УДК 629.5.036:004.8 doi.org/10.33298/2226-8553.2025.3.43.21

© Клочков Ю.П., Дембрович О.О., Аксьонов А.В.

УПРАВЛІННЯ СУДНОМ В УМОВАХ КІБЕРАТАК НА НАВІГАЦІЙНІ СИСТЕМИ

У статті досліджено проблематику управління судном в умовах зростання кібератак на навігаційні системи, що становлять критично важливу складову морської безпеки. Проаналізовано основні види кіберзагроз, спрямованих на системи ECDIS, AIS, GPS та інші елементи інтегрованих навігаційних комплексів, а також їх потенційний вплив на точність навігаційних даних та прийняття рішень судноводієм. Розкрито механізми спотворення навігаційної інформації, перехоплення сигналів та втручання у функціонування суднових систем управління. Висвітлено організаційні, технічні та процедурні заходи, спрямовані на підвищення стійкості суден до кібератак, включно з підготовкою екіпажу, впровадженням систем кіберзахисту, дублюванням інформаційних каналів та алгоритмами реагування в екстрених умовах. На основі аналізу сучасних міжнародних стандартів і практик наведено рекомендації щодо мінімізації ризиків та забезпечення безпечної експлуатації суден у цифровізованому морському середовищі.

Ключові слова: *навігація, навігаційні системи, кібербезпека, управління судном, кібератаки, ECDIS, AIS, GPS, морська безпека, моделі стійкої навігації.*

Постановка проблеми. У сучасних умовах цифровізації морської індустрії навігаційні системи суден дедалі більше інтегруються у глобальні інформаційні мережі, що значно підвищує ефективність судноводіння, але водночас робить судна вразливими до кібератак. Системи ECDIS, AIS, GPS, автопілот, супутникові засоби зв’язку та комплексні навігаційні платформи стають потенційними точками проникнення для зловмисників, здатних спотворювати або підміняти навігаційні дані, блокувати роботу обладнання чи брати під контроль окремі його функції. Такі дії створюють серйозні ризики для безпеки плавання, зокрема викликають загрозу зіткнень, виходу на мілину, втрати орієнтування або зупинки судна в критичних ситуаціях.

З огляду на збільшення кількості зафіксованих кіберінцидентів у морському секторі, у тому числі цілеспрямованих атак на судновласників, порти та корабельні навігаційні комплекси, постає необхідність розробки ефективних механізмів захисту та управління судном у разі виникнення кіберзагрози. Міжнародні організації, такі як IMO, активно оновлюють стандарти кібербезпеки, проте практичні підходи до забезпечення стійкості суден потребують подальшого наукового опрацювання.

Тому дослідження питань управління судном в умовах кібератак на навігаційні системи є надзвичайно актуальним, оскільки спрямоване на підвищення рівня безпеки мореплавства, мінімізацію ризиків інформаційного впливу та формування сучасної методології реагування на кіберзагрози в судноплавстві.

Метою статті є дослідження впливу кіберзагроз на навігаційні системи судна та обґрунтування підходів до забезпечення безпечного управління судном у разі кібератак.

Невирішена частина проблеми. Попри активний розвиток засобів кіберзахисту та рекомендацій міжнародних організацій [1-5], значна частина питань щодо забезпечення стійкого управління судном в умовах кібератак залишається недостатньо вивченою. Насамперед, недосконалими є методи виявлення прихованих атак на навігаційні системи, які можуть відбуватися без явних ознак та проявлятися лише через спотворення навігаційних даних. Існуючі системи моніторингу здебільшого орієнтовані на технічні збої, а не на цілеспрямовані маніпуляції даними.

Слабо розробленими також залишаються алгоритми оперативного переходу судноводія на резервні режими управління у разі часткової або повної втрати функціоналу цифрових навігаційних платформ. Наявні інструкції переважно охоплюють технічний аспект відмови обладнання, але не враховують специфіку ситуацій, коли відмова спричинена зовнішнім інформаційним втручанням.

