ВІСНИК
ОДЕСЬКОГО НАЦІОНАЛЬНОГО
МОРСЬКОГО УНІВЕРСИТЕТУ
№ 1 (79), 2026

HERALD
OF THE ODESA NATIONAL
MARITIME UNIVERSITY
№ 1 (79), 2026

ISSN 2226-1893

УДК 656.61:355.01:004.056
DOI 10.47049/2226-1893-2026-1-187-201

СИСТЕМНИЙ АНАЛІЗ ГІБРИДНИХ ЗАГРОЗ У МОРСЬКІЙ ГАЛУЗІ ТА ОБҐРУНТУВАННЯ ПЕРЕХОДУ ДО КОМПЛЕКСНИХ АДАПТИВНИХ МОДЕЛЕЙ БЕЗПЕКИ

К.С. Корякін
к.т.н., доцент кафедри судноводіння і морської безпеки
ORCID ID: 0000-0003-2388-645X
В.Ю. Дехта
аспірант кафедри судноводіння і морської безпеки
ORCID ID: 0000-0002-0488-5972
А.І. Довгошеєнко
аспірант кафедри судноводіння і морської безпеки
ORCID ID: 0009-0007-0431-0013

Одеський національний морський університет, Одеса, Україна

О.М. Мазур
к.т.н., доцент кафедри теорії та устрою судна
ORCID ID: 0000-0002-9316-288X

Національний університет «Одеська морська академія», Одеса, Україна

Анотація. *У статті здійснено системний аналіз сучасних гібридних загроз у морській галузі, які поєднують фізичні, кібернетичні, інформаційні та соціально-економічні вектори впливу.*

Проведено класифікацію гібридних загроз морському судноплавству та портовій інфраструктурі, визначено обмеження класичних підходів до забезпечення морської безпеки та обґрунтовано необхідність переходу до комплексних адаптивних моделей управління ризиками.

Запропоновано формалізовану математичну модель оцінювання ризику гібридних загроз з урахуванням ефекту їх взаємного підсилення, а також порогову логіку прийняття управлінських рішень у реальному часі.

Отримані результати можуть бути використані для розроблення систем підтримки прийняття рішень, цифрових двійників морських об'єктів та підвищення стійкості морської інфраструктури в умовах гібридних загроз.

Ключові слова: *морська безпека, гібридні загрози, управління ризиками, кіберфізичні системи, адаптивні моделі, цифровий двійник, портова інфраструктура, підводні операції.*

ВІСНИК
ОДЕСЬКОГО НАЦІОНАЛЬНОГО
МОРСЬКОГО УНІВЕРСИТЕТУ
№ 1 (79), 2026

HERALD
OF THE ODESA NATIONAL
MARITIME UNIVERSITY
№ 1 (79), 2026

ISSN 2226-1893

UDC 656.61:355.01:004.056
DOI 10.47049/2226-1893-2026-1-187-201

SYSTEMIC ANALYSIS OF HYBRID THREATS IN THE MARITIME SECTOR AND JUSTIFICATION FOR THE TRANSITION TO COMPREHENSIVE ADAPTIVE SECURITY MODELS

K. Koryakin
Department of Navigation and Maritime Safety
ORCID ID: 0000-0003-2388-645X
V. Dekhta
Department of Navigation and Maritime Safety
ORCID ID: 0000-0002-0488-5972
A. Dovhosheyenko
Department of Navigation and Maritime Safety
ORCID ID: 0009-0007-0431-0013

Odesa National Maritime University, Odesa, Ukraine

O. Mazur
Department of Ship Theory and Design
ORCID ID: 0000-0002-9316-288X

Odesa Maritime Academy National University, Odesa, Ukraine

Abstract. *The article provides a systematic analysis of contemporary hybrid threats in the maritime sector, which combine physical, cybernetic, informational, and socio-economic vectors of influence. It classifies hybrid threats to maritime shipping and port infrastructure, identifies the limitations of traditional approaches to maritime security, and justifies the need to transition to comprehensive adaptive risk management models. A formalized mathematical model for assessing the risk of hybrid threats, taking into account the effect of their mutual reinforcement, as well as threshold logic for making management decisions in real time, has been proposed. The results obtained can be used to develop decision support systems, digital twins of maritime objects, and to increase the resilience of maritime infrastructure in the face of hybrid threats.*

Keywords: *maritime security, hybrid threats, risk management, cyber-physical systems, adaptive models, digital twin, port infrastructure, underwater operations.*

Вступ. Глобальна морська галузь у XXI столітті перебуває під безпрецедентним тиском багатовекторних загроз – від геополітичних конфліктів і піратства до кібератак і маніпуляцій з логістичними даними. Зростаюча складність морського середовища зумовлює необхідність переосмислення концепції безпеки: від реактивних заходів до адаптивних систем прогнозування, виявлення і протидії загрозам у режимі реального часу. Класичні підходи, орієнтовані на фізичну охорону суден і портів, втрачають ефективність у середовищі, де атака може мати як матеріальний, так і цифровий чи когнітивний характер. Таким чином, формування комплексної

ISSN 2226-1893

моделі морської безпеки є ключовим завданням сучасної морської політики України та міжнародного співтовариства.

