УДК 004.056:656.61
Зайцева Т. В.
Херсонська державна морська академія, Херсон, Україна
ORCID ID: 0000-0001-6780-719X

ІНТЕГРОВАНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ТА ЗАСТОСУВАННЯ МІЖНАРОДНИХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ У СУДНОПЛАВСТВІ

DOI 10.14308/ite000821

Анотація. *Морський сектор стикається зі зростаючими кіберзагрозами, які ставлять під сумнів експлуатаційну безпеку суден, портів. Дане дослідження аналізує операції та стандарти виявлення кіберінцидентів, розглядає сучасні виклики для морського кіберзахисту, на основі цього впроваджує новий підхід для створення плану реагування на кіберінциденти.*

Запровадження в практику кіберзахисту міжнародних стандартів ISO/IEC 27001, NIST CSF, IEC 62443 та рекомендацій міжнародної морської організації (IMO) [12, 13, 14, 22] на сьогодні є обов'язковим. Після ретельного аналізу документів, публікацій та проведеного попереднього дослідження, було зроблено висновок, що ефективність запровадження даних стандартів обмежується через неповне охоплення життєвого циклу систем, через деякі складнощі технічної інтеграції інформаційних та операційних технологій, через неповне врахування особливостей взаємодії бортових систем суден різного виду чи типу, через недостатнє врахування впливу людського фактора на забезпечення сталої безпекової роботи морського сектору. Отже, на сьогодні залишається актуальною задача розробки методологічного підходу до створення адаптивного плану реагування на кіберінциденти для суден різних типів з урахуванням міжнародних стандартів і специфіки суднових операційних технологій.

Метою даного дослідження є обґрунтування та розробка інтегрованого підходу до оцінювання та рекомендацій щодо застосування міжнародних стандартів кібербезпеки в умовах експлуатації суден, що поєднує методики багатокритеріального аналізу стандартів, технологічні, організаційні та людські фактори, а також враховує сучасні кіберзагрози морської галузі.

Для зменшення впливу людського фактора та апробації запропонованої моделі наступним кроком є впровадження проєкту у систему освіти відповідного напрямку та його практичне використання під час проходження курсантами плавальних практик; подальше його застосування для оперативного навчання членів екіпажів на суднах. Практичне значення дослідження полягає у можливості використання отриманих результатів судноплавними компаніями, портовими адміністраціями та для навчання персоналу відповідно до вимог міжнародних стандартів.

За даними звіту Thetius, CyberOwl і HFW, тільки у 2024 році кожна п'ята судноплавна компанія зазнала тих чи інших прояви кібератак [35]. За результатами опитувань, 93% членів екіпажів зізналися, що не відчувають здатності до розв'язування задач в області кібербезпеки, 70% впевнені, що навчання та своєчасне тренування допомогло б покращити їх підготовку. Це пояснює результати нещодавніх досліджень CyberOwl, які свідчать про те що з більш ніж 12 тисяч випадків кібератак на судна, які зафіксовані у 2024 році, 60% - це зараження суднових систем шкідливим програмним забезпеченням, прикро те, що 77% з них здійснено через USB – накопичувачі та інші носії, такі як ноутбуки персоналу. Своєчасне інформування персоналу, проходження ними відповідних тренінгів, отримання сертифікатів, підписання актів відповідальності - ось шлях суттєвого зниження кіберризиків у цій сфері. Створення стандартів кібербезпеки та неухильне дотримання вимог є одним з головних шляхів підвищення кібербезпеки.

Ключові слова: *кіберінцидент, кібербезпека суднових систем, стандарти безпеки, інформаційні технології, операційні технології, людський фактор, TRL-аналіз.*

Постановка проблеми та її актуальність

Морський сектор являє собою цифрову систему взаємопов'язаної інфраструктури. На сьогодні майже 90% світової торгівлі перевозиться морем, тому цей сектор завжди був мішенню для зловмисників, але в сьогоднішніх реаліях напрямок атак змінився, вони перейшли в цифрове поле. Принципи кібербезпечної роботи інформаційних (IT) та операційних технологій (OT) стають стратегічно необхідною основою для підтримки безперервної діяльності всієї транспортної системи та економічної стабільності. Відбуваються постійні тактичні та технологічні зміни в векторах кібератак, а шахрайські методи поєднують фізичний, логістичний та людський впливи, використовуючи дослідження в цифровій сфері та методи соціальної інженерії.

Сьогодні кіберзахист у морській галузі вже не може обмежуватися виключно технічними засобами контролю. Міжнародні стандарти та нормативні документи формують загальні рамки управління кіберризиками, проте їх практична реалізація на борту судна стикається з низкою обмежень, серед яких:

- несумісність між інформаційними та операційними технологіями;
- технологічне різноманіття на борту;
- використання технологій різних поколінь;
- несвоєчасне оновлення програмного забезпечення;
- велика кількість учасників процесу (судно, порт, судновласник…);
- необхідність співпраці на відстані, поява третьої сторони;
- непідготовленість екіпажу та проблеми міжособистісного спілкування.

Результати опитування курсантів і чинних фахівців морської галузі підтверджують наявність розриву між задекларованими вимогами стандартів і реальними операційними сценаріями, у межах яких екіпаж змушений діяти в умовах дефіциту часу, інформації, ресурсів та часто і виконавців. Це зумовлює необхідність пошуку нових підходів до розробки планів реагування на кіберінциденти, орієнтованих на практичне застосування.

