МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА МОРСЬКА АКАДЕМІЯ»
Навчально-науковий інститут морського права та менеджменту

Кафедра морського права

УДК: 004.056.53:656.61 (079.2)

Абу Аль-Нуджум Аль-Махамід Аліна Фірасівна

КІБЕРБЕЗПЕКА МОРЕПЛАВСТВА: ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ

Дипломна робота магістра

Науковий керівник,
д.ю.н., професор,
Шемякін О.М.

освітньо-професійна програма
«Морське право»,
спеціальність 081 «Право»

Здобувач _____ 10.12.24
Науковий керівник _____ 12.12.24
Завідувач кафедри _____ Наталя КРЕСТОВСЬКА
Нормоконтроль _____ Наталя КРЕСТОВСЬКА

м. Одеса – 2024 р.

ЗМІСТ

ВСТУП 3
РОЗДІЛ 1. РОЗВИТОК ТА СТАНОВЛЕННЯ ІНСТИТУТУ КІБЕРБЕЗПЕКИ МОРЕПЛАВСТВА 9
1.1. Генезис кібербезпеки: правові основи та етапи становлення 9
1.2. Співвідношення кібербезпеки та інформаційної безпеки 16
1.3. Кібербезпека як невід'ємна складова безпеки мореплавства 20
РОЗДІЛ 2. ПРАВОВИЙ АНАЛІЗ ЦИФРОВИХ ЗАГРОЗ ТА КІБЕРРИЗИКІВ У МОРСЬКІЙ СФЕРІ 25
2.1. Кіберризики та вразливості комп'ютерних систем на морському транспорті 25
2.2. Види кібератак у морському секторі 31
2.3. Запровадження новітніх технологій як потенційних ризиків у забезпеченні кібербезпеки мореплавства 37
РОЗДІЛ 3. ПРАВОВЕ РЕГУЛЮВАННЯ МОРСЬКОЇ КІБЕРБЕЗПЕКИ ТА ШЛЯХИ ЙОГО УДОСКОНАЛЕННЯ 45
3.1. Міжнародно-правові засади боротьби з кіберзлочинністю на морі 45
3.2. Національні нормативно-правові акти та стратегії морської кібербезпеки 55
3.3. Сучасний стан і потенціал правового врегулювання морської кібербезпеки в Україні 64
ВИСНОВКИ 75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 80

ВСТУП

Обґрунтування вибору теми та її актуальність. Сучасний розвиток інформаційних технологій докорінно змінив всі сфери суспільного життя, і мореплавство не є винятком. Наразі морський транспорт забезпечує близько 90% світової торгівлі, а його безперебійне функціонування має критичне значення для глобальної економіки. Інтеграція цифрових технологій у морську галузь, включаючи автоматизовані системи управління судном, електронні навігаційні системи, системи відстеження вантажів та комунікаційні мережі, створює нові вразливості для кібератак, що можуть мати катастрофічні наслідки для безпеки мореплавства. Морська галузь дедалі більше залежить від автоматизованих систем управління, цифрових технологій та штучного інтелекту, що зумовлює виникнення нових викликів у сфері кібербезпеки.

Кібератаки на морський транспорт та портову інфраструктуру стають все більш поширеними, і загрози кіберзлочинності значно ускладнюють забезпечення безпеки на морі. Тому необхідність правового регулювання кібербезпеки мореплавства та розробки надійних механізмів боротьби з кіберзлочинністю стає надзвичайно актуальною проблемою як на міжнародному, так і на національному рівнях.

Особливої гостроти проблема набуває в умовах геополітичної напруженості та зростання кількості кіберінцидентів у морському секторі. Атаки на морську інфраструктуру можуть призводити до порушення роботи портів та цілих логістичних ланцюгів, зміни курсу руху суден, викрадення конфіденційної інформації та навіть повної втрати контролю над судновими системами.

У контексті національної безпеки України дослідження набуває додаткової актуальності з огляду на необхідність захисту критичної морської інфраструктури від кібератак в умовах гібридної війни. Розвиток

національної системи кібербезпеки мореплавства є важливим елементом забезпечення морської безпеки держави та її економічних інтересів.

Таким чином, дослідження організаційно-правових аспектів кібербезпеки мореплавства є надзвичайно актуальним та своєчасним, оскільки спрямоване на вирішення комплексу взаємопов'язаних проблем технологічного, правового та організаційного характеру в умовах зростаючих кіберзагроз. Результати такого дослідження можуть стати основою для удосконалення національного законодавства, розвитку міжнародного співробітництва та підвищення ефективності захисту морської інфраструктури від кіберзагроз.

Мета та задачі роботи. Метою роботи є всебічне дослідження правових аспектів забезпечення кібербезпеки мореплавства, аналіз цифрових загроз і кіберризиків, а також визначення шляхів удосконалення правового регулювання у цій сфері.

Для досягнення поставленої мети визначено такі основні задачі роботи:

1. Дослідити генезис та етапи розвитку інституту кібербезпеки у морській галузі.
2. Проаналізувати співвідношення кібербезпеки та інформаційної безпеки у контексті мореплавства.
3. Виявити основні види кіберризиків та вразливості комп'ютерних систем морського транспорту.
4. Здійснити правовий аналіз видів кібератак у морському секторі та їх наслідків.
5. Визначити потенційні ризики запровадження новітніх технологій для кібербезпеки мореплавства.
6. Окреслити міжнародно-правові засади боротьби з кіберзлочинністю на морі та національні нормативно-правові акти держав у цій сфері.
7. Виокремити шляхи удосконалення правового регулювання та механізмів забезпечення кібербезпеки мореплавства в Україні.

Об'єкт і предмет дослідження. Об'єктом дослідження є суспільні відносини, що виникають у сфері забезпечення кібербезпеки мореплавства. Предметом дослідження є організаційно-правові механізми забезпечення кібербезпеки мореплавства.

Методи дослідження. Для проведення дослідження автор керувався сукупністю загальнонаукових та спеціально-наукових методів: історико-правовий (дослідження еволюції становлення інституту кібербезпеки у морській галузі, вивчення історичних передумов формування системи захисту морської інфраструктури від кіберзагроз та розвитку міжнародного співробітництва), порівняльно-правовий (зіставлення різних національних підходів до правового регулювання кібербезпеки мореплавства, порівняння міжнародних стандартів та національних нормативно-правових актів, досвіду різних країн щодо організації системи кіберзахисту морської інфраструктури), системний (дозволив розглянути кібербезпеку мореплавства як комплексне явище, що включає взаємопов'язані елементи організаційного та правового характеру, дослідити структуру системи забезпечення кібербезпеки морського транспорту та взаємодію її складових частин), опис, логічний (поділ та дослідження матеріалу по частинах), аналітичний (вивчення нормативно-правової бази з питань кібербезпеки мореплавства, аналіз практики застосування правових норм у цій сфері, оцінка ефективності існуючих організаційно-правових механізмів забезпечення кібербезпеки морської інфраструктури), соціологічний (визначено сучасний стан використання та запровадження інновацій у морську галузь). Використання цих методів дозволило комплексно дослідити проблему кібербезпеки мореплавства та запропонувати шляхи її вирішення.

Аналіз використаних джерел та літератури. У процесі підготовки роботи були використані міжнародні угоди, національні стратегічні документи та нормативно-правові акти, акти Міжнародної морської організації (ІМО), Організації Об’єднаних Націй (ООН) та Ради Європи,

наукові статті вітчизняних та іноземних дослідників у галузі інформаційної безпеки та кібербезпеки мореплавства, аналітичні матеріали, рекомендації та доповіді міжнародних організацій, дисертації, монографії, бази даних, електронні ресурси. Науково-теоретичною базою стали праці О.А. Баранова, Н.А. Савінової, О.М. Мельника, Д.В. Дубова, О.В. Краснікової, Т.М. Плачкової, R. Borum, J. Felker, S. Kern, M. Kenney, P. Marlow та інших вчених.

Наукова новизна одержаних результатів:

- вперше доведено, що кібербезпека мореплавства є комплексним правовим інститутом, який поєднує норми міжнародного морського права, національного законодавства та галузевих стандартів, спрямованих на захист морської інфраструктури від кіберзагроз в умовах цифровізації морської галузі;

- удосконалено теоретичні підходи до визначення організаційно-правового механізму забезпечення кібербезпеки в морській галузі з урахуванням специфіки морської діяльності та сучасних кіберзагроз;

- вперше основним безпосереднім об’єктом є суспільні відносини, що виникають у процесі забезпечення безпеки інформаційно-комунікаційних систем морських суден, портових споруд та іншої морської інфраструктури від кіберзагроз.

- дістали подальшого розвитку положення щодо взаємодії міжнародного та національного правового регулювання кібербезпеки мореплавства;

- вперше розроблено пропозиції щодо вдосконалення українського законодавства з питань кібербезпеки морського транспорту.

Практичне значення одержаних результатів. Викладені у магістерському (дипломному) дослідженні положення, висновки та пропозиції можуть бути використані: а) у науково-дослідницькій сфері – як основа для подальшої теоретичної розробки питань щодо кібербезпеки мореплавства та практичному втіленні рішень; б) у правотворчості – як основа для вдосконалення національних нормативних актів та міжнародних

актів у сфері морської кібербезпеки; в) у правозастосовній діяльності – як рекомендації для компаній-судновласників, портових операторів та урядів щодо забезпечення кібербезпеки; г) у навчальному процесі – при викладанні дисциплін, пов'язаних з кібербезпекою та її правовим регулюванням у мореплавстві, безпекою мореплавства, а також підготовці підручників та навчальних посібників, методичних вказівок, а також у науково-дослідницькій роботі здобувачів.

Апробація результатів. Основні положення магістерського (дипломного) дослідження розглядались на засіданні кафедри морського права та оприлюднені на таких наукових конференціях: XVII Міжнародній науково-практичній конференції НУОМА «Морське право та менеджмент: еволюція та сучасні виклики» (м. Одеса, 26 квітня 2024 р.), назва роботи: «Правове регулювання кібербезпеки в мореплавстві», X Міжнародній науково-практичній конференції НУОМА «Морське право та менеджмент: еволюція та сучасні виклики» (м. Одеса, 28 листопада 2024 р.), назва роботи: «Кібербезпека мореплавства: досвід правової регламентації у США» та VII Міжнародній студентській конференції «Глобалізація наукових знань: міжнародна співпраця та інтеграція галузей наук» (м. Суми, 29 листопада 2024 р.), назва роботи: «Кібербезпека як невід’ємна складова безпеки мореплавства».

Обґрунтування структури роботи. Виходячи з мети та основних завдань роботи, враховуючи актуальність обраної теми, робота складається зі вступу, трьох розділів, шістьох підрозділів, висновків та списку використаних джерел (у кількості 81 джерела), які в свою чергу дозволяють розкрити тему даного дослідження.

У Першому розділі окреслено тенденції розвитку та становлення інституту кібербезпеки мореплавства, розмежовано поняття кібербезпеки та інформаційної безпеки, проаналізовано їхні відмінності та схожості, запропоновано власне визначення кібербезпеки з огляду на наростаючу

потребу в уніфікованому трактуванні цього явища, обґрунтовано позицію кібербезпеки як невід'ємної складової безпеки мореплавства, виокремлено визначення кібербезпеки мореплавства.

Другий розділ присвячено правовому аналізу цифрових загроз та кіберризиків у морській сфері, розкрито вразливості комп'ютерних систем на морському транспорті та морській інфраструктурі, зведено основні види кібератак у морській галузі, визначено перспективи та ризики впровадження автономних суден, штучного інтелекту та Інтернету речей у сучасній практиці морських перевезень, проаналізовано існуючі тенденції правового регулювання у цій сфері.

У Третьому розділі досліджується правова регламентація кібербезпеки і основні засади боротьби з кіберзлочинністю, зокрема, з кіберзлочинністю у мореплавстві, розкрито тему морської кібербезпеки у світлі масштабних кібератак сьогодення, проаналізовано сучасний стан забезпечення міжнародного та національного правового регулювання держав світу та України щодо мінімізації кіберризиків та механізмів боротьби із кіберзлочинністю на морі, запропоновано шляхи їхнього вдосконалення.

У Висновках наведено основні результати дослідження.

РОЗДІЛ 1

РОЗВИТОК ТА СТАНОВЛЕННЯ ІНСТИТУТУ КІБЕРБЕЗПЕКИ МОРЕПЛАВСТВА

1.1. Генезис кібербезпеки: правові основи та етапи становлення

Історію виникнення кібербезпеки (кібернетичної безпеки) пов'язують з появою перших електронно-обчислювальних машин (ЕОМ) у 1940-х роках, коли розпочалося активне використання комп'ютерних технологій для обробки даних, що зумовило виникнення поступово зростаючої необхідності у захисті інформації від посягань з використанням несанкціонованого доступу.

Кібернетика (гр. kybernetike – мистецтво керування) – галузь знань, що досліджує універсальні принципи та закономірності процесів збирання, накопичення, передачі та обробки інформаційних даних. Вона досліджує кібернетичні системи, які складаються з багатьох взаємопов'язаних об'єктів, здатних сприймати, запам'ятовувати, обробляти та обмінюватися інформацією. Кібернетика займається розробкою універсальних принципів побудови систем управління і автоматизації інтелектуальної діяльності, її виникнення та розвиток пов'язані з прогресом у галузі комп'ютерної техніки. Кібернетичні системи можна спостерігати в різноманітних формах, починаючи від автоматизованих технічних комплексів та нейронної структури людського мозку, і закінчуючи складними біологічними популяціями та масштабною системою людського суспільства в цілому [42, с. 54]. Дійсно, подібні системи являють собою сукупність взаємозалежних компонентів, які володіють здатністю отримувати, зберігати та опрацьовувати інформаційні дані, забезпечуючи при цьому їх взаємний обмін між елементами.

Уперше поняття «кіберпростір» на міжнародному рівні було використано у 2000 році на саміті лідерів країн G8, закріплено у прийнятій Окінавській

хартії глобального інформаційного суспільства. Саме на цей документ прийнято посилатися в міжнародній юридичній спільноті для обґрунтування державної політики в галузі розвитку Інтернет-технологій. Він присвячений загальним уявленням лідерів країн щодо можливостей інформаційних технологій. У ньому визначено, що інформаційно-комунікаційні технології (ІКТ) – одні із найважливіших факторів, які впливають формування суспільства XXI століття. Інформаційні технології докорінно змінили повсякденне життя, освітні процеси та професійну діяльність людей, а також трансформували характер взаємовідносин між державними структурами та громадськістю. При цьому міжнародна спільнота, працюючи над розбудовою всесвітнього інформаційного суспільства, має координувати свої зусилля для забезпечення захищеного кіберпростору, вільного від злочинних проявів [9].

Згодом, у Конвенції про кіберзлочинність від 23.11.2001 року, прийнятою Радою Європи, держави вперше домовились криміналізувати злочини, пов'язані з несанкціонованим втручанням у роботу комп'ютерних систем (ст. 2) і даних (ст. 4), виготовленням комп'ютерного обладнання з метою вчинення злочину (ст. 6), шахрайством (ст. 8), розповсюдженням дитячої порнографії за допомогою комп'ютерних систем (ст. 9), порушенням авторських та суміжних прав (ст. 10) [3]. Але визначення поняття «кібербезпека» надано у Конвенції не було.

У Великій українській енциклопедії, що створена Державною науковою установою «Енциклопедичне видавництво» та Інститутом програмних систем НАН України, вона визначається як комплексна система організаційних, юридичних, технічних та освітніх заходів, що забезпечує стабільне функціонування кіберпростору та мінімізує ризики для захисту фундаментальних прав, свобод та інтересів особи, суспільства та державних інституцій. Будучи невіддільною частиною інформаційної безпеки, кібербезпека зосереджується на захисті інформаційних ресурсів і технологічних систем від різноманітних кіберзагроз, включаючи хакерські

атаки, вірусні програми та інші форми кібератак. Її сфера охоплює налаштування комп'ютерного обладнання та інформаційно-комунікаційних мереж, використання криптографічних методів, систематичний моніторинг та виявлення потенційних атак, розробку планів реагування на інциденти, а також підготовку та навчання персоналу [39].

Британський науковець Д. Шатц у своєму дисертаційному дослідженні, звертаючи увагу на проблему відсутності єдиного визначеного поняття, розробив власне визначення кібербезпеки: «...підхід та дії, пов'язані з процесами управління ризиками безпеки, які реалізуються організаціями і державами для захисту основних властивостей даних та інформації у кіберпросторі. Визначення включає керівні принципи, стратегії та засоби захисту технологій, інструментів та навчання для забезпечення найкращого захисту для стану кіберсередовища та його користувачів» [72, с. 277].

Інші дослідники, як Д. Крейген, Н. Діакун-Тібо та Р. Перс відзначають у своїй науковій роботі, що відсутність прийнятного визначення кібербезпеки перешкоджає технологічному та науковому прогресу, і пропонують своє визначення, відповідно до якого кібербезпека є системою організації, яка включає ресурси, процеси та структури, спрямовані на захист кіберпростору і пов’язаних з ним систем від загроз, що порушують права власності де-юре та де-факто» [48, с. 13].

На думку вітчизняного науковця О.А. Баранова, кібербезпека означає захищеність ключових інтересів особистості, суспільства та держави при користуванні комп’ютерними системами і телекомунікаційними мережами, цей стан забезпечує мінімізацію шкоди, пов’язаної з неповнотою, несвоєчасністю або недостовірністю інформації, злочинним впливом, небажаними наслідками роботи інформаційних технологій, а також недозволеним поширюванням, використанням чи порушенням цілісності, приватності та доступності даних [26, с. 61]. Тобто це властивість захищеності даних (усе, що має значення для людини, організації або уряду)

від загроз у кіберпросторі, які можуть порушити конфіденційність, цілісність, доступність інформації.

Задля того, щоб виокремити повне та точне визначення поняття «кібербезпека», доцільним був би аналіз дефініцій, які наведені у деяких національних стратегічних документах держав.

Наприклад, у Стратегії кібербезпеки Франції, це явище визначено як бажаний стан інформаційної системи, що полягає у її здатності протидіяти загрозам з кіберпростору, які можуть потенційно загрожувати доступності, цілісності або конфіденційності даних, що зберігаються, обробляються чи передаються, а також забезпечувати безпеку послуг, пов'язаних з цими даними [13]. Вважаємо, що дане визначення охоплює широкий спектр аспектів, пов'язаних із місцем і значенням проблем кібербезпеки у загальному контексті інших видів безпеки.

У першій редакції Стратегії Федеративної Республіки Німеччина 2011 року кібербезпека визначається як сукупність необхідних і відповідних заходів, реалізація яких спрямована на мінімізацію ризиків, причому наголошується, що вона повинна ґрунтуватися на комплексному підході. О.А. Баранов має рацію в тому, що ця точка зору досить прагматична, вона дає змогу розробляти практичні заходи для забезпечення кібербезпеки, втім не забезпечує достатньої методологічної основи для проектування та оцінювання систем, які мають гарантувати цю безпеку [26, с. 55]. Зазначене підтверджується змістом стратегічних напрямків у стратегії забезпечення кібербезпеки, представленій Федеральним урядом Німеччини.