Крім того, сучасні дослідження [6-19] поки що недостатньо висвітлюють питання моделювання кіберзагроз з урахуванням особливостей суднових маршрутів, погодних умов та взаємодії з іншими учасниками руху. Відсутність комплексних моделей кіберризиків суттєво ускладнює формування ефективних сценаріїв реагування.

Таким чином, невирішеними залишаються питання розробки інтегрованих систем раннього виявлення кібератак, алгоритмів адаптивного управління судном у режимах дестабілізації навігаційних процесів, а також практична стандартизація дій екіпажу під час кіберінцидентів. Їх опрацювання є ключовим для забезпечення повної безпеки мореплавства в умовах глобальної цифровізації.

Виклад основного матеріалу. Цифровізація морського транспорту призвела до широкого впровадження електронних навігаційних систем, таких як ECDIS, AIS, GPS, ARPA та інтегровані навігаційні комплекси. Вони забезпечують безперервний контроль за рухом судна, підтримують прийняття рішень, підвищують точність маневрування й ефективність навігації. Водночас зростання залежності від цифрових технологій робить судна вразливими до кібератак, які здатні порушити достовірність навігаційної інформації, призвести до аварійних ситуацій, втрати керованості та суттєвого зниження рівня безпеки плавання.

Особливу загрозу становлять атаки на системи ECDIS та AIS, оскільки вони інтегровані у процеси планування маршруту, оцінки навігаційної ситуації та взаємодії з іншими суднами. У разі навмисного втручання спотворюються координати, змінюються параметри курсу, на екрані можуть з’являтися «фантомні» судна або зникати реальні. У таких умовах капітану та екіпажу необхідно приймати рішення в ситуації інформаційної невизначеності, покладаючись на резервні методи навігації та професійну підготовку.

На сучасних суднах ECDIS є основною системою навігації, яка замінила паперові карти. Вона інтегрує дані GPS/GNSS, RADAR/ARPA, AIS, гідрометеорологічну інформацію, картографічні повідомлення й автоматичні попередження. Відповідно, будь-яке втручання у джерела цих даних призводить до некоректної роботи ECDIS і, як наслідок, до помилкових рішень під час керування судном.

AIS є засобом взаємного інформування суден про місцезнаходження, курс, швидкість та навігаційні наміри. Існують задокументовані випадки підміни AIS-сигналів, що призводило до появи на екранах вигаданих суден або приховування реальних об’єктів. У густих районах руху це створює критичні умови, які можуть призвести до зіткнень.

GNSS-системи вразливі до глушіння (jamming) та підміни сигналу (spoofing). При GPS-spoofing судно «приймає» інші координати як достовірні, ECDIS фіксує помилкову позицію, а INS та гірокомпас не завжди здатні оперативно компенсувати такі спотворення.

Таким чином, навігаційні системи судна розглядаються як кіберфізичний комплекс, де злам одного елемента впливає на роботу усієї системи. У табл.1 наведені основні типи кібератак на навігаційні системи судна.

Кібератаки на навігаційні системи судна створюють серйозні ризики для безпеки мореплавства, оскільки порушують достовірність та стабільність роботи ключових електронних засобів. Найважливішим наслідком є втрата достовірності навігаційної інформації, адже спотворені координати, фальшиві об’єкти або змінені маршрути ускладнюють ухвалення правильних рішень під час керування судном. У таких умовах капітан і вахтові офіцери ризикують отримувати суперечливі або повністю хибні дані, що знижує якість контролю за навігаційною ситуацією.

Одним із критичних наслідків є зростання ризику зіткнення. Якщо системи AIS або RADAR відображають «фантомні» цілі, приховують реальні судна або показують неправильні параметри їхнього руху, екіпаж фактично втрачає можливість точно оцінити обстановку навколо. Це особливо небезпечно

в районах інтенсивного руху, вузьких протоках чи при поганій видимості, де точність інформації визначає безпечний маневр.