У відповідь на ці виклики, ми вирішили застосувати структурний підхід, який охоплює стратегічне планування системи кіберзахисту, включає кіберпсихологію, операційну стійкість, аналіз всього життєвого циклу судна.

Метою дослідження є формування обґрунтованого методологічного підходу до створення адаптивних рекомендацій із застосування міжнародних стандартів кібербезпеки для суден різних типів з урахуванням їх експлуатаційних особливостей, кіберризиків, а також технологічної та організаційної зрілості.

Для досягнення поставленої мети у роботі вирішуються такі завдання: аналіз сучасних кіберзагроз у морській галузі; оцінка обмежень застосування міжнародних стандартів у судновому середовищі; застосування TRL-аналізу для оцінки готовності кібербезпекових рішень; формування основ інтегрованої аналітичної моделі плану реагування.

Аналіз останніх досліджень і публікацій, в яких започатковано розв’язання даної проблеми

Аналіз наукових публікацій і звітів міжнародних організацій свідчить про зростання кількості кібератак на об’єкти морської інфраструктури. Інциденти, пов’язані з атаками NotPetya та WannaCry, продемонстрували вразливість як судноплавних компаній, так і портових систем [18]. Особливо небезпечними є атаки на навігаційні системи GPS та ECDIS, наслідками яких можуть стати аварії та екологічні катастрофи.

Автори даної статті попередньо наголошують на потребі адаптації універсальних стандартів кібербезпеки саме для морських систем, тому що брак адаптованих стандартів ускладнює захист.

Моніторинг останніх досліджень і публікацій, які стосуються зазначеної тематики, вказує на те, що безпека судноплавства значною мірою залежить, по-перше, від оснащеності судна, та, по-друге, від кваліфікації його офіцерського складу. Такі автори, Складальний П., Костюк Ю. [28] та др. пропонують застосування інтелектуальних технологій та штучного

інтелекту для моделювання персоналізованих траєкторій навчання в підготовці фахівців з кібербезпеки та інформаційної безпеки.

Питанням підвищення кіберстійкості морської екосистеми на національному рівні приділяли увагу Айбарс Орук та Цзяньїн Чжоу [24]. У роботах ми знаходимо опис модульного підходу, який охоплює стратегічне планування системи кіберзахисту на основі двох факторів: соціальної інженерії та операційної стійкості.

Питання, пов’язані з безпекою судноплавства часто стають головною тематикою інтернаціональних досліджень та міжнародних конференцій. Ці виклики привертають увагу іноземних дослідників, наприклад, таких як Ф. Акпан, Г. Бендіаб [1], Дж. Алкаід, Р. Лаве [2, 3], Г. Кесслер, С. Шепард [18], Г. Каваліраторс, А. Карас [16, 17], Й. Челіч, М. Вукшич [8, 9] і др. [5], так і вітчизняних науковців: В. Горбов, І. Ратушняк [30], О. Корнієнко [32], А. Вавіленкова [29]. Так, у своїй роботі «Система дипломування судноводіїв» Кочерєв О. [33] відзначив необхідність вдосконалення системи підготовки моряків, звернувши увагу саме на їх комплексній підготовці.

Автори даної статті вже кілька років приділяють увагу питанням комплексного підходу до підготовки фахівців морського профілю, акцентуючи на питаннях забезпечення та підтримання безпечного робочого середовища, а саме на розв’язуванні питань управління кібербезпекою в судноплавстві [15, 34].

Виклад основного матеріалу

Аналіз законодавчих баз європейських країн або нормативних актів, що стосуються безпекових питань морської галузі, надають загальну інформацію по видах кіберзагроз, плану реагування на кіберінциденти. Але тільки група спеціалістів, в яку входять представники судноплавної галузі та компетентні особи з комп’ютерних технологій і питань кібербезпеки, можуть надати адаптований план реагування на кіберінциденти, який враховує наявне обладнання та специфіку роботи саме операційних технологій, наприклад, морського судна. А це під силу крупним судновласникам чи великим портам. В малих портах та невеликих суднах замість дієвого плану реагування на кіберінциденти, ми спостерігаємо документи, в яких зазначені загальні положення, які не завжди стають в пригоді під час кіберінциденту. Отже, актуальним є формування методологічного підходу до створення адаптивних рекомендацій та алгоритму розробки плану реагування на кіберінциденти для суден різних типів, який базується на міжнародних стандартах кібербезпеки та враховує експлуатаційні особливості, рівень кіберризиків і технологічну та організаційну зрілість суднових систем.

Методологія дослідження. Методологічну основу дослідження сформовано з урахуванням міждисциплінарного характеру проблеми кібербезпеки у морській галузі, яка поєднує технічні, організаційні та людські фактори. У процесі роботи застосовано системний підхід, що дозволяє розглядати судно як складну кіберфізичну систему, у межах якої інформаційні та операційні технології функціонують у тісній взаємодії, а безпека залежить не лише від технічних рішень, але й від рівня підготовки персоналу та організації процесів управління.