Звернувшись до останньої на даний момент редакції вищевказаної стратегії, прийнятої у 2021 р., вважаємо за доцільне навести більш «сучасне» у розумінні німецького законодавця визначення кібербезпеки – це інформаційно-технологічна (IT) безпека всіх інформаційно-технологічних систем, які є і можуть бути взаємопов'язані на рівні даних у кіберпросторі. У свою чергу, кіберпростір визначається як віртуальний простір усіх

інформаційно-технологічних систем у світі, які є або можуть бути взаємопов’язані на рівні даних. Кіберпростір як публічно-доступна мережа функціонує на базі мережі Інтернет, який можна розширити за допомогою будь-яких інших мереж передачі даних [19, с. 125]. Таким чином, по мірі розвитку технологій, їхньої популяризації, глобального впливу на суспільство та розширення можливостей людства у користуванні мережі Інтернет, все більше аспектів стосовно безпеки даних починає знаходити своє відображення у правовій регламентації питань обробки даних в Інтернеті, їхнього зберігання і захисту.

У стратегічному баченні Турецької Республіки кібербезпека являє собою комплекс заходів для захисту інформаційних систем кіберпростору від атак, гарантування приватності, неушкодженості та доступності інформаційних ресурсів, а також виявлення та запобігання кібератакам і кіберінцидентам. Кіберпростір – глобальне середовище взаємопов'язаних інформаційних систем та мереж, що їх об'єднують по всьому світу. При цьому національний кіберпростір окреслюється як сукупність інформаційних систем, що належать суб'єктам під юрисдикцією Турецької Республіки [15, с. 47].

Відповідно до Стратегії кібербезпеки Сполучених Штатів Америки, кібербезпека становить собою інтегровану систему захисних заходів, що забезпечують охорону комп'ютерної інфраструктури, включно з фізичними компонентами, програмним забезпеченням та інформаційними даними, від несанкціонованого втручання чи зловмисних нападів, здійснюваних через глобальну мережу Інтернет [16].

Вперше визначення терміну «кібербезпека» на рівні ЄС було включено до Стратегії кібербезпеки ЄС 2013 року – Відкритий, безпечний та надійний кіберпростір, яка означає заходи та дії для захисту кіберпростору, як у цивільній, так і у військовій сферах, від тих загроз, які пов'язані або можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі. Кібербезпека прагне зберегти доступність і цілісність мереж та

інфраструктури, а також конфіденційність інформації, яка в них міститься [14].

Вперше термін «кібербезпека» в юридично-обов'язковому акті ЄС у досліджуваній сфері був розтлумачений у Законі про кібербезпеку (Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та сертифікацію інформаційно-комунікаційних технологій у сфері кібербезпеки та скасування Регламенту (ЄС) № 526/2013). У ньому кібербезпека значить діяльність, яка спрямована на захист мережевих і інформаційних систем, їх користувачів, а також осіб, які зазнали впливу кіберзагроз [10]. Дане визначення відрізняється від попереднього тим, що діяльність із захисту від загроз спрямована не лише на саму інформаційну інфраструктуру, а й на користувачів. Отже, беззаперечним є факт вдосконалення, модернізації і розширення визначення досліджуваного поняття.

В Україні дефініція надається вперше у Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року, а саме у пункті 5 статті 1 документа виокремлено, що кібербезпека – це стан захищеності ключових інтересів особи, суспільства та держави при застосовуванні кіберпростору, який забезпечує звичний розвиток інформаційного суспільства та кіберпростору, а також ефективне виявлення, запобігання та нейтралізацію дійсних і можливих загроз національній безпеці України у кіберпросторі. Пунктом 11 тієї ж статті наведено визначення кіберпростору: середовище, яке створюється внаслідок функціонування взаємопов'язаних комунікаційних систем і забезпечення електронних комунікацій через Інтернет та/або інші глобальні мережі передачі даних, надаючи можливості для комунікацій та/або реалізації суспільних відносин [21].

Прийняття вказаного закону було обумовлено і тим, що саме в Україні у 2017 році вперше було проведено масштабну кібератаку з використанням

програми-вимагача «NotPetya» російськими спецслужбами, яка спричинила мільярди доларів збитків, розповсюдившись по всій Європі, Азії, США [20]. З того часу проблема кібербезпеки все частіше почала турбувати суспільство.

Важливо зауважити, що прикметною рисою і тенденцією щодо спрямованості державної політики на розвиток та вдосконалення кібербезпеки виступає постійна модернізація країнами свого внутрішнього законодавства, зокрема галузевих законів у цій сфері і стратегій кібербезпеки. Ці акти не можна залишити без уваги, зважаючи на те, що вони самі по собі є логічною реакцією законодавців на зміни у суспільному ладі, технічний прогрес, збільшення кількості кіберзлочинів тощо. Проаналізовані вище стратегічні документи являють собою здебільшого політичні, а не нормативні акти, але вони є частиною правового підґрунтя функціонування кожної держави, оскільки саме від таких програмних документів і бере свій початок розробка ефективної нормативної бази у сфері регулювання певних суспільних відносин.

Масштабні можливості Інтернету підкреслюють глобальну небезпеку віртуальних злочинів, кібертероризму та кібервійни. Наразі багато науковців та політичних діячів вважають, що на території нашої держави відбувається не тільки повномасштабна «фізична» війна із тотальним знищенням українського населення, але і гібридна війна, яку характеризують саме ознакою використання ворогом інформаційних, електронних ресурсів задля вчинення кіберзлочинів.

Проаналізувавши думки різних авторів, законодавців, експертів, необхіднім є виокремлення власного розуміння та визначення поняття «кібербезпека». З огляду на багатогранність, міжгалузевий характер, дискусії науковців, на нашу думку, під кібербезпекою розуміється стан захищеності кіберпростору від ризику будь-якого несанкціонованого доступу і впливу та відповідні заходи по збереженню цілісності та конфіденційності даних, включаючи вчасне виявлення, запобігання та протидію існуючим і можливим

загрозам (кіберзагрозам) особистим, корпоративним, інституціональним та/або національним інтересам.

1.2. Співвідношення кібербезпеки та інформаційної безпеки

Як і більшість нормативно-правових актів, ті, що стосуються кібербезпеки, містять у собі визначення основних категорій, які використовуватимуться. Однак у світі відсутня загальноприйнята термінологія для позначення аналізованої в даному дослідженні області: деякі держави використовують поняття «кібербезпека», інші – «інформаційна безпека». Необхідно відзначити, що в іноземній та вітчизняній літературі для позначення Інтернету та похідних від нього виразів все ширше вдаються до терміну «кіберпростір» та інших слів, що містять префікс «кібер».

Британські науковці М. Вілл і Я. Браун приходять до висновку, що термін «комп'ютерна безпека» був найбільш поширений з 1974 року, з 1997 року його випередив термін «інформаційна безпека», а в 2015 році – «кібербезпека» (при чому термін «кібербезпека» стає все більш популярним з 1996 року, але протягом усього цього періоду використання терміна «кібербезпека» було незначним) [79, с. 4]. Інші вчені, порівнюючи ці два поняття, зазначають, що інформаційна безпека зародилася тоді, коли більшість інформаційних систем були автономними і рідко перетинали державні кордони, тоді як кібербезпека спрямована на боротьбу з глобальними загрозами в умовах правової необмеженості. Таким чином, кібербезпека – це інформаційна безпека з невизначеністю юрисдикції та питаннями ідентифікації [59].

Практика застосування термінів «інформаційна безпека» та «кібербезпека» у юридичній сфері виявляє їх значні розбіжності, що вказує на необхідність розробки пропозицій для уніфікації правового регулювання шляхом упорядкування понятійного апарату.

У сучасних умовах інформаційна безпека поєднує безпеку інформації та безпеку «від інформації» (структурний підхід), а також включає постійну

діяльність уповноважених органів з попередження та протидії інформаційним загрозам, застосування діяльних заходів реагування та створення умов для довготривалого контролю цієї діяльності (діяльнісний підхід) [43, с. 27]. У свою чергу, кібербезпека є явищем цифрового світу з більш вираженим технологічним характером, що передбачає використання різноманітних протоколів безпеки. Таким чином, вказані сфери інформаційної дійсності не можуть визначатися однаковими поняттями.

Кібербезпеку можна визначити через три складові: інформаційні ресурси, комп'ютерну та мережеву інфраструктуру, а також методи взаємодії користувачів.

Поняття «кібербезпека» має ґрунтуватися на понятті «кіберпростір», яке доцільно розглядати як середовище, в якому функціонують і взаємодіють кіберсистеми (сукупність пов'язаних між собою елементів, здатних сприймати, зберігати, обробляти та обмінюватися інформацією у цифровому форматі). Кіберпростір є складовою частиною інформаційного простору, що включає автоматизовані інформаційні системи, інтернет-канали та інші телекомунікаційні мережі, технологічну інфраструктуру та цифрові інформаційні ресурси. Його функціонування також окреслює суспільну діяльність суб'єктів кіберпростору (осіб, спільнот, держав). Кіберпростір виникає внаслідок цифрової діяльності, а інформаційний зміст та дії реалізуються за допомогою цифрових мереж [64]. Тобто основна суть кіберпростору полягає у активності користувачів цифрових інформаційних ресурсів та інфраструктури інформаційно-комунікаційних систем.

Під інформаційною безпекою Л. Ірвін розглядає способи, якими особи захищають важливі данні та інформацію (особисту інформацію, результати творчості або бізнес-ідеї), що зберігаються в різних форматах і на різноманітних пристроях, таких як сервери, жорсткі диски, хмарні сховища або флеш-носії [60]. Технічні експерти розглядають це поняття як сукупність

способів, спрямованих на захист даних від стороннього доступу або змін під час зберігання і при пересиланні між пристроями [54].

Проаналізувавши обидва поняття, варто виокремити у чому саме вони розрізняються.

Відтак, інформаційний простір можна охарактеризувати як комплексне середовище, що включає як природні, так і штучно створені елементи. В цьому просторі циркулюють інформаційні відображення матеріальних об'єктів. На противагу цьому, кіберпростір є повністю штучним «технологічним світом», який створюється та еволюціонує завдяки людській діяльності. Важливо зазначити, що кіберпростір може бути джерелом не лише загроз інформаційній безпеці, але й ризиків для інших сфер безпеки, таких як економічна, фінансова та військова. Це твердження знаходить своє відображення у визначенні кібербезпеки, яке наведено в Законі України «Про основні засади забезпечення кібербезпеки України» і згадано у попередньому підрозділі дослідження.

Кібербезпека фокусується на захисті кіберпростору від зовнішніх загроз, зокрема кібератак. Її основна мета – забезпечити надійне використання цифрового середовища. Кібербезпека є комплексною системою захисту, що охоплює різноманітні цифрові об'єкти, які піддаються кіберзагрозам. Вона забезпечує захист комп'ютерів, цифрових пристроїв, мереж, серверів і програмного забезпечення [41, с. 112].

Ключова особливість кібербезпеки полягає в тому, що вона зосереджена виключно на захисті даних у цифровому форматі. Це є принциповою відмінністю між кібербезпекою та інформаційною безпекою. Кібербезпека спрямована на протидію трьом основним видам загроз: зламу (хакінгу), кібератакам різного типу, несанкціонованому доступу до цифрових ресурсів.

Інформаційна безпека охоплює значно ширший спектр завдань, ніж кібербезпека, зосереджуючись на захисті інформації у всіх її проявах. Ключові аспекти включають забезпечення конфіденційності, цілісності та

доступності інформації, незалежно від її форми [54]. Це означає, що інформаційна безпека однаково стосується як захисту фізичних документів, наприклад, картотеки особливих паперів, так і електронних даних, таких як корпоративні бази даних.

Таким чином, кібербезпека спрямовується на захист цифрового простору та цифрових даних, а інформаційна безпека охоплює захист інформації у всіх її формах, включаючи нецифрові. Тобто кіберпростір виступає частиною інформаційного простору, тому об'єкти в цьому контексті є однаковими, включаючи як матеріальні, так і нематеріальні предмети і процеси, що спрямовані на задоволення інформаційних потреб для забезпечення збереження життєвої діяльності живих істот.

Але, незважаючи на схожість, поняття інформаційна безпека є набагато ширшим і охоплює більше коло проблем, ніж кібербезпека. Хоча обидві галузі тісно пов'язані та часто перетинаються, інформаційна безпека постає як більш всеохоплювальний підхід до захисту інформації, що включає як технічні, так і стратегічні аспекти, тоді як кібербезпека зосереджена переважно на технічному захисті цифрових систем та даних.

Аналіз термінів «інформаційна безпека» та «кібербезпека» виявляє їхні відмінності, але підкреслює рівнозначну важливість для організацій та держави загалом. Інформаційна безпека має ширший спектр, охоплюючи захист важливих даних від різноманітних загроз, незалежно від їх форми - цифрової чи аналогової. Кібербезпека, зі свого боку, фокусується на цифровій інформації та міцно пов'язана з такими поняттями як кіберзлочинність та кібератаки.

Людський досвід вказує на необхідність постійного вдосконалення культури як інформаційної, так і культури кібербезпеки. У контексті інформаційного суспільства свідомість людини, будучи носієм інформації, здатна через психіку сприймати, трансформувати, зберігати, обробляти та передавати інформацію, вона може стати як предметом, так і засобом

вчинення суспільно небезпечних діянь. Вона буває предметом, коли кінцевою метою суспільно небезпечного впливу є саме свідомість і психіка людини, та засобом, коли посягання на свідомість відбувається для використання людини в цілях вчинення злочину [40, с.140]. Критично важливо, щоб працівники організацій усвідомлювали масштаб та спільну мету забезпечення кібербезпеки у своїй діяльності.

Таким чином, хоча інформаційна безпека та кібербезпека мають свої особливості, вони є взаємодоповнюваними концепціями, що вимагають комплексного підходу для ефективного захисту інформації у сучасному технологічному світі.

1.3. Кібербезпека як невід'ємна складова безпеки мореплавства

З розвитком цифрових технологій і зростаючою інтеграцією комп'ютерних систем у морські перевезення, питання кібербезпеки стає одним із ключових аспектів забезпечення безпеки мореплавства. Морська індустрія дедалі більше залежить від цифрових систем управління, таких як системи автоматизації суден, навігаційні системи, радіокомунікації та логістика портів. Це робить судна, порти та інші об'єкти морської інфраструктури вразливими до кіберзагроз, що можуть призвести до руйнівних наслідків, таких як вади в роботі навігаційних систем, зупинка судна, порту або навіть катастрофічні аварії.

Проблема кібербезпеки в мореплавстві полягає у складності захисту не тільки окремих суден, але й цілих мереж, які забезпечують функціонування світової морської логістики. Багато сучасних суден оснащені системами автоматизованого управління, які стають мішенню для хакерів. Вразливі системи можуть застосовуватись для того, щоб змінити курс руху судна, перешкоджати навігації або викрасти конфіденційну інформацію. Атаки на порти можуть привести до припинення роботи важливих транспортних вузлів, порушення постачання товарів та економічних втрат.

Необхідність міжнародно-правового регулювання кібербезпеки у морській галузі обумовлена постійним процесом автоматизації суден, портової інфраструктури та впровадження електронних баз даних, які можуть бути вразливими до кібератак. У цьому контексті варто погодитися з думкою Д. Дімітріоса, який стверджує: «чим вищий рівень автоматизації морських суден, тим більший ризик кібератак» [52].

Як безпека судна, так і кібербезпека є ключовими складовими, оскільки вони мають потенційний вплив на екіпаж, судно, навколишнє середовище, компанію та вантаж. Забезпечення кібербезпеки судна передбачає захист його інформаційних технологій (IT) і експлуатаційних (операційних) технологій (OT) від несанкціонованого доступу, маніпуляцій або інших порушень.

Системи операційних технологій відповідають за управління фізичним світом, тоді як системи інформаційних технологій займаються обробкою даних. Експлуатаційні технології та системи відокремлюються від звичних IT-систем, оскільки в основному це обладнання, яке прямо керує фізичними пристроями і процесами. Інформаційні технології, в свою чергу, охоплюють широкий діапазон технологій обробки даних, включаючи програмне забезпечення, апарати та комунікаційні технології. Раніше ці технології були розділені, але завдяки Інтернету вони стали взаємодіяти, і автономні системи тепер інтегровані між собою [61]. Сьогодні безпека систем експлуатаційних технологій переважно виступає за захист операцій та даних від кіберінцидентів через посилення зв’язку між кібер- та фізичною сферами. Він передбачає виявлення та мінімізацію слабких місць та змін у системах, що керують фізичними пристроями, такими як клапани та насоси.

Таким чином, IT – це світ, який ми всі знаємо (комп'ютери, клавіатури, екрани та миші). IT-середовище включає хмари для збереження даних, сервери, брандмауери, антивірус тощо, вони функціонують завдяки технологічним протоколам, які є в кожному пристрої (HTTP, SSH, RDP).

Натомість до ОТ технологій відносяться абсолютно різні компоненти, які можна знайти, насамперед, у промислових умовах, вони часто не мають традиційного вигляду комп’ютера або екрану (обладнання як напр. ECDIS, GNSS тощо), вони функціонують через промислові протоколи, які ніколи не зустрічаються в ІТ-мережах (напр., Modbus, Ethernet/IP, Profinet), часто їм не вистачає засобів захисту (брандмауери, антивірус), вони навіть запрограмовані інакше, ніж «звичайні» комп'ютери [66].

Кібербезпека включає ризики, що виникають через втрату доступу до важливих даних або порушення їх цілісності. Тому порушення кібербезпеки може мати місце у результаті випадку, який впливає на відкритість та неподільність ІТ та ОТ технологій. Наприклад, це може бути ушкодження картографічних показників, які зберігаються в Електронно-картографічній навігаційно-інформаційній системі (ECDIS), збої під час технічного обслуговування програм, втрата або зміна даних, що є критично важливими для функціонування судна, включно з Глобальною навігаційною супутниковою системою (GNSS).

Т. М. Плачкова у своєму дисертаційному дослідженні дійшла до висновку, що безпеку мореплавства слід розуміти як стан найвищої захищеності людини та її здоров'я, майна та навколишнього середовища під час використання морського транспорту, а також як відсутність ризиків, здатних призвести до смерті чи травм осіб, речових або грошових втрат або забруднення довкілля. Забезпечення безпеки мореплавства полягає у створенні визначальних умов для гарантування захищеності життя і здоров'я людини, майна та довкілля під час експлуатації морського транспорту, а також для запобігання ризикам, які можуть призвести до згаданих негативних наслідків [38, с. 123].

Виходячи з положень пункту 3 статті 94 Конвенції ООН з морського права 1982 р до безпеки мореплавства слід відносити, зокрема і заходи, що стосуються конструкції, оснащення та належного стану суден,

комплектування, умов роботи та освіти моряків, а також використання засобів підтримки зв'язку і запобігання зіткненням суден [2].