Огляд літератури по темі дослідження та постановка проблеми. Опанований масив джерел демонструє, що гібридні загрози в морській галузі формуються на перетині глобального тероризму, кіберризиків, енергетичного переходу та цифрової трансформації. На макрорівні роботи Islam et al. (2025) та Ghufran і Breuer (2024) показують, як тероризм, глобальне врядування та фінансові ефекти безпекових криз задають фон для формування ризиків у транспортно-логістичних ланцюгах, тоді як Khan et al. (2025) і Adamu et al. (2026) пов'язують розвиток AI-орієнтованих бізнес-моделей і «зеленої» водневої економіки з цілями сталого розвитку. У суто морському вимірі Islam et al. (2025), Uğurlu (2025), Tonoğlu et al. (2022) та Zhu et al. (2025) демонструють, що управління навігаційними ризиками, евакуацією й рятувальними операціями на основі AIS-даних і мультикритеріальних методів (fuzzy AHP, BWM, гібридні хмарні моделі) потребує інтеграції людського фактору, ситуаційної обізнаності та інтелектуальних алгоритмів. Роботи Skare і Haugdal Jore (2024) вводять поняття гібридних загроз у нафтогазовому секторі як нової категорії ризиків для safety-science, що є безпосередньо релевантним для морських енергетичних коридорів, тоді як Hoang et al. (2026) та Zhaka і Samuelsson (2024) акцентують на переході до метанолу й водню як частини декарбонізації флоту, що створює нові техногенні й регуляторні ризики. Цифровий вимір гібридних загроз підсилюється роботами Ledesma і Lamo (2025), які пропонують гібридні IoT-мережі для моніторингу контейнерів, та Melnyk et al. (2024-2025), де послідовно розвиваються стратегії кіберзахисту, інтеграції людського фактору в проектно-орієнтоване управління ризиками й єдиний системний підхід до забезпечення безпеки судноплавства. Сукупно вказані дослідження обґрунтовують перехід від фрагментованих, «галузевих» заходів та вказують на необхідність побудови нових комплексних адаптивних моделей безпеки, які поєднують геополітичний, техніко-енергетичний, кіберфізичний і гуманітарний виміри, спираючись на інтелектуальну обробку даних, сценарне моделювання та ієрархічне управління ризиками на рівні глобальних мереж, окремих акваторій, портів та навіть конкретних суден.

Мета статті. Розробити концептуальну модель трансформації систем морської безпеки з класичних методів до комплексних адаптивних структур, здатних функціонувати в умовах гібридних загроз. Завдання дослідження:

- проаналізувати сучасний спектр гібридних загроз у морському середовищі;
- визначити слабкі місця традиційних систем безпеки;
- сформувати структурно-логічну модель адаптивної морської системи захисту;
- обґрунтувати роль штучного інтелекту, цифрових двійників та iot-технологій у забезпеченні стійкості портової інфраструктури;
- запропонувати алгоритм міжвідомчої взаємодії у межах єдиного інформаційного простору морської безпеки.

ISSN 2226-1893

Наукова новизна роботи полягає у формалізації гібридних загроз у морській галузі як інтегрованого багатовекторного процесу з урахуванням ефекту взаємного підсилення фізичних, кібернетичних та інформаційних впливів.

Уперше для оцінювання рівня морської безпеки запропоновано адаптивну математичну модель ризику, доповнену пороговою логікою прийняття рішень, що дозволяє перейти від реактивного до проактивного управління безпекою. Отримані результати створюють методологічну основу для побудови систем підтримки прийняття рішень і цифрових двійників морських об'єктів в умовах гібридних загроз.

Виклад основного матеріалу. Заходи, що вживаються судноплавними компаніями з метою запобігання порушенням комерційної діяльності, зокрема зміна маршрутів перевезень і збільшення витрат на безпеку, призводять до зростання вартості морського страхування та мають негативний вплив на глобальні ланцюги енергопостачання. І тут показовим прикладом є інтенсифікація таких заходів безпеки в Аденській затоці, що суттєво ускладнила умови здійснення морської торгівлі та вплинула на ефективність транспортних потоків у регіоні.

Зміна маршрутів судноплавства обумовлює збільшення тривалості рейсів і, відповідно, зростання обсягів викидів забруднюючих речовин в атмосферу, тоді як морські аварії, пов'язані з актами захоплення або перехоплення суден, істотно підвищують ризики забруднення морського середовища, що особливо критично з огляду на те, що зазначені процеси відбуваються на стратегічно важливих морських шляхах і в районах, безпосередньо пов'язаних з видобутком і транспортуванням енергетичних ресурсів. Одним із найбільш резонансних інцидентів останніх років став напад на контейнерне судно V/S Mozart під ліберійським прапором поблизу узбережжя Нігерії в Гвінейській затоці, внаслідок якого один член екіпажу загинув, а п'ятнадцять осіб було викрадено.