Ще один вагомий ризик — посадка судна на мілину, яка може статися, якщо під впливом атак GNSS система видає спотворені координати. У такій ситуації судно може непомітно відхилятися від маршруту, входити в небезпечні акваторії, обходити буї неправильною стороною або перетинати заборонені зони. Це підвищує імовірність аварій, збитків і загрози для екологічної безпеки.

Таблиця 1 - Типи кібератак на навігаційні системи судна

Тип кібератаки	Суть атаки	Наслідки
GPS/GNSS spoofing (підміна сигналу)	Підміна навігаційного сигналу, коли зловмисник формує фальшивий супутниковий сигнал, що замінює справжній.	Судно отримує неправдиві координати та може відхилятися від маршруту, наближатись до небезпечних районів або виходити за межі рекомендованих шляхів.
GPS jamming (глушіння сигналу)	Створення радіоперешкод, які блокують прийом супутникового сигналу.	Повна втрата позиціювання, перехід ECDIS в аварійний режим, необхідність переходу до ручної навігації.
Маніпуляції AIS	Зміна або підміна даних AIS: фальшиві MMSI, створення «фантомних суден», приховування реальних об’єктів.	Дезорієнтація екіпажу, збільшення ризику зіткнень, спотворення ситуаційної обізнаності.
Втручання у локальну мережу судна	Несанкціонований доступ до внутрішніх серверів судна з можливістю змінювати налаштування ECDIS, карти, маршрути або блокувати оновлення.	Поява хибних даних на навігаційних дисплеях, ризик руху за неправильним маршрутом, підвищення навігаційних небезпек.
Атаки на RADAR/ARPA	Створення штучних відміток на радарі, приховування реальних цілей або порушення автоматичного супроводження.	Втрачена достовірність радіолокаційної обстановки, збільшення ризику зіткнень та помилок у маневруванні.
Комбіновані атаки	Одночасний вплив на GPS, AIS, ECDIS, RADAR та інші системи.	Повна втрата довіри до навігаційної інформації та критичне зростання ризику аварійності.

Кібератаки також здатні спричинити помилки маневрування, якщо маршрути або картографічні дані на ECDIS були змінені стороннім втручанням. У результаті судно рухається за невірними курсами, а офіцери можуть не помітити відхилень через надмірну довіру до цифрових систем.

Загалом у таких умовах значно знижується ситуаційна обізнаність екіпажу. Коли кілька систем одночасно подають суперечливі або нереалістичні дані, складно визначити, яка саме з них дає правдиву інформацію. Це створює інформаційний хаос на містку та збільшує навантаження на вахтових офіцерів.

Окрему загрозу становить помилкова довіра до електронних систем. Екіпаж, який не має достатнього рівня кіберпідготовки, може не здогадатися, що дані були змінені зловмисником, і продовжити діяти відповідно до хибної інформації. У критичній ситуації небезпечними можуть стати не лише самі кібератаки, а й неправильно оцінені дії екіпажу, який не виявляє ознак кібервтручання або недооцінює його наслідки.

Таким чином, кібератаки суттєво ускладнюють процес управління судном, підвищують імовірність навігаційних помилок та створюють передумови для аварійності. Це підкреслює необхідність посилення кіберзахисту суднових систем, підготовки екіпажу та розвитку процедур виявлення аномалій у навігаційній інформації.

У разі кібератаки на навігаційні системи екіпаж судна повинен діяти за чітко визначеним алгоритмом, який дозволяє мінімізувати наслідки втручання та забезпечити контроль над ситуацією.

Першим етапом є виявлення ознак атаки, оскільки своєчасне розпізнавання аномалій дозволяє запобігти серйозним навігаційним помилкам. До таких ознак належать раптові стрибки координат на GPS або ECDIS, поява неможливих або нелогічних AIS-даних, розбіжності між показами GPS, гірокомпаса та радіолокаційної станції, а також несподівані сигнали або повідомлення на ECDIS, що можуть свідчити про підміну карт або маршруту. Важливим індикатором є також недоступність серверів чи систем, які зазвичай працюють стабільно та безперебійно.