Беручи до уваги все вищезазначене, можна підсумувати, що інформаційна безпека мореплавства розуміється як врегульовані інформаційно-правовими нормами інформаційні суспільні відносини з приводу збереження людського життя на морі, захисту морських суден та навколишнього природного середовища. Суб’єктами інформаційної безпеки мореплавства є учасники морського підприємства (уряди держав, портова влада, судноплавні і логістичні компанії, постачальники телекомунікаційних послуг, екіпаж судна і т.д.), іншу групу суб’єктів складають зловмисники.

Так, Команда реагування на надзвичайні ситуації щодо кіберзахисту промислових систем управління (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT), що утворена Агентством з кібербезпеки та захисту інфраструктури Сполучених Штатів Америки (Cybersecurity and Infrastructure Security Agency, CISA) кіберзлочинців розподіляє на п’ять категорій: національні уряди (так звані державні хакери, спецслужби), промислові шпигуни та угруповання організованої злочинності, хактивісти (не мають на меті отримання прибутку) та хакери (мають на меті отримання прибутку) [67].

Під кібербезпекою мореплавства, як складовою інформаційної безпеки мореплавства, пропонуємо розуміти систему технічних, організаційних та правових відносин і заходів, які спрямовані на захист інформаційно-комунікаційних технологій, систем управління та даних, що використовуються у морській галузі, з метою забезпечення надійного функціонування морської інфраструктури, збереження людського життя на морі, захищеності від кібернетичних загроз та запобігання забрудненню природнього середовища.

Науковці звертають увагу на той факт, що кібербезпека справді стала частиною безпеки мореплавства, але все-ж таки маємо звернути увагу на

незначну кількість наукових публікацій, зокрема вітчизняних, на цю тему. Кібербезпека стала важливою складовою безпеки мореплавства через зростаючу залежність морської галузі від цифрових технологій, автоматизації та інформаційних систем. Це стосується як суден, так і портів, вантажоперевезень і логістичних процесів. Загрози кібератак можуть призвести до значних порушень, що загрожують не лише економічній стабільності компаній, а й безпеці екіпажу, навколишньому середовищу та вантажу.

Отже, кібербезпека стала невіддільною складовою безпеки мореплавства, без якої неможливо забезпечити надійну та безпечну експлуатацію сучасних суден. Успішне вирішення проблем кібербезпеки вимагає співпраці всіх учасників морської галузі – від судноплавних компаній та екіпажів до регуляторних органів та виробників обладнання. Тільки спільними зусиллями можна створити ефективну систему захисту від кіберзагроз і гарантувати безпечне мореплавство в цифрову епоху.

РОЗДІЛ 2

ПРАВОВИЙ АНАЛІЗ ЦИФРОВИХ ЗАГРОЗ ТА КІБЕРРИЗИКІВ У МОРСЬКІЙ СФЕРІ

2.1. Кіберризики та вразливості комп'ютерних систем на морському транспорті

Морська сфера, як одна з найважливіших складових елементів світової економіки, є дуже вразливою до кібератак. Під час щорічної конференції «Асоціації операторів балкерних терміналів 2019 року», було наголошено, що кібербезпека залишається особливо слабким місцем інтерфейсу між судном і берегом, що підкреслює необхідність посилення кібербезпеки портів та суден [34, с.82].

Вразливими та потенційно задіяними в кіберінциденті науковці вважають такі комп'ютерно-інформаційні системи сучасної морської інфраструктури:

- AIS (Automatic Identification System) – система автоматичної ідентифікації.

Правило 19 глави V Міжнародної конвенції з охорони людського життя на морі (SOLAS) встановлює, що всі судна повинні мати системи AIS, які здатні автоматично надавати інформацію про судно іншим суднам та владі прибережної держави. Функції системи: надавати інформацію, включаючи ідентифікаційні дані, тип, положення, курс, швидкість, навігаційний стан і іншу інформацію, пов'язану з безпекою судна, - автоматично відповідним чином обладнаним береговим станціям, іншим суднам і літакам; автоматично отримувати таку інформацію з аналогічно обладнаних суден; контролювати і відстежувати судна [1].

Дослідники компанії Trend Micro провели масштабне дослідження, присвячене безпеці AIS, результати якого були представлені на конференції Black Hat Asia 2014. Розглядалися два напрямки атаки: перший - на AIS-

провайдерів, які збирають дані для надання комерційних і безкоштовних сервісів в реальному часі (наприклад, MarineTraffic).

Другий тип атаки - на рівні радіопередачі, тобто самого протоколу AIS, адже структура протоколу була створена досить давно і на той час не було впроваджено методи ідентифікації відправника та кодування інформації, що передається. Загалом було доведено можливість численних сценаріїв порушення безпеки судна з використанням AIS: підміна інформації стосовно судна, разом з його розташуванням та курсом руху, зміна даних щодо вантажу; створення «суден-привидів», яких насправді не існує, але яке «бачать» інші судна на радарі; надсилання хибної інформації певним суднам, щоб ввести в оману та змусити їх відхилитися від свого курсу; неправдиві попередження про зіткнення; перетворення існуючого судна в «невидиме» тощо [45].

- ECDIS (Electronic Chart Display and Information System) – електронно-картографічна навігаційна система, визначена в резолюції Міжнародної морської організації (IMO) A.817 (19), як інформаційна система, що при адекватному резервному копіюванні може бути прийнята як відповідна сучасній карті, необхідної правилом V/20 Конвенції SOLAS 1974 року, шляхом відображення обраної інформації з системної електронної навігаційної карти (SENC), разом з інформацією про місцезнаходження від навігаційних датчиків, щоб допомогти морякам виконувати попередню та виконавчу прокладку, і, якщо потрібно, відображає додаткову інформацію стосовно навігації [5]. Тобто вказана комп'ютерна система використовується в якості альтернативи паперовим навігаційним картам.

- EPIRB (Emergency Position Indicating Radio Beacon) – передавач, який при активації передає сигнал лиха в різноманітних діапазонах. Це аварійний радіобуй, що подає при активації сигнал лиха, передача якого в залежності від технології виконання може здійснюватися через супутник. Крім сигналу

лиха деякі EPIRB можуть також передавати інформацію про судно (при синхронізації з AIS) [46].

- VDR (Voyage Data Recorder) - реєстратор даних рейсу. Це система збору інформації, розроблена для суден, які повинні відповідати стандартам SOLAS, і призначена для збирання відомостей з датчиків та сенсорів на борту з їхнім подальшим кодуванням, зменшенням обсягу і зберіганням цих даних у спеціальному захищеному пристрої [6].

Приміром, у 2012 році сінгапурське вантажне судно Prabhu Daya протаранило рибальське судно в прибережних водах Індії і зникло з місця події. В результаті зіткнення, загинули троє рибалок. Після того, як індійські правоохоронні органи затримали судно і почали розслідування, спливла цікава деталь: «під час прибуття посадових осіб на сінгапурське судно, один з членів вставив USB-носій у VDR; це привело до зараження системи вірусом та стирання всіх файлів і голосових записів, дані відновити не вдалося» [71]. Ця справа доводить, що видалення даних на VDR може вкрай ускладнити, або ж повністю завести в глухий кут розслідування інциденту, що стався на морі. Більш того, якщо у зловмисників є можливість редагування даних та їхньої підміни, існує ве лика ймовірність організації підробки, що направить розслідування в помилкове русло.

- TOS (Terminal Operating System) – одна або кілька систем, що дозволяють автоматизувати процеси навантаження та розвантаження судна в порту. TOS є ключовою частиною ланцюжка поставок і в першу чергу призначена для контролю за переміщенням і зберіганням різних типів вантажів всередині і навколо контейнерного терміналу або порту [80, p. 47]. Найвідоміший інцидент зламування цієї системи, стався в порту Антверпена у 2012 році. Схема, за якою контрабанда поставлялася до Європи, полягала в наступному: до контейнерів, у яких перевозилися зареєстровані і належним чином оформлені товари, які прибувають з Латинської Америки, в порту

відправлення довантажувати контрабандні товари (більше 1 тони наркотиків, зброя) [70].

Банда злочинців перехоплювала 9-знакові PIN-коди, які необхідні для проведення операцій з контейнерами у відповідних системах. Після того, як контейнер з контрабандою прибував у Антверпен, контрабандисти, підключені до однієї з портових бездротових мереж, віддавали команду вантажним системам переміщати обраний контейнер на свою вантажівку до приїзду власника. Оперативна робота, що почалася після скарг компаній про періодичної зникнення контейнерів, привела до серії обшуків і рейдів у Данії, Нідерландах і Бельгії, під час яких було знайдено зброю, гроші і кокаїн, п'ятнадцять членів приступної організації були затримані та згодом отримали обвинувальні вироки [70].

- CTS (Container Tracking System) – система, що дозволяє відстежувати рух контейнерів за допомогою GPS.

- ICN (Internal Computer Network) – внутрішня комп’ютерна мережа, яка вирішує локальні задачі.

- Центральний пункт управління машинною установкою [28, с. 127].

Не можна оминути увагою системи супутникового зв'язку, які є також одними з найважливіших технологій на судні, адже супутникові системи мають ключове значення для забезпечення безпеки мореплавства.

Так, система супутникового зв'язку INMARSAT забезпечує послуги радіотелефонного зв'язку, телекса, факсимільного зв'язку, передачі даних та персональних радіовикликів по всьому світу, і призначена виключно для мирного використання. У 1979 році Міжнародна організація морського супутникового зв’язку, була першим оператором супутникового зв’язку, який відповідав суворим вимогам Глобальної морської системи повідомлень про лихо та забезпечення безпеки (GMDSS). Основна задача системи полягала у забезпеченні безперебійним зв'язком морських суден, що пересуваються Світовим океаном, а пізніше її почали використовувати сухопутні і повітряні

споживачі. Згодом, замість національних агентств із забезпечення зв’язку, які були державними органами, членами INMARSAT стали приватні компанії. Так, міжнародна організація перетворилася на компанію, яка наразі оперує одинадцятьма супутниками [58].

Система COSPAS-SARSAT являє собою створену у 1977 р. міжнародну супутникову пошуково-рятувальну систему, що розроблена для передачі повідомлень про аварії та визначення розташування радіобуїв, які вбудовані на суднах і літаках на випадок аварійних ситуацій, є одним з основних елементів GMDSS і призначена для виявлення й визначення місцезнаходження суден, літаків та інших об'єктів, що зазнали лиха [59].

Іншою складовою GMDSS, відповідно до конвенції SOLAS, є NAVTEX (NAVigational TEXt Messages), компонент Всесвітньої служби навігаційних попереджень (WWNWS). Згідно з Резолюцією Асамблеї IMO A.617(15), NAVTEX надає суднам навігаційні і метеорологічні попередження і термінову інформацію через спеціальний приймач із автоматичним надрукуванням. Служба використовує єдину частоту (518 кГц), на якій берегові станції передають інформацію англійською мовою, при цьому кожна станція працює за розкладом, щоб уникнути перешкод від інших станцій [4].

Супутникові системи зв'язку на суднах мають деякі уразливості, що робить їх потенційними цілями для кібератак. Основною проблемою є відкрита архітектура цих систем - вони часто використовують стандартні протоколи та порти, які добре відомі потенційним зловмисникам. Багато суден досі експлуатують застаріле обладнання без сучасних механізмів захисту, що значно збільшує ризики успішних атак. Людський фактор також відіграє критичну роль – недостатня підготовка екіпажу з питань кібербезпеки, використання слабких паролів та необережне підключення особистих пристроїв до суднових мереж створюють додаткові вразливості.

Циркуляром MSC-FAL.1/Circ.3 (Керівництво з управління кіберризиками на морі) визначено, що уразливі системи можуть включати, але не обмежуються:

- системами навігаційного містка;
- системами обробки і управління вантажем (вантажні системи);
- системами управління двигунами, машинами і живленням;
- системами контролю доступу;
- системами обслуговування пасажирів;
- публічними інтернет-мережами судна, призначеними для використання пасажирами;
- адміністративними системами та мережами;
- системами зв'язку [8].

Важливо розуміти, що кіберзагрози в морській галузі мають свою специфіку. Відрізняючись від звичайних комерційних систем, морське обладнання часто працює в автономному режимі тривалий час, що ускладнює процес оновлення програмного забезпечення та усунення вразливостей. Крім того, судна можуть перебувати в різних державах і юрисдикціях, що створює додаткові складнощі в забезпеченні кібербезпеки.

Зважаючи на таку вагому частку вразливих систем на судні, вітчизняні науковці наголошують на необхідності спеціального навчання членів екіпажу та забезпеченні можливістю оволодіти всіма необхідними навичками та компетенціями у сфері кібербезпеки [36, с. 130].

Ключову роль у забезпеченні кібербезпеки відіграє людський фактор. Екіпаж судна повинен мати відповідну підготовку та розуміння основних принципів кібербезпеки. Це включає вміння розпізнавати потенційні загрози, правильне поводження з електронними пристроями та даними, дотримання протоколів безпеки при роботі з судновими системами. Тому, вважаємо вкрай актуальним розробку та запровадження спеціального навчання членів екіпажу та майбутніх моряків щодо «культури» кібербезпеки, прививаючи їм

такі навички, щоб члени екіпажу були в змозі вирішувати необхідні задачі, пов’язані з кібербезпекою судна, оцінки кібербезпеки судна, складати разом із судноплавними компаніями та керуватися планом дій екіпажу при настанні кіберінциденту.

При цьому, зараження програмного забезпечення на судні є одним з найнебезпечніших і розповсюджених шляхів надання кіберзлочинцям доступу до управління судном. Наприклад, підключення флеш-носія або мобільного пристрою будь-якого члена екіпажу до вищенаведених суднових систем може обернутися наданням несанкціонованого доступу хакерам до критично важливих систем на судні, які безпосередньо пов’язані із безпекою людського життя, вантажу і самого судна.

2.2. Види кібератак у морському секторі

Кібератаки – цілеспрямовані дії у кіберпросторі, що вчиняються завдяки електронним засобам і мають певну мету, наприклад, порушення приватності, неподільності чи відкритості даних, несанкціонований доступ до них, а також порушення безпеки, стабільної та надійної роботи комунікаційних і/або технологічних систем. У свою чергу, кіберінцидент – подія або серія негативних випадків ненавмисного характеру та/або таких, що мають властивості кібератаки, які загрожують безпеці систем електронних комунікацій та технологічних систем, створюють ризик порушення нормальної роботи таких систем (включаючи блокування їх функціонування, а також несанкціоноване управління їх ресурсами) і загрожують захищеності електронних інформаційних ресурсів [21].

Тільки за останні декілька років новини про морські кібератаки не зникають з порядку денного у засобах масової інформації.

Приміром, порт Лісабона у грудні 2022 р. став мішенню програм LockBit, які шифрують дані на сервері та вимагають кошти за надання доступу до них. Через це роботу порту було призупинено на 4 дні, що потягнуло за собою великі матеріальні збитки усіх сторін відносин у сфері

морських перевезень. У лютому 2022 року нафтові компанії Oiltanking та Mabanaft зазнали кібератаки, яка пошкодила їхні системи розвантаження і завантаження, через що керівництвом компаній було оголошено форс-мажор [28, с. 127]. За даними Ради Національної Безпеки і Оборони України, норвезьке класифікаційне товариство DNV (Det Norske Veritas) у 2023 р. заявило про кібератаку на власне програмне забезпечення через яку постраждало близька 1000 обслугованих суден, включаючи мобільні офшорні установки [49].

Навіть IT-системи Міжнародної морської організації (IMO) у 2020 році піддалися кібератаці, внаслідок чого були відключені онлайн-сервіси організації та веб-сайт IMO [32, с. 105]. Важливо зазначити, що такі випадки не є поодинокими, кібератаки здійснюються майже щодня. На жаль, компанії досі побоюються розголошувати інформацію про понесення ними колосальних збитків в результаті таких обставин, через можливість втрати іміджу на світовому ринку. І на нашу думку, це є помилкою з боку головних акторів галузі, бо саме вони, поєднавшись, зможуть стати рушійною силою в ініціюванні ефективної боротьби з кіберзлочинами.

Задля того, щоб усвідомити всю значущість проблеми кібербезпеки на морі та масштаби загрози усій галузі від потенційних кібератак, вважаємо за необхідне розглянути детальніше їхні витоки у сучасній історії.

Кіберзлочини поступово з’являлися на порядку денному, активізація розпочалась з 2010-х років, по мірі комп’ютеризації галузі. Згадувана кібератака на порт Антверпен була початком масштабування таких явищ по всьому світу.

У липні 2013 року студентам з університету Остіна, Штату Техас (США), вдалося відхилити від курсу 213-футову приватну яхту вартістю 80 мільйонів доларів США за допомогою GPS-спуфінгу. Цікавим виступає те, що при цьому групою дослідників було використано саморобне обладнання ціною менше трьох тисяч доларів США. Таким чином, вони сформулювали в

опублікованих матеріалах про цей експеримент, що спуфінг (spoofing) – це вид кібератаки, за якої створюються фальшиві сигнали GPS для отримання контролю над GPS-приймачами судна. Мета експерименту полягала в тому, щоб визначити ступінь складності проведення такої кібератаки на морі та дізнатися, наскільки швидко і легко суднові системи можуть ідентифікувати загрозу [78].

На даний час, майже усі відомі на світовому ринку копанії-судновласники побували в ролі жертви кібератаки.

У 2017 році, внаслідок масштабної кібератаки із зараженням вірусу з програмою-вимагачем «NotPetya» комп'ютерних систем державних та приватних установ, підприємств та організацій в Україні, в одеському офісі компанії Maersk також було вражено корпоративну мережу компанії, тим самим вірус «NotPetya» дістав аж до Копенгагену. 17 з 76 вантажних терміналів компанії по всьому світу зупинили свою роботу, загалом знадобилося більше тижня, щоб відновити повністю функціонування усіх серверів та сервісів. Вважається, що вже з того часу було розпочато кібератаки російських спецслужб на українські сервери, з метою послаблення державного суверенітету України. При цьому, постраждалими стали і міжнародні корпорації, офіційно Maersk було визнано понесених збитків на 300 млн доларів США, утім за неофіційними даними співробітників компанії, збитки внаслідок кібератаки сягали суми вдвічі більше названої [63, p.11].

У 2021 році від кібератаки постраждала компанія Mediterranean Shipping Co (MSC). Через вимкнення мережі в одному з головних центрів компанії у Женеві, веб-сайт MSC був вимкнений протягом 10 годин, а соціальні мережі та інші засоби Інтернет-комунікації були недоступні, не працювали поштові служби [28, с. 126].