З метою мінімізації зазначених ризиків учасники морського ринку були змушені впроваджувати додаткові заходи безпеки, зокрема розміщення на борту суден озброєного персоналу охорони, а також використання механізмів міжнародного співробітництва, які забезпечують безпечне проходження суден у складі військово-морських конвоїв. У глобальному вимірі визначальну роль у формуванні таких практик відіграють політична, економічна та соціальна стабільність, тоді як їх порушення в окремих регіонах світу виступає тригером зростання загроз морській безпеці. Окремої уваги потребує проблема кібербезпеки, яка набуває дедалі більшої актуальності в умовах цифровізації логістичних процесів. Сучасне судноплавство значною мірою залежить від автоматизованих систем управління, супутникової навігації, цифрових платформ моніторингу та електронного документообігу, що водночас підвищує вразливість галузі до кібератак.

Потенційні загрози включають несанкціонований доступ до портових інформаційних систем, маніпуляції з даними щодо вантажів і маршрутів їх переміщення, а також порушення функціонування ланцюгів постачання і у відповідь на ці виклики сучасні страхові продукти все частіше передбачають покриття кібер-

ISSN 2226-1893

ризиків (cyber risk coverage), спрямоване на компенсацію збитків від кіберінцидентів, здатних паралізувати роботу транспортно-логістичних систем.

1. Сучасні гібридні загрози в морській сфері як об'єкт наукового аналізу

1.1. Поняття та природа гібридних загроз у морському середовищі

У сучасних умовах розвитку глобального судноплавства морська безпека перестала бути виключно сферою фізичного захисту суден, портів і морських комунікацій. Зростання ролі цифрових технологій, автоматизованих систем управління, супутникової навігації та глобальних логістичних платформ призвело до формування нового класу загроз – гібридних, які поєднують у собі фізичні, кібернетичні, інформаційні та організаційно-технічні компоненти.

У контексті сучасної морської безпеки *гібридні загрози* доцільно визначати як сукупність скоординованих впливів різної природи – фізичної, кібернетичної, інформаційної, економічної та організаційної, – що реалізуються одночасно або послідовно з метою порушення стійкого функціонування морських систем. На відміну від традиційних загроз, гібридні загрози характеризуються асиметричністю, латентністю та здатністю до взаємного підсилення окремих компонентів впливу, що ускладнює їх своєчасне виявлення та оцінювання. У морському середовищі такі загрози можуть проявлятися у вигляді поєднання підводних диверсій, кібератак на навігаційні та портові системи, інформаційних операцій і економічного тиску, формуючи комплексний ризик для судноплавства, портової інфраструктури та глобальних ланцюгів постачання. На практиці гібридні загрози в морській галузі доцільно визначати як комплекс координованих впливів, спрямованих на порушення безпеки морських операцій шляхом одночасного або послідовного використання різнорідних інструментів: від фізичного саботажу та піратства до кібератак, дезінформації та маніпуляцій з даними навігаційних систем.

На рисунку 1 представлена структурована класифікація сучасних гібридних загроз.

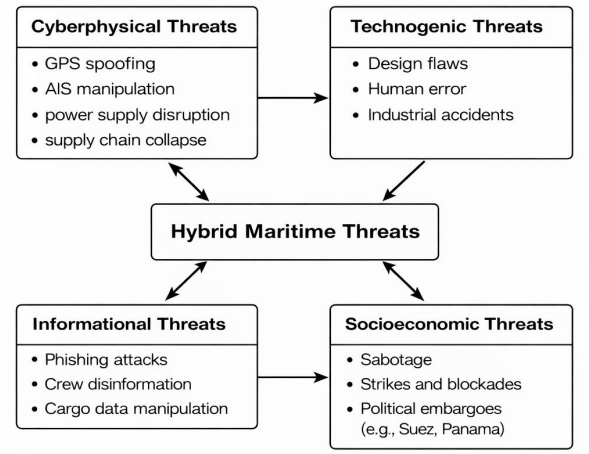

Рис. 1. Класифікація гібридних загроз у морській сфері

ISSN 2226-1893

Ті загрози впливають на морську інфраструктуру, структура об'єднує категорії кіберфізичних, техногенних, інформаційних та соціально-економічних загроз і підкреслює їх взаємопов'язаний характер у рамках морських операційних систем.

Особливістю морського середовища є:

- протяжність морських кордонів;
- транскордонний характер перевезень;
- критична залежність від GPS, AIS, ECDIS, IoT-датчиків;
- уразливість підводної інфраструктури (кабелі, трубопроводи, гідротехнічні споруди).

Перераховані фактори формують високу чутливість морської галузі до гібридних сценаріїв впливу, що обумовлює необхідність їх системної класифікації та моделювання.

1.2. Класифікація гібридних загроз у морській галузі

Для формування адаптивної системи безпеки першочерговим є завдання структурованої класифікації загроз, що дозволяє формалізувати ризики та пов’язати їх з відповідними засобами протидії.

