МОРСЬКЕ ПРАВО

DOI: https://doi.org/10.18524/2411-2054.2025.59.340314
УДК 341.225.5:004.056

Б. М. Орловський, докт. юрид. наук, доцент, професор
Одеський національний університет імені І. І. Мечникова
Кафедра кримінального права, кримінального процесу та криміналістики
Французький бульвар, 24/26, Одеса, 65058, Україна
e-mail: b.orlovskyi@onu.edu.ua
ORCID iD: https://orcid.org/0000-0002-9161-2904

Д. О. Зозулянський, адвокат,
член Комітету з питань ІТ-права
при Раді адвокатів Одеської області
e-mail: pravnic@ukr.net

КІБЕРБЕЗПЕКА МОРСЬКОГО ТОРГОВЕЛЬНОГО СУДНА: ПОНЯТТЯ, СКЛАДОВІ ТА МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ

Стаття присвячена комплексному дослідженню кібербезпеки морського торговельного судна, розкриттю його сутності, ознак, основних складових, міжнародно-правового регулювання. У статті здійснено поглиблений аналіз поняття «кібербезпека морського торговельного судна», що виходить за межі суто технічного захисту й охоплює «забезпечення безперебійного, безпечного та надійного функціонування судна як цілісного технологічного комплексу в умовах постійних та зростаючих кіберзагроз». Для морського торговельного судна кібербезпека означає всебічний захист його критично важливих систем управління, до яких належать навігаційні, комунікаційні, двигунові, баластні, вантажні та інші бортові системи, від будь-якого несанкціонованого доступу, маніпуляцій, пошкодження або виведення з ладу, що може бути спричинене кібератаками.

Охарактеризовано ключові ознаки кібербезпеки, до яких віднесено системність, превентивність, динамічність та комплексність, що підкреслює необхідність багатовекторного підходу до захисту. Наприклад, системність вказує на те, що заходи захисту повинні бути інтегровані на всіх рівнях: від глобальних навігаційних систем до локальних бортових мереж, створюючи єдиний, взаємопов'язаний захисний контур. Динамічність відображає постійну еволюцію кіберзагроз, що вимагає безперервного оновлення методів і засобів захисту, щоб відповідати викликам кіберзлочинців.

Проаналізовано перелік об'єктів кібербезпеки згідно зі статтею 4 Закону України «Про основні засади забезпечення кібербезпеки України», до яких відносяться: конституційні права і свободи людини і громадянина; сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; а також об'єкти критичної інфраструктури, до яких, безумовно, належать морські торговельні судна, їхні бортові та наземні системи управління, порти й термінали, що забезпечують їхнє функціонування.

Детально розглянуто основні складові кібербезпеки морського торговельного судна,

а саме: 1) захист інформаційних систем та мереж; 2) безпека операційних технологій (ОТ); 3) управління ризиками; 4) навчання та підвищення обізнаності екіпажу; 5) фізична безпека. Кожна з цих складових виступає невід'ємним елементом загальної системи захисту та вимагає специфічних заходів для забезпечення стабільної та надійної роботи. Особливу увагу приділено безпеці операційних технологій, що є критично важливою для запобігання втраті контролю над судном та уникненню серйозних аварій.

У статті проаналізовано міжнародно-правове регулювання кібербезпеки на морі, що знаходиться на стадії постійного розвитку. Вивчено роль Міжнародної морської організації (ІМО), Резолюції MSC.428(98), що пов'язана з управлінням морськими кіберризиками у системах управління безпекою, вплив її рекомендацій на держави, що приєдналися до цієї резолюції. Поряд із цим, акцентовано увагу на діяльності інших міжнародних інституцій та галузевих асоціацій, які сприяють розробці стандартів та найкращих практик.

Наголошено на тому, що морські торговельні судна, безумовно, належать до об'єктів критичної інфраструктури, що зумовлює їх особливий статус та необхідність першочергового захисту. У висновках підкреслено необхідність подальшої гармонізації міжнародного та національного законодавства, а також розробки більш детальних і обов'язкових норм для забезпечення стабільної та безпечної морської торгівлі.

Ключові слова: кібербезпека, кіберризик, ознаки кібербезпеки, об'єкти кібербезпеки, складові кібербезпеки, торгівельне мореплавство.