Звернувшись до закордонних досліджень, проведених на міжнародному рівні, визначено, що кожного року кібератаки спричиняють бізнесу все більше збитків, що не може не лякати акторів галузі мореплавства. У

дослідженні міжнародної юридичної фірми HFW та компанії, яка займається комп’ютерним обслуговуванням суден CyberOwl дослідники провели опитування професіоналів і працівників морської галузі та дійшли висновку, що зараз середня вартість одної кібератаки коштує 3,2 мільйони доларів США, які компанії виплачують кіберзлочинцям в обмін на розблокування своїх серверів та комп’ютерних систем. При цьому, 14% опитуваних зізналися, що заплатили такий «викуп» кіберзлочинцям в 2023 році, порівняно з 3% в 2022 році, тобто за останні роки збільшилася як сама кількість кібератак, разом з їхньою потужністю та серйозними наслідками, так і суми, які кіберзлочинці вимагають від постраждалих взамін на доступ до своїх даних і комп’ютерних систем [63, p.14].

Зазначимо, що на сьогоднішній день існують багато онлайн-платформ та міжнародних організацій, які аналізують тенденції розвитку цифрових ризиків у світі, створено електронну мапу з даними щодо кібератак в морській галузі. Наряду з ними і така авторитетна організація, як норвезьке класифікаційне товариство DNV, у 2023 році опублікувало звіт «Maritime cyber priority 2023» («Морські кіберпріорітети 2023»), в якому, серед іншого, чітко вбачається статистика розвитку і збільшення кібератак саме під час російсько-українського конфлікту, активізація в останні роки кіберзлочинців пов’язується з початком повномасштабного вторгнення держави-терориста на територію України, а найсерйозніші кібератаки майже щодня здійснюються російськими хакерами [65].

Дійсно, міжнародним співтовариством вже не раз було визнано безпосередній зв'язок війни в Україні з такими важливими питаннями, як світова економіка і безпека, міжнародний правопорядок тощо. Тому, на нашу думку, необхідно звернути увагу на той факт, що загарбницькі дії рф, починаючи з 2014 року, мають вплив не тільки на всі держави та економіки світу, а включають ще і безпеку мореплавства та навколишнього природнього середовища. Адже потенційно внаслідок таких подій може постраждати

природнє середовище. Приміром, наприкінці жовтня 2023 р. в Балтійському морі біля Шведського містечка Хьорвік пароплав Marco Polo сів на мілину через «невірні дії екіпажу судна, слідуючи за несправним сигналом GPS», внаслідок чого стався витік нафти та дизельного палива, діставши до узбережжя. Розслідування обставин інциденту ще триває, але припускається вірогідність кібератаки, внаслідок якої було змінено курс руху судна або пошкоджено сигнал навігатора [73].

Таким чином, проаналізувавши випадки різних кібератак на системи портової інфраструктури та суден по всьому світу, можна виділити кілька основних видів кібератак, які успішно здійснюються у морській сфері:

- фішинг (phishing) та соціальна інженерія. Здійснюється надсилання масових електронних листів із шкідливими посиланнями або вкладеннями, які виглядають як звичайні повідомлення від відомих компаній чи осіб. Злочинці отримують доступ до конфіденційних даних членів екіпажу або навіть суднових агентів через масову розсилку електронних листів від вигаданих/підроблених відправників [45]. Варто сказати, що багато чого залежить від уважності та обізнаності працівника, який, наприклад, активувавши посилання та ввівши свою конфіденційну інформацію, яка є ключом доступу до важливих систем, може дати зловмиснику «по іншу сторону» можливість впливати на рух судна через одержання контролю над судновими системами або на роботу судноплавної компанії, залежно від цілі хакера. Тому в обов’язковому порядку правила поведінки і план дій у таких ситуаціях повинні чітко регламентуватися, реалізовуватися та контролюватися керівництвом.

- спуфінг, за якого створюються фальшиві сигнали GPS для отримання контролю над GPS-приймачами судна.

- шкідливе ПЗ (програмне забезпечення, віруси) багато кібератак починаються із зараження систем шкідливим програмним забезпеченням. Шкідливі програми можуть впроваджуватись через електронну пошту,

фішинг, заражені веб-сайти або навіть фізичні пристрої (флешки). Після проникнення вірус може шпигувати, красти дані або виводити системи з ладу.

- DDoS-атаки (розподілені атаки на відмову в обслуговуванні) цілеспрямовані на перевантаження технологій трафіком, що призводить до їх недоступності. У контексті морських портів та суден такі атаки можуть паралізувати роботу систем управління та моніторингу, що створює серйозні перебої в логістиці і спричиняє великі економічні втрати [30, с. 26]. Зауважимо, що цей перелік не є вичерпним.

Цілком зрозумілим є факт того, що по мірі збільшення кількості комп'ютерних та автоматизованих систем збільшуються і ризики їхнього зламу. Таким чином, забезпечення кібербезпеки мореплавства стає критично важливим елементом глобальної безпеки. Необхідність розробки та впровадження новітніх технологій для запобігання кібератакам, а також проведення навчань і підвищення кваліфікації персоналу є ключовими кроками для захисту морських перевезень [81, с. 70].

Зважаючи на стрімкий розвиток технологій та наміри ввести в дію автономні судна і порти, які будуть повністю оперуватися комп'ютерними системами (та штучним інтелектом) навіть поза людським контролем, необхідно розглядати усі наявні комп'ютерні системи на суднах та у портах, на мобільних офшорних установках та ін. – як потенційно вразливі до кібератак, а так зване «кіберпіратство» стає поступово заміняти піратство за масштабністю наслідків та збитків. Тому морське право, будучи системою, яка постійно розвивається, має адаптуватися до нових викликів і реалій, щоб залишатися ефективним регулятором міжнародних відносин у сфері мореплавства.

Відмінно від звичного морського піратства, яке передбачає фізичне захоплення суден, кіберпіратство діє у віртуальному просторі, але може мати не менш руйнівні наслідки для судноплавства та морської торгівлі. Особливо

небезпечними є атаки, спрямовані на навігаційні системи, системи управління вантажними операціями та критично важливе обладнання суден. Особливу небезпеку становить те, що кіберпірати можуть атакувати судна, перебуваючи на значній відстані від них.

Протидія кіберпіратству вимагає комплексного підходу, що включає технічні, організаційні та правові заходи, якими є постійне вдосконалення систем захисту, проведення регулярних аудитів безпеки та навчання персоналу навичкам розпізнавання і реагування на кіберзагрози. Важливим є також розвиток міжнародного співробітництва у сфері протидії кіберпіратству, включаючи обмін інформацією про загрози та координацію дій правоохоронних органів різних країн. Значну роль у протидії кіберпіратству відіграє превентивний підхід. Судноплавні компанії повинні впроваджувати сучасні системи кіберзахисту, регулярно оновлювати програмне забезпечення, проводити тестування та мати чіткі процедури реагування на кіберінциденти. Першочерговим завданням є забезпечення надійного та безпечного стану критично важливої інформації та систем.

Надалі, проблема кіберпіратства може стати ще більш актуальною з появою автономних суден та розширенням використання штучного інтелекту в морській галузі. Для цього буде необхідно постійно вдосконалювати методи захисту та розробляти нові підходи для забезпечення кібербезпеки.

Таким чином, кіберпіратство є серйозною загрозою для сучасного мореплавства, що вимагає постійної уваги та системного підходу до протидії. Успішна боротьба з цим явищем можлива лише за умови тісної співпраці всіх учасників морської галузі, включаючи судноплавні компанії, портову владу, виробників обладнання та міжнародні організації.

2.3. Запровадження новітніх технологій як потенційних ризиків у забезпеченні кібербезпеки мореплавства

Морська галузь має тенденцію до невпинного розвитку. Технічний прогрес безперервно розвивається, а вчені продовжують вражати своїми

винаходами, перетворюючи фантастичні проекти на реальність, яка з часом стає частиною повсякденного життя. Яскравий приклад цього – ідея та практичне її втілення у створення автоматизованих, безпілотних суден. Через активний розвиток і впровадження автономного судноплавства, штучного інтелекту та Інтернету речей в реальне життя, це питання потребує правової регламентації та аналізу на рівні міжнародного права.

На даний час вже реалізовано ряд дороговартісних проектів стосовно цього, деякі ще продовжують розвиватися, але вбачається подальша активізація зацікавленості судноплавних компаній та міжнародних організацій. Так, за даними аналітиків BIS Research, очікуваний прибуток завдяки продажу автономних суден по всьому світу сягає близько чотирьох мільярдів доларів США до 2035 року [35, с.152].

Автономні судна мають низку очевидних переваг, до яких можемо віднести усунення людського фактору як потенційної причини аварій, можливість прокладати оптимальні маршрути з урахуванням погодних умов і навігаційних небезпек, значне зменшення витрат на підготовку та утримання екіпажу, а також мінімізація шкідливих викидів вуглекислого газу завдяки екологічності сучасних технологій, що робить їх особливо актуальними у наш час.

Водночас використання автономних суден може породжувати низку викликів, зокрема пов’язаних із забезпеченням кібербезпеки автоматизованих систем управління, щоб запобігти несанкціонованому втручанню в їхню роботу. Потрапивши під контроль зловмисника, судно може бути використане на його розсуд, що створює ризики для безпеки мореплавства, довкілля, а також загрожує значними збитками судновласникам та іншим сторонам відносин морських перевезень. Крім того, виникають проблеми з оперативним ремонтом на борту під час плавання, відсутністю чітких протоколів дій у разі втрати зв’язку з судном

або необхідності термінової зміни курсу, що підкреслює складність інтеграції таких технологій у морську галузь.

Насправді, багато практичних та правових питань виникає, коли йдеться про автономне судноплавство. Правові проблеми стосуються, здебільшого, визначення їхнього правового статусу, регулювання їхнього руху з урахуванням вимог безпеки судноплавства, встановлення відповідальної особи за безпеку на борту, забезпечення дотримання міжнародних стандартів у галузі та охорони природнього середовища.

Міжнародна морська організація (IMO) досі плідно займається розробкою правової та технічної бази для забезпечення ефективного використання таких суден. Відправною точкою став 2017 рік, прийнято рішення провести аналітичний огляд проблем, що виникають у процесі впровадження морських автономних надводних суден. А вже влітку того ж року Комітетом IMO з безпеки на морі (MSC) було прийнято рішення провести регуляторний огляд морських автономних надводних суден (Maritime Autonomous Surface Ships, MASS), в результаті чого було запропоновано визначити автономні судна, як такі, які через автоматизовані процеси можуть здійснювати прийняття рішень або виконання функцій, зазвичай покладених на людину, забезпечуючи частковий або повний контроль та управління судном, незалежно від місцезнаходження [31, с. 257].

Робота над Кодексом MASS триває, його прийняття як необов'язкового документу очікується у 2025 році. Кодекс охоплюватиме питання операційного контексту, оцінки ризиків, принципів проектування, програмного забезпечення, зв'язку, управління сигналами та людського фактору для MASS. Він також визначатиме цілі та функціональні вимоги щодо навігації, віддалених операцій, зв'язку, остійності, безпеки, пошуку і рятування, поводження з вантажем та безпеки персоналу.

Особливо турбує міжнародне співтовариство проблема кібербезпеки, адже автономне судно без екіпажу контролюється лише береговим

оператором та являє собою легку мішень для кіберзлочинців. Тому, на нашу думку, для того, щоб автономне судноплавство було запроваджено ефективно та безпечно для усіх акторів галузі мореплавства, існує нагальна потреба у розробці уніфікованих правил, стандартів та правової бази, яка б регулювала процеси починаючи від будування відповідного судна (напр., обов'язкова наявність певних вбудованих програм і систем, детекторів або інших технологій чи обладнання, яке б забезпечувало безпеку судна у кіберпросторі) до його експлуатації (напр., чіткий план дій у випадку можливої кібератаки або протидії кібератаці з подальшим відновленням усіх суднових систем тощо).

Постійно зростаюча потреба в передачі великих обсягів інформації у напрямку берег-судно-берег і судно-судно позначилося на розвитку супутникових систем зв'язку на всьому морському просторі, і це є одним із вагомих стадій розвитку технології Інтернету речей в мореплавстві.

У морській індустрії поступово впроваджуються різні додаткові супутникові сервіси, такі як згадуваний INMARSAT і VSAT (Very Small Aperture Terminal, мала супутникова наземна станція), які можуть забезпечити безперебійний зв'язок для будь-якого морського чи річкового судна за сучасними широкосмуговими стандартами. Взагалі, Інтернет речей (Internet of Things, IoT) представляє собою всесвітню мережу фізичних пристроїв, з'єднаних з Інтернетом, які обладнані сенсорами, датчиками тощо для обміну інформацією. Відповідні технології з'єднані через підключення до центрів контролю, управління та обробки даних [33, с. 213]. У наш час це явище зустрічається в повсякденному житті кожної людини.

Промисловий Інтернет речей вже здійснює вплив на всі сфери судноплавства – від вантажних перевізників до круїзних лайнерів і риболовецьких суден і виступає також дуже вразливою мережею до кібератак з огляду на свою функцію з об'єднання систем в один «ланцюг». Один з ключових нюансів використання IoT полягає у великій кількості

різних пристроїв, технологій та безпекових програм, що ускладнює впровадження єдиного підходу до забезпечення безпеки усієї мережі.

Найсуттєвішими викликами у сфері Інтернету речей постають питання безпеки та захисту інформації. Специфіка технологій IoT, яка передбачає збирання, поширення та опрацювання величезних масивів інформації та персональних даних, що територіально та технологічно розподілені, суттєво підвищує вразливість приватної інформації про кожного користувача та створює додаткові загрози для її конфіденційності [33, с. 213]. Така ситуація природно породжує занепокоєння щодо надійності систем збереження персональної інформації та належного законодавчого забезпечення її захисту від неправомірного використання сторонніми особами.

Слід зауважити, що поступово, як галузь судноплавства швидко трансформується від традиційних суден до дистанційно керованих суден і автономних суден, вона і ширше використовує досягнення людства у запровадженні штучного інтелекту, які на наразі є застосованими у житті суспільства.

Відмітимо, що Сінгапурський університет управління (SMU), корпорація Fujitsu та Інститут високопродуктивних обчислень (IHPC) розробляють передові технології опрацювання даних та штучного інтелекту для оптимізації навігації суден у сінгапурському порту та вздовж найінтенсивніших морських шляхів планети – Сінгапурської та Малаккської проток [25, с. 315]. Мета проекту полягає у впровадженні новітньої системи координації морського трафіку, сінгапурський порт планує до 2025 року повністю автоматизувати процес бункерування, відмовившись від паперового документообігу. Додатково передбачається запуск двох програмних рішень на основі штучного інтелекту, покликаних оптимізувати швидкість та підвищити точність процедури оновлення сертифікатів для суден під сінгапурським прапором. Перед сінгапурським портом поставлено

амбітну мету: до 2040 року трансформуватися у провідний, повністю автоматизований морський порт [25, с. 316].

Розглядаючи досвід Сінгапуру в розрізі застосування новітніх технологій у галузі мореплавства зазначимо, що законодавство держави у сфері використання штучного інтелекту здобуло високу оцінку від провідних світових експертів.

Важливу роль у розвитку і впровадженню новітніх технологій, зокрема штучного інтелекту, відіграє дотримання етичних засад та забезпечення прозорості та ефективності врегулювання таких процесів. Для досягнення цієї мети уряд держави впровадив комплексну систему регулювання, що включає стратегію кібербезпеки, галузеві закони щодо захисту персональних даних, кодифіковані акти стосовно користування штучним інтелектом та іншими цифровими технологіями тощо. Подібна нормативно-правова база дає змогу завчасно виявляти потенційні ризики, пов'язані із застосуванням новітніх технологій. С.Р. Асірян констатує, що законодавче підґрунтя Сінгапуру відзначається гнучкістю та адаптивністю, містить дієві механізми оцінювання ситуації та внесення змін до нормативних актів, що дає змогу державі оперативно вирішувати нові проблеми сучасності, поєднуючи з надійним захистом прав та інтересів своїх підданих [25, с. 317].

На наше переконання, позитивний досвід Сінгапуру в інтеграції передових технологій для оптимізації морської інфраструктури може бути важливим орієнтиром для міжнародного співтовариства, зокрема й для України. Враховуючи стратегічне географічне розташування України, її потенціал у розвитку портової інфраструктури, а також інноваційні можливості в цифрових технологіях, наша країна має всі передумови для того, щоб стати провідним гравцем на морській арені після відновлення. Сінгапур уже довів, як використання штучного інтелекту та автоматизації може суттєво підвищити ефективність і безпеку морських перевезень, а також трансформувати морські порти в центр високих технологій і сталого

розвитку. Україна, з її потужними морськими портами, доступом до Чорного і Азовського морів, а також сильним науково-технічним потенціалом, має шанс не лише адаптувати ці інноваційні підходи, але й впроваджувати їх на місцевому рівні, зокрема для покращення національної економіки, безпеки і розвитку морського транспорту. Тому важливо, щоб міжнародне співтовариство, в тому числі й Україна, враховувало цей досвід і активно впроваджувало аналогічні практики в галузі цифровізації морської інфраструктури. Це дозволить не лише зміцнити позиції України в глобальному морському бізнесі, а й забезпечити безпечне, ефективне та технологічно передове функціонування всіх компонентів морської галузі.

Іноземні науковці зазначають, що зараз штучний інтелект (ШІ) посідає вагоме місце у розробці та експлуатації автономних транспортних засобів, до яких відносять і судна. Інтеграція алгоритмів ШІ дозволяє їм керувати, сприймати та адаптуватися до динамічного середовища, що робить їх безпечнішими та ефективнішими. Очікується, що постійне вдосконалення технологій штучного інтелекту ще більше розширить можливості та безпеку автономних транспортних засобів у майбутньому. Розробка автономних систем переживає трансформаційну еволюцію через інтеграцію штучного інтелекту, який стає невід'ємною частиною багатьох аспектів розробки програм та використання автономних транспортних засобів. Звертається увага на тому, що кібератаки з фальсифікацією даних матимуть вирішальну роль у контексті безпілотної автономної навігації [55, p. 20].

Інтеграція штучного інтелекту в галузь мореплавства відкриває нові перспективи для вдосконалення морських операцій за критеріями ефективності, точності та безпеки їх проведення. Завдяки технологіям штучного інтелекту можна автоматизувати складні процеси, такі як навігація, управління судном і виявлення перешкод, що дозволяє скоротити витрати на екіпаж, зменшити людський фактор і підвищити загальну продуктивність. Названі системи можуть опрацьовувати значні обсяги даних у реальному

часі, визначати погодні умови, попереджати зіткнення, оптимізувати маршрути та зменшувати споживання палива, що позитивно впливає на екологічну стійкість галузі.

Однак, разом з цими перевагами, інтеграція ШІ в мореплавство посилює залежність від кіберінфраструктури та підвищує рівень кіберризиків. Зважаючи на те, що автономні судна й інтелектуальні системи керування покладаються на підключення до мереж, передачу даних та віддалений моніторинг, вони стають вразливими до кіберзагроз. Кібератаки на ці системи можуть призвести до колосальних наслідків: втрати контролю над судном, навмисного змінення курсу, блокування комунікацій, збоїв у навігаційних системах та навіть повного захоплення управління судном кіберзлочинцями. Такі атаки можуть не тільки загрожувати життю екіпажу та пасажирів, але й спричинити екологічні катастрофи, якщо судно перевозить небезпечні вантажі чи нафтопродукти.