Для побудови адаптивної системи безпеки у морській галузі необхідним етапом є формалізована класифікація гібридних загроз, яка дозволяє системно охопити різнорідні джерела ризиків та встановити причинно-наслідкові зв’язки між загрозами, їх проявами та потенційними наслідками. Така класифікація (табл. 1) створює методологічну основу для подальшого кількісного аналізу ризиків, розроблення сценаріїв реагування та інтеграції відповідних механізмів захисту у структуру систем підтримки прийняття рішень.

Таблиця 1

Класифікація гібридних загроз у морському середовищі

Група загроз	Джерело впливу	Характер впливу	Потенційні наслідки
Кіберфізичні	Хакерські угруповання, державні актори	GPS spoofing, втручання в AIS, ECDIS	Втрата навігації, зіткнення, аварії
Техногенно-організовані	Людський фактор, аварії	Вибухи, пожежі, відмови систем	Руйнування суден, портів
Інформаційні	Дезінформаційні кампанії	Фальшиві дані, фішинг	Неправильні управлінські рішення
Підводні	Диверсійні групи, БПА	Саботаж, пошкодження кабелів, труб	Втрата зв’язку, енергокриза
Соціально-економічні	Політичний тиск	Блокади, санкції	Порушення ланцюгів постачання

Наведена класифікація демонструє багатовимірний характер гібридних загроз у морській галузі, де технічні, інформаційні, соціально-економічні та фізичні

ISSN 2226-1893

впливи взаємодіють між собою та підсилюють сукупний ризик для судноплавства і портової інфраструктури. Особливістю таких загроз є їх асиметричність та складність виявлення, що обумовлює необхідність переходу від традиційних реактивних підходів до ризик-орієнтованого та прогностичного управління безпекою.

Отримані результати слугують базисом для формування інтегрованої моделі оцінювання ризиків, у межах якої кожна група загроз може бути відображена через відповідні змінні стану, вагові коефіцієнти та сценарії розвитку, що, у свою чергу, забезпечує можливість кількісного аналізу стійкості морських систем та обґрунтованого вибору оптимальних заходів протидії в умовах гібридних впливів.

1.3. Структурна схема гібридних загроз у морській системі

Для узагальнення взаємопов'язаних загроз безпеці судноплавства доцільно застосувати інтегральний підхід, який поєднує фізичні, кібернетичні та інформаційні чинники впливу. Такий підхід дозволяє простежити причинно-наслідкові зв'язки між різними типами загроз і їх сукупним впливом на рівень морської безпеки.

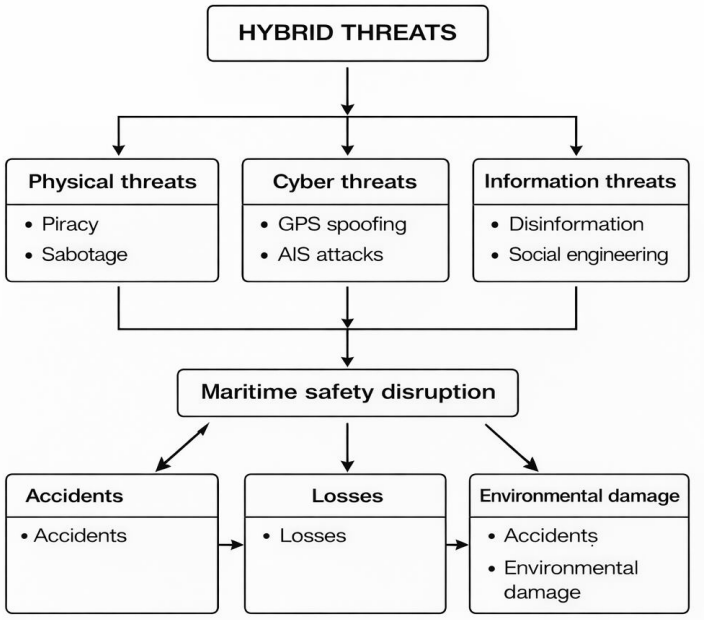

Рис. 2. Структура гібридних загроз та їх вплив на безпеку мореплавства

Подана схема ілюструє, що гібридні загрози формуються на перетині фізичних, кібернетичних та інформаційних впливів, які в сукупності призводять до порушення морської безпеки. Наслідки таких впливів проявляються у вигляді аварій, економічних втрат та екологічних збитків. Це підтверджує необхідність комплексних систем управління ризиками, орієнтованих не на окремі загрози, а на їх взаємодію та кумулятивний ефект у морському середовищі.

Окремий клас гібридних загроз у морській галузі формують підводні операції, спрямовані на прихований вплив на критично важливу інфраструктуру

ISSN 2226-1893

морського дна. До таких об'єктів належать підводні кабелі зв'язку, трубопроводи, гідротехнічні споруди, системи гідроакустичного спостереження та елементи підводних енергетичних мереж. Особливість підводних операцій полягає у складності їх виявлення, високому рівні латентності та можливості реалізації як із застосуванням диверсійних груп, так і за допомогою безпілотних підводних апаратів. Поєднання підводного фізичного впливу з кібернетичними атаками на системи моніторингу та управління створює типові гібридні сценарії, наслідками яких можуть бути порушення навігаційної безпеки, втрата зв'язку, збої в енергопостачанні та дестабілізація логістичних процесів. У зв'язку з цим підводний компонент морської безпеки потребує інтеграції у загальну адаптивну модель управління ризиками поряд із надводним, повітряним та інтелектуальними сегментами.