На першому етапі дослідження проведено аналіз нормативно-правових документів і міжнародних стандартів у сфері кібербезпеки та безпеки судноплавства, зокрема рекомендацій Міжнародної морської організації, стандартів ISO/IEC 27001, NIST Cybersecurity Framework та IEC 62443 [11, 14, 19]. Аналіз дозволив виявити структурні обмеження їх практичного застосування у морському середовищі, пов’язані з фрагментарністю вимог, неповним охопленням життєвого циклу цифрових активів та складністю інтеграції IT та OT систем.

Другий етап включав аналіз результатів анкетування та опитування курсантів старших курсів і студентів заочної форми навчання, які мають практичний досвід роботи на суднах. Отримані дані дозволили оцінити реальний рівень обізнаності членів екіпажів у питаннях кібербезпеки, а також виявити розрив між формально задекларованими вимогами стандартів і фактичними діями персоналу під час кризових ситуацій. Особливу увагу приділено впливу

людського фактора, зокрема когнітивним помилкам, стресу, обмеженню знань та ресурсів, що безпосередньо впливають на ефективність реагування на кіберінциденти.

На завершальному етапі дослідження застосовано елементи TRL-аналізу для оцінки рівня готовності кібербезпекових рішень до впровадження в реальних суднових умовах. Використання TRL-підходу дало змогу сформувати основу для розробки інтегрованої моделі плану реагування на кіберінциденти, орієнтованої не лише на відповідність стандартам, але й на практичну експлуатацію у морському середовищі [13].

Досягнення зазначеної вище мети потребувало попереднього аналізу нормативних та методологічних підходів, які наразі застосовуються для забезпечення кібербезпеки у морській галузі. Саме міжнародні стандарти та рекомендації формують основу більшості корпоративних і суднових політик безпеки, однак їх практична ефективність у реальних умовах експлуатації суден залишається дискусійною.

Аналіз вимог міжнародних стандартів кібербезпеки свідчить, що кожен із них орієнтований на окремий рівень управління ризиками. Так, рекомендації IMO формують загальну регуляторну рамку, стандарт ISO/IEC 27001 зосереджується на побудові системи управління інформаційною безпекою, тоді як стандарт IEC 62443 розглядає технічні аспекти захисту промислових та операційних систем.

На наш погляд, розмежування створює низку практичних проблем. Судно функціонує як єдина кіберфізична система, у межах якої навігаційні, енергетичні та інформаційні підсистеми перебувають у постійній взаємодії, а реагування на інцидент відбувається в умовах обмеженого часу та людських ресурсів. За таких обставин роздільне застосування стандартів не забезпечує цілісного бачення процесу реагування.

Це зумовлює необхідність інтегрованої моделі, у межах якої план реагування розглядається як проєкт із чітко визначеними фазами, ролями та механізмами контролю.

Далі для знайомства з висновками порівняльного аналізу стандартів, ми наводимо частину таблиці, яка стосується двох головних міжнародних стандартів кібербезпеки (табл. 1).

Таблиця № 1.

Порівняльний аналіз міжнародних стандартів кібербезпеки у морській галузі

Критерій	**Міжнародний морський кібербезпековий кодекс (IMO)**	**ISO/IEC 27001**
Основна мета та сфера застосування	Інтеграція кібербезпеки в систему управління безпекою судна та компанії як невід’ємної частини плану охорони судна. Застосовується до суден, портів та компаній, що займаються морськими перевезеннями.	Забезпечення комплексного управління інформаційною безпекою в організації. Застосовується до будь-якої компанії чи організації, включаючи морську галузь (судна, порти).
Зазначені в стандарті вимоги	Вимагає від компаній обов’язково включити кібербезпеку до своєї системи управління безпекою.	Вимагає впровадження системи управління інформаційною безпекою на основі стандартів Міжнародної організації зі стандартизації (ISO).
Основні компоненти	Політика кібербезпеки, оцінка ризиків, реагування на інциденти,	Політика безпеки, оцінка ризиків, контроль безпеки, управління інцидентами,

	навчання персоналу.	безперервність процесів.
Адаптивність	Стандарт є менш гнучким, оскільки базується на загальних вимогах до судна та компанії.	Більш гнучкий, оскільки може бути адаптований до потреб будь-якої організації.
Висновки	Забезпечує відповідність вимогам міжнародних стандартів.	Забезпечує комплексний підхід до управління інформаційною безпекою, підвищує довіру до компанії.

Порівняльний аналіз міжнародних стандартів кібербезпеки свідчить, що, попри їх широке впровадження у морській галузі, жоден із них не забезпечує комплексного покриття специфічних потреб судноплавства на всіх етапах життєвого циклу цифрових систем. Наприклад, рекомендації IMO орієнтовані передусім на інтеграцію кібербезпеки в систему управління безпекою судна відповідно до вимог Міжнародного кодексу з управління безпекою суден та запобігання забрудненню (ISM Code). Такий підхід створює нормативну основу для управління кіберризиками, однак не пропонує детальних технічних процедур, інструментів аудиту чи методів перевірки ефективності реалізованих заходів. В цьому і є прояв низької адаптивності цього стандарту.

Міжнародний стандарт для системи управління інформаційною безпекою (ISO/IEC 27001) своєю чергою забезпечує системний підхід до управління інформаційною безпекою на рівні організації, дозволяючи вибудувати чітку структуру політик, процедур та відповідальності. Попри універсальність, стандарт має обмеження, він не враховує особливості експлуатації операційних технологій, характерні для суднових систем, а також специфіку обмеженого доступу до мережевих ресурсів у морі.

