Руденко Сергій Васильович, доктор наук, Одеський національний морський університет, Кафедра судноводіння та морської безпеки, Одеса, Україна, https//orcid.org/0000-0002-1671-605X

Корякін Костянтин Сергійович, доктор філософії, Одеський національний морський університет, Кафедра судноводіння та морської безпеки, Одеса, Україна, https//orcid.org/0000-0003-2388-645X

Довгошеєнко Анатолій Ігорович, аспірант, Одеський національний морський університет, Кафедра судноводіння та морської безпеки, Одеса, Україна, https//orcid.org/0009-0007-0431-0013

Rudenko Sergey Vasilyovich, Doctor of Science, Odessa National Maritime University, Department of Navigation and Maritime Safety, Odessa, Ukraine, https//orcid.org/0000-0002-1671-605X

Koryakin Konstantin Serhiyovych, Doctor of Philosophy, Odessa National Maritime University, Department of Navigation and Maritime Safety, Odesa, Ukraine, https//orcid.org/0000-0003-2388-645X

Dovgosheenko Anatoly Igorovich, graduate student, Odessa National Maritime University, Department of Navigation and Maritime Safety, Odessa, Ukraine, https://orcid.org/0009-0007-0431-0013

ТРАНСФОРМАЦІЯ СИСТЕМ МОРСЬКОЇ БЕЗПЕКИ: ВІД КЛАСИЧНИХ МЕТОДІВ ДО КОМПЛЕКСНИХ АДАПТИВНИХ МОДЕЛЕЙ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

TRANSFORMATION OF MARITIME SECURITY SYSTEMS: FROM CLASSIC METHODS TO COMPLEX ADAPTIVE MODELS IN THE CONTEXT OF HYBRID THREATS

Анотація

Глобальне судноплавство, що забезпечує перевезення вантажів стикається з підвищенням витрат і наростаючою невизначеністю через поточні загальносвітові виклики: війни, конфлікти, глобальні кліматичні катаклізми та ескалація геополітичної напруженості, про що йдеться в повідомленні. за 2025 рік. конференції Організації Об'єднаних Націй з торгівлі та розвитку (UNCTAD). Компанії зайняті перевезенням вантажів у морі стикаються з необхідністю адаптувати маршрути, заздалегідь враховувати всі ризики – від геополітичних до кліматичних – і формувати ефективні, захищені ланцюжки поставок. Крім геополітичних та економічних викликів, судноплавство переживає внутрішні трансформації, пов'язані з цифровізацією та змінами у складі робочої сили. Цифрові рішення стають незамінними підвищення ефективності портів і спрощення торгівлі. Але зростаюча залежність галузі від цифрових технологій посилила кіберриски та вразливості, які необхідно враховувати. Перед галуззю стоять завдання, вирішення яких вимагатиме справедливого підходу, координації та глобальної співпраці. У цій статті розглядаються традиційні системи безпеки на морському транспорті, дана класифікація існуючих загроз, розглянуто компоненти моделі захисту від загроз та наведено обґрунтування переходу від класичних методів охорони до комплексних адаптивних моделей.

Ключові слова: безпека плавання, морські гібридні загрози, кіберфізична морська безпека, стійкість портової інфраструктури, штучний інтелект в управлінні морською безпекою.

Abstract

Global shipping, which provides transportation of goods, is facing rising costs and growing uncertainty due to current global challenges: wars, conflicts, global climate disasters and escalating geopolitical tensions, as stated in the report.

for 2025. conference of the United Nations Organization on Trade and Development (UNCTAD). Companies engaged in the transportation of goods at sea are faced with the need to adapt routes, take into account all risks in advance – from geopolitical to climatic – and form efficient, secure supply chains. In addition to geopolitical and economic challenges, shipping is experiencing internal transformations associated with digitalization and changes in the composition of the workforce. Digital solutions are becoming indispensable for increasing port efficiency and facilitating trade. But the industry's growing dependence on digital technologies has increased cyber risks and vulnerabilities that need to be considered. The industry faces challenges that will require a fair approach, coordination and global cooperation. This article reviews traditional maritime security systems, classifies existing threats, examines the components of a threat protection model, and provides a rationale for the transition from classical security methods to complex adaptive models.

Keywords: navigation safety, maritime hybrid threats, cyber-physical maritime security, port infrastructure resilience, artificial intelligence in maritime security management.