1.4. Формалізація ризику гібридних загроз

Для кількісної оцінки гібридних загроз у морській галузі доцільно застосовувати формалізований підхід, що дозволяє врахувати імовірнісний характер загроз, масштаб їх наслідків, рівень вразливості об'єктів морської інфраструктури, а також ефект взаємного підсилення різнорідних впливів.

Базова модель інтегрального ризику окремої *i*-тої загрози визначається як

$$R_i = P_i \cdot C_i \cdot V_i, \tag{1}$$

де R_i – інтегральний ризик і-ї загрози;

P_i – ймовірність реалізації загрози;

C_i – масштаб наслідків (економічних, екологічних, людських);

V_i – рівень вразливості системи.

З урахуванням багатовекторного характеру гібридних загроз загальний ризик не є простою сумою окремих складових. Для врахування синергетичного ефекту доцільно ввести коефіцієнт інтеграції загроз

$$R_{\text{hyb}} = \sum_{i=1}^{n} R_i \cdot K_{\text{int}}, \tag{2}$$

де: $K_{\text{int}} \geq 1$ – коефіцієнт взаємного підсилення загроз, який відображає ступінь одночасного впливу фізичних, кібернетичних та інформаційних чинників.

Нормалізація параметрів ризику. Для забезпечення порівнянності оцінок у рамках системи підтримки прийняття рішень параметри P_i, C_i та V_i доцільно нормалізувати в інтервалі [0;1]

$$P_i = \frac{p_i}{p_{\max}}, \quad C_i = \frac{c_i}{c_{\max}}, \quad V_i = \frac{v_i}{v_{\max}}, \tag{3}$$

де $P_{\max}$, $C_{\max}$, $v_{\max}$ – максимально можливі значення відповідних показників у розглянутій системі.

ISSN 2226-1893

Матричне подання гібридного ризику. Для комплексної оцінки стану системи ризик доцільно подати у вигляді векторно-матричної моделі

$$\mathbf{R} = \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}, \quad \mathbf{W} = \begin{bmatrix} w_1 & 0 & \cdots & 0 \\ 0 & w_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & w_n \end{bmatrix}, \tag{4}$$

де w_i – вагові коефіцієнти значущості окремих загроз, визначені експертним шляхом або на основі статистичних даних.

Тоді інтегральний показник ризику морської системи може бути визначений як

$$R_{\text{sys}} = \mathbf{R}^{\text{T}} \mathbf{W} \mathbf{R}, \tag{5}$$

Динамічна модель ризику в реальному часі. З урахуванням змінності операційної обстановки у морському середовищі ризик доцільно розглядати як функцію часу

$$R_{\text{sys}}(t) = f\left(P(t), C(t), V(t)\right), \tag{6}$$

де зміна параметрів з часом визначається надходженням нових даних від датчиків, інформаційних систем та зовнішніх джерел.

Такий підхід створює математичну основу для реалізації адаптивних алгоритмів управління рівнями безпеки, у межах яких система автоматично коригує захисні заходи залежно від поточного значення $R_{sys}(t)$.

Таким чином гібридні загрози у морській галузі мають системний характер, що унеможливлює їх ефективну нейтралізацію за допомогою класичних методів безпеки, тому як було вказано, багатовимірність, динамічність і здатність гібридних загроз до взаємного підсилення вимагають переходу до адаптивних організаційно-технічних моделей, здатних працювати в умовах невизначеності та реального часу.

Порогова модель прийняття рішень. Для практичної реалізації управління безпекою вводяться порогові значення ризику

$$L(t) = \begin{cases} 0, & R_{\text{sys}}(t) < R_1, \\ 1, & R_1 \le R_{\text{sys}}(t) < R_2, \\ 2, & R_{\text{sys}}(t) \ge R_2. \end{cases} \tag{7}$$

де $L(t)$ – дискретний рівень безпеки і-ої системи у момент часу t; R_1, R_2 – порогові значення інтегрального ризику, що визначають зміну режимів функціонування системи.

ISSN 2226-1893

Алгоритм реалізації порогової логіки управління рівнями безпеки. Реалізація порогової логіки управління рівнями безпеки в рамках запропонованої моделі ґрунтується на безперервному моніторингу інтегрального показника ризику $R_{\text{sys}}(t)$, який обчислюється у реальному часі на основі актуальних даних про ймовірність загроз, масштаб можливих наслідків та рівень вразливості морської системи. На першому етапі збираються та проводиться попередня обробка даних від навігаційних, технічних та інформаційних підсистем. Далі виконується нормалізація параметрів і розрахунок значення $R_{\text{sys}}(t)$, порівняння отриманого результату з визначеними порогами R_1 і R_2. Другий етап полягає у тому, що такі дії дозволяють формально визначити поточний дискретний рівень безпеки $L(t)$. На завершальному етапі система автоматично ініціює відповідні управлінські дії – зміну режимів охорони, активацію додаткових засобів контролю або посилення взаємодії між елементами системи. Такий алгоритм забезпечує адаптивне та проактивне реагування на зміну операційної обстановки і може бути інтегрований у системи підтримки прийняття рішень та цифрові двійники.