Постановка проблеми. Сучасний етап розвитку глобальної економіки та міжнародної торгівлі нерозривно пов'язаний з функціонуванням морського транспорту, який забезпечує значну частку світових вантажоперевезень. Морські торговельні судна, будучи ключовими елементами логістичних ланцюгів, все більше інтегруються в цифрові мережі, оснащуючись передовими інформаційними та навігаційними системами. Ця цифровізація, безумовно, сприяє оптимізації процесів та підвищенню ефективності судноплавства. Поряд з цим виникають значні виклики, що пов'язані із правильним формуванням кібербезпеки морського торгівельного судна, заходами її правового регулювання та забезпечення для належної протидії кіберзагрозам, що посягають на неї. Кіберризики та кібератаки на морські торгівельні судна можуть мати катастрофічні наслідки: від виведення з ладу навігаційного обладнання та систем управління, що загрожує зіткненнями та катастрофами, до несанкціонованого доступу до конфіденційних даних та порушення функціонування критичних систем, що забезпечують безпеку екіпажу та вантажу. Існуючі правові механізми та законодавство досить часто виявляються недостатньо ефективними для належної протидії гібридним кіберзагрозам, що не знають державних кордонів і вимагають комплексного підходу.

Тому актуальною і дискусійною є тематика, що пов'язана із дослідженням кібербезпеки морського торговельного судна, її складових, ознак та об'єктів, заходів правового забезпечення і проблем нормативно-правового регулювання у контексті взаємодії міжнародного та національного законодавства. Актуальність обраної теми дослідження зумовлена багатогранним характером кіберзагроз для морського торговельного судноплавства, що охоплює не лише технічні аспекти, а й нормативно-правову складову, яка вимагає належного правового регулювання таких процесів.

Аналіз останніх досліджень і публікацій показує, що дослідження проблемних аспектів кібербезпеки привертало увагу різних вчених і прямо чи побічно зустрічалося у працях І. В. Арістова, О. А. Баранова, В. С. Веремчука, А. О. Волошина, О. В. Гайдука, І. В. Діордіци, Є. О. Живило, В. В. Куцаєва, С. Б. Майданевича, О. М. Мельника, В. Г. Пядишева, А. О. Трофименко, О. О. Тихомирова, В. П. Шеломенцева, В. С. Цимбалюка та інших. В той же час комплексний розгляд ключових складових кібербезпеки, системи її об'єктів та ознак залишився малодослідженим. Також немає однозначного трактування поняття кібербезпеки, зміст якого розглядається в залежності від сфери його застосування. Тому автор, спираючись на попередні дослідження, згідно із метою цієї статті здійснює комплексне дослідження поняття, ключових складових, системи об'єктів та ознак кібербезпеки і їх впливу на сферу торгівельного мореплавства, з акцентуванням уваги на правових аспектах цієї тематики.

Відповідно до визначеної проблеми та актуальності, завданнями дослідження стали: 1) розглянути поняття «кібербезпека», його ключові складові, систему ознак та об'єктів в межах чинного законодавства; 2) здійснити аналіз особливостей міжнародно-правового регулювання кібербезпеки у сфері торгівельного мореплавства, зокрема ролі міжнародних конвенцій та резолюцій у цьому питанні; 3) сформулювати поняття «кібербезпека морського торговельного судна» та визначити його складові елементи, що стосуються саме сфери торгівельного мореплавства.

Виклад основного матеріалу. У сучасному світі, що динамічно розвивається та всебічно цифровізується, термін «кібербезпека» набув статусу одного з фундаментальних понять, що визначає «…здатність будь-якої системи протистояти загрозам у кіберпросторі». В широкому розумінні, кібербезпека є станом захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечується цілісність, доступність та конфіденційність інформації, а також надійність функціонування інформаційно-комунікаційних систем. Це багатогранне явище, що включає в себе комплекс організаційно-правових, інженерно-технічних та соціально-психологічних заходів, спрямованих на запобігання, виявлення та нейтралізацію кіберризиків й кіберзагроз, а також мінімізацію їхніх наслідків.