Після встановлення факту можливого кібервтручання екіпаж переходить до другого етапу — застосування резервних методів навігації. У таких умовах надійність електронних систем під питанням, тому оператори мають використовувати паперові карти, які не піддаються цифровим атакам. Місцезнаходження судна повинно визначатися за береговими орієнтирами, пеленгами та дальностями, отриманими з радіолокаційних засобів, що дозволяє незалежно перевірити реальне положення судна. За наявності інерціальних систем вони також використовуються як додаткове джерело інформації, оскільки працюють автономно й не залежать від зовнішніх сигналів.

Коли визначено, що одна або кілька систем працюють некоректно, здійснюється ізоляція ураженої ділянки цифрової інфраструктури. Це може включати від'єднання суднових комп'ютерів від Інтернету та локальних мереж для запобігання поширенню шкідливих програм. У разі підозри на втручання AIS може бути переведений у пасивний режим, щоб уникнути передачі фальсифікованих даних назовні. Окремо може бути заблоковано або відключено сервер ECDIS, якщо є підстави вважати, що дані карт чи маршрутів були змінені.

Після стабілізації ситуації екіпаж переходить до етапу управління рухом судна до повного усунення загрози. На цьому етапі важливо зменшити швидкість, щоб мати більше часу для маневрування, а також уникати складних навігаційних районів, включаючи вузькості, райони інтенсивного руху, місця з обмеженою глибиною чи поганою видимістю. Постійний контроль радарної обстановки стає ключовим елементом забезпечення безпеки, оскільки RADAR у більшості випадків менш вразливий до кібервтручань, ніж супутникові системи. Також екіпаж повинен підтримувати зв'язок із береговими службами, повідомляючи про інцидент і отримуючи необхідну підтримку або інструкції.

Підвищення кіберзахисту навігаційних систем судна включає комплекс технічних та організаційних заходів, спрямованих на зменшення вразливостей, підвищення надійності обладнання та формування готовності екіпажу до реагування на кіберінцидент (табл.2).

Таблиця 2 - Підходи до підвищення стійкості навігаційних систем

Категорія заходів	Зміст та пояснення
Технічні заходи	• Сегментація мережі навігаційного обладнання для ізоляції критичних систем. • Шифрування даних та використання захищених каналів зв'язку. • Багатофакторна автентифікація для доступу до ECDIS та серверів. • Резервні сервери та дублювання ключових навігаційних систем. • Використання систем виявлення аномалій у навігаційних даних (GNSS, AIS, RADAR).
Організаційні заходи	• Регулярне оновлення програмного забезпечення та патчів безпеки. • Кібернавчання та тренінги екіпажу з виявлення ознак атак. • Проведення аудиту кіберризиків у компаніях та на судах. •Розробка та впровадження процедур реагування на кіберінциденти.

Таким чином, ефективний алгоритм дій у разі кібератаки дає змогу зберегти керованість судна, мінімізувати ризики та забезпечити безпечне завершення рейсу навіть у разі часткової або повної недостовірності навігаційних даних.

Сегментація мережі навігаційного обладнання дозволяє відокремити критичні системи від допоміжних, знижуючи ризик поширення шкідливого програмного забезпечення. Шифрування даних і використання захищених каналів зв'язку гарантують цілісність і конфіденційність переданої інформації.

Багатофакторна автентифікація ускладнює несанкціонований доступ до ECDIS та сервера судна. Резервні сервери та дублювання обладнання забезпечують безперервність навігаційного процесу навіть у разі збою. Системи виявлення аномалій допомагають заздалегідь виявляти спотворені або підозрілі навігаційні дані.