Відтак, гарантування належного рівня кібербезпеки в морській галузі набуває першочергового значення. Необхідно розробляти новітні технології кіберзахисту, зокрема для автономних систем і мережевої інфраструктури суден. До таких технологій відносяться багаторівнева автентифікація, шифрування даних, алгоритми виявлення кіберзагроз тощо.

РОЗДІЛ 3

ПРАВОВЕ РЕГУЛЮВАННЯ МОРСЬКОЇ КІБЕРБЕЗПЕКИ ТА ШЛЯХИ ЙОГО УДОСКОНАЛЕННЯ

3.1. Міжнародно-правові засади боротьби з кіберзлочинністю на морі

Незважаючи на критичну важливість кібербезпеки, на глобальному рівні досі не існує всеосяжного міжнародного договору, що встановлював би єдині міжнародні стандарти у цій сфері. Адже кіберпростір є відносно новим явищем, міжнародні організації не ухвалили якусь значну кількість юридично-обов'язкових угод чи конвенцій стосовно цього. Дискусії з даного питання тривають, але через різні підходи країн, зокрема щодо термінології та недопущення втручання у внутрішні справи, вони просуваються повільно і з труднощами.

Український науковець Д. В. Дубов у своїх дослідженнях, присвячених кіберпростору як нового фронту в геополітиці, неодноразово звертає увагу на протистояння між США, рф та Китаєм і констатує: «США наразі є найбільшою країною світу, яка зуміла вибудувати сучасний кібернетичний простір й одноосібно задає в ньому правила гри» [29, с. 172], що дійсно не влаштовує її контрагентів, які також вважають кіберпростір частиною власних територій, на яку розповсюджується суверенітет.

Згадувана у першому розділі дослідження Конвенція Ради Європи про кіберзлочинність 2001 року на сьогоднішній день являється єдиним юридично-обов’язковим міжнародним документом у сфері кібербезпеки. Будучи взірцем для країн, які розробляють національне законодавство з протидії кіберзлочинності, а також основою для міжнародної співпраці між державами-учасниками, вона набула чинності в 2004 році. Україна ратифікувала її у 2005 році.

Положення Конвенції про кіберзлочинність мали на меті не тільки класифікувати кібернетичні злочини та встановити механізми боротьби з

ними, але й запропонувати державам-учасницям Ради Безпеки модельні положення для впровадження у їхнє національне законодавство норм щодо визначення категорій та конкретних видів кіберзлочинів. Додатковий протокол до цієї Конвенції розширив її сферу дії, криміналізувавши расистські та ксенофобні діяння, скоєні через комп'ютерні системи. Ці міжнародні документи містять два важливі переліки: обов'язкових для криміналізації у національному законодавстві держав-учасниць правопорушень, а також порушень, рекомендованих Радою Європи для включення до внутрішнього законодавства країн-підписантів [40, с. 98].

На проблематику кібербезпеки звертає увагу і така спеціалізована установа Організації Об’єднаних Націй, як Міжнародний союз електрозв’язку (МСЕ), що здійснює щорічну публікацію глобального індексу кібербезпеки, який відображає залученість країн до розвитку галузі на світовому рівні, що сприяє підвищенню усвідомлення важливості цього питання. Організація проводить комплексний моніторинг глобального прогресу за п'ятьма ключовими напрямами:

1) впровадження законодавства;

2) реалізація технічних заходів;

3) реалізація організаційних заходів;

4) зміцнення потенціалу галузі;

5) розвиток міжнародної співпраці [56].

Станом на 2024 рік, Україна знаходиться в числі «держав, чия участь у протидії кіберзагрозам перебуває на етапі становлення» через незадовільний стан, у порівнянні з іншими європейськими державами, організаційних та технічних заходів, міжнародної співпраці [56].

Взагалі, хоча наразі не існує єдиного універсального міжнародного договору з питань кібербезпеки, базовими документами, що визначають принципи посилення захисту в кіберпросторі для держав, слугують також Конвенція ООН проти транснаціональної організованої злочинності 2000

року та Статут Міжнародного союзу електрозв'язку 1992 року, доповнений положеннями Доповіді ООН про кібербезпеку 2015 року.

На сьогодні розроблено низку рекомендацій щодо забезпечення кібербезпеки на морському транспорті, підготовлених провідними міжнародними морськими організаціями. Водночас відсутній єдиний врегульований підхід до опису визначених кіберзагроз і, тим більше, до їх оцінки.

У розробці правової бази у цій сфері найбільш ефективно доклала зусиль ІМО, прийнявши у 2017 році два вкрай важливі документи, які сьогодні практично виступають правовою основою в галузі морської кібербезпеки та періодично оновлюються. Перш за все, це схвалені у квітні 2017 року рекомендації щодо захисту морської галузі від реальних та потенційних кіберзагроз та мінімізації чинників уразливості, запроваджені у Циркулярі MSC-FAL.1/Circ.3 «Guidelines on maritime cyber risk management» (Керівництво з управління кіберризиками на морі, остання редакція 2022 р.).

У п.п. 1.1 цього Документу визначено, що морський кіберризик означає ступінь вразливості технологічного ресурсу (системи) до потенційних ситуацій чи подій, здатних спричинити збої у функціонуванні судна та становити загрозу безпеці судноплавства через пошкодження або втрату інформації та систем управління. Відповідно до п.п. 2.1.4 до загроз входять зловмисні дії (напр., зламування або впровадження шкідливого програмного забезпечення) та ненавмисні наслідки сумлінних дій (напр., обслуговування програмного забезпечення або надання прав доступу користувачам). Загалом, такі дії або виявляють вразливості (застаріле програмне забезпечення або неефективне), або пов'язані з навмисним використанням вразливостей експлуатаційних або інформаційних технологій. Ефективне управління кіберризиками має враховувати обидва ці види загроз (п.п. 2.1.4) [8].

Також акцентується увага на інформаційних та операційних системах, а саме у п.п. 2.1.2 закріплено, що IT-системи орієнтовані на використання

даних як інформації, натомість ОТ-системи можна розглядати як спрямовані на користування даними заради контролю або моніторингу фізичних процесів. Ефективне управління кіберризиками повинне також зважати на вплив на безпеку та захищеність, що виникає внаслідок виявлення або використання вразливостей в інформаційно-технологічних системах. Це може бути наслідком неналежного підключення до операційних технологічних систем або процедурних помилок персоналу чи третіх осіб, які можуть скомпрометувати ці системи (наприклад, неналежне використання знімних носіїв, таких як карта пам'яті) (п.п.2.1.6). Для цілей цього документу, управління кіберризиками означає процес виявлення, аналізу, оцінки та інформування про кіберризики, а також прийняття, уникнення, передачу або зменшення їх до прийнятного рівня, враховуючи витрати та прибуток від вжитих заходів для зацікавлених сторін, метою управління морськими кіберризиками проголошено підтримку безпечного судноплавства, яке є непохитним до кіберризиків (п.п.3.1-3.2) [8].

Загалом, Керівництво з управління кіберризиками на морі складають п’ять ключових компонентів, спрямованих на ефективне управління ризиками: 1) ідентифікація: розподіл обов'язків персоналу щодо управління кіберризиками та виявлення ресурсів і технологій, які у разі порушення їхньої роботи можуть становити загрозу для суднових операцій.; 2) захист: впровадження процесів і заходів контролю ризиків, а також планування на випадок надзвичайних ситуацій для захисту від кіберінцидентів; 3) виявлення: створення та запровадження заходів, спрямованих на оперативне розпізнання кіберінциденту; 4) реагування: розробка та введення заходів і програм для забезпечення стійкості та відновлення систем, робота яких порушена через кіберінцидент; 5) відновлення: проведення резервного копіювання та регенерації систем, важливих для процесів, які були порушені внаслідок кіберінциденту [8].

Сторони відносин морських перевезень мають застосовувати відповідні механізми для захисту галузі від існуючих та потенційних небезпек і вразливостей, виникаючих через діджиталізацію та автоматизацію операцій і систем на морському транспорті. Організація наголошує, що ефективне управління ризиками повинно походити від керівництва, поступово формуючи культуру обізнаності в усіх ланках організації та перетворюючись на ефективний механізм управління кіберризиками (п.п.3.3) [8].

Другим важливим документом виступає Резолюція MSC.428(98) «Управління кіберризиками в морській галузі в рамках систем управління безпекою», що закликає країни створити належні умови для того, щоб кіберризики були враховані в наявних системах безпеки, відповідно до вимог Міжнародного кодексу з управління безпечною експлуатацією суден та запобігання забрудненню (МКУБ). Резолюція передбачає перевірку документів судноплавних компаній на відповідність МКУБ з 1.01.2021 року [7]. Ця дата стала першим обов'язковим етапом у впровадженні вимог кібербезпеки мореплавства та вагомим поштовхом для захисту галузі від постійно зростаючих кіберзагроз.

Однак, галузеві неурядові міжнародні організації активно сприяють введенню управління кіберризиками у культуру забезпечення безпеки, з метою запобігання серйозним інцидентам, створюючи основні принципи та рекомендації технічного характеру.

Так, Балтійська та міжнародна морська рада (BIMCO), Міжнародна асоціація судновласників суховантажних суден (INTERCARGO), Міжнародна асоціація незалежних власників танкерів (INTERTANKO), Міжнародна палата судноплавства (ICS) у співпраці з іншими судноплавними організаціями випускають «Guidelines on Cyber Security on board Ships» (Керівництво з кібербезпеки на борту суден, у 2020 р. вийшла 4 оновлена версія). Цей документ рекомендований ІМО у п.п. 4.2 Циркуляру MSC-FAL.1/Circ.3 [8]. Відповідно, Керівництво пропонує власникам суден і

операторам інструкції щодо здійснення оцінки їх процесів і створення необхідних процедур та дій для вдосконалення стійкості і підтримці цілісності систем на суднах, також наведено основні теоретичні, технічні, практичні аспекти кібербезпеки мореплавства, вперше описані нюанси управління морськими кіберризиками, описана різниця між операційними та інформаційними технологіями, основні кіберризики у галузі тощо. Також керівництво пропонує відповідні заходи та методи по усуненню кіберризиків у галузі [74].

Також увага акцентується на важливості оцінки ризиків у кожній системі на судні. Для забезпечення актуальності результатів, оцінка ризиків має бути повторюваною процедурою, а не одиночним заходом. Вона складається з чотирьох етапів: 1) попереднє оцінювання, під час якого здійснюється вивчення документації з технічного обслуговування та підтримки систем; 2) основна оцінка судна, що полягає у вивченні кожної системи окремо; такі заходи можуть включати перевірку конфігурації усіх комп'ютерів, серверів, маршрутизаторів тощо, до цього залучається екіпаж судна разом з «командою з оцінки кіберризиків», яка може складатися з працівників судноплавної компанії; 3) підсумки та звітність: відбиття на документі основної інформації щодо виявлених вразливостей систем, ймовірність їх несанкціонованого використання, наслідки для екіпажу, судна і навколишнього середовища, а також відповідні технічні рекомендації щодо усунення і пом'якшення наслідків; 4) надіслання звітів зацікавленим сторонам та виробникам систем [74].

Підхід до глибоко інтегрованого захисту заохочує поєднання: фізичної безпеки судна відповідно до плану безпеки судна (Ship Security Plan, SSP); захист мереж, включаючи їхню ефективну сегментацію; виявлення кіберризиків та кіберінцидентів; періодичне сканування і тестування вразливостей; якісний та надійний, оновлений стан програмного забезпечення; контроль доступу до мереж та обладнання з відповідними

кількома рівнями ідентиіфкації; відповідні процедури щодо використання змінних носіїв і «культури кібербезпеки» – систематичне оновлення паролів, правила користуванням соціальними мережами та обладнанням і т.д.; обізнаність персоналу про наявні кіберризики, наявність у працівників навичок безпечного користування IT та OT технологіями та керування з відповідними процедурами щодо оцінки і мінімізації ризиків кібератак, захисту, реагування і відновлення внаслідок кіберінциденту [74]. Навчання та інформування повинні бути адаптовані до відповідних рівнів для суднового персоналу, включаючи капітана, офіцерів і членів екіпажу, береговий персонал, який підтримує управління, завантаження, вивантаження та експлуатацію судна.

Багато інших міжнародних організацій не залишаються осторонь проблематики кібербезпеки мореплавства, наприклад, Міжнародна спілка морського страхування (International Union of Marine Insurance, IUMI) у 2020 році опублікувала стратегічну програму, яка включає розділ 3. «Кіберризики» [36, с. 169].

Міжнародна асоціація класифікаційних товариств (IACS) суттєво сприяє аналізу цього питання, опублікувавши у 2020 році Рекомендацію з кіберстійкості (Рекомендація № 166). Ціль Рекомендації №166 полягає в тому, щоб надати зацікавленим сторонам вимоги для підтримки кіберстійкості суден протягом усього терміну експлуатації та побудови системи управління кібербезпекою (СУКБ). Ця рекомендація розроблена у розвиток документів ІМО з кібербезпеки. Так, має забезпечуватися якість даних (Data Quality), що виділяється як дії, спрямовані на забезпечення безпеки даних, що генеруються, оброблюються, передаються та зберігаються в процесі експлуатації комп'ютерних систем судна [69].

Три нижченаведені терміни є основними рисами, які відносяться до якості даних та інформації, які сприяють захищеності від кібератак: конфіденційність (confidentiality) – властивість інформації бути недоступною

чи закритою для неавторизованих осіб чи процесів; цілісність (integrity) – властивість збереження правильності та повноти даних; доступність (availability) - властивість бути в доступності та готовим до використання на запит авторизованого суб'єкта [69]. Тобто будь-які дані повинні бути конфіденційними, цілісними та доступними задля їхнього ефективного захисту, зберігання, обробки.

У п.п. 4.1.8 кібератака розглядається як будь-який тип посягання, який спрямований на IT- та OT-системи, комп’ютерні мережі та/або персональні комп’ютерні пристрої та намагається скомпрометувати, знищити або отримати доступ до систем і даних компанії та судна. Кіберінцидент розуміється як подія, яка фактично або потенційно призводить до несприятливих наслідків для бортової системи, мережі та комп’ютера або інформації, яку вони обробляють, зберігають або передають, і яка може вимагати відповідних дій для пом’якшення наслідків [69].

Рекомендація включає вимоги щодо: інвентаризації суднового комп'ютерного обладнання (hardware) та програмного забезпечення (software); технічного обслуговування суднового комп'ютерного обладнання та програмного забезпечення; готовності до аварійних збоїв у роботі суднового комп'ютерного обладнання та програмного забезпечення; документації та звітності.

З метою забезпечення необхідності підвищення кіберстійкості суден, минулого року IACS опублікувала нові вимоги до суден: UR E26 «Кіберстійкість суден» і UR E27 «Кіберстійкість бортових систем і обладнання», які застосовуються до нових суден з 1 січня 2024 року. Організацією введено нове поняття – «кіберстійкість», яке означає властивість інформаційної системи, що дозволяє екіпажу та судну існувати в умовах безперервних або постійних кібератак щодо суднових комп'ютерних систем [57].

Вимога UR E26 націлена на забезпечення безпечної інтеграції обладнання як OT так і IT технологій у мережу судна під час проектування, будівництва, введення в експлуатацію та терміну служби судна. Тим самим судно розглядається як колективний об'єкт для забезпечення кіберстійкості і охоплює п'ять ключових аспектів: ідентифікацію обладнання, захист, виявлення атак, реагування та відновлення [76].

Вимога URE27 спрямована на забезпечення захисту та зміцнення цілісності системи сторонніми постачальниками обладнання. Встановлює вимоги до кіберстійкості бортових систем та обладнання і містить додаткові вимоги щодо інтерфейсу між користувачами та комп'ютерними системами на борту, а також вимоги до дизайну та розробки нових пристроїв до їх впровадження на суднах [77].

Міжнародна асоціація портів і гаваней (IAPH), членом якої є українське Державне підприємство «Адміністрація морських портів України», випустила у 2021 р. Рекомендації щодо кібербезпеки для портів та портових споруд [36, с. 169]. Організація наголосила, що помітне зростання кіберзагроз, особливо після спалаху пандемії COVID-19. Тільки з лютого по травень 2020 року морська галузь в цілому постраждала від чотириразового збільшення кількості кібератак, вона збільшилася майже на 900% у порівнянні з 2017 роком. Забезпечення кібербезпеки визнано колективною відповідальністю [50]. Оскільки ідеального стану забезпечення безпеки досягти неможливо, створення здатності захищати критично важливі дані та інформацію, ідентифікувати загрози, виявляти порушення та ініціювати відповідні контрзаходи в рамках скоординованих дій реагування мають вирішальне значення.

З метою забезпечення ефективних заходів з кібербезпеки порту або об’єкту портової інфраструктури, слід: окреслити всі критично-важливі системи, мережі, дані та їхні вразливості (р. 6.4); оцінити та визначити пріоритетність усіх кіберризиків, з метою їх зменшення (р. 6); ідентифікувати

та регулярно переглядати всі загрози кібербезпеці, оцінюючи, як кожна з них може вплинути на діяльність об’єкта (р. 4); розробити систему безпеки, адаптувати її до конкретної організації з безперервним вдосконаленням (р. 11) разом із розробкою плану з реагування на кіберінцидент та відновлення [50].

Крім того, на рівні організації слід утворити внутрішню команду безпеки (або залучити третіх сторін) для контролю і закріплення заходів кібербезпеки в порту або об’єкті портової інфраструктури. Для всіх співробітників, які мають права доступу до цифрових даних, систем та/або інфраструктури, повинні бути встановлені захисні заходи. Вони включають ідентифікацію, інструктажі з кібербезпеки, визначення зобов'язань щодо забезпечення кібербезпеки та регулярні тренінги. При зміні персоналу слід своєчасно переглядати та/або відкликати дозволи на доступ, щоб уникнути накопичення облікових даних та запобігти потенційному ненавмисному доступу до них. Технологічним заходам відведена ключова роль, до них відносять контроль доступу, моніторинг мережі та захист систем, обладнання, даних та мережевої інфраструктури. Також, важливо створити групи реагування на інциденти кібербезпеки (CSIRT) [50].

Напрацювання міжнародних організацій неможливо оминути увагою, адже їхні розробки є дійсно важливими та користуються попитом у розвинутих країнах задля забезпечення кібербезпеки, але вони мають лише рекомендаційний характер.