Обговорення. Формалізація ризику гібридних загроз із використанням інтегральної моделі, доповненої коефіцієнтом взаємного підсилення, створює передумови для кількісного аналізу складних сценаріїв впливу та є основою для подальшого розвитку ризик-орієнтованих систем управління морською безпекою. Застосування такого підходу дозволяє перейти від реактивного реагування на інциденти до проактивного управління загрозами з урахуванням їх імовірності, масштабів наслідків і рівня вразливості системи.

Отримані результати підтверджують доцільність переходу від класичних методів охорони до комплексних адаптивних моделей морської безпеки, які інтегрують організаційні та технічні засоби захисту, використовують сучасні цифрові технології, елементи штучного інтелекту та механізми міжвідомчої взаємодії. Запропонований підхід формує наукове підґрунтя для подальших досліджень у напрямі розроблення систем підтримки прийняття рішень та цифрових моделей управління ризиками у сфері морської безпеки в умовах гібридних загроз.

Висновки. У результаті проведеного дослідження встановлено, що сучасні загрози у морській галузі мають гібридний характер і формуються внаслідок поєднання фізичних, кібернетичних, інформаційних та соціально-економічних чинників. Їх багатовимірність, динамічність і асиметричність суттєво ускладнюють процеси виявлення, оцінювання та нейтралізації, що знижує ефективність традиційних підходів до забезпечення морської безпеки.

Запропонована класифікація гібридних загроз дозволяє систематизувати основні джерела ризиків у морському середовищі та встановити причинно-наслідкові зв’язки між характером загрози, об’єктами впливу та потенційними наслідками для судноплавства і портової інфраструктури. Показано, що гібридні загрози не діють ізольовано, а взаємно підсилюють одна одну, формуючи куму ля-

ISSN 2226-1893

тивний ефект ризику, який може призводити до масштабних техногенних, економічних та екологічних наслідків.

СПИСОК ЛІТЕРАТУРИ

1. Islam, S., Roshid, M.M., Bhowmik, R.C., Dhar, B.K., Islam, M.S., Raihan, A., & Akter, F. (2025). Global governance and security challenges: Transnational pathways to reducing terrorism mortality in a globalized world. *Research in Globalization*, *11*, 100312. https://doi.org/10.1016/j.resglo. 2025.100312.
2. Ghufran, B., & Breuer, W. (2024). Terrorism, national security, and takeover performance. *International Review of Financial Analysis*, *96*, 103634. https://doi.org/10.1016/j.irfa.2024.103634.
3. Khan, M.A., Rahman, A., Mahmud, F.U., Bishnu, K.K., Ahmed, M., Mridha, M., & Aung, Z. (2025). A systematic review of AI-driven business models for advancing Sustainable Development Goals. *Array*, *28*, 100539. https://doi.org/10.1016/j.array.2025.100539.
4. Adamu, H., Bello, U., Tafida, U.I., Zango, Z.U., Muhammad, K.Y., & Qamar, M. (2026). Review on the intersection of materials science and policy: A dual-track approach to realizing a green hydrogen economy for climate-neutral energy transition. *Sustainable Energy Technologies and Assessments*, *86*, 104831. https://doi.org/10.1016/j.seta.2026.104831.
5. Islam, S., Shi, Y., Nahar, R., Ahmed, J. U., & Wang, M. (2025). Identifying and analyzing barriers to ship-based evacuation planning using AIS data. *Transportation Research Part E: Logistics and Transportation Review*, *203*, 104357. https://doi.org/10.1016/j.tre.2025.104357.
6. Chiodelli, F., Coppola, A., Belotti, E., Berruti, G., Clough Marinaro, I., Curci, F., & Zanfi, F. (2021). The production of informal space: A critical atlas of housing informalities in Italy between public institutions and political strategies. *Progress in Planning*, *149*, 100495. https://doi.org/ 10.1016/j.progress.2020.100495
7. Skare, E., & Haugdal Jore, S. (2024). Hybrid threats in the Norwegian petroleum sector. A new category of risk problems for safety science? *Safety Science*, *176*, 106521. https://doi.org/10.1016/j.ssci.2024.106521
8. Zhu, X., Zhang, A., Bi, W., & Huang, Z. (2025). Novel situation assessment method for amphibious aircraft maritime rescue using probabilistic linguistic hybrid cloud model and best-worst method. *Engineering Applications of Artificial Intelligence*, *156*, 111065. https://doi.org/ 10.1016/ j.engappai. 2025.111065
9. Zhu, X., Zhang, A., Bi, W., & Huang, Z. (2025). Novel situation assessment method for amphibious aircraft maritime rescue using probabilistic linguistic hybrid cloud model and best-worst method. *Engineering Applications of Artificial Intelligence*, *156*, 111065. https://doi.org/10.1016/j.engappai. 2025. 111065.