У правовій науці існують різні погляди на поняття «кібербезпека» в залежності від сфери її застосування. Наприклад, у сфері торгівельного мореплавства В. С. Веремчук визначає кібербезпеку при експлуатації морських суден як один із основних аспектів потенційних змін у морському праві у процесі його адаптації до технологічних викликів [5, с. 77]. У сфері інформаційної безпеки О. А. Баранов характеризує «кібербезпеку» як окремий випадок інформаційної безпеки в умовах використання комп'ютерних систем та/або телекомунікаційних мереж [3, с. 60-61].

Законодавчо поняття «кібербезпека» визначено у пункті 5 частини 1 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України», де воно характеризується як «…захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового

комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Аналіз наведеної дефініції дозволяє виокремити ключові складові кібербезпеки, що є нерозривно пов'язаними та взаємозалежними:

1) Захищеність життєво важливих інтересів особи (людини). Такий аспект підкреслює нам кінцеву мету кібербезпеки – це забезпечення непорушності та стійкості основних благ, що є фундаментальними для існування та розвитку особистості, соціуму та держави. До них належать права та свободи людини, економічна стабільність, суверенітет, територіальна цілісність тощо.

2) Використання кіберпростору. Зазначена складова чітко вказує на контекст (сферу), у якому (якій) реалізується кібербезпека – це середовище інформаційних та комунікаційних систем (кіберпростір), де здійснюється обмін даними, функціонує критична інфраструктура та формуються нові суспільні відносини.

3) Сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, як складова кібербезпеки акцентує нашу увагу на необхідності не лише захисту такого суспільства і середовища, а й створення умов для прогресивного розвитку цифрових технологій та їх інтеграції у повсякденне життя без потенційних кіберзагроз. Це передбачає можливість вільного та безпечного доступу до цифрової інформації, її обміну та використання у повсякденному житті людей.

4) Своєчасне виявлення, запобігання і нейтралізація загроз. Така складова кібербезпеки відображає її активний характер і показує, що сфера кібербезпеки не обмежується лише реагуванням на вже існуючі загрози, а передбачає за собою постійний моніторинг, ідентифікацію потенційних ризиків, розробку та впровадження превентивних заходів, а також швидке та ефективне усунення наслідків кіберінцидентів.

5) Загрози національній безпеці держави у кіберпросторі, як складова кібербезпеки конкретизує характер загроз, проти яких спрямовані заходи кібербезпеки – це реальні та потенційні небезпеки, що можуть підірвати стабільність держави, її інституцій, економіки та суспільства через кіберпростір.

Далі у тексті зазначеного Закону варто звернути увагу на положення ст. 4, які деталізують перелік об'єктів кібербезпеки, що підлягають захисту в кіберпросторі [1]. Систематизація цих об'єктів дозволяє чітко окреслити сферу застосування Закону та пріоритети державної політики у сфері кібербезпеки. Отже, до системи об'єктів кібербезпеки входять:

1) Конституційні права і свободи людини і громадянина, що є фундаментальним об'єктом кібербезпеки та підкреслює її людиноцентричний підхід. Захист прав і свобод у кіберпросторі означає забезпечення приватності даних, свободи вираження поглядів, доступу до інформації, а також запобігання кіберзлочинам, які можуть порушувати особисті немайнові права людини (наприклад, кібербулінг, шахрайство, несанкціоноване використання персональних даних). Це також включає захист виборчих прав у цифровому середовищі.

В межах описаного людиноцентричного підходу варто звернути увагу на ратифікацію в Україні «Конвенції про кіберзлочинність», у якій прямо вказується на необхідність формування кожною країною-учасником певної системи

власних «умов та запобіжних заходів» (ст. 15 Конвенції) для адекватного захисту прав і свобод людини на своїй території [2]. Тобто такий об'єкт кібербезпеки визначається фундаментальним на міжнародному рівні.

2) «Суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища» як об'єкт відображає колективний вимір кібербезпеки. Забезпечення захищеності суспільства означає збереження його стабільності, цілісності, функціонування соціальних інститутів у цифровому просторі. Це передбачає захист від дезінформаційних кампаній, кіберзлочинів, що можуть спричинити паніку або дестабілізацію, а також створення умов для гармонійного та безперервного розвитку цифрових комунікацій.

3) «Держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність» є ключовим об'єктом національної безпеки, який прямо переноситься у сферу кіберпростору. Захист держави у кіберпросторі передбачає убезпечення державних інформаційних ресурсів, систем державного управління, оборонного комплексу від кібератак, що можуть загрожувати суверенітету, порушувати конституційний лад або ставити під сумнів територіальну цілісність країни. Це включає протидію кібершпигунству, кібердиверсіям та кібератакам на критичну інфраструктуру, що контролюється державою.