Необхідно на міжнародному рівні визначити поняття і сутність морської кібербезпеки, закріпити її основні положення та ризики, окреслити необхідність, а найголовніше – шляхи забезпечення належного і високого стану захисту комп’ютерних систем як на судні, так і на березі, у портах та у судноплавних компаніях тощо. Впровадивши єдині вимоги, правила і принципи у сфері морської кібербезпеки на рівні міжнародних конвенцій, як наприклад було зроблено у Міжнародній конвенції з охорони людського

життя на морі 1974 р. (SOLAS) стосовно забезпечення безпеки людини на морі, вдасться мінімізувати випадки кіберпіратства та посилити колективну світову боротьбу з цими злочинами, не залишаючи акторів галузі мореплавства боротися самотужки, як це відбувається зараз. Не менш важливою є підготовка персоналу, проведення спеціальних навчань і тренінгів для працівників морської галузі щодо кібербезпеки.

Для розробки комплексного підходу до кібербезпеки у морському секторі необхідне створення міждержавної платформи співпраці через формування спеціалізованої робочої групи, яка має зосередитись на розробці деталізованих інструкцій з кібербезпеки та впровадженні найкращих практик у сфері морських ІКТ-технологій.

3.2. Національні нормативно-правові акти та стратегії морської кібербезпеки

Держави, як основні суб'єкти міжнародного права, також активно впроваджують у своє внутрішнє законодавство важливі засади та механізми боротьби із кіберзлочинністю. Так, розроблена у 2014 році Національним інститутом стандартів і технологій (NIST) США «Рамкова структура для поліпшення кібербезпеки критично важливої інфраструктури» (NIST CSF) рекомендована згадуваним циркуляром IMO MSC-FAL.1/Circ.3 (п.п. 4.2) [8].

NIST CF призначена для організацій усіх розмірів, секторів та рівнів, вона є універсальною, включаючи об'єкти критичної інфраструктури. Документ періодично оновлюється, з урахуванням динамічних глобальних змін, тому на сьогоднішній день діє актуальна версія від 26 лютого 2024 року. Він є консолідованим напрацюванням з кращих практик і стандартів, які описують побудову кібербезпеки в компаніях, складається з 3-х основних частин: ядро (бажані результати кібербезпеки організовані в ієрархію та приведені у відповідність до більш докладних інструкцій та засобів контролю), профілі (узгодження вимог та цілей організації, схильності до ризику та ресурсів з використанням бажаних результатів Framework Core) та

рівні реалізації (якісний захід організаційної практики управління ризиками кібербезпеки). Ключові атрибути фреймворку – адаптація до технологій і фаз життєвого циклу компаній, ризик-орієнтованість, застосовність у різних сферах, зведення багатьох міжнародних документів в один [75].

Основа надійного стану кібербезпеки складається з кількох одночасних і безперервних функцій; управління, визначення, захист, виявлення, реагування, відновлення. Вочевидь, ці положення стали основою для розробки вищезгаданих документів ІМО. У новій редакції документу з'явилася шоста функція – управління, яка визначає стратегію, очікування та політику організації, основу для визначення пріоритетів у розробці та виборі заходів в інших функціях.

Рівні реалізації (безпеки) визначають стан забезпечення організацією заходів щодо керування ризиками: 1) частковий (partial) – неповний підхід до управління кіберризиками і впровадження заходів безпеки; 2) інформований (risk informed) – визнається значення управління ризиками, запроваджуються дії для постійної оцінки та покращення власних заходів безпеки; 3) системний (repeatable) – регулярно використовуються власні розробки та заходи щодо забезпечення кібербезпеки; 4) адаптивний (adaptive) – постійно вдосконалюються підходи, зважаючи на стан ризиків та технологічні нововведення [75].

Таким чином, Рамкова структура для поліпшення кібербезпеки критично важливої інфраструктури є важливим документом, який не має жорстких приписів, що дозволяє організаціям адаптувати його відповідно до унікальних потреб та ризиків. Зокрема, він може бути використаний для оновлення методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інфраструктури, зокрема української.

Сполучені Штати Америки виступають взірцем не тільки демократії, а і всеохоплюючої роботи у сфері забезпечення кібербезпеки, політика країни

визначає пріоритетність захисту об’єктів критичної інфраструктури, до яких відносяться морські порти. Президентська директива від 26 липня 2016 року стала визначальним етапом у розвитку правового регулювання та організації системи кібербезпеки США, документ встановив ключові процедури виявлення, аналізу та реагування на кіберінциденти, які визначаються як подія в комп'ютерній мережі, що створює загрозу для цілісності, конфіденційності або доступності комп'ютерів, інформаційних чи комунікаційних систем, мереж та серверів. Це поняття також охоплює загрози для фізичної або віртуальної інфраструктури, що перебуває під контролем комп'ютерів чи інформаційних систем, включаючи інформацію, яка в них зберігається [17].

Загальновизнано, що Сполучені Штати Америки володіють найпотужнішою та найбільш комплексною системою управління інформаційною безпекою. Американська національна стратегія кібербезпеки зазнала останнього оновлення у березні 2023 року. Документ встановлює важливий принцип спільної відповідальності за захист критичної інфраструктури країни та управління кіберризиками, який розподіляється між приватним сектором та Федеральним Урядом. Стратегія окреслює сім ключових сфер, в яких пріоритетно провадиться діяльність щодо зменшення ризиків: національна безпека, що включає кібербезпеку, енергетичний сектор та енергетичні потужності, банківська справа та фінанси, система охорони здоров'я та безпеки, комунікаційні системи, інформаційні технології, а також транспортна інфраструктура [16]. Її основною метою є створення надійної та стійкої цифрової екосистеми, яка забезпечить повний захист конфіденційної та приватної інформації.

Адміністрація Джо Байдена наголошує, що для ефективної боротьби з неправомірною поведінкою в кіберпросторі необхідна злагоджена співпраця та координація між урядами різних країн світу [20]. Особливе значення цей документ має для України, оскільки містить п'ять конкретних пунктів, що

безпосередньо стосуються російського вторгнення в Україну та враховують досвід бойових дій, які тривають більше дев'яти років.

Захист урядових систем та державної інфраструктури США забезпечується розгалуженою мережею державних та федеральних структур, включаючи Федеральне агентство кібербезпеки та інфраструктури (CISA), Раду національної безпеки (NSC), Федеральне бюро розслідувань (FBI), Агентство національної безпеки (NSA), Міністерство оборони та Комісію з цінних паперів та бірж. Кожна з цих установ має у своїй структурі спеціалізовані відділи, що займаються питаннями кібербезпеки, запобіганням кібератакам та підготовкою до протидії, до складу всіх організацій входять висококваліфіковані експерти з кібербезпеки.

Адміністрація Президента активно працює з метою розширення партнерства із приватними компаніями та іншими державами, створивши Об'єднану групу з питань кіберзахисту (JCDC) при CISA для інтеграції планування і операцій з кіберзахисту в рамках федерального уряду, а також з приватним сектором і міжнародними партнерами; зміцнивши можливості Національної об'єднаної цільової групи з розслідування кіберзагроз (NCIJTF) для координації правоохоронних органів та інших заходів з протидії кіберзагрозам; і активізувавши роль Центру інтеграції розвідувальної інформації про кіберзагрози (CTIIC) в координації збору розвідувальних даних, їхнього аналізу і вдосконалення партнерських відносин з іншими країнами [16].

Галузь мореплавства також не залишається поза увагою американського законодавця, наряду із чисельними нормативними актами у галузі діє План відновлення морської інфраструктури (MIRP), який є одним із восьми планів, що підтримують Національну стратегію морської безпеки. У свою чергу, Берегова охорона США (USCG), яка є частиною Збройних Сил США, наділена повноваженнями і відповідальністю у секторі морських перевезень в частині, що стосується кібербезпеки. Служба Берегової охорони США,

зокрема її Управління охорони портів і споруд (CG-FAC), виконує провідну роль у забезпеченні кібербезпеки морської транспортної системи (MTS). Управління розробляє та надає керівні вказівки для формування послідовного та ефективного підходу до забезпечення морської кібербезпеки.

США активно розвивають міжнародну співпрацю, зокрема, проводяться спільні навчання та здійснюється обмін інформацією з союзниками НАТО та іншими міжнародними партнерами. Така співпраця дозволяє США забезпечувати колективну безпеку своїх союзників, включаючи доступ до новітніх інформаційних технологій, обмін досвідом, підвищення рівня обороноздатності та захист від потенційних розвідувальних загроз.

Сполучені Штати активно підтримують розвиток української кібербезпеки та системні заходи щодо її забезпечення. Влітку цього року було прийнято закон США про безпекове партнерство з Україною, який розширяє безпекову співпрацю та забезпечить довгострокову допомогу держави-партнера. США взяли на себе зобов’язання допомагати Україні в зміцненні кібербезпеки та захисті критичної інфраструктури, зокрема через посилення кіберзахисту від зловмисних дій росії та інших ворожих спільнот. Держави домовилися разом спрямовувати свої зусилля на підвищення здатності України протидіяти кіберінцидентам, зокрема за рахунок допомоги від Сполучених Штатів. США спрямовують зусилля для того, щоб сприяти Україні у покращенні кіберстійкості критичної інфраструктури та оперативному відновленню пошкоджених об'єктів інфраструктури [12].

Інтеграція морської кібербезпеки з національною системою захисту дозволяє оперативно реагувати на загрози і мінімізувати потенційні втрати. Уряд держави інвестує значні ресурси у кіберзахист портів, що включає встановлення сучасного захисного обладнання, розгортання систем моніторингу загроз та підвищення безпеки мережевої інфраструктури портів. Проводяться регулярні тренінги та навчання для працівників, щоб вони могли ідентифікувати кіберзагрози та правильно реагувати на них. З метою

стандартизації підходів до кібербезпеки на морі, США розробляють єдині протоколи та керівні засади, що допомагають акторам галузі підтримувати високий рівень захищеності інфраструктури. Федеральні органи, такі як Міністерство внутрішньої безпеки США (DHS) та Берегова охорона США, забезпечують постійний моніторинг та обмін інформацією з іншими відомствами, що відповідають за національну безпеку, для швидкої реакції на інциденти.

Всі ці заходи у сукупності допомагають США знижувати ризики кібератак на морську інфраструктуру та зберігати її безпеку, що є стратегічно важливим для економіки та національної безпеки країни.

Європейський Союз також здійснює рішучі кроки у боротьбі з кіберзлочинністю в усіх сферах життя суспільства. У 2020 р. Агентство Європейського Союзу з кібербезпеки (ENISA) опублікувало Керівництво для європейських портових операторів з управління кіберризиками в умовах цифрової трансформації та жорсткості регулювання та аналіз «Кібербезпека портів – Передовий досвід кібербезпеки у морській галузі» та Керівництво з управління кіберризиками для портів. ENISA, як одна з найперших у світі інституцій, ще у 2011 р. констатувала, що поінформованість про потреби та виклики кібербезпеки у морському секторі низька або взагалі відсутня [32, с. 105].

Наприкінці грудня 2022 року Європейським Союзом було опубліковано текст нової Директиви (ЄС) 2022/2555 щодо заходів забезпечення високого рівня кібербезпеки на території Союзу (On measures for a high common level of cybersecurity across the Union, NIS 2), прийнятої Європарламентом та Радою ЄС. Директива є одним із виконавчих документів Стратегії кібербезпеки Європейського Союзу на цифрове десятиріччя (2020), у якій висунуто пропозиції щодо реалізації законотворчих, політичних та інвестиційних ініціатив. В рамках однієї зі сфер діяльності ЄС, названої у Стратегії «Стійкість, технологічний суверенітет та лідерство» (розділ II, пункт 1),

Єврокомісією запропоновано реформувати правила безпеки мережевих та інформаційних систем для підвищення стійкості критично важливих об'єктів: енергосистем, залізниць, портів, центрів обробки даних та ін. [18].

При цьому, за новоприйнятою Директивою 2022/2555, заходи спрямовуються саме на підвищення загального рівня кібербезпеки всіх держав Євросоюзу, на покращення управління кіберризиками, гармонізацію вимог до рівня кібербезпеки в країнах та запроваджується зобов'язання щодо звітності для організацій у таких важливих секторах як охорона здоров'я, енергетика та транспорт, акцентується увага і на морському транспорті [11].

На відміну від Директиви (ЄС) 2016/1148 (NIS, яка втратила чинність 18.10.2024 р.) дія нового документа (NIS 2) поширюється на ширший спектр галузей економіки, які мають життєво важливе значення для економічного та суспільного життя країн ЄС, адже відповідно до NIS, держави ЄС самі визначали, які організації віднести до категорії критично важливих [27, с. 44]. А згідно з Директивою (ЄС) 2022/2555 (NIS 2), усі підприємства, які мають критичне значення для економіки та життя суспільства, підпадають під її дію, а держави-члени ЄС до 17.10.2024 р. зобов’язані прийняти національні стратегії кібербезпеки, заснувати відповідні державні органи контролю у цій сфері, єдині контактні центри з кібербезпеки та «CSIRTs» (computer security incident response teams, групи реагування на кіберінциденти, ст. 10). Важливо, що буде створена і Європейська мережа органів з протидії кіберкризам (EU-CyCLONe, ст. 16) для співпраці національних органів з кібербезпеки держав-членів Союзу, з метою забезпечення ефективної співпраці для реагування на великомасштабні та транскордонні кібератаки [11].

Директиву NIS 2 узгоджено з галузевими нормативно-правовими актами та приведено у відповідність з Директивою (ЄС) 2022/2557 про стійкість критично важливих об'єктів (CER), Регламентом (ЄС) 2022/2554 про цифрову операційну стійкість фінансового сектору (DORA) та Регламентом (ЄС) 2019/881 про ENISA (Агентство Європейського Союзу з питань кібербезпеки)

та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій. ENISA, Європол і Європейське оборонне агентство (EDA) є трьома основними організаціями, відповідальними за координацію кібер-зусиль для всіх країн-членів ЄС.

Інституції ЄС розробили та впровадили значну кількість нормативних актів, що окреслюють різноманітні підходи до встановлення високого рівня кібербезпеки у державах-членів ЄС. До них належать: рамкове рішення Ради ЄС 2005/222/JHA 2005 року, що стосується атак на інформаційні системи; повідомлення Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» 2007 року, яке визначає термін «кіберзлочинність» і головні задачі політики ЄС у цій галузі; Стратегія кібербезпеки ЄС «Відкритий, надійний і безпечний кіберпростір» 2013 року, що спонукає удосконалювати міжурядову співпрацю для протидії кіберзагрозам; а також Директива Європейського парламенту і Ради ЄС 2016 року, що встановлює заходи для забезпечення високого ступеня безпеки інформаційних систем на рівні Союзу та інші документи [27, с. 44].

Європейський Союз реалізує комплексний підхід до забезпечення морської кібербезпеки через багаторівневу систему регулювання та технічної підтримки. Вирішальну роль у цьому процесі відіграє Європейське агентство з морської безпеки (EMSA), яке координує зусилля держав-членів та впроваджує єдині стандарти кібербезпеки для всього морського сектору ЄС. Агентство здійснює постійний моніторинг кіберзагроз та надає державам-членам актуальну інформацію про потенційні ризики через Систему обміну інформацією про морську безпеку (SafeSeaNet) [53].

Таким чином, вбачається досить вагома нормативно-правова база з питань кібербезпеки у Європейському Союзі, куди прямує і українська держава, маючи європейське законодавство взірцем для власного подальшого розвитку.

Національні стратегії з кібербезпеки розроблені та ухвалені урядами більшості держав світу: США, України, Британії, Данії, Австралії, Австрії, Німеччини, Канади, Індії, Японії, Фінляндії, Швеції, Естонії тощо. Стратегія кібербезпеки Німеччини передбачає ефективну співпрацю між усіма державними інституціями та вдосконалення координації дій для захисту інформації і мінімізації кіберризиків, а також діяльність Національного центру кібербезпеки. Зазначена установа координує зусилля щодо кіберзахисту і служить платформою для оперативної комунікації між державними установами, судноплавними компаніями й іншими учасниками морського сектора. Німеччина дотримується комплексного підходу до захисту інформаційних систем та мереж у морському секторі, зокрема шляхом впровадження єдиної системи моніторингу загроз і регулярних оцінок уразливостей [27, с. 44]. Крім того, країна розвиває новітні технології, такі як блокчейн, для забезпечення цілісності та надійності даних, що обмінюються в межах морського сектору.

Схожа національна Стратегія кібербезпеки діє і у Великій Британії з 2011 року. Уряд Великобританії, котрий теж ретельно працює над питанням забезпечення кібербезпеки критичної інфраструктури, опублікував Звід практичних правил для забезпечення безпеки Інтернету речей 2016 р., у якому основна увага приділяється необхідності забезпечення кібербезпеки пристроїв, на противагу оновленню програмного забезпечення для посилення безпеки [27, с. 45].

Данія виступає однією з країн-членів ЄС, які ефективно вдосконалюють свою національну систему морської кібербезпеки. Для реалізації стратегії кібербезпеки та інформаційної безпеки в морському секторі Датське морське управління створило Підрозділ морської кібербезпеки, відповідальний за впровадження ініціатив, передбачених стратегією. Спираючись на актуальні оцінки загроз і глибокі знання про морський сектор, підрозділ надає консультації та виступає центром зв’язку з питань кібербезпеки й

інформаційної безпеки для всього морського сектора, а також виконує експертні функції у розслідуваннях з кібербезпеки в межах Датського морського управління [51].

Франція реалізує масштабну програму кібербезпеки мореплавства в рамках національної стратегії захисту критичної інфраструктури. Французька морська кібербезпека координується Національним агентством з кібербезпеки (ANSSI), яке тісно співпрацює з морськими й транспортними установами для забезпечення кіберзахисту портів, суден і морських інформаційних систем.

Таким чином, більшість країн ЄС мають комплексний і високорозвинений підхід до забезпечення морської кібербезпеки, що включає заходи моніторингу, аналізу загроз, координацію між державними установами й учасниками морського сектора, а також впровадження новітніх технологій для забезпечення стабільності та безпеки морської інфраструктури.

Заслуговує на увагу Європейський санкційний список кіберзлочинців. Громадянам і юридичним особам ЄС заборонено здійснювати будь-які фінансові операції з суб'єктами, дані про яких містяться у Європейському санкційному списку кіберзлочинців, започаткованому у 2019 р. До списку віднесені такі відомі організації, як WannaCry, NotPetya, Operation Cloud Hopper тощо [81, p. 65]. Важливим є і те, що європейські країни також активно допомагають нашій державі у становленні власної системи кібербезпеки, зважаючи на сьогоднішні реалії та надзвичайну важливість захисту об’єктів критичної інфраструктури.

3.3. Сучасний стан і потенціал правового врегулювання морської кібербезпеки в Україні

В Україні засади морської кібербезпеки лише починають розвиватися і поступово впроваджуватися. Варто відмітити, що ще до повномасштабного вторгнення у 2022 р., наша держава стрімко розвивалася у сфері

інформаційних технологій, запровадивши концепцію «уряду у смартфоні». На даний період часу галузеве законодавство України у сфері кібербезпеки являє собою низку законів, постанов Кабінету Міністрів України, указів Президента України та інших актів і стратегічних документів.