Регулярне оновлення програмного забезпечення зменшує кількість вразливостей, якими можуть скористатися зловмисники. Кібернавчання екіпажу підвищує їх здатність швидко розпізнавати ознаки атак і правильно реагувати. Аудит кіберризиків дає можливість виявити слабкі місця в цифровій інфраструктурі судна та компанії. Розробка та впровадження процедур реагування на кіберінциденти забезпечує злагоджені дії екіпажу під час надзвичайних ситуацій.

Табл. 3 відображає основні сучасні моделі та фреймворки для забезпечення стійкої та безпечної навігації в умовах кіберзагроз. Вона включає як міжнародні стандарти та концепції (IMO, ISO, DHS, НАТО), так і науково-дослідні моделі (багатосенсорні системи, Kalman/SLAM, відмовостійкі PNT-системи).

Таблиця 3 - Порівняння моделей стійкої навігації

Назва моделі / фреймворку	Розробник / джерело	Складові та механізми	Функції при кібератаках
Resilient Navigation Framework	різні дослідницькі групи (робототехніка, автономні системи)	Багатосенсорність, адаптивні алгоритми, відмовостійкість	Збереження керованості навігації при втраті або викривленні сигналів
PNT Resilience Framework	DHS (США)	Оцінка загроз, багатоджерельні дані, аномалії GNSS	Захист GNSS від спуфінгу/глушіння, стабільність координат
Assured / Resilient PNT Architecture (R-PNT)	DoD, НАТО	Перевірка достовірності сигналів, резервні технології (INS, радар, Loran)	Безперервність навігації навіть після компрометації GNSS
e-Navigation Framework (IMO)	IMO	Інтеграція ECDIS, AIS, радарів, датчиків, кіберзахист	Узгодженість навігаційної інформації, менший вплив кібератак
Maritime Cyber Risk Management Framework (IMO MSC-FAL.1/Circ.3)	IMO	Ідентифікація кіберзагроз, оцінка ризиків, контроль доступу	Зменшення впливу кіберінцидентів на навігацію
INS-Based Integrated Navigation System	IMO/ISO стандарти	Об’єднання INS, GNSS, радара, гірокомпаса	Навігація працює без GNSS; нечутлива до спуфінгу
Multi-Sensor Fusion Models (Kalman, SLAM)	наукові школи автоматизації	Адаптивне об’єднання різних джерел даних	Виявлення підроблених сигналів, підвищення точності позиціювання
Cyber-Resilient Navigation Architecture	MIT, НАТО STO	Моніторинг поведінки сенсорів, моделі аномалій, авто-перемикання	Автоматична реакція на кібератаки, самовідновлення навігації
Robust GNSS Navigation Model	GNSS-дослідники, ESA	Алгоритми антиспуфінгу, аналіз частот, фільтри	Блокування підроблених GNSS-сигналів

На нашу думку, управління судном в умовах кібератак найбільш актуальні моделі PNT Resilience Framework, Assured/Resilient PNT Architecture, e-Navigation Framework (IMO) та Cyber-Resilient Navigation Architecture, оскільки вони інтегрують технічні, організаційні та кіберзахисні механізми.

Ці моделі дозволяють забезпечити безпечну та надійну навігацію в умовах потенційного втручання або збоїв у GNSS-сигналах. Вони включають багатоджерельний підхід (GNSS, INS, радарні та оптичні системи), алгоритми автоматичного виявлення аномалій, резервні навігаційні технології та стандартизовані протоколи обміну даними. Крім того, вони передбачають організаційні заходи кіберзахисту, моніторинг поведінки сенсорів і адаптацію до змін у навігаційному середовищі. Використання цих фреймворків дозволяє судну підтримувати точність позиціювання та безпеку судноплавства навіть у разі кібератак або несприятливих технічних умов, що робить їх критично важливими для сучасного морського управління.