З огляду на ці висновки ми зупинилися на аналізі стандарті IEC 62443, який фокусується на безпеці промислових автоматизованих систем управління, і саме він є більш адаптованим до операційних технологій, наприклад, на судні. Положення цього стандарту частково відповідають архітектурі суднових ОТ систем, зокрема електронній системі відображення навігаційних карт та інформації (ECDIS), систем управління енергетичними установками та автоматизованих систем контролю. Водночас практичне застосування цього стандарту у морській галузі залежить від налаштувань ОТ, від виробників обладнання, обмеженим доступом до електронних схем, неможливістю повної реалізації вимог безпеки без втручання сертифікованих сервісних інженерів, що може створювати суттєві затримки [16, 17].

Порівняльна оцінка показує, що ключовими слабкими місцями усіх розглянутих стандартів залишаються інтеграція інформаційних і операційних технологій, недостатнє врахування людського фактора та відсутність формалізованих процедур управління цифровими активами на різних етапах: від модернізації до виведення з експлуатації. Крім того, рівень практичного впровадження стандартів значною мірою залежить від політики судновласника, фінансових можливостей компанії та державного регулювання, що призводить до нерівномірного рівня кіберзахищеності в різних сегментах морської галузі [7].

Таким чином, проведений порівняльний аналіз підтверджує, що чинні міжнародні стандарти кібербезпеки формують необхідну, але недостатню основу для ефективного реагування на кіберінциденти у реальних умовах судноплавства. Їх фрагментарність, обмежена адаптація до гібридної IT/OT-архітектури бортових систем суден та формальний підхід до людського фактора зумовлюють розрив між нормативними вимогами та практикою експлуатації.

Особливістю запропонованої моделі є врахування повного життєвого циклу цифрових активів судна, зокрема етапів оновлення, модернізації та виведення з експлуатації систем. Це дає змогу мінімізувати так звані «мертві зони» безпеки, що виникають під час докових

ремонтів, заміни обладнання на судні, або часткового оновлення програмного забезпечення без належного усвідомлення комплексної взаємодії цифрових технологій та програмних інтерфейсів. Додатковим чинником, який ускладнює експлуатацію ОТ є одночасне використання на судні систем різних технологічних поколінь, що істотно обмежує можливість застосування уніфікованого підходу до забезпечення кібербезпеки.

Важливим компонентом моделі є включення людського фактора як окремого елементу управління ризиками. Запропонований підхід передбачає використання навчальних сценаріїв і симуляцій кіберінцидентів, які можуть застосовуватися як у процесі підготовки курсантів, так і під час підвищення кваліфікації чинних членів екіпажу. Це дозволяє не лише перевірити ефективність плану реагування, але й підвищити психологічну стійкість персоналу до кризових ситуацій, що є критично важливим для безпеки судноплавства.

Таким чином, інтегрована модель плану реагування на кіберінциденти створює підґрунтя для переходу від формального виконання вимог стандартів до практично орієнтованої системи управління кіберризиками, здатної функціонувати в реальних умовах морської експлуатації та бути масштабованою для різних типів суден.

Сучасним підходом для оцінки готовності кібербезпекових рішень у морській галузі є застосування TRL-аналізу. Для оцінки практичної придатності підходів до кіберзахисту у морському середовищі доцільно застосовувати методологію TRL (Technology Readiness Level), яка дозволяє визначити рівень технологічної зрілості рішень у контексті їх готовності до реального впровадження. Метод TRL був розроблений Національним управлінням з аеронавтики і дослідження космічного простору (NASA) та згодом стандартизований у міжнародному стандарті ISO 16290:2013, що розширило можливості його застосування у різних галузях, зокрема у сфері критичної інфраструктури та безпеки складних технічних систем [12].

На відміну від класичних підходів до оцінки відповідності стандартам, TRL-аналіз дозволяє перейти від формальної перевірки наявності політик і процедур до оцінки реальної здатності системи функціонувати в умовах операційного середовища. Це є особливо важливим для морської галузі, де кібербезпекові рішення повинні працювати в умовах обмеженого зв’язку, різнотипового обладнання та високої залежності від людського фактора.

TRL-аналіз базується на дев’ятирівневій шкалі, яка охоплює весь життєвий цикл технології — від формування базових принципів до її стабільної експлуатації в реальному середовищі. У контексті морської кібербезпеки більшість заходів, формально впроваджених відповідно до міжнародних стандартів, зазвичай знаходяться на рівнях TRL 3–5, тобто на стадії концептуальної або частково валідаційної готовності. Це означає, що навіть за наявності документально оформлених процедур реагування, вони не завжди проходять перевірку в умовах реального рейсу або кризової ситуації, що суттєво знижує їх практичну цінність [25].

Таким чином, TRL-аналіз дозволяє не лише ідентифікувати рівень готовності окремих технічних рішень, але й виявити системні прогалини у взаємодії між інформаційними та операційними технологіями, а також у підготовці екіпажів до реагування на кіберінциденти.

Для формалізації процесу оцінки ефективності покриття вимог стандартів у межах плану реагування доцільно використати узагальнену математичну модель.