У Статті 17 Конституції України вказано, що захист інформаційної безпеки являється однією з найважливіших функцій держави і справою всього українського народу [44].

Указом Президента України В.О. Зеленського у 2021 році, приблизно за пів року до повномасштабного вторгнення рф, прийнято нову «Стратегію кібербезпеки України: Безпечний кіберпростір – запорука успішного розвитку країни». Наголошено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки держави, де рф лишається одним з головних джерел загроз національній та міжнародній кібербезпеці, активно використовуючи відповідні механізми в рамках гібридної війни проти України (п. 1 абз. 5) [22].

У документі (п. 2 абз. 9) констатовано, що діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і спрямованою на роботу з поточними задачами, критичними викликами залишаються забезпечення швидкого обміну інформацією про кіберзагрози, створення дієвої системи навчання фахівців та впровадження ефективних моделей взаємодії державного і приватного секторів. Серйозне занепокоєння викликає недостатній розвиток наукових досліджень у галузі кібербезпеки. Також спостерігається низка правових недоліків: застарілість законодавчої бази щодо захисту інформації, повільна імплементація європейських правових норм, недосконале регулювання цифрових аспектів кримінальних розслідувань та недостатній рівень правової відповідальності за порушення законодавства у сфері кібербезпеки [22].

Важливим кроком для галузі мореплавства стало прийняття 17 липня 2024 року Стратегії морської безпеки України, у якій вперше акцентується

увага на проблемі забезпечення кібербезпеки на морському транспорті. Стратегія спрямована на формування комплексної системи запобігання та протидії загрозам у морській безпеці, що стосуються як прибережних територій і морських просторів держави, так і тих районів Світового океану, де зосереджені економічні та інші національні інтереси України. Ключовим завданням є забезпечення постійної готовності до ефективного реагування на такі загрози.

Морська безпека України є комплексним поняттям, що охоплює захист національних інтересів держави на морі від актуальних і потенційних загроз, а також забезпечує її наскрізний розвиток як морської та річкової держави. Державна політика в цій сфері має на меті захист інтересів людини, суспільства та держави, при цьому кіберзагрози визнано одним із ключових викликів морській безпеці. Особливу небезпеку становлять наявні та можливі явища у кіберпросторі, які загрожують життєво важливим національним інтересам України, негативно впливають на стан кібербезпеки держави та захищеність її об'єктів, зокрема тих, що забезпечують морську безпеку [23].

Зразковим є положення про напрями забезпечення державної політики у сфері морської безпеки України, яке фактично позичено в наших партнерів, стратегічні документи яких вже аналізувались вище, в якості найкращих практик сьогодення. Так, до напрямів український законодавець відносить:

1) обізнаність - глибоке розуміння її першочергового значення для національних інтересів держави, а також спроможність органів державної влади ефективно оперувати та здійснювати обмін актуальними даними, що є необхідними для розробки та втілення державної політики у галузі морської безпеки України з урахуванням національного, регіонального та глобального вимірів;

2) вплив - спроможність державних інституцій забезпечувати захист національних інтересів на морі через скоординоване застосування комплексу заходів, що охоплюють інформаційну, дипломатичну, економічну,

правоохоронну та військову сфери діяльності, а також інші форми державного реагування на виклики морській безпеці;

3) запобігання - здатність органів держави впроваджувати систему попереджувальних заходів, спрямованих на відвертання та максимальне зниження рівня загроз у сфері морської безпеки України;

4) захист - спроможність відповідних суб'єктів забезпечення морської безпеки держави здійснювати скоординовані та рішучі заходи, спрямовані на досягнення належного рівня стійкості й захищеності об'єктів інфраструктури та реалізацію національних інтересів України;

5) відповідь - забезпечувати своєчасне та адекватне реагування на будь-які спроби посягання на національні інтереси України в морському просторі, а також підтримувати й закріплювати досягнуті результати визначеного політичного курсу у сфері морської безпеки [23].

Виступаючи документом середньострокового планування, дана Стратегія закладає фундаментальні засади для формування подальших планувальних документів у галузі морської безпеки держави, які конкретизуватимуть механізми та інструментарій її практичного впровадження. Очевидно, що всі вказані позиції, тією чи іншою мірою, стосуються Морської доктрини України на період до 2035 року. Втім, цей документ був прийнятий ще у 2009 р. та не має жодної згадки про кібербезпеку.

Також до законодавства з досліджуваної тематики в Україні відносять Доктрину інформаційної безпеки України 2016 року та Стратегію інформаційної безпеки 2021 року. Документи визначають національні інтереси України в інформаційній сфері та відповідні загрози, напрями і пріоритети державної політики. Ці програмні документи спрямовані лише на загальні питання, які в основному направленні на протиборство застосування рф технологій гібридної війни проти України і ніякою мірою не стосуються сфери мореплавства.

Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. визначає правові та організаційні засади забезпечення захисту національних інтересів України у кіберпросторі, основні положення та приписи політики держави щодо кібербезпеки, встановлює основні підходи до координації діяльності з її забезпечення. Провевши аналіз цього нормативно-правового акту зазначимо, що він є універсальним для всіх галузей суспільного життя та не акцентує увагу на морському транспорті. Але в ньому окреслено важливе правове підґрунтя, необхідне для належного функціонування системи.

У ст. 4 вказаного Закону до об’єктів кібербезпеки та кіберзахисту віднесено, зокрема, об’єкти критичної інфраструктури. У свою чергу, об’єкти критичної інфраструктури можна визначити як елементи інфраструктури, системи, їхні складові чи сукупності, що мають ключове значення для економіки, національної безпеки та оборони. Порушення їхньої роботи може завдати шкоди життєво важливим інтересам держави [21].

Координація заходів у сфері кібербезпеки, яка є невід'ємною частиною національної безпеки України, здійснюється Президентом України через Раду національної безпеки і оборони (РНБО), яку він очолює. Національний координаційний центр кібербезпеки, функціонуючи як робочий орган РНБО, відповідає за узгодження та моніторинг діяльності суб’єктів безпекового й оборонного сектору, що опікуються питаннями кіберзахисту. Центр також подає Президенту України рекомендації щодо розробки та уточнення Стратегії кібербезпеки України. Кабінет Міністрів України відповідає за формування і впровадження державної політики у сфері кібербезпеки, захист прав і свобод громадян, національних інтересів України в цифровому просторі та боротьбу з кіберзлочинністю. Крім того, уряд організовує забезпечення функціонування національної системи кіберзахисту, надаючи необхідні ресурси та засоби. Він також визначає вимоги та забезпечує

ефективну роботу системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури [21].

Ключовими суб’єктами національної системи кібербезпеки виступають Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Національна поліція України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.

Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку), заснована у 2006 році, є спеціалізованим центральним органом виконавчої влади, відповідальним за сферу спеціального зв’язку та захисту інформації. Вона входить до складу сектору безпеки та оборони, виконуючи ключову роль у національній системі кібербезпеки. Держспецзв’язку виступає основним координатором діяльності суб’єктів, які забезпечують кіберзахист у рамках загальної системи кібербезпеки [47].

Державна служба спеціального зв’язку та захисту інформації України виконує ключову роль у формуванні та реалізації державної політики у сфері кібербезпеки. Її діяльність охоплює захист державних інформаційних ресурсів і даних у кіберпросторі, активну протидію кіберзагрозам, забезпечення безпеки критичної інформаційної інфраструктури та координацію зусиль інших суб’єктів у цій сфері. Держспецзв’язку створює та підтримує функціонування Національної телекомунікаційної мережі, впроваджує організаційно-технічні моделі кіберзахисту, а також здійснює заходи щодо попередження, виявлення, реагування на кіберінциденти й кібератаки та ліквідації їх наслідків. Вона забезпечує інформування про кіберзагрози і методи захисту, впроваджує аудит інформаційної безпеки на об’єктах критичної інфраструктури та підтримує роботу Державного центру кіберзахисту, Центру активної протидії агресії у кіберпросторі та урядової команди CERT-UA для реагування на комп’ютерні надзвичайні ситуації [21].

Урядова команда реагування на комп'ютерні надзвичайні події України з 2021 р. зазнає реформ та розпочала «Кіберреформу UA30, також з 2009 року є акредитованим членом Форуму команд реагування на інциденти інформаційної безпеки FIRST (міжнародна спільнота, яка налічує понад 600 команд реагування, які забезпечують кіберзахист і вивчення кіберінцидентів у понад 90 країнах, комунікують між собою щодо виявлених кіберінцидентів) [47]. Ще одним гарним здобутком є досить зручний та інформативний веб-сайт органу, безпосередньо через який можна повідомити про кіберінцидент.

Загалом до правової бази у сфері кібербезпеки України входять також: постанови Кабінету Міністрів України (№ 1772 про «Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», № 373 про «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», № 1295 про «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки тощо), накази та рекомендації Адміністрації Державної служби спеціального зв'язку та захисту інформації України (Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570, Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 тощо).

У Постанові Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 р. у переліку секторів критичної інфраструктури виокремлено сектор «Транспорт і пошта», до якого безпосередньо віднесено морський та внутрішній водний транспорт, а

секторальним органом у сфері захисту критичної інфраструктури визначено Міністерство розвитку громад та територій України, підпорядкованим органом якого є Державна служба морського і внутрішнього водного транспорту та судноплавства України [24].

Провевши аналіз діяльності вказаних органів визначено, що жоден з них не опікується питаннями морської кібербезпеки, тобто реалізація законодавчо-визначених програм та цілей щодо забезпечення морської кібербезпеки все ще перебуває на етапі свого становлення та розвитку.

Морські порти становлять одну з найважливіших складових національної транспортної та виробничої інфраструктури, забезпечуючи з'єднання з європейськими та світовими торговими шляхами. Україна володіє найбільшим портовим потенціалом серед усіх країн Чорноморського регіону. На узбережжі Чорного та Азовського морів працює 13 морських торгових портів, хоча на сьогоднішній день їх кількість зменшилась через тимчасову окупацію частини українських територій. На жаль, належної уваги до транспорту, в тому числі морського, поки що не приділено в жодному акті, що стосується кібербезпеки України, галузь мореплавства згадується у документах лише опосередковано. Тому ця тема є актуальною для українського законодавця також. Хоча загарбницька війна на нашій території і змінила орієнтир законодавців на посилення національної безпеки держави, Україна, як морська держава, має неабиякий потенціал у винаходженні новітніх механізмів боротьби із морською кіберзлочинністю, адже кібербезпека є складовою національної безпеки держави.

Оскільки Україна не є членом Європейського Союзу, Директива NIS не має для неї юридичної обов'язковості, проте вона слугує орієнтиром для розробки та впровадження відповідних стандартів і практик.

Україна повинна також розробити механізм повідомлення держав-членів ЄС про інциденти, які можуть мати на них вплив. Через обмежену співпрацю між українськими державними органами, що відповідають за кібербезпеку,

важко визначити установу, яка б виконувала роль єдиного контактного центру. Такий орган має бути відповідальним за координацію та взаємодію з українськими органами влади, а також виконувати функцію сполучної ланки для ефективної транснаціональної співпраці з іншими державами-членами ЄС. Також варто посилити роботу у сфері державно-приватного партнерства та партнерства із міжнародними організаціями.

Для забезпечення кібербезпеки мореплавства в Україні необхідно впровадити багаторівневу систему захисту, яка враховуватиме специфіку регіону та сучасні виклики, включно з війною. Першочерговим завданням має стати продовження розробки відповідної нормативно-правової бази, що включатиме спеціальне законодавство щодо кібербезпеки морського транспорту та гармонізацію українських стандартів з інструментами IMO.

На технічному рівні важливо створити національний морський центр моніторингу загроз та впровадити системи раннього виявлення кібератак, доповнені криптографічним захистом критичних систем управління суднами. Особливу увагу слід приділити модернізації портової інфраструктури та створенню захищених каналів зв'язку між суднами та береговими службами. Враховуючи географічне положення України та поточні геополітичні виклики, необхідно посилити захист від GPS-спуфінгу та забезпечити додатковий захист систем зв'язку в Чорному та Азовському морях.

Важливим компонентом є також підготовка кваліфікованого персоналу через регулярні тренінги та навчання з кібербезпеки для екіпажів суден та берегових служб, працівників державних структур і портів. Створення механізмів співпраці з міжнародними партнерами для обміну інформацією про кіберзагрози, розробка спільних стандартів кібербезпеки виступають важливими аспектами разом з необхідністю активно брати участь у міжнародних ініціативах для забезпечення кібербезпеки мореплавства.

Впровадження інноваційних технологій, таких як блокчейн та штучний інтелект для виявлення аномалій, разом з розробкою національних підходів

для кіберзахисту морської галузі, дозволить створити надійну систему захисту українського мореплавства [37, с. 519]. Для стимулювання впровадження цих заходів доцільно розробити програми економічної підтримки та податкових пільг для компаній, які інвестують у кібербезпеку. Активна міжнародна співпраця та обмін досвідом з країнами-партнерами також сприятимуть підвищенню загального рівня захищеності морської галузі України.

Для посилення захисту від кіберзагроз як зовнішнього, так і внутрішнього характеру важливо впровадити комплекс захисних оборонних механізмів і стратегій. Основою цього підходу має стати впровадження постійно діючої системи моніторингу, що дозволить отримувати аналітичні дані про стан суднових систем у реальному часі.

Технологія блокчейн у цьому векторі може розглядатися як перспективний інструмент підвищення рівня кібербезпеки в управлінні морськими суднами, оскільки вона надає такі важливі переваги як можливості відстеження, прозорість операцій, контроль доступу, незмінність записів та децентралізована архітектура [62, p. 922]. Це забезпечує надійну та захищену комунікацію між суднами та береговими центрами управління, а також безпечне зберігання даних.

Зокрема, можна впровадити систему, де кожен член екіпажу або будь-який інший працівник галузі має доступ лише до певних даних, а всі зміни та операції з ними фіксуються у блокчейн-сховищі. Це дозволяє відслідковувати історію змін та виявляти будь-які несанкціоновані дії. Ретельна увага має надаватися авторизації та ідентифікації користувачів, які мають доступ до критично важливих даних. Тобто культура кібербезпеки має дійсно пронизувати усі ланки суспільства та галузі економіки. Новітні технології мають бути використані задля усунення небезпек під час використання кіберпростору.

Приміром, блокчейн може застосовуватися для управління контейнерами - кожен контейнер матиме унікальний код, зареєстрований у блокчейн-системі, що забезпечить більш безпечний та ефективний контроль за їх переміщенням. Впровадження блокчейну дозволить значно знизити ключові ризики для суднових комунікаційних мереж, включаючи можливість втрати, несанкціонованої зміни чи викрадення даних зловмисниками [68, p. 30]. Сучасні дослідження підтверджують, що ця технологія стане одним із основних елементів системи кіберзахисту морської галузі в майбутньому, гарантуючи цілісність та безпеку інформації.

ВИСНОВКИ

Підбиваючи підсумки дослідження, ми дійшли до наступних висновків:

1. Першим міжнародним документом, що закріпив поняття «кіберпростір», стала Окінавська хартія глобального інформаційного суспільства 2000 року, подальший розвиток правового регулювання у цій сфері був зумовлений стрімким технологічним прогресом.

Визначення кібербезпеки еволюціонувало від суто технічного захисту інформаційних систем до комплексного підходу, що охоплює захист життєво важливих інтересів людини, суспільства і держави в кіберпросторі. Сучасне розуміння кібербезпеки включає не лише технічні аспекти захисту інформації, але й організаційні, правові та освітні заходи, спрямовані на забезпечення сталого розвитку інформаційного суспільства та захист національних інтересів у кіберпросторі.

Кібербезпека мореплавства є складовою безпеки мореплавства та вкрай важливим компонентом в умовах сучасної цифровізації та автоматизації життя людства, судна та порти стають потенційно вразливими до кіберзагроз, які можуть мати катастрофічні наслідки для безпеки екіпажу, судна, вантажу та навколишнього середовища.

2. Під кібербезпекою мореплавства, як складовою інформаційної безпеки мореплавства, визначено систему технічних, організаційних та правових відносин і заходів, які спрямовані на захист інформаційно-комунікаційних технологій, систем управління та даних, що використовуються у морській галузі, з метою забезпечення безпечного функціонування морської інфраструктури, збереження людського життя на морі, захисту від кібернетичних загроз та запобігання забрудненню природнього середовища.

Кібербезпека, маючи специфічну спрямованість на захист цифрового простору, включає в себе систему технічних, організаційних та правових відносин і заходів, спрямованих на захист інформаційно-комунікаційних технологій, систем управління та даних у електронному вигляді. При цьому

інформаційна безпека мореплавства охоплює більш широкий спектр питань, включаючи ще й забезпечення інформаційної цілісності всієї морської галузі, захист конфіденційної інформації, комерційної таємниці та інших аспектів інформаційної діяльності, охоплюючи і фізичний світ.

3. Критично важливими для захисту та вразливими є переважна більшість усіх існуючих систем на судні, як, наприклад, AIS, ECDIS, GPS-системи, EPIRB, VDR тощо. Кібератаки на ці системи можуть призвести до руйнівних наслідків, включаючи, щонайменше зміни курсу суден або створення «суден-привидів». При цьому, зараження програмного забезпечення, нехтування його обслуговуванням на судні та на підприємствах є одним з найнебезпечніших і розповсюджених шляхів надання кіберзлочинцям доступу до управління судном.

Зважаючи на стрімкий розвиток технологій та наміри ввести в дію автономні судна і порти, які будуть повністю оперуватися комп’ютерними системами та штучним інтелектом поза людським контролем, необхідно розглядати усі наявні комп’ютерні системи на суднах та у портах, на мобільних офшорних установках та ін. – як потенційно вразливі до кібератак, а так зване «кіберпіратство» стає поступово заміняти піратство за масштабністю наслідків та збитків.

4. Аналіз останніх випадків кібератак на морську інфраструктуру свідчить про постійне збільшення кількості та видів ризиків. Розвиток комп'ютерних систем на суднах та в портах, що інтегруються в загальну мережу Інтернету, відкривають нові можливості для хакерів, включаючи GPS-спуфінг, фішинг, DDoS-атаки та інші методи впливу на критично важливі системи. Кібератаки є навмисними діями у кіберпросторі, які спрямовані на порушення стабільної роботи технологічних систем, а кіберінцидент є випадком (не завжди результатом навмисних дій), що загрожує безпеці систем та може спричинити порушення їх роботи. Міжнародне співтовариство визнало, що війна в Україні безпосередньо

впливає не лише на світову економіку та міжнародний правопорядок, але й на безпеку мореплавства.

5. Сучасний розвиток морської галузі тісно пов’язаний із впровадженням автономних суден, Інтернету речей та технологій штучного інтелекту. Переваги інновацій відкривають нові можливості для морської індустрії. Досвід Сінгапуру демонструє, як вони можуть впроваджуватися та в майбутньому поступово використовуватися для оптимізації морського руху, підвищення ефективності портових операцій. Успішний приклад цієї держави є важливим орієнтиром для України, яка має потенціал для впровадження аналогічних технологій у власну морську галузь.