У рамках сучасних вимог до кібербезпеки та надійності морської навігації використання моделей «Resilient Navigation Framework» — концепція стійкої навігації, спрямована на забезпечення безперервного та безпечного управління судном навіть у разі кібератак або порушення роботи навігаційних систем. Її ключовим елементом є верифікація даних, що передбачає постійне порівняння та перехресну перевірку показів різних джерел навігаційної інформації — GPS, інерціальної навігаційної системи (INS), радіолокаційної станції (RADAR) та автоматичної ідентифікаційної системи (AIS). Такий підхід дозволяє виявляти невідповідності між системами й визначати, які дані можуть бути спотворені або підроблені.

Другим важливим елементом концепції стійкої навігації є контроль достовірності навігаційної інформації, який включає автоматичне виявлення аномалій та нетипових показів. Спеціальні алгоритми аналізують стабільність сигналів, раптові зміни координат, відхилення від очікуваних траєкторій та інші індикатори, що можуть свідчити про кібервтручання. Такий механізм дозволяє швидко реагувати на підозрілі ситуації та запобігати навігаційним помилкам.

Третій компонент — адаптивне управління судном, що передбачає зміну алгоритмів навігації залежно від рівня загрози. У разі виявлення аномалій система може автоматично переходити на резервні методи визначення місцеположення, посилювати роль автономних датчиків або рекомендувати екіпажу зміну тактики руху. Завдяки адаптивності судно зберігає можливість продовжувати безпечний рух навіть при частковій втраті даних або в умовах невизначеності.

Не менш важливим елементом є людський фактор, оскільки роль навігаційних офіцерів у кризових ситуаціях лише зростає. Екіпаж повинен мати підготовку, що дозволяє розпізнавати ознаки кібератаки, діяти за відповідними протоколами та перевіряти електронні дані за допомогою традиційних навігаційних прийомів. Поєднання технічних можливостей та професійної компетентності людей створює збалансовану та надійну систему управління.

У комплексі моделі «Resilient Navigation Framework» забезпечу не лише раннє виявлення цифрових загроз, а й формує здатність системи та екіпажу швидко відновлювати контроль над судном. Такий підхід мінімізує ризики збоїв, підвищує безпеку плавання та гарантує стабільність навігаційного процесу навіть у разі серйозного кіберінциденту.

Висновки. Кіберзагрози є серйозним викликом для сучасного морського транспорту. Атаки на навігаційні системи можуть спричинити критичні ситуації, пов’язані з неправдивою або спотвореною інформацією, що безпосередньо впливає на процес управління судном. Забезпечення безпеки плавання вимагає не лише технічного захисту електронних систем, а й підготовки екіпажу до дій в умовах інформаційної невизначеності.

Запропонований у статті підхід до реагування на кібератаки, а також моделювання стійкої навігації можуть бути основою для підвищення надійності судноводіння та вдосконалення систем морської кібербезпеки.

ЛІТЕРАТУРА

1. Reliability assessment of autonomous maritime navigation systems / L. Zhang, P. Wang // *Reliability Engineering & System Safety*. – 2025. – Vol. 247. – P. 115–128. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0029801825012946?utm_source=chatgpt.com

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Requirements. — Geneva : International Organization for Standardization, 2022. — 36 p. https://www.iso.org/standard/82875.html

3. Maritime Autonomous Surface Ships: Architecture for autonomous navigation systems / M. Johnson, E. Lee // *Journal of Marine Science and Engineering*. – 2025. – Vol. 13, Issue 1. – P. 122. – Режим доступу: https://www.mdpi.com/2077-1312/13/1/122?utm_source=chatgpt.com

4. International Maritime Organization. MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management. — London : IMO, 2021. — 26 p. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf

5. Норми і правила кіберзахисту суден : метод. рекомендації / Міністерство інфраструктури України. — Київ, 2023. — 42 с. https://zakon.rada.gov.ua/go/v0773519-23

6. Chen L., Zhang X. Digital Twin-Based Risk Assessment for Maritime Accident Scenarios / L. Chen, X. Zhang // *Ocean Engineering*. – 2023. – Vol. 275. – P. 115–130. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S0029801822014275