4) «Національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави» як об'єкт охоплює широкий спектр інтересів, які можуть бути підірвані у кіберпросторі. Йдеться про економічні, політичні, соціальні, культурні, науково-технічні та інші інтереси, реалізація яких залежить від безпечного функціонування кіберпростору. Захист національних інтересів вимагає системного підходу до кібербезпеки у всіх галузях – від фінансів до освіти.

5) «Об'єкти критичної інфраструктури» охоплюють підприємства, установи та організації, незалежно від форми власності, що мають важливе (критичне) значення для держави і можуть забезпечувати функціонування певних сфер життєдіяльності чи економіки у суспільстві [1]. У контексті морського торговельного судноплавства, морські торговельні судна, їхні бортові системи та наземні системи управління, а також порти та термінали, які забезпечують їхнє функціонування, беззаперечно належать до об'єктів критичної інфраструктури. Це зумовлено їхньою непересічною роллю у глобальних логістичних ланцюгах, забезпеченні міжнародної торгівлі, енергетичній безпеці та загальній економічній стабільності. Кібератаки на ці об'єкти можуть призвести не лише до значних фінансових збитків, а й до зупинки поставок життєво важливих товарів, порушення міжнародних зобов'язань, техногенних катастроф та навіть людських жертв.

Питання міжнародно-правового регулювання кібербезпеки у сфері морського торговельного судноплавства є динамічним та перебуває на стадії активного формування, що зумовлено як стрімким розвитком цифрових технологій, так і зростанням викликів у кіберпросторі. Хоча наразі не існує єдиного всеосяжного міжнародного договору, який би виключно та всебічно регулював кібербезпеку суден, цей напрямок розвивається через низку міжнародних інструментів та ініціатив, які поступово формують міжнародну правову основу.

Ключову роль у цьому процесі традиційно відіграє Міжнародна морська організація (ІМО) – спеціалізована установа ООН, що відповідальна за безпеку та

захист судноплавства, а також за запобігання забрудненню моря з суден. Вона є глобальним органом, що створює нормативну базу для судноплавної галузі, формує правила та стандарти безпеки у сфері торговельного мореплавства [4, с. 15]. Знаковим кроком у її діяльності стало прийняття Резолюції MSC.428(98) «Управління морськими кіберризиками у системах управління безпекою» у якій Комітет з морської безпеки: підтверджує, що система управління безпекою в морі повинна обов'язково враховувати управління поточними кіберризиками; закликає адміністрації усіх портів забезпечити належний облік кіберризиків у своїх системах управління безпекою; визначає систему запобіжних заходів, які можуть знадобитися для збереження конфіденційності різних складових управління кіберризиками; надає рекомендації державам-членам, що приєдналися до резолюції, пов'язані із доведенням її змісту до усіх зацікавлених суб'єктів управління кіберризиками [6, с. 81]. Положення цієї Резолюції на практиці є не просто рекомендаціями, а свого роду вимогами, виконання якої може бути перевірено під час інспекцій портового контролю, що потенційно може впливати на допуск судна до порту або навіть його затримання.

Крім цього основоположного документа, важливе значення мають й інші керівництва та рекомендації, розроблені ІМО, які надають детальніші вказівки щодо впровадження ефективних заходів кібербезпеки на суднах. Рекомендації Міжнародної морської організації щодо регулювання морської кібербезпеки на території держав-учасниць зазвичай реалізується шляхом їх доповнення певними вимогами та положеннями із нормативних актів держави-учасниці.

При цьому інші міжнародні об'єднання та організації теж не залишаються осторонь у процесах врегулювання кібербезпеки. З 2018 року оцінка кібербезпеки стала обов'язковою частиною комерційних контрактів у «Міжнародному морському форумі нафтових компаній» (OCIMF). А класифікаційне товариство «DNV GL» з 2017 року надає послугу із затвердження типу кібербезпеки судна, а з 2018 року розробило позначення класу кібербезпеки, пов'язаного з рівнем охорони [7, с. 181].