Вступ. В даний час морська галузь стикається з низкою критичних проблем безпеки, включаючи війни між країнами, кібертерористичні атаки на пасажирські та вантажні судна, незаконний обіг наркотиків та людей, а також піратство та збройні пограбування останніми роками.

Заходи, що вживаються судноплавними компаніями для запобігання порушення комерційної діяльності, такі як зміни маршрутів, збільшення витрат на безпеку, збільшує вартість морського страхування, негативно впливає на глобальне енергопостачання, особливо оскільки вона здійснюється на важливих морських шляхах і в районах, близьких до енергетичних ресурсів. Такі дії, як зміна маршрутів, призводять до

збільшення забруднення повітря за рахунок збільшення викидів, а морські аварії, які можуть статися через діяльність із захоплення та перехоплення суден, підвищують ризик забруднення морського середовища. Наприклад, інтенсивні заходи безпеки в Аденській затоці дуже негативно вплинули на морську торгівлю.

Для запобігання цим проблемам учасники морського ринку вжили заходів безпеки, компанії почали розміщувати на борту озброєний персонал охорони, а міжнародне співробітництво забезпечило безпечне проходження суден через регіон під захистом військових конвоїв. Ще один важливий момент, який слід підкреслити у глобальному масштабі, полягає в тому, що політична, економічна та соціальна стабільність є найважливішими факторами, що безпосередньо впливають на ці дії, а нестабільність у різних частинах світу є тригером. Одним із найсерйозніших інцидентів останніх років вважається напад на ліберійський контейнеровоз V/S Mozart, який прямував біля берегів Нігерії в Гвінейській затоці. Внаслідок нападу один член екіпажу загинув, а п'ятнадцять членів екіпажу було викрадено.

Кібербезпека – ще один критичний аспект. Логістика все більше залежить від цифрових інструментів: автоматизованих систем керування, GPS-трекінгу, електронного документообігу. Але при цьому зростає ризик кібератак: зламування портових систем, маніпуляція з даними про вантажі або їх переміщення. Сучасні страхові продукти вже включають cyber risk coverage - покриття збитків від кіберінцидентів, які можуть паралізувати ланцюжок постачання.

Постановка проблеми. Тема управління безпекою морського транспорту в умовах гібридних загроз зараз є вкрай актуальною. Сучасні виклики поєднують у собі кібератаки, фізичні диверсії, економічний тиск та інформаційний вплив, що вимагає переходу від класичних методів охорони до комплексних адаптивних моделей, так як традиційні системи безпеки

(фізична охорона) не справляються з багатовекторними (гібридними) атаками, що збільшує попит на комплексні продукти, що включають Конфлікти. Технології, такі як штучний інтелект та аналітика даних у реальному часі, допомагають краще прогнозувати ризики та швидше реагувати на зміни.

Аналіз останніх досліджень і публікацій. Існуючі типи загроз вивчені за допомогою Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans (2nd ed.). (2024) [7]. Правові аспекти використання комерційних судів у гібридних цілях викладені Alexander Lott. Brill, (2022) [16]. Актуальне дослідження цифрової стійкості проведено Melnyk, O., et al. (2025) [10]. Роль штучного інтелекту визначає Miller, J., та ін. (2025) [11]. Аналіз реальних інцидентів у Малакській протоці та гібридній безпеці проводить Giannopoulos, G., et al. (2024) [12]. Аналіз захисту портів та газопроводів в умовах гібридної дії зроблено Mietkiewicz, R. (2022) [15]. Сукупно зазначені дослідження обґрунтовують необхідність побудови нових комплексних адаптивних моделей безпеки, які поєднують інтелектуальну обробку даних, сценарне моделювання та формують організаційно-технічну модель управління безпекою, що забезпечує проактивний захист в умовах гібридних загроз.

Метою статті є дослідження існуючих загроз на морському транспорті, аналіз існуючих компонентів протидії ризикам, пошук технічних рішень та правил, що сприяють підвищенню безпеки плавання в складних умовах гібридних загроз та визначення концепції організаційно-технічної моделі, здатної працювати в режимі реального часу для забезпечення необхідного рівня безпеки мореплавання.