Нехай S_i позначає конкретний стандарт кібербезпеки (наприклад, ISO/IEC 27001, NIST CSF або IEC 62443), а C_j — набір критеріїв оцінювання (1…10), що охоплюють ключові аспекти морської кібербезпеки, включаючи життєвий цикл цифрових активів, інтеграцію IT/OT, людський фактор та операційну стійкість (табл. 2). Вага кожного критерію (w_j) визначається з урахуванням його критичності для безпечної експлуатації судна (формула 1).

$$\sum_{j=1}^{n} w_j = 1 \qquad (1)$$

Вагові коефіцієнти визначено експертним методом з урахуванням критичності критеріїв для безпечної експлуатації судна. Параметр p_{ij} відображає рівень покриття

відповідного критерію конкретним стандартом у діапазоні від 0 до 1. Зазвичай цей розподіл виглядає наступним чином:

- 0 – не покривається;
- 0,25 – трохи згадується;
- 0.5 – частково покривається;
- 0,75 – добре покривається;
- 1 – повністю покривається та враховується специфіка.

Інтегральний індекс морської придатності стандарту може бути визначений наступним чином:

$$MSI\left(S_i\right)=\sum_{j=1}^{n} w_j \cdot p_{ij} \qquad (2)$$

де $MSI\left(S_i\right)$ — зведений показник ефективності стандарту в морських умовах.

Таблиця № 2.

Показники ефективності стандарту

Критерій	**C_j**	**w_j**	**p_{ij}**	**$w_j \cdot p_{ij}$**
Управління кіберризиками протягом життєвого циклу судна	C_1	0.15	0.8	0.12
Інтеграція IT/OT систем	C_2	0.15	0.9	0.135
Управління доступом і автентифікація	C_3	0.10	0.9	0.09
Моніторинг та виявлення інцидентів	C_4	0.10	0.8	0.08
Реагування на інциденти	C_5	0.10	0.7	0.07
Відновлення та забезпечення безперервності	C_6	0.10	0.7	0.07
Людський фактор і навчання екіпажу	C_7	0.10	0.5	0.05
Взаємодія з підрядниками та береговими системами	C_8	0.08	0.6	0.048
Відповідність морським регуляторним вимогам	C_9	0.07	0.5	0.035
Операційна стійкість судна	C_{10}	0.05	0.6	0.03
MSI				**0.678**

Для обґрунтування значень параметрів p_{ij} у дослідженні застосовано метод аналітичної ієрархії (Analytic Hierarchy Process, AHP), запропонований Томасом Л. Сааті [26, 27]. Даний

метод є структурованою процедурою прийняття рішень і широко використовується для багатокритеріального аналізу складних систем.

Процес оцінювання було подано у вигляді трирівневої ієрархічної структури:

- *Мета*: визначення інтегрального показника морської придатності стандартів кібербезпеки.
- *Критерії*: набір критеріїв C_j, що охоплюють ключові аспекти морської кібербезпеки.
- *Альтернативи*: стандарти кібербезпеки S_i, зокрема ISO/IEC 27001, NIST Cybersecurity Framework та IEC 62443.

Для кожного критерію C_j здійснювалося попарне порівняння стандартів S_i з використанням фундаментальної шкали відносної важливості Сааті. Порівняння базувалися на аналізі змісту стандартів, їх вимог, рекомендацій та рівня адаптації до умов експлуатації суден. На основі отриманих матриць визначалася нормалізована векторна оцінка, що відповідає максимальному власному значенню матриці. Отримані нормалізовані значення інтерпретувалися як параметри p_{ij}, які набувають значень у діапазоні [0;1] та відображають відносний рівень покриття критерію C_j конкретним стандартом S_i.

Для перевірки надійності експертних оцінок обчислювався коефіцієнт узгодженості *CR* (Consistency Ratio). Значення оцінок вважалися прийнятними за умови CR < 0.1, відповідно до рекомендацій Сааті [26].

Таким чином, параметри p_{ij} визначалися на основі формалізованої та відтворюваної аналітичної процедури, що знижує суб'єктивність оцінювання та підвищує обґрунтованість результатів дослідження. Значення, близькі до 1, свідчать про повне та специфічне врахування морських умов, але значення, близькі до 0, означають відсутність або декларативний характер відповідних положень.

Більш детально розглянемо процес розрахунку для одного конкретного критерію, який викликає багато питань, наприклад: *Інтеграція IT/OT систем у морському середовищі*. Для прикладу візьмемо 3 стандарти:

- S_1 — IMO Guidelines;
- S_2 — NIST CSF;
- S_3 — IEC 62443.

На основі шкали Сааті отримуємо матрицю попарних порівнянь (табл. 3).

Таблиця № 3.

Матриця попарних порівнянь стандартів

	IMO	**NIST CSF**	**IEC 62443**
IMO	1	1/3	1/5
NIST	3	1	1/3
IEC 62443	5	3	1
p_{ij}	**9**	**4.33**	**1.53**

Якщо зробити висновок, то IEC 62443 має помірну перевагу над NIST і значну перевагу над стандартом IMO. Але нагадаємо, це стосується тільки критерію «Інтеграція IT/OT технологій».

Наступний крок – це нормалізація матриці та обчислення середнього значення p_{ij} (табл. 4).

Таблиця № 4.

