps://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MS-C-FAL.1-Circ.3-Rev.3.pdf>
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
8. Про національну безпеку України: Закон України від 21 червня 2018 року. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
9. Про транспорт: Закон України від 10 листопада 1994 року. URL: <https://zakon.rada.gov.ua/laws/show/232/94-%D0%B2%D1%80#Text>
10. Про морські порти України: Закон України від 17 травня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/4709-17#Text>
11. Кодекс торговельного мореплавства України від 23 травня 1995 року. URL: <https://zakon.rada.gov.ua/laws/show/176/95-%D0%B2%D1%80#Text>
12. Стратегія кібербезпеки України на 2021-2025 роки, затверджена Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
13. Про схвалення Стратегії імплементації положень директив та регламентів Європейського Союзу у сфері міжнародного морського та внутрішнього водного транспорту («дорожньої карти») Розпорядження Кабінету Міністрів України від 11 жовтня 2017 р. № 747-р. URL: <https://zakon.rada.gov.ua/laws/show/747-2017-%D1%80#Text>
14. Recommendation on Cyber Resilience 166, IMO Guidelines v4. URL: https://www.steamshipmutual.com/sites/default/files/downloads/articles/2020/IACS-Recommendation-on-Cyber-resilience-No-166-2020_04.pdf

Borshchevska O. Cybersecurity in shipping: international-legal and national-legal aspects

Summary. The actualization of the topic of cyber security of shipping in its international legal and national legal aspects is due to the progress of digitalization of almost all spheres of human life. The digitalization of life, including shipping, has created certain progressive opportunities on the one hand, and on the other hand has provoked a certain risk of cyber risks. Seagoing vessels, both autonomous and with a crew, operate as separate cyber-material systems that are very vulnerable to both external material factors and intangible factors, in particular, cyberattacks. This issue is gaining particular importance at the present stage not only in the context of global trade, but also in the context of the war in Ukraine and other global armed conflicts, as an element of international and national security, which includes a full range from military and state security to environmental security, including at the global level.

The comprehensive implementation of digital technologies leads to the emergence of relevant relations that should be regulated by legal norms, since the lack of regulation by law of such a global segment of technologies may tend to commit actions that will intentionally or through negligence violate the rights of other persons.

Modern examples of cyberattacks threaten the functioning of many electronic registers, access to databases, remote control of processes, in particular aircraft and sea vessels. This is especially true for ensuring the activities of autonomous vessels.

The article considers the position of the international community on ensuring cybersecurity in shipping. The international legal framework, standards and guidance documents regulating cyber risks at sea are analyzed.

An overview of national regulatory and legal material that implements or should implement relevant international norms is provided. The issue of the expediency of giving such norms an imperative (mandatory) character in order to achieve regulatory efficiency is raised. It was determined that the implementation of international standards and norms on cybersecurity in the shipping sector is a critically important strategic element of Ukraine's integration into the international community.

The development and adoption of a systematized national regulatory act is proposed, which would ensure comprehensive compliance with cybersecurity requirements in shipping. The issue of compliance with national, including environmental, security through compliance with cybersecurity rules is highlighted.

The need to create a special program for training cybersecurity specialists specifically for shipping in higher educational institutions is assessed.

Key words: national security, shipping safety, cybersecurity, cyber incident, cyber attack, cyber risk, ship, ports, environmental safety.



Стаття надійшла 203.10.2025

Стаття прийнято 24.10.2025

Статтю опубліковано 17.11.2025