Виклад основного матеріалу дослідження. Морські перевезення, найважливіший вид морського ланцюга поставок, стикаються з різними ризиками безпеки. За даними Міжнародного морського бюро (IMB), щорічні

витрати на вирішення критичних проблем безпеки становлять близько 25 мільярдів доларів. Ці витрати включають крадіжки, викупи, заходи, що вживаються судноплавними компаніями, зміни маршрутів, витрати, що виникають через порушення комерційної діяльності, та збільшення витрат на морське страхування. Аварії на морі також спричиняють проблеми з психологічним та психічним здоров'ям моряків. Крім того, діяльність з аварії та аварії на морі негативно впливає на глобальне енергопостачання, особливо враховуючи те, що вона відбувається на важливих морських шляхах та в районах, близьких до енергетичних ресурсів. Такі дії, як зміна маршрутів, призводять до збільшення забруднення повітря через збільшення викидів, а морські аварії, які можуть статися через діяльність з аварії та аварії на морі, збільшують ризик забруднення морського середовища. Інші непрямі наслідки аварії та аварії на морі включають регіональну продовольчу безпеку та той факт, що організації, які здійснюють цю діяльність, взаємодіють з більшими терористичними групами, створюючи більші ризики для безпеки.

Визначимо наявні загрози на морському транспорті. Загрози на морському транспорті є набір різних загроз, які можуть бути спрямовані на безпеку і стабільність морського транспорту, тобто є гібридними. Ці загрози можуть включати морське тероризм, піратство, наркоторгівлю, нелегальну міграцію і кіберзлочинність. Загрози можуть бути використані для створення хаосу та загрози безпеці морських коридорів, таких як Суецький та Панамський канали, які є стратегічно важливими для міжнародної торгівлі. Гібридні загрози також можуть виявлятися у вигляді саботажу інфраструктури морського транспорту, що може призвести до значних затримок та фінансових втрат. Важливо відзначити, що морські коридори є стратегічно важливими для міжнародної торгівлі і можуть бути схильні до нападів, що ускладнює операційну обстановку на морі [1]. Стратегічні

аспекти гібридних загроз на морському транспорті також включають захист інфраструктури, таких як телекомунікаційна та енергетична інфраструктура на дні Балтійського моря. Це вимагає активніших заходів протидії, щоб забезпечити безпеку та стабільність морського транспорту [2].

Класифікація загроз наведено на рис. 1.



Рис. 1. Класифікація загроз на морському транспорті.

Наведемо коротку характеристику кожного виду.

Кіберфізичні атаки – це особлива категорія кібератак, які навмисно чи ні також негативно впливають на фізичний простір, націлюючись на обчислювальну та комунікаційну інфраструктуру, яка дозволяє людям та системам контролювати датчики та виконавчі механізми. Кіберфізичні атаки зазвичай розглядаються у зв'язку з кіберфізичними системами та вразливістю їх обчислювальних та комунікаційних елементів. Наприклад, зловмисник, який взяв під контроль обчислювальні або комунікаційні компоненти водяних насосів, медичних імплантатів, автомобілів і клапанів газопроводів, може використовувати їх для впливу на фізичний простір, завдаючи шкоди майну або навколишньому середовищу та наражаючи на ризик життя людей. У результаті безпека повсюдно сприймається як одне з

найважливіших завдань під час проектування надійних кіберфізичних систем. Зловмисник може передати потужні сигнали, що запобігають прийому допустимих сигналів GPS. Результатом атаки є втрата доступності GPS, що може призвести до: порушення здатності мети визначати своє місцезнаходження, автономно переміщатися або отримувати зручність із синхронізації на основі GPS. Основною метою такої атаки є судна, літаки, наземні транспортні засоби, інтелектуальна мережа та будь-яка друга кіберфізична система, яка значною мірою покладається на доступність GPS для визначення розташування, навігації або синхронізації часу [3].

Техногенно-організовані загрози — це потенційні ризики та небезпеки для людей і довкілля, що виникають через діяльність людини, аварій і катастроф на об'єктах техносфери, які включають хімічні, радіаційні, пожежі, вибухи, транспортні аварії, руйнування будівель, а також збої в комунальних системах, викликаних персоналу, порушенням процесів, недостатнім контролем. Їхня реалізація призводить до НС (надзвичайних ситуацій) із серйозними наслідками, що потребують заходів щодо підвищення техногенної безпеки, наголошуючи на важливості людського фактора та надійності систем. Види техногенних загроз наведено у таблиці 1.

Інформаційні загрози - це потенційні дії або події, здатні завдати шкоди даним, системам або інфраструктурі, порушуючи їх конфіденційність, цілісність або доступність, і можуть виходити від кібератак (віруси, фішинг), людського фактора (помилки, інсайдери) або природних явищ.