Але водночас інновації породжують проблеми, пов’язані з кібербезпекою. Кібератаки на автономні судна та інші системи керування можуть призвести до повного захоплення управління судном. Тому разом із новаціями необхідно впроваджувати і новітні технології кіберзахисту, зокрема багаторівневу автентифікацію, шифрування даних, алгоритми виявлення кіберзагроз тощо.

6. Міжнародні акти обов’язкового характеру у сфері морської кібербезпеки дозволили б істотно обмежити і скоротити кількість кібератак, запровадивши дієві механізми боротьби з ними. Хоча існують певні рекомендації з кібербезпеки на морі, єдиних узгоджених засад для запобігання кіберзлочинам у цій сфері наразі немає.

У розробці правової бази найбільш ефективно доклала зусиль ІМО, прийнявши у 2017 році два надважливі документи, які сьогодні фактично являють собою правову основу в галузі морської кібербезпеки. Це рекомендації щодо захисту міжнародного судноплавства від існуючих та виникаючих загроз кібербезпеці та зменшення відповідних факторів уразливості, що були закріплені у Циркулярі MSC-FAL.1/Circ.3 «Керівництво з управління кіберризиками на морі» та Резолюції MSC.428(98) «Управління кіберризиками в морській галузі в рамках систем управління безпекою».

Галузеві неурядові міжнародні організації, як BIMCO, МАКО INTERTANKO, ICS теж роблять активні зусилля для інтеграції управління кіберризиками у культуру забезпечення безпеки, щоб запобігти виникненню серйозних інцидентів, вони продовжують розробляти технічні рекомендації.

Впровадивши єдині вимоги, правила і принципи на рівні міжнародних конвенцій, як наприклад було зроблено у Конвенції SOLAS стосовно забезпечення безпеки людини на морі, вдасться мінімізувати випадки кіберпіратства та посилити колективну світову боротьбу з цими злочинами, не залишаючи акторів галузі мореплавства боротися самотужки. Також, можливо було б доречним внести певні зміни у низці міжнародних конвенцій, наприклад, Конвенції про боротьбу з незаконними актами, спрямованими проти безпеки судноплавства 1988 р., додавши до неї таке поняття як «кіберпіратство». У Конвенції STCW, додавши до неї обов'язкові вимоги до моряків щодо навичок з культури кібербезпеки, адже важливою є підготовка персоналу, проведення спеціальних навчань і тренінгів для працівників морської галузі щодо кібербезпеки.

Для розробки комплексного підходу до кібербезпеки у морському секторі необхідне створення міждержавної платформи співпраці, яка має зосередитись на розробці деталізованих інструкцій та впровадженні найкращих практик у сфері кібербезпеки мореплавства.

Інтеграція морської кібербезпеки з національною системою захисту дозволяє оперативно реагувати на загрози і мінімізувати потенційні втрати. З метою стандартизації підходів до кібербезпеки на морі, США розробляють єдині протоколи та принципи, які допомагають підтримувати високий рівень захищеності інфраструктури. ЄС реалізує комплексний підхід до забезпечення морської кібербезпеки через багаторівневу систему регулювання та технічної підтримки. Європейське агентство з морської безпеки координує зусилля держав-членів та впроваджує єдині стандарти кібербезпеки для всього морського сектору.

7. В Україні засади морської кібербезпеки лише починають розвиватися і поступово впроваджуватися. На жаль, уваги до транспорту, в тому числі морського, не приділено в жодному акті, що стосується кібербезпеки України, галузь мореплавства згадується у документах лише опосередковано. Для забезпечення кібербезпеки мореплавства в Україні необхідно впровадити багаторівневу систему захисту, яка враховуватиме специфіку регіону та сучасні загрози.

Через низький рівень співпраці між українськими органами влади, відповідальними за кібербезпеку, досить важко визначити орган, що стане єдиною точкою контакту, адже він має відповідати за координацію та співробітництво з українськими органами влади, стати сполучною ланкою і забезпечувати успішне транскордонне співробітництво з іншими державами і приватним сектором. Варто зміцнити роботу у сфері державно-приватного та міжнародного партнерства.

На технічному та реалізаційному рівні важливо створити національний морський центр моніторингу загроз та впровадити системи виявлення і реагування на кібератаки. Особливу увагу слід приділити модернізації портової інфраструктури та створенню захищених каналів зв'язку між суднами та береговими службами. Впровадження інноваційних технологій, таких як блокчейн та штучний інтелект для виявлення аномалій, разом з розробкою національних підходів для кіберзахисту морської галузі, дозволить створити надійну систему захисту українського мореплавства.

Технологія блокчейн у цьому векторі може розглядатися як перспективний інструмент підвищення рівня кібербезпеки в управлінні морськими суднами, оскільки вона надає такі важливі переваги як можливості відстеження, прозорість операцій, контроль доступу, незмінність записів та децентралізована структура. Це забезпечує надійну та захищену комунікацію між суднами та береговими центрами управління, а також безпечне зберігання даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Convention for the Safety of Life at Sea (SOLAS). 1974. URL: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx (дата звернення: 10.09.2024).

2. United Nations Convention on the Law of the Sea. 1982. URL: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (дата звернення: 10.09.2024).

3. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 05.09.2024).

4. Resolution IMO A.617(15). Implementation of the NAVTEX system as a component of the world-wide navigational warning service. 1987. URL: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.617(15).pdf (дата звернення: 10.09.2024).

5. Resolution IMO A.817(19): Performance standards for Electronic Chart Display and Information Systems (ECDIS). 1995. URL: https://media.liscr.com/marketing/liscr/media/liscr/online%20library/maritime/a.817(19).pdf (дата звернення: 10.09.2024).

6. IMO MSC/Circ.1024. Guidelines on Voyage Data Recorder (VDR) ownership and recovery. 2002. URL: https://www.classnk.or.jp/hp/pdf/activities/statutory/ism/imo/MSC_Circ.1024.pdf (дата звернення: 10.09.2024).

7. Resolution IMO MSC.428(98). Maritime cyber risk management in safety management systems. Ann. 10. 2017. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (дата звернення: 10.09.2024).

8. IMO MSC-FAL.1/Circ.3/Rev.2. Guidelines on maritime cyber risk management. 2022.URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf (дата звернення: 05.09.2024).

9. Okinawa Charter on Global Information Society. Adopted at the Group of Eight (G-8) Summit in Late July 22, 2000. URL: https://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf (дата звернення: 05.09.2024).

10. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881 (дата звернення: 05.09.2024).

11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 12.09.2024).

12. Bilateral Security Agreement Between the United States of America and Ukraine. June 13, 2024. The White House. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/13/bilateral-security-agreement-between-the-united-states-of-america-and-ukraine/#:~:text=It%20is%20the%20policy%20of%20the%20United%20States%20to%20assist,concern%20to%20the%20other%20Party (дата звернення: 10.09.2024).

13. Information systems defence and security: France’s strategy. French Network and Information Security Agency. 2011. 23 p.

14. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN/2013/01. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001 (дата звернення: 05.09.2024).

15. National Cyber Security Strategy and 2013-2014 Action Plan. Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. 47 p.

16. National Cyber Strategy of the United States of America. The White House. 2018. 40 p.

17. Presidential Policy Directive PPD-41 United States Cyber Incident Coordination. 2016. The White House. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (дата звернення: 10.09.2024).

18. Joint communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. JOIN/2020/18. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 (дата звернення: 11.09.2024).

19. Cyber Security Strategy for Germany. Federal Ministry of the Interior, Building and Community. 2021. 133 p.

20. National Cybersecurity Strategy. The White House. 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 10.09.2024).

21. Про основні засади забезпечення кібербезпеки України : Закон від 05.10.2017. № 2163-VIII. База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.09.2024).

22. Стратегія кібербезпеки України : Затверджена Указом Президента України від 26 серпня 2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 11.09.2024).

23. Стратегія морської безпеки України: Затверджена Указом Президента України від 17 липня 2024 року № 468/2024. URL: https://www.president.gov.ua/documents/4682024-51461 (дата звернення: 07.09.2024).

24. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 9 жовтня 2020. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 07.09.2024).

25. Асірян С.Р. Законодавча практика Сінгапуру щодо використання штучного інтелекту. *Аналітично-порівняльне правознавство*. 2023. № 3. С.313-317.

26. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С.54-62.

27. Грубі Т.В. Світові та вітчизняні практики в сфері кібербезпеки: виклики сучасності. *Збірник матеріалів Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи»*. Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. С.42-47.

28. Даус Ю.В., Даус М.Є., Полікаровських О.І., Ларін Д.Г. Кібербезпека на морському транспорті. *Вісник Одеського національного морського університету*. 2023. № 2 (69). С.124-132.

29. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. К. : НІСД, 2014. 328 с.

30. Коновалов С. М., Чумак О. А., Тузова І. А., Тузов О. В., Панченко Т. Д., Хотін С. Ю. Аналіз кібератак на інформаційні системи морських портів та методи протидії їм. *Таврійський науковий вісник*. 2024. № 3. С.20-28.

31. Краснікова О. Тенденції трансформації міжнародного морського права як наслідок упровадження автономних суден. *Юридичний вісник*. 2020. № 6. С. 256-262.

32. Краснікова О.В. Нормативно-правове регулювання у сфері кібербезпеки в судноплавстві. *International scientific conference*. Odessa. 2021. С.104-107.

33. Криворот І. А. Дослідження моделі взаємодії інтернет речей з доповненою та віртуальною реальністю. «*Світ телекомунікації та інформатизації*»: *матеріали Міжнародної науково-технічної конференції студентства Державного університету телекомунікацій*. Київ, 2017. С.212-214.

34. Мельник О.М., Корякін К.С., Саф'ян О.С., Заяц С.В., Щенявський Г.С. Актуальні питання кібербезпеки морських портів. *Modern scientific researches*, 2022. № 18(1). С.81-87.

35. Мельник О.М. Безпілотне судноплавство як розвиток технологічних інновацій у морських перевезеннях. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Технічні науки. 2023. Том 34 (73). № 2. С.152-157.

36. Мельник О.М., Корякін К.С., Пастернак О.Я., Чеча О.П., Никиктюк П.В. Огляд нормативного регулювання кібербезпеки у морській галузі. *Modernization of todays science: experience and trends: collection of scientific papers «SCIENTIA» with Proceedings of the Ill International Scientific and Theoretical Conference*. Singapore. 2023. С.167-171.

37. Муц Д.С., Четверіков І.О. Блокчейн в критичній інфраструктурі. *Актуальні проблеми управління інформаційною безпекою держави : зб. матер. всеукр. наук.-практ. конференції*. Київ : Нац. акад. СБУ, 2023. С.518-521.

38. Плачкова Т. М. Адміністративно-правове забезпечення безпеки мореплавства в Україні:. дисертація на здобуття ступеня доктора філософії за

спеціальністю 081 «Право». Національний університет «Одеська юридична академія», Одеса, 2020. 233 с.

39. Плескач В.Л., Плескач М.В. Безпека кібернетична. Велика українська енциклопедія. URL: https://vue.gov.ua/Безпека кібернетична (дата звернення: 06.09.2024).

40. Савінова Н.А. Кримінально-правова політика забезпечення інформаційного суспільства в Україні: дис. … д.ю.н.: 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Львів, 2013. 510 с.

41. Сопілко І.М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*. 2021. № 2 (59). С.110-115.

42. Тарасюк А. В. Теоретико-правові основи забезпечення кібербезпеки України: дис. … д.ю.н.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2021. 461 с.

43. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. д.ю.н.: 12.00.07. Ужгород, 2019. 487 с.

44. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні*, 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf (дата звернення: 12.09.2024).

45. Balduzzi M. AIS Exposed: Understanding Vulnerabilities & Attacks 2.0. *Black Hat Asia 2014.* URL: https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf (дата звернення: 10.09.2024).

46. Borum R., Felker J., Kern S. Cyber Intelligence Operations: More than just ones and zeroes. *Journal of Safety and security. Proceedings*. 2014. P.65-68.

47. Computer Emergency Response Team of Ukraine (CERT-UA): база даних Урядової команди реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/about-us (дата звернення: 07.09.2024).

48. Craigen, D., Diakun-Thibault N. and R. Purse. Defining Cybersecurity. *Technology Innovation Management Review*. 2014. P.13-21.

49. Cyber digest: огляд подій в сфері кібербезпеки. Рада національної безпеки і оборони України. 2023. 42 с. URL: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf (дата звернення: 05.09.2024).

50. Cybersecurity Guidelines for Ports and Port Facilities. International Association of Ports and Harbors. 2021. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf (дата звернення: 10.09.2024).

51. Danish Maritime Cybersecurity Unit: база даних Данської морської адміністрації. URL: https://www.dma.dk/safety-at-sea/danish-maritime-cybersecurity-unit (дата звернення: 10.09.2024).

52. Dimitrios D. Exploring the Issue of Technology Trends in the «Era of Digitalisation». *World Maritime Day Parallel Event*. Szczecin-Poland, 2018. URL: https://www.researchgate.net/publication/325877588_Exploring_the_Issue_of_Technology_Trends_in_the_Era_of_Digitalisation (дата звернення: 10.09.2024).

53. European Maritime Safety Agency (EMSA): база даних Європейського агентства з морської безпеки. URL: https://www.emsa.europa.eu/we-do/digitalisation.html (дата звернення: 10.09.2024).

54. Fruhlinger J. What is information security? Definition, principles, and jobs. *CSO United States*. 2020. URL: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html (дата звернення: 05.09.2024).

55. Garikapati D., Shetiya S.S. Autonomous Vehicles: Evolution of Artificial Intelligence and the Current Industry Landscape. *Big Data Cognitive Computing*. 2024. № 8. 25 p.

56. Global Cybersecurity Index 2024, 5th edition. International Telecommunication Union Development Sector. 2024. 151 p. URL:

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf. (дата звернення: 10.09.2024).

57. IACS UR E26 and E27 Press Release. International Association of Classification Societies. 2023. URL: https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release (дата звернення: 10.09.2024).

58. INMARSAT: база даних INMARSAT maritime. URL: https://www.inmarsat.com/en/about.html (дата звернення: 10.09.2024).

59. International Telecommunication Union National cybersecurity strategy guide. 2011. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf (дата звернення: 05.09.2024).

60. Irwin L. What's the difference between information security and cyber security? *IT Governance*. 2020. URL: https://www.itgovernance.eu/blog/en/whats-the-difference-between-information-security-and-cyber-security (дата звернення: 05.09.2024).

61. IT/OT cyber security solution introduced for marine and offshore operations. *Safety4sea*. 2019. URL: https://safety4sea.com/it-ot-cyber-security-solution-introduced-for-marine-and-offshore-operations/ (дата звернення: 10.09.2024).

62. Karaś A. Maritime Industry Cybersecurity: A Review of Contemporary Threats. *European research studies journal*. XXVI (Issue 4). 2023. P. 921-930.

63. Kenney M., Macdonald F. Shifting Tides, Rising Ransoms and Critical Decisions: Progress on maritime cyber risk management maturity. Global industry report 2023 by CyberOwl, HFW, Thetius. URL: https://cyberowl.io/wp-content/uploads/2023/10/CyberOwl_HFW_Thetius-Cyber-Security-Report-2023-Shifting-Tides-Rising-Ransoms.pdf (дата звернення: 11.09.2024).

64. Klimburg A. et al. National cyber security framework manual. *NATO CCD COE Publications*. 2012. URL:

http://belfercenter.hksharvard.edu/files/hathaway-klimburg-nato-manualch-1.pdf (дата звернення: 05.09.2024).

65. Maritime cyber priority 2023. Staying secure in an era of connectivity. DNV Research.URL:https://brandcentral.dnv.com/original/gallery/10651/files/original/5edc9dcb-4dfb-448c-a766-cb065f28a47b.pdf?utm_campaign=AC_CS_GLOB_23Q2_AUTO_Report-Maritime-Cyber-Priority-2023-confirmation-email&utm_medium=email&utm_source=Eloqua (дата звернення: 11.09.2024).

66. Marlow P. B. Maritime Security: An update of key issues. *Maritime Policy & Management,* 2010. Vol. 37 (7). URL: https://www.researchgate.net/publication/241717365_Maritime_security_An_update_of_key_issues (дата звернення: 10.09.2024).

67. Marshall E. Newberry. Maritime Critical Infrastructure Cyber Risk. *Coast Guard Proceedings*. 2014. Vol. 71, № 4. URL: https://trid.trb.org/view/1346294 (дата звернення: 10.09.2024).

68. Melnyk O. Ship's information security: technologies, international regulations and practical aspects. *Intellectual capital is the foundation of innovative development*. 2023. P.8-38.

69. Recommendation on Cyber Resilience №166. International Association of Classification Societies. 2022. URL: https://iacs.org.uk/resolutions/recommendations/161-180/rec-166-new-corr2-cln (дата звернення: 10.09.2024).

70. Robertson J., Riley M., The Mob’s IT Department: How two technology consultants helped drug traffickers hack the Port of Antwerp. *Bloomberg Businessweek*. 2015. URL: https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/ (дата звернення: 10.09.2024).

71. Ruben S. Maritime Security: Hacking into a Voyage Data Recorder (VDR). *IOActive Labs*. 2015. URL: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/ (дата звернення: 10.09.2024).

72. Schatz D. Towards a comprehensive evidence-based approach for information security value assessment: dissertation of Doctor of Philosophy. London, 2018. 301 p.

73. Several European ferry operators suffered a coordinated cyber attack. *Shippax*. 2023. URL: https://www.shippax.com/en/news/several-european-ferry-operators-suffered-a-coordinated-cyber-attack.aspx (дата звернення: 10.09.2024).

74. The Guidelines on Cyber Security Onboard Ships produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss. Version 4. 2020. URL: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (дата звернення: 10.09.2024).

75. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 10.09.2024).

76. UR E26 Cyber resilience of ships. Rev.1. International Association of Classification Societies. 2023. URL: https://iacs.org.uk/resolutions/unified-requirements/ur-e (дата звернення: 10.09.2024).

77. UR E27 Cyber resilience of on-board systems and equipment. Rev.1. International Association of Classification Societies. 2023. URL: https://iacs.org.uk/resolutions/unified-requirements/ur-e (дата звернення: 10.09.2024).

78. UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. UT News. 2013. URL: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-

sea/#:~:text=Led%20by%20assistant%20professor%20Todd,openly%20acknowledged%20GPS%20spoofing%20device (дата звернення: 10.09.2024).

79. Veale M., Brown I. Cybersecurity. *Internet Policy Review*, 2020. № 9 (4). P. 1-22.

80. Ward T. Terminal operating system selection. *Port technology international*. 2013. №58. P.46-48.

81. Zayats, S. Ensuring maritime security and measures against cyber threats and cyber piracy at sea. *European Science*. 2023. №1. P. 63–89.