Перейдемо до розгляду поняття «кібербезпеки морського торговельного судна» у сфері торгівельного мореплавства, де воно набуває особливого значення та специфіки, виходячи за рамки суто технічного захисту. Під ним розуміється забезпечення безперебійного, безпечного та надійного функціонування судна як цілісного технологічного комплексу в умовах постійних та зростаючих кіберзагроз. Для морського торговельного судна кібербезпека означає всебічний захист його критично важливих систем управління, до яких належать навігаційні, комунікаційні, двигунові, баластні, вантажні та інші бортові системи, від будь-якого несанкціонованого доступу, маніпуляцій, пошкодження або виведення з ладу, що може бути спричинене кібератаками. Такий захист безпосередньо впливає на безпеку мореплавства в цілому, сприяє охороні людського життя на морі, забезпечує захист морського середовища від потенційних екологічних катастроф, а також гарантує збереження вантажу, що є економічною основою торговельного флоту.

До основних ознак кібербезпеки морського торговельного судна можна віднести системність, превентивність, динамічність та комплексність.

Системність вказує на те, що заходи захисту повинні бути інтегровані на всіх рівнях функціонування судна, починаючи від глобальних навігаційних систем, які забезпечують позиціонування та прокладку курсу, і до локальних бортових мереж та окремих пристроїв, що контролюють роботу суднових механізмів. Ця системність передбачає взаємозв'язок і взаємозалежність усіх елементів кіберзахисту, які працюють як єдиний організм.

Превентивність наголошує на необхідності випереджального виявлення потенційних загроз та усунення вразливостей до того, як вони будуть реалізовані зловмисниками. Це означає постійний моніторинг, аналіз ризиків, впровадження оновлень програмного забезпечення та проактивне виявлення слабких місць у системі захисту.

Динамічність відображає постійну еволюцію кіберзагроз, що вимагає безперервного оновлення методів і засобів захисту. Кіберзлочинці постійно розробляють нові, більш витончені атаки, тому система кібербезпеки має бути гнучкою та адаптивною, здатною швидко реагувати на зміни в ландшафті загроз.

Комплексність означає поєднання різних підходів до забезпечення захисту, які охоплюють технічні рішення, організаційні процедури, відповідне правове регулювання та, що важливо, врахування людського фактору. Це свідчить про те, що ефективна кібербезпека не може бути досягнута лише за допомогою технологій, але потребує всебічного підходу.

Кібербезпека морського торговельного судна складається з кількох взаємопов'язаних елементів (складових частин), кожен з яких відіграє критично важливу роль. Складові кібербезпеки морського торговельного судна включають:

По-перше, захист інформаційних систем та мереж, що вимагає забезпечення конфіденційності, цілісності та доступності даних, які обробляються на судні. Це охоплює захист електронної пошти, систем обміну інформацією, баз даних екіпажу та вантажу, а також інших цифрових ресурсів від несанкціонованого доступу чи пошкодження, що забезпечує безперебійну комунікацію та збереження важливих даних. Сюди належить впровадження надійних міжмережевих екранів, систем виявлення вторгнень, а також використання криптографічних методів для захисту інформації, що передається або зберігається. Це також вимагає регулярного аудиту безпеки та оновлення антивірусних програм для протидії новітнім загрозам.

По-друге, захист операційних технологій (ОТ), під яким розуміється безпека критично важливих систем управління судном. Йдеться про системи управління двигунами, що забезпечують рух судна, навігаційні системи, які визначають його місцезнаходження та курс, системи управління баластом, що впливають на остійність, вантажні операції, які є ключовими для комерційної діяльності, та інше життєво важливе обладнання. Несанкціоноване втручання в ОТ може призвести до втрати контролю над судном та серйозних аварій, що ставить під загрозу безпеку екіпажу та збереження судна. Це включає сегментацію мереж ОТ, використання спеціалізованих систем моніторингу та контролю за промисловими системами управління (ICS/SCADA), а також впровадження жорстких протоколів доступу для персоналу.

По-третє, управління ризиками, яке передбачає постійну ідентифікацію, ретельну оцінку та ефективну мінімізацію кіберризиків. Цей процес також

включає розробку та регулярне оновлення планів реагування на кіберінциденти, що дозволяє швидко та скоординовано діяти у випадку атаки, мінімізуючи її потенційні негативні наслідки. Важливою складовою є також проведення регулярних навчань та симуляцій кібератак для перевірки ефективності розроблених планів реагування та їх адаптації до нових викликів.