Основні види інформаційних загроз:

- Шкідливе програмне забезпечення: Віруси, черв'яки, програми-вимагачі (ransomware), шпигунське програмне забезпечення (spyware, keyloggers).
- Кібератаки:

- Фішинг: Обман користувачів для отримання конфіденційних даних.

Таблиця 1

Основні види техногенно-організованих загроз.

Види техногенно-організованих загроз	
Назва	Загроза
Хімічні аварії	Викиди токсичних речовин
Радіаційні аварії	неконтрольовані викиди радіації
Пожежі та вибухи	Ушкодження промислових об'єктів, складів, транспорту
Транспортні аварії	Великі ДТП, аварії на залізниці, в авіації та водному транспорті
Гідродинамічні аварії	Прориви гребель
Обвалення будівель та споруд	Помилки при будівництві або природних впливів
Аварії на комунальних системах	Пошкодження водопостачання, опалення, газо- та електромереж
Біологічні загрози	Руйнування підприємств медичної та оборонної промисловості

- DDoS-атаки: Перевантаження системи для порушення доступності.
- SQL-ін'єкції, XSS-атаки: Експлоітація уразливостей веб-додатків.
- Атаки "людина посередині" (Man-in-the-Middle): Перехоплення комунікації.
- Соціальна інженерія: Психологічні маніпуляції для отримання інформації.

- Витоку інформації: Передача даних незахищеними каналами або через помилки співробітників.
- Інсайдерські загрози: Умисні або випадкові дії співробітників, що призводять до витоків, крадіжок або псування даних.
- Загрози доступності: Атаки, які роблять системи недоступними (наприклад, DDoS).
- Технічні збої: Помилки ПЗ, апаратні збої.
- Фізичні небезпеки: Крадіжки обладнання, стихійні лиха.

Класифікація за джерелом

- Зовнішні: Хакери, кіберзлочинці, конкуренти (атаки ззовні).
- Внутрішні: Співробітники компанії (помилки, навмисні дії).
- Природні (об'єктивні): природні катастрофи, стихійні лиха.

Класифікація за спрямованістю:

- Погрози конфіденційності: Порушення секретності даних (відпливу).
- Загрози цілісності: Спотворення чи зміна даних.
- Загрози доступності: Блокування або утруднення доступу до інформації.

Інформаційні атаки спрямовані на дезінформацію екіпажів або диспетчерських служб, що може призвести до аварійних приходів на море і значною мірою використовують специфіку морської галузі: велика довжина кордонів, транскордонний характер перевезень та залежність від супутникових даних.

Протидія загрозам, що виникають і передбачуваним, складається з організаційних і технічних засобів.

Організаційна компонента моделі управління ризиками у свою чергу складається з нормативно-правової бази, ризик-орієнтованого підходу, міжвідомчої взаємодії та людського фактору.

Нормативно-правова база адаптується відповідно до вимог Кодексу ОСПС (ISPS Code) до сучасних реалій. Відповідно до Кодексу ISPS обов'язкова присутність відповідних співробітників із забезпечення безпеки на кожному судні, у портовій споруді та судноплавній компанії. Ці працівники відповідають за оцінку, а також підготовку та реалізацію ефективних планів забезпечення безпеки, здатних впоратися з будь-якою потенційною загрозою безпеці.

Ризик-орієнтований підхід із динамічною оцінкою ризиків означає методологію безперервного моніторингу, що фокусує ресурси на найбільш критичних загрозах через усвідомлену поведінку. Вона включає триетапний цикл: оцінку небезпек, аналіз запобігання та виконання безпечних дій. Цей підхід дозволяє адаптувати заходи безпеки до поточної ситуації, переходячи від формального дотримання вимог проактивного управління. Основні етапи цього підходу:

- Виявлення небезпек та можливих наслідків;
- Визначення способів мінімізації ризиків;
- безпечне виконання необхідних заходів чи звернення за допомогою [4].

Така стратегія управління, спрямована на ідентифікацію, оцінку та мінімізацію ризиків на всіх етапах, дозволяє адаптувати контроль до конкретних потреб організації та забезпечує усвідомлену безпеку, зниження інтенсивності перевірок у зонах з низьким ризиком та фокусування на зонах високого ризику.