ISSN 2226-1893

10. Hoang, A.T., Chen, W., López-Escalante, M.C., Guerrero-Pérez, M.O., Rodríguez-Castellón, E., Kowalski, J., Le, T.T., Bui, V.G., & Nguyen, X.P. (2026). Methanol for decarbonization of the maritime sector: From ideological strategy to practical solutions. *Renewable and Sustainable Energy Reviews*, *229*, 116638. https://doi.org/10.1016/j.rser.2025.116638.
11. Ledesma, O., & Lamo, P. (2025). Hybrid IoT network for real-time monitoring of maritime containers. *Computer Networks*, *271*, 111627. https://doi.org/10.1016/j.comnet.2025.111627.
12. Zhaka, V., & Samuelsson, B. (2024). Hydrogen as fuel in the maritime sector: From production to propulsion. *Energy Reports*, *12*, 5249-5267. https://doi.org/10.1016/j.egyr.2024.11.005.
13. Uğurlu, Ö. (2025). Real-time intelligent maritime accident prediction and prevention system for narrow waterways. *Autonomous Transportation Research*. https://doi.org/10.1016/j.atres.2025.09.002.
14. Tonoğlu, F., Atalar, F., Başkan, İ. B., Yildiz, S., Uğurlu, Ö., & Wang, J. (2022). A new hybrid approach for determining sector-specific risk factors in Turkish Straits: Fuzzy AHP-PRAT technique. *Ocean Engineering*, *253*, 111280. https://doi.org/10.1016/j.oceaneng.2022.111280.
15. Melnyk, O., Onishchenko, O., Lohinov, O., Konoplov, A., & Lohinova, L. (2024). Contemporary strategies for advancing cybersecurity in maritime cargo transportation. In V. Babak & A. Zaporozhets (Eds.), *Systems, Decision and Control in Energy VI* (Vol. 561, P. 293-308). Springer, Cham. https://doi.org/10.1007/978-3-031-68372-5_21.
16. Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cyber- security in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. *Lex Portus, 11*(1), P. 7-19. https://doi.org/10.62821/lp11101.
17. Melnyk, O., Burmaka, I., Zaporozhets, A., Onishchenko, O., Burlachenko, D., & Nykytuik, P. (2025). In-depth analysis of strategies and techniques of navigational safety improvement and ship collision risk reduction. In *Studies in Systems, Decision and Control* (Vol. 580, P. 65-87). Springer. https://doi.org/ 10.1007/978-3-031-82027-4_5.
18. Onyshchenko, S., Bychkovsky, Y., Melnyk, O., Onishchenko, O., Zaporozhets, A., & Bedrii, D. (2025). Integrating human factors in project-oriented risk management for maritime safety. In *Studies in Systems, Decision and Control* (Vol. 580, P. 183-195). Springer. https://doi.org/ 10.1007/978-3-031-82027-4_12.
19. Melnyk, O., Onyshchenko, S., Voloshyn, A., Demiduik, O., Zaporozhets, A., & Cheredarchuk, N. (2025). Principles to ensure safe ship operation on the basis of a four-component model. In Studies in Systems, Decision and

ISSN 2226-1893

Control (Vol. 580, P. 17-29). Springer. https://doi.org/10.1007/978-3-031-82027-4_2.

20. Melnyk, O., Onyshchenko, S., Onishchenko, O., Fomin, O., Zaporozhets, A., & Moskaliuk, O. (2025). Single-system approach to integrated ship safety provision. In Studies in Systems, Decision and Control (Vol. 580, P. 1-15). Springer. https://doi.org/10.1007/978-3-031-82027-4_1.

REFERENCES

1. Islam, S., Roshid, M.M., Bhowmik, R.C., Dhar, B.K., Islam, M.S., Raihan, A., & Akter, F. (2025). Global governance and security challenges: Transnational pathways to reducing terrorism mortality in a globalized world. *Research in Globalization*, *11*, 100312. https://doi.org/10.1016/j.resglo.2025.100312.
2. Ghufran, B., & Breuer, W. (2024). Terrorism, national security, and takeover performance. *International Review of Financial Analysis*, *96*, 103634. https://doi.org/10.1016/j.irfa.2024.103634.
3. Khan, M.A., Rahman, A., Mahmud, F.U., Bishnu, K.K., Ahmed, M., Mridha, M., & Aung, Z. (2025). A systematic review of AI-driven business models for advancing Sustainable Development Goals. *Array*, *28*, 100539. https://doi.org/10.1016/j.array.2025.100539.
4. Adamu, H., Bello, U., Tafida, U.I., Zango, Z.U., Muhammad, K.Y., & Qamar, M. (2026). Review on the intersection of materials science and policy: A dual-track approach to realizing a green hydrogen economy for climate-neutral energy transition. *Sustainable Energy Technologies and Assessments*, *86*, 104831. https://doi.org/10.1016/ j.seta.2026. 104831.
5. Islam, S., Shi, Y., Nahar, R., Ahmed, J.U., & Wang, M. (2025). Identifying and analyzing barriers to ship-based evacuation planning using AIS data. *Transportation Research Part E: Logistics and Transportation Review*, *203*, 104357. https://doi.org/10.1016/j.tre.2025. 104357.
6. Chiodelli, F., Coppola, A., Belotti, E., Berruti, G., Clough Marinaro, I., Curci, F., & Zanfi, F. (2021). The production of informal space: A critical atlas of housing informalities in Italy between public institutions and political strategies. *Progress in Planning*, *149*, 100495. https://doi.org/10.1016/j.progress.2020.100495.
7. Skare, E., & Haugdal Jore, S. (2024). Hybrid threats in the Norwegian petroleum sector. A new category of risk problems for safety science? *Safety Science*, *176*, 106521. https://doi.org/10.1016/j.ssci.2024. 106521.