Нормалізована матриця попарних порівнянь стандартів

	IMO	**NIST CSF**	**IEC 62443**	**Середнє p_{ij}**
IMO	0.11	0.08	0.13	**0.11**
NIST	0.33	0.23	0.22	**0.26**

IEC 62443	0.56	0.69	0.65	**0.63**

Значення параметрів p_{ij} отримано на основі методу AHP шляхом попарного порівняння стандартів кібербезпеки за заданим критерієм з подальшою нормалізацією власного вектора. За таким же алгоритмом можна знайти значення *MSI* для кожного критерію C_j.

Дослідження інших науковців [20] демонструють схожу тенденцію. Їх результати оцінювання показали, що значення індексу для рекомендацій IMO становить близько 0.41, для NIST CSF — приблизно 0.63, тоді як для IEC 62443 — близько 0.71.

На основі чого ми робимо висновок, що жоден із проаналізованих стандартів не перевищує порогове значення 0.75, що свідчить про їх обмежену ефективність у реальних умовах експлуатації суден [12].

Результати дослідження

Міжнародні стандарти кібербезпеки демонструють високий рівень теоретичного покриття, але їх практичне застосування у морському середовищі стикається з рядом обмежень. Як було сказано вище, однією з ключових проблем є принципова відмінність між інформаційними та операційними технологіями. Якщо IT-системи орієнтовані на захист даних і допускають регулярні оновлення, то OT-системи зосереджені на фізичній безпеці та стабільності процесів і часто працюють на застарілому, але сертифікованому обладнанні, втручання в яке обмежене вимогами виробників.

Додатковим ускладненням є одночасна експлуатація на судні систем різних поколінь, обмежена пропускна здатність супутникового зв’язку – все це говорить, що на практиці повноцінне застосування рішень, які, наприклад, передбачені рамками одного з найпоширеніших стандартів NIST CSF не працює [23].

Як показало наше дослідження, що попри наявність таких нормативних стандартів, як ISO/IEC 27001, NIST Cybersecurity Framework, IEC 62443 та рекомендацій IMO, їхнє застосування у морському середовищі зіштовхується зі структурними обмеженнями. Зупинимось на трьох найважливіших чинників: обмежена сумісність між IT- та OT-систем, технологічне різноманіття на борту та прогалини у підготовці екіпажу.

Інтеграція IT/OT залишається основною слабкою ланкою більшості рамок. У морському секторі відбувається конвергенція IT (інформаційні системи: Windows/Linux, часті оновлення, несвоєчасні оновлення, несумісність програмних систем або додатків, антивіруси/EDR) та OT (операційні технології: PLC, SCADA, ECDIS, оновлення раз на 1–5 років, несумісність з антивірусами, а іноді й з оновленими операційними системами).

Ця несумісність призводить до того, що:

- Стандарти ISO/IEC 27001 та NIST CSF добре працюють для IT, але лише помірно або частково охоплюють OT.

- Стандарти IEC 62443 не повністю адаптовані до морського контексту та не можуть бути повністю реалізовані через закриті прошивки обладнання.

- Обмеженість підключення до супутникового трафіку унеможливлює виконання вимог щодо постійного моніторингу та логування, передбачених NIST.

Неповне охоплення життєвого циклу. Жоден із традиційних стандартів (ISO, NIST, IMO) не охоплює повний життєвий цикл цифрових систем. Зокрема, немає охоплення фази безпечного виведення з експлуатації / деактивації. Це створює так звані "мертві зони", коли носії або нерозсекречене обладнання, виведене з експлуатації, можуть стати вектором атаки або витоку конфіденційних даних.

Слабке врахування людського фактору. Людський фактор представлений недостатньо у більшості стандартів. Це критична прогалина, оскільки значна кількість опитаних членів екіпажів зізналися, що не відчувають здатності вирішувати завдання в області кібербезпеки. Проблематика людського фактора у морському секторі посилюється через:

- Когнітивні чинники: екіпаж схильний до недооцінки кіберризиків.

- Постійні зміни екіпажів: команди змінюються кожні 4–6 місяців, що руйнує сталі практики безпеки.

- Психоемоційний стан (стрес і втома): у критичних ситуаціях (GPS-spoofing, збій ECDIS) зростає рівень розгубленості, неспроможності чітко аналізувати ситуацію, зменшується час на аналіз, що погіршує дотримання процедур з кібербезпеки.

- В умовах підвищеного навантаження, стресу та дефіциту персоналу екіпажі змушені поєднувати кілька ролей, що суттєво підвищує ризик помилок і знижує ефективність формальних протоколів реагування [25].

Особливим напрямком розв'язування питання кібербезпеки морської галузі – є зменшення ролі особистості в забезпеченні безпеки системи в цілому. Недоліком сучасних систем управління морськими транспортними суднами є висока частка участі людини у процедурі прийняття рішень. Тому важливо використовувати системний підхід до розв'язування цієї проблеми.

Організації повинні розробляти не лише політики безпеки, а й плани реагування на кіберінциденти (Cyber Incident Response Plan – CISP), як інструменти підтримки функціонування морських підприємств та запобігання катастрофічним наслідкам. План реагування на кіберінциденти — це документ, що визначає політику, ролі, процеси, відповідальність та ресурси, необхідні для своєчасного виявлення, реагування, локалізації та відновлення після кіберінцидентів.