Міжвідомча взаємодія дозволяє створити алгоритми зв'язку між судновласниками, портовою владою та державними службами безпеки для найбільш ефективної протидії різним видам загроз та проводити заходи щодо запобігання виникненню загрози безпеці.

Людський фактор враховується в аспекті навчання персоналу розпізнаванню латентних ознак гібридної дії і в даний час фокусується на виявленні аномалій на стику цифрового, фізичного та психологічного середовища.

Організаційні заходи, спрямовані на протидію та запобігання загрозам безпеці спираються на технічні засоби, які створюють ешелоновану систему захисту та використовують проактивну, інтелектуальну систему захисту з використанням штучного інтелекту.

У систему захисту включають такі сегменти:

Підводний сегмент: Гідроакустичні датчики та безлюдні підводні апарати;

Надводний сегмент: РЛС, тепловізори та системи автоматичної ідентифікації (AIS) з обов'язковим захистом від заміни даних;

Повітряний сегмент: Дрони-монітори для патрулювання акваторій.

Цифрова екосистема та використання Штучного Інтелекту (AI) – найсучасніша тенденція для аналізу аномальної поведінки суден і Блокчейна для захисту логістичних даних. Аналіз сучасного стану застосування штучного інтелекту показав, що організації можуть використовувати інструменти штучного інтелекту для більш ефективного виявлення шкідливих програм та інших загроз, а також використовувати модель прогнозування для запобігання майбутнім атакам та підготовці до них. Дозволяє керувати вразливістю, які дуже складно відстежувати одночасно, ІІ визначає найбільш серйозні загрози, сортує їх та визначає порядок пріоритету, щоб впоратися з ними насамперед. Замість того, щоб просто перевіряти загрози, виявлені раніше, ІІ допомагає організаціям виявляти інші загрози, які, можливо, не були виявлені раніше. Він може використовувати великі дані та іншу доступну інформацію для визначення ймовірних проблем, які звичайні інструменти можуть не виявити, доки не станеться

подія. ІІ покращує моніторинг навколишнього мережевого середовища та покращує розробку політик, підвищуючи мережну безпеку, перевіряючи політики, щоб переконатися, що не створюються шкідливі програми для підключення, та відстежує середовище, щоб переконатися, що немає лазівок, які можуть бути використані. ІІ також можна використовувати для оптимізації критично важливих процесів у центрі обробки даних, таких як резервне харчування, енергоспоживання, використання смуги пропускання, внутрішня температура та охолодження. Він забезпечує найкращі значення забезпечення ефективної роботи інфраструктури [5].

Синтез організаційно-технічної моделі попередження та протидії гібридним угрозам передбачає створення центру управління безпекою та створення єдиного інформаційного простору для його ефективного функціонування. Концепція єдиного інформаційного простору запропонована EMSA (Європейське агентство з безпеки на морі) і представлена на рисунку 2.