ISSN 2226-1893

8. Zhu, X., Zhang, A., Bi, W., & Huang, Z. (2025). Novel situation assessment method for amphibious aircraft maritime rescue using probabilistic linguistic hybrid cloud model and best-worst method. *Engineering Applications of Artificial Intelligence*, *156*, 111065. https://doi.org/10.1016/j.engappai.2025.111065.
9. Zhu, X., Zhang, A., Bi, W., & Huang, Z. (2025). Novel situation assessment method for amphibious aircraft maritime rescue using probabilistic linguistic hybrid cloud model and best-worst method. *Engineering Applications of Artificial Intelligence*, *156*, 111065. https://doi.org/10.1016/j.engappai.2025.111065.
10. Hoang, A.T., Chen, W., López-Escalante, M.C., Guerrero-Pérez, M.O., Rodríguez-Castellón, E., Kowalski, J., Le, T. T., Bui, V.G., & Nguyen, X.P. (2026). Methanol for decarbonization of the maritime sector: From ideological strategy to practical solutions. *Renewable and Sustainable Energy Reviews*, *229*, 116638. https://doi.org/ 10.1016/j.rser.2025.116638.
11. Ledesma, O., & Lamo, P. (2025). Hybrid IoT network for real-time monitoring of maritime containers. *Computer Networks*, *271*, 111627. https://doi.org/10.1016/j.comnet.2025.111627.
12. Zhaka, V., & Samuelsson, B. (2024). Hydrogen as fuel in the maritime sector: From production to propulsion. *Energy Reports*, *12*, 5249-5267. https://doi.org/10.1016/j.egyr.2024.11.005.
13. Uğurlu, Ö. (2025). Real-time intelligent maritime accident prediction and prevention system for narrow waterways. *Autonomous Transportation Research*. https://doi.org/10.1016/j.atres.2025.09.002.
14. Tonoğlu, F., Atalar, F., Başkan, İ. B., Yildiz, S., Uğurlu, Ö., & Wang, J. (2022). A new hybrid approach for determining sector-specific risk factors in Turkish Straits: Fuzzy AHP-PRAT technique. *Ocean Engineering*, *253*, 111280. https://doi.org/10.1016/j.oceaneng.2022. 111280.
15. Melnyk, O., Onishchenko, O., Lohinov, O., Konoplov, A., & Lohinova, L. (2024). Contemporary strategies for advancing cyber-security in maritime cargo transportation. In V. Babak & A. Zaporozhets (Eds.), *Systems, Decision and Control in Energy VI* (Vol. 561, P. 293-308). Springer, Cham. https://doi.org/10.1007/978-3-031-68372-5_21.

ISSN 2226-1893

16. Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cyber- security in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. *Lex Portus, 11*(1), P. 7-19. https://doi.org/10.62821/lp11101.
17. Melnyk, O., Burmaka, I., Zaporozhets, A., Onishchenko, O., Burlachenko, D., & Nykytuik, P. (2025). In-depth analysis of strategies and techniques of navigational safety improvement and ship collision risk reduction. In *Studies in Systems, Decision and Control* (Vol. 580, pp. 65–87). Springer. https://doi.org/10.1007/978-3-031-82027-4_5.
18. Onyshchenko, S., Bychkovsky, Y., Melnyk, O., Onishchenko, O., Zaporozhets, A., & Bedrii, D. (2025). Integrating human factors in project-oriented risk management for maritime safety. In *Studies in Systems, Decision and Control* (Vol. 580, P. 183195). Springer. https://doi.org/10.1007/978-3-031-82027-4_12.
19. Melnyk, O., Onyshchenko, S., Voloshyn, A., Demiduik, O., Zaporozhets, A., & Cheredarchuk, N. (2025). Principles to ensure safe ship operation on the basis of a four-component model. In Studies in Systems, Decision and Control (Vol. 580, P. 17-29). Springer. https://doi.org/10.1007/978-3-031-82027-4_2.
20. Melnyk, O., Onyshchenko, S., Onishchenko, O., Fomin, O., Zaporozhets, A., & Moskaliuk, O. (2025). Single-system approach to integrated ship safety provision. In Studies in Systems, Decision and Control (Vol. 580, P. 1-15). Springer. https://doi.org/10.1007/978-3-031-82027-4_1.

Дата надходження статті: 28.01.2026
Дата прийняття статті: 27.02.2026
Дата публікації статті: 02.04.2026