По-четверте, навчання та підвищення обізнаності екіпажу, що є критично важливим для нівелювання людського фактору, який часто виступає найслабшою ланкою у системі кібербезпеки. Регулярні тренінги та підвищення обізнаності щодо фішингових атак, соціальної інженерії, правил безпечного використання цифрових пристроїв та інших загроз дозволяють сформувати культуру кібербезпеки серед членів екіпажу, що значно підвищує загальний рівень захисту. Це також передбачає розробку чітких політик щодо використання особистих пристроїв на борту та постійне інформування про актуальні кіберзагрози, з якими може зіткнутися морський персонал.

По-п'яте, фізичну безпеку, яка доповнює цифрові заходи захисту. Вона полягає у захисті доступу до критично важливого обладнання та інфраструктури судна, що може бути використане для кібератаки, забезпечуючи додатковий рівень захисту від зовнішніх загроз. Це включає контроль доступу до серверних приміщень, навігаційного мостику та інших зон, де розміщено чутливе обладнання, що дозволяє запобігти прямому фізичному втручанню, яке може передувати чи супроводжувати кібератаку. Забезпечення фізичної безпеки також передбачає впровадження систем відеоспостереження та суворого контролю за всіма, хто має доступ до критичних зон судна.

Висновки і пропозиції. Підсумовуючи результати проведеного дослідження, слід зазначити, що кібербезпека морського торговельного судна є не просто технічним питанням, а комплексною проблемою, що потребує глибокого правового аналізу, виваженого міжнародно-правового регулювання та ефективних заходів забезпечення. У контексті стрімкої цифровізації та інтеграції суден у глобальні інформаційні мережі, загрози у кіберпросторі набувають особливої гостроти, що безпосередньо впливає на безпеку мореплавства, збереження людського життя, захист морського середовища та стабільність світової торгівлі. Визначення поняття «кібербезпеки морського торговельного судна» як забезпечення безперебійного, безпечного та надійного функціонування судна як цілісного технологічного комплексу в умовах постійних кіберзагроз є фундаментальним для розбудови ефективної системи захисту. Аналіз цього поняття через призму Закону України «Про основні засади забезпечення кібербезпеки України» дозволив виокремити його ключові складові, визначити систему його об'єктів та сформулювати його ознаки. Варто розуміти, що розбудова ефективної системи кібербезпеки на морі є запорукою стабільного економічного розвитку, безперебійного функціонування логістичних ланцюгів та захисту національних інтересів у глобальному морському просторі.

Список використаної літератури

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради України. 2017. № 45. Стор. 42. Ст. 403.
2. Стратегія кібербезпеки України: затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021. Офіційний вісник України. 2021. № 70. Стор. 42. Ст. 4417.
3. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. № 2. С. 54-62.
4. Веремчук В. С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. Вісник Одеського національного університету. Серія: Правознавство. 2024. № 38. С. 12-17.
5. Веремчук В. С. Міжнародно-правові аспекти експлуатації автономного морського судна: постановка питання. Правова держава. 2023. № 50. С. 72-80.
6. Пядишев В. Г. Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. Морська безпека та оборона. 2023. № 1. С. 78-86.
7. Трофименко А. О., Майданевич С. Б., Войченко Т. О., Дорофєєва З. Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. Водний транспорт. 2023. № 37. С. 179-188.

References

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 2163-VIII vid 05.10.2017 roku. Vidomosti Verkhovnoi Rady Ukrainy. 2017. № 45. Stor. 42. St. 403 [in Ukrainian].
2. Stratehiya kiberbezpeky Ukrainy: zatverdzhena Ukazom Prezydenta Ukrainy vid 26 serpnia 2021 roku № 447/2021. Ofitsiinyi visnyk Ukrainy. 2021. № 70. Stor. 42. St. 4417 [in Ukrainian].
3. Baranov O. A. (2014). Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka». Pravova informatyka, 2, 54-62 [in Ukrainian].
4. Veremchuk V. S. (2024). Mizhnarodno-pravove rehuliuvannia kiberbezpeky u morskii haluzi: suchasnyi stan ta perspektyvy rozvytku. Visnyk Odeskoho natsionalnoho universytetu. Seriia: Pravoznavstvo, 38, 12-17 [in Ukrainian].
5. Veremchuk V. S. (2023). Mizhnarodno-pravovi aspekty ekspluatatsii avtonomnoho morskoho sudna: postanovka pytannia. Pravova derzhava, 50, 72-80 [in Ukrainian].
6. Piadyshev V. H. (2023). Pytannia vdoskonalennia kiberbezpeky morskoho transportu: zarubizhnyi dosvid. Morska bezpeka ta oborona, 1, 78-86 [in Ukrainian].
7. Trofimenko A. O., Maidanevych S. B., Voichenko T. O., Dorofieieva Z. Ya. (2023). Deiaki problemni pytannia vprovadzhennia standartiv kiberbezpeky na morskomu transporti. Vodnyi transport, 37, 179-188 [in Ukrainian].