Замість заздалегідь розробленого або описаного детального плану реагування у даній статті пропонується інший підхід - концептуальна модель реагування на кіберінциденти в судноплавстві, побудована на гібридному застосуванні рекомендацій IMO, вимог найвідомішого міжнародного стандарту для системи управління інформаційною безпекою ISO/IEC 27001, функціональної структури NIST Cybersecurity Framework та технічних вимог стандарту IEC 62443. В попередніх дослідженнях ми показали, що собою може уявляти план реагування на кіберінциденти розроблений на принципах класичного проєктного менеджменту (PMBOK) або гнучких методологіях (Agile/Scrum) [31].

Але в даній статті ми подивились на цей процес під іншим кутом зору. Запропонована модель розглядає реагування на кіберінциденти як багаторівневий процес, що включає стратегічний, тактичний та технічний рівні управління, без прив'язки до конкретних операційних процедур. На стратегічному рівні модель спирається на вимоги IMO щодо управління ризиками та інтеграції кібербезпеки в систему управління безпекою судна. Тактичний рівень формалізується через функції *Визначити–Захистити–Виявити–Відреагувати–Відновити*, визначені в NIST CSF. Технічний рівень реалізується шляхом використання принципів сегментації зон і каналів, рівнів безпеки, визначених у стандарті IEC 62443.

Таким чином, концептуальна модель дозволяє узгодити регуляторні, організаційні та технічні аспекти кіберреагування, не перевантажуючи систему деталізованими операційними сценаріями та дає чітке уявлення якими стандартами краще користуватися для забезпечення комплексної кібербезпечної політики на судні.

Для ілюстрації практичного застосування запропонованої аналітичної моделі розглянемо умовний приклад використання стандарту ISO/IEC 27001 на торгівельному судні з частково інтегрованими IT/OT-системами.

Теоретичне покриття стандарту ISO/IEC 27001 (T) оцінюється як високе (приблизно 0.8–0.9), оскільки стандарт охоплює управління ризиками, політики безпеки, контроль доступу, реагування на інциденти та безперервність діяльності. Проте під час перенесення цих вимог у морське середовище виникає низка обмежувальних факторів [13, 14].

Фактор I (інтеграція IT/OT) проявляється через фрагментованість суднових систем управління, використання застарілих протоколів зв'язку та обмежену сумісність між навігаційними, машинними та інформаційними системами. Для більшості суден цей фактор може становити 0.15–0.2.

Фактор O (обмеження обладнання) пов’язаний із тривалими життєвими циклами суднового обладнання, обмеженими обчислювальними ресурсами та складністю оновлення програмного забезпечення під час рейсу. Його вплив оцінюється на рівні 0.1–0.15.

Фактор H (людський фактор) зумовлений багатонаціональним складом екіпажу, обмеженим рівнем кіберпідготовки та високим когнітивним навантаженням персоналу в аварійних ситуаціях. Типове значення цього фактору становить 0.1–0.15.

Фактор G (повний життєвий цикл) відображає відсутність системного підходу до кібербезпеки на етапах проєктування, модернізації та списання суднових цифрових систем і може додатково знижувати ефективність на 0.05–0.1.

Таким чином, навіть за оптимістичної оцінки сумарний вплив факторів становить:

$$I + O + H + G \approx 0.4–0.6 \quad (3)$$

що призводить до зниження фактичної ефективності стандарту до рівня 0.3–0.5. Це пояснює розрив між формальним впровадженням стандартів кібербезпеки та їх реальною ефективністю в умовах експлуатації суден.

Оскільки універсальний план реагування не може врахувати специфіку різних типів суден, у дослідженні запропоновано підхід до формування рекомендацій для екіпажу на основі відповідності окремих критеріїв кібербезпеки конкретним стандартам. Такий підхід дозволяє поєднати результати аналізу стандартів із практичними потребами суднової експлуатації без деталізації операційних процедур. Ми пропонуємо простий методологічний процес (рис. 1):

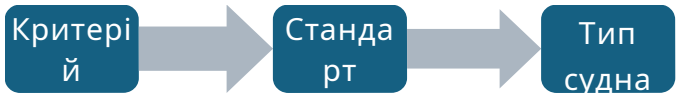

Рис. 1. Процес узгодження критеріїв кібербезпеки зі стандартами та типами суден.

Як було сказано вище, зупинимося на трьох важливих критеріях:

- *Критерій C1 — Управління кіберризиками протягом життєвого циклу судна.*

Для забезпечення безпечної експлуатації судна за даним критерієм доцільно використовувати базовий стандарт ISO/IEC 27001, який забезпечує формалізований підхід до ідентифікації, оцінювання та обробки кіберризиків, інтеграцію процесів управління ризиками в систему управління безпекою судна.

Для торгівельних (транспортних) суден, особливо для суден із тривалими рейсами, ISO/IEC 27001 є особливо релевантним на етапах експлуатації та модернізації, де ризики можуть бути пов’язані з оновленням програмного забезпечення, взаємодією з береговими системами та залученням зовнішніх підрядників.

Для пасажирських суден управління ризиками відповідно до ISO/IEC 27001 повинно доповнюватися вимогами NIST CSF щодо безперервного моніторингу та реагування, з огляду на підвищені вимоги до доступності сервісів і безпеки персональних даних.