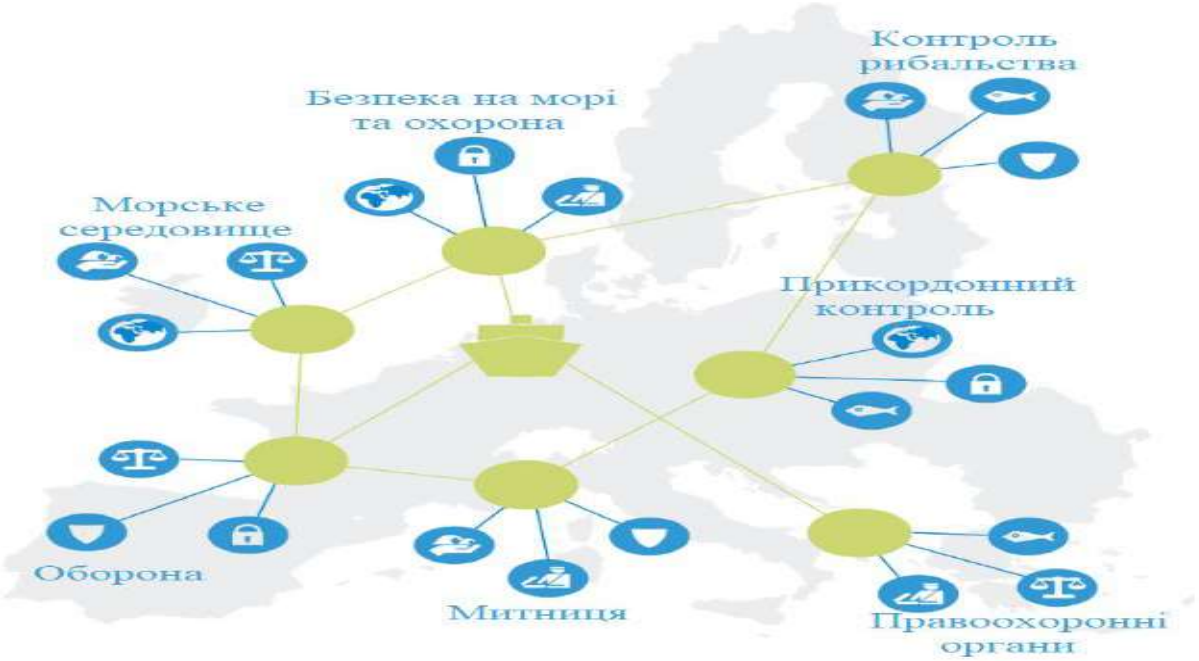


Рис. 2 Спільне середовище обміну інформацією [6]

Технічна складова протидії загрозам трансформує сигнали від підводного, надводного та повітряного сегмента в організаційні команди та визначає алгоритм прийняття рішень, що адаптивно змінює рівні охорони. Створена модель «цифрового двійника» порту/судна тестує сценарії відображення загроз у віртуальному середовищі і за допомогою ІІ визначає найбільш ефективний метод попередження загроз безпеки або відображення варіанта нападу, що виник.

Висновки. Розглянуто види існуючих загроз на морському транспорті та надано їх кваліфікацію. Визначено засоби протидії гібридним загрозам та переведено їх характеристики та цілі, для яких вони призначені. Запропоновано створення моделі проактивного управління безпекою з використанням штучного інтелекту та створенням цифрових двійників судна та портової інфраструктури.

Щоб мінімізувати ризики та ефективно працювати, компаніям, зайнятим у морській галузі, варто звернути увагу на оцінку ризиків у реальному часі, для чого необхідне використання сучасних цифрових платформ, які оперативно аналізують загрози та ризики. Це дозволяє швидко реагувати зміни маршрутів чи ситуації у портах. Необхідно диверсифікувати маршрути та постачальників, щоб знизити вплив локальних криз.

Використання IoT-датчиків, GPS-трекінгу для контролю за вантажем дозволяє знизити ймовірність пошкоджень вантажу, що перевозиться, і убезпечити екіпаж і судно.

Особливу увагу слід приділити захищеності інформаційних систем, оскільки кібератаки можуть призвести до втрат і зупинки ланцюжків поставок. Перехід до проактивного управління системами безпеки – це вже не теоретичне обговорення, а нагальна потреба.

Список використаних джерел

1. Review of Maritime Transport 2024 Navigating maritime chokepoints UNCTAD/RMT/2024 22 Oct 2024

2. Захист Балтійського моря: The Economist розібрав, що НАТО може протиставити Росії. 23.12.25 Електронный ресурс, URL: https://www.unian.ua/world/nato-ta-rosiya-cherez-gibridni-zagrozi-rosiji-na-baltici-krajini-nato-posilyuyut-sviy-flot-13235400.html?_gl=1*19cnt5*_ga*MTY3OTE3NTUxNi4xNzY4ODE4NzIz*_ga_TECJ2YKWSJ*czE3Njg4MTg3MjMkbzEkZzEkdDE3Njg4MTkxNTAkajU1JGwwJGgw*_ga_DENC12J6P3*czE3Njg4MTg3MjMkbzEkZzEkdDE3Njg4MTkxNTAkajU1JGwwJGgxODcyNDEwNTY1 Дата доступу 03.01.2026.

3. Мустафаєв О.В. сучасні технології захисту від gps спуфінгу у системах навігації. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. УДК 621.396 DOI https://doi.org/10.32782/2663-5941/2024.5.1/10

4. FATF (2021), Guidance on Risk-Based Supervision, FATF, Paris, http://www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html

5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №4 (квітень) . – 188 с.

6. The 2025 european maritime safety report, EUROPEAN MARITIME SAFETY AGENCY, https://emsa.europa.eu/publications/reports/download/8409/5598/23.html, Дата доступу 15.01.2026.

7. Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans (2nd ed.). European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 2024.