Стаття надійшла 15.08.2025 р.

B. M. Orlovskyi, Doctor of Juridical Sciences, Associate Professor, Professor
Odesa I. I. Mechnikov National University
the Department of Criminal Law, Criminal Procedure and Criminalistics
24/26 Frantsuzkyi Blvd, Odesa, 65058, Ukraine
e-mail: b.orlovskyi@onu.edu.ua
ORCID iD: https://orcid.org/0000-0002-9161-2904

D. O. Zozulianskyi, Attorney
Member of the IT Law Committee
at the Council of Lawyers of the Odesa region
e-mail: pravnic@ukr.net

CYBERSECURITY OF MERCHANT SHIPS: CONCEPT, COMPONENTS AND INTERNATIONAL LEGAL REGULATION

Summary

The article is dedicated to a comprehensive study of the cybersecurity of merchant ships, revealing its essence, characteristics, key components, and international legal regulation. The study provides an in-depth analysis of the concept of "cybersecurity of a merchant ship", which extends beyond purely technical protection to encompass the "provision of uninterrupted, safe, and reliable functioning of a vessel as a holistic technological complex in conditions of constant and growing cyber threats". For a merchant vessel, cybersecurity means the comprehensive protection of its critical control systems, including navigation, communication, engine, ballast, cargo, and other onboard systems, from any unauthorized access, manipulation, damage, or disablement that may be caused by cyberattacks.

The article outlines the key characteristics of cybersecurity, which include systemic nature, preventiveness, dynamism, and comprehensiveness, underscoring the need for a multifaceted approach to protection. For example, the systemic nature indicates that protective measures must be integrated at all levels, from global navigation systems to local onboard networks, to create a single, interconnected protective perimeter. Dynamism reflects the constant evolution of cyber threats, requiring continuous updates of methods and means of protection to counter the challenges posed by cybercriminals.

The list of cybersecurity objects is analyzed in accordance with Article 4 of the Law of Ukraine "On the Main Principles of Cybersecurity of Ukraine", which includes: constitutional rights and freedoms of individuals and citizens; sustainable development of the information so-ciety and the digital communication environment; the state, its constitutional order, sovereign-ty, territorial integrity, and inviolability; national interests in all spheres of life of individuals, society, and the state; and critical infrastructure objects, which undoubtedly include merchant ships, their onboard and onshore control systems, as well as the ports and terminals that ensure their operation.

The main components of merchant ship cybersecurity are examined in detail: 1) protection of information systems and networks; 2) security of operational technologies (OT); 3) risk management; 4) crew training and awareness; and 5) physical security. Each of these components is an integral part of the overall protection system and requires specific measures to ensure stable and reliable operation. Particular attention is paid to the security of operational technologies, which is critical for preventing the loss of control over a vessel and avoiding serious accidents.

The article also analyzes the international legal regulation of maritime cybersecurity, which is in a constant state of development. The role of the International Maritime Organization (IMO), particularly Resolution MSC.428(98) concerning maritime cyber risk management in safety management systems, and the impact of its recommendations on signatory states are examined. In addition, the activities of other international institutions and industry associations that contribute to the development of standards and best practices are highlighted.

It is emphasized that merchant ships are, without a doubt, critical infrastructure objects, which gives them a special status and makes their protection a priority. The conclusions stress the need for further harmonization of international and national legislation, as well as the development of more detailed and binding norms to ensure stable and safe maritime trade.

Keywords: cybersecurity, cyber risk, cybersecurity features, cybersecurity objects, cybersecurity components, merchant shipping.