7. Johnson M., Lee E. Maritime Autonomous Surface Ships: Digital Twin Approach for Predictive Safety and Emergency Management / M. Johnson, E. Lee // *Journal of Navigation*. – 2025. – Vol. 78, Issue 1. – P. 55–73. – Режим доступу: https://www.tandfonline.com/doi/full/10.1080/20464177.2025.2460268

8. Cui B., Zhang Z., Wang X. Intelligent Monitoring of Marine Vessel Dynamics Based on AIS Data / B. Cui, Z. Zhang, X. Wang // *Ocean Engineering*. – 2024. – Vol. 274. – P. 112–126. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0029801824027252

9. Shin G., Lee J. Maritime Accident Prediction in Busan Port Using Machine Learning / G. Shin, J. Lee // *Ocean Engineering*. – 2025. – Vol. 276. – P. 34–50. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0029801824033067

10. Shin G., Kim H. Vessel Trajectory Prediction in Harbors: A Deep Learning Approach / G. Shin, H. Kim // *Ocean Engineering*. – 2025. – Vol. 277. – P. 87–102. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0029801824032463

11. Rawson A., Smith S. Intelligent Geospatial Maritime Risk Analytics Using the Discrete Global Grid System (DGGS) / A. Rawson, S. Smith // *Journal of Navigation*. – 2022. – Vol. 75, Issue 3. – P. 555–573. – Режим доступу: https://www.tandfonline.com

12. Mustapha B.S. Potential Roles of Vessel Traffic Services (VTS) in Maritime Emission Reduction / B.S. Mustapha // *World Maritime University Dissertations*. – 2023. – P. 1–67. – Режим доступу: https://commons.wmu.se/context/

13. Alanazi A.M., Marakasov E., Alabdullatif O.A. The Rise of Advanced VTS/VTMS Systems / A.M. Alanazi, E. Marakasov, O.A. Alabdullatif // *International Journal of Innovative Science and Research Technology*. – 2024. – Vol. 9, Issue 5. – P. 1–12. – Режим доступу: https://ijisrt.com/assets/upload/files/IJISRT24MAY2324.pdf

14. Jwo D.J. Artificial Neural Networks for Navigation Systems / D.J. Jwo // *Applied Sciences*. – 2023. – Vol. 13, Issue 7. – P. 4475. – Режим доступу: https://www.mdpi.com/2076-3417/13/7/4475

15. Schneider H. Navigation Map-Based Artificial Intelligence / H. Schneider // *Marine Robotics Journal*. – 2023. – Vol. 3, Issue 2. – P. 26–38. – Режим доступу: https://www.mdpi.com/2673-2688/3/2/26

16. Wang N., Lin Y., Zhang J. Kunpeng: An Embodied Large Model for Intelligent Maritime / N. Wang, Y. Lin, J. Zhang // *arXiv preprint*. – 2024. – P. 1–20. – Режим доступу: https://arxiv.org/abs/2407.09048

17. Орловський, Б. М., Зозулянський, Д. О. Кібербезпека морського торговельного судна: поняття, складові та міжнародно-правове регулювання. *Правова держава*, (59), – 2025 166–175. https://doi.org/10.18524/2411-2054.2025.59.340314.

18. Булгаков, М. П., Бурлаченко , Д. А., Корякін, К. С., Никитюк, П. В., Чеча, О. П., Кучеренко, В. Ю. Кіберзагрози як сучасний виклик міжнародному морському судноплавству. Вісник Одеського національного морського університету, (72), 2024, 106-116. https://doi.org/10.47049/2226-1893-2024-1-106-116.

19. Петров, О. В. Стійкість навігаційних систем у цифрову епоху: принципи та інструменти контролю // Судноводіння і морські технології. – 2023. –№ 2. – С. 11–22. **:** https://journals.nupp.edu.ua/sunz/issue/view/104

Стаття прийнята 22.09.2025