8. The Landscape of Hybrid Threats: A Conceptual Model.European Commission, Joint Research Centre (JRC), 2021.

9. Maritime Security Law in Hybrid Warfare. Edited by Alexander Lott. Brill, 2022.

10. Melnyk, O., et al. (2025). Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. Lex Portus.

11. Miller, J., et al. (2025). Big Language Models for Risk Analysis and Security of Maritime Operations. Journal of Marine Science and Engineering.

12. Giannopoulos, G., et al. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System. MDPI - Water.

13. Jiang, L., et al. (2025). The Risk Life Cycle of Cargo Ships Based on Probabilistic Models. Reliability Engineering & System Safety.

14. Hybrid CoE Research Report 14 (2025). Protecting Maritime Infrastructure from Hybrid Threats: Legal Options.

15. Mietkiewicz, R. (2022). Hybrid Threats in the Baltic Sea: Analysis of Countermeasure Options. ABW Security Review.

16. Lott, A. (2022). Hybrid Threats and the Law of the Sea. Brill/Nijhoff.

17. International Maritime Organization (IMO). MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management.

18. European Union. Revised EU Maritime Security Strategy (EUMSS) and its Action Plan (2023).

19. International Ship and Port Facility Security (ISPS) Code. – London : International Maritime Organization, 2020.

Reference

1. Review of Maritime Transport 2024 Navigating maritime chokepoints UNCTAD/RMT/2024 22 Oct 2024

2. Zakhyst Baltiiskoho moria: The Economist rozibrav, shcho NATO mozhe protystavyty Rosii. 23.12.25 Web, URL: https://www.unian.ua/world/nato-ta-rosiya-cherez-gibridni-zagrozi-rosiji-na-baltici-krajini-nato-posilyuyut-sviy-flot-13235400.html?_gl=1*19cnt5*_ga*MTY3OTE3NTUxNi4xNzY4ODE4NzIz*_ga_TECJ2YKWSJ*czE3Njg4MTg3MjMkbzEkZzEkdDE3Njg4MTkxNTAkajU1JGwwJGgw*_ga_DENC12J6P3*czE3Njg4MTg3MjMkbzEkZzEkdDE3Njg4MTkxNTAkajU1JGwwJGgxODcyNDEwNTY1 Access date 03.01.2026.

3. Mustafaiev O.V. suchasni tekhnolohii zakhystu vid gps spufinhu u systemakh navihatsii. Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Tekhnichni nauky. UDK 621.396 DOI https://doi.org/10.32782/2663-5941/2024.5.1/10

4. FATF (2021), Guidance on Risk-Based Supervision, FATF, Paris, http://www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html

5. Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest / vidp. red. O.Dovhan; uporiad. O.Dovhan, L.Lytvynova, S.Dorohykh; Derzhavna naukova ustanova «Instytut informatsii, bezpeky i prava NAPrN Ukrainy»; Natsionalna biblioteka Ukrainy im. V.I.Vernadskoho. – K., 2023.– №4 (kviten) . – 188 s.6. The 2025 european maritime safety report, EUROPEAN MARITIME SAFETY AGENCY, https://emsa.europa.eu/publications/reports/download/8409/5598/23.html, Дата доступу 15.01.2026.

7. Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans (2nd ed.). European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), 2024.

8. The Landscape of Hybrid Threats: A Conceptual Model. European Commission, Joint Research Centre (JRC), 2021.

9. Maritime Security Law in Hybrid Warfare. Edited by Alexander Lott. Brill, 2022.

10. Melnyk, O., et al. (2025). Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. Lex Portus.

11. Miller, J., et al. (2025). Big Language Models for Risk Analysis and Security of Maritime Operations. Journal of Marine Science and Engineering.

12. Giannopoulos, G., et al. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System. MDPI - Water.

13. Jiang, L., et al. (2025). The Risk Life Cycle of Cargo Ships Based on Probabilistic Models. Reliability Engineering & System Safety.

14. Hybrid CoE Research Report 14 (2025). Protecting Maritime Infrastructure from Hybrid Threats: Legal Options.

15. Mietkiewicz, R. (2022). Hybrid Threats in the Baltic Sea: Analysis of Countermeasure Options. ABW Security Review.

16. Lott, A. (2022). Hybrid Threats and the Law of the Sea. Brill/Nijhoff.

17. International Maritime Organization (IMO). MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management.

18. European Union. Revised EU Maritime Security Strategy (EUMSS) and its Action Plan (2023).

19. International Ship and Port Facility Security (ISPS) Code. – London : International Maritime Organization, 2020.