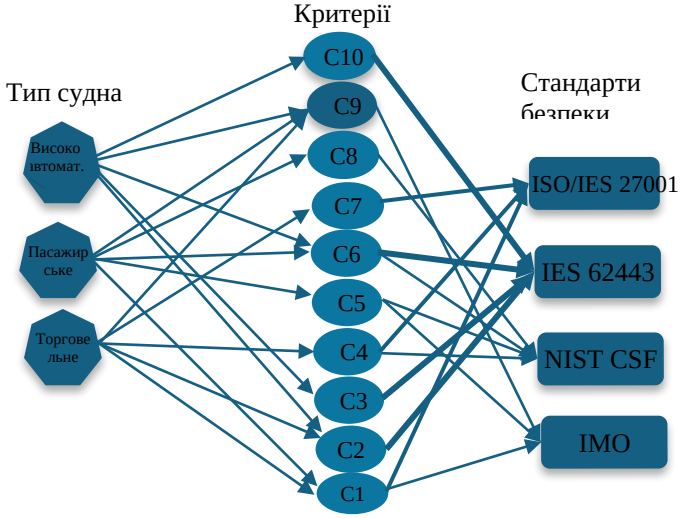

Рис. 2. Тришаровий граф з урахуванням індексу MSI стандартів

- Критерій С2 — Інтеграція IT- / OT-систем.

Для забезпечення критерію С2 ключову роль відіграє стандарт IEC 62443, який надає технічні принципи сегментації, зон і каналів, а також визначає рівні безпеки для операційних систем.

На суднах із високим рівнем автоматизації (танкери, контейнеровози) IEC 62443 може застосовуватися як основний стандарт для технічної реалізації заходів безпеки, тоді як ISO/IEC 27001 навпаки - використовується як організаційна надбудова.

Для суден із застарілими системами стандарт IEC 62443 доцільно застосовувати вибірково, зосереджуючись на критичних сегментах OT, щоб уникнути негативного впливу на стабільність обладнання.

- Критерій С7 — Людський фактор.

Даний критерій найкраще підтримується вимогами ISO/IEC 27001 та NIST CSF, які приділяють увагу питанням навчання персоналу, розподілу ролей і відповідальності.

Для суден із багатонаціональним екіпажем доцільно зосередитися на простих, уніфікованих процедурах і мінімізації когнітивного навантаження, що відповідає підходам NIST CSF у частині функцій «Ідентифікація загроз» та «Захист».

Для урахування специфіки різних типів суден запропоновано трирівневий граф відповідності критеріїв кібербезпеки стандартам безпеки (рис. 2). Лівий рівень відображає типи суден, центральний — конкретні критерії, а правий — відповідні стандарти. Такий підхід дозволяє систематизувати аналіз стандартів та формувати практичні рекомендації для екіпажу.

Висновки

У результаті проведеного дослідження встановлено, що міжнародні стандарти кібербезпеки (IMO Guidelines, ISO/IEC 27001, NIST CSF, IEC 62443) є необхідною, проте недостатньою умовою забезпечення кіберстійкості суден у реальних умовах експлуатації. Основними чинниками, що знижують ефективність формального впровадження стандартів, на наш погляд, є фрагментарність вимог, складність інтеграції IT- та OT-систем, обмеження суднового обладнання, а також суттєвий вплив людського фактора.

Інтеграція вимог Міжнародного морського кібербезпекового кодексу IMO з процесним підходом ISO/IEC 27001, технічними механізмами IEC 62443 та методологією реагування на кіберінциденти NIST забезпечує комплексну, багаторівневу модель кіберзахисту судноплавних компаній та суден.

Проведений багатокритеріальний аналіз дозволив кількісно оцінити придатність міжнародних стандартів до морського середовища за допомогою інтегрального індексу морської придатності (MSI). Отримані значення MSI підтверджують, що жоден зі стандартів не забезпечує повного покриття всіх критичних аспектів морської кібербезпеки, що обґрунтовує доцільність їх комбінованого використання залежно від типу судна, рівня автоматизації та експлуатаційних ризиків.

Запропонований у статті інтегрований підхід ґрунтується на поєднанні критеріїв морської кібербезпеки (С1–С10) з відповідними міжнародними стандартами та дозволяє перейти від універсальних декларативних вимог до адаптивних рекомендацій, орієнтованих на конкретні умови експлуатації суден. Такий підхід забезпечує методичну цілісність оцінювання та дозволяє врахувати технологічні, організаційні та людські фактори без деталізації операційних процедур.

Практична значущість дослідження полягає у можливості використання запропонованої методології та аналітичних моделей у навчальному процесі, зокрема під час викладання дисциплін, пов’язаних із кібербезпекою суднових систем, а також при розробці внутрішніх рекомендацій судноплавних компаній. Подальші дослідження доцільно спрямувати на емпіричну апробацію моделі шляхом сценарного моделювання кіберінцидентів, уточнення вагових коефіцієнтів критеріїв та адаптацію підходу до різних класів суден і рівнів автоматизації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, 2(1), 123-138. https://doi.org/10.3390/network2010009
2. Alcaide, J., & Llave, R. (2020). Maritime cyber risk: A review of incidents and mitigation strategies. *Safety Science*, 130, 104821. https://doi.org/10.1016/j.ssci.2020.104821
3. Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, 45, 547-554. https://doi.org/10.1016/j.trpro.2020.03.058
4. American Club. (n.d.). *A primer on IMO cyber risk management guidelines*. https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf
5. Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10), 776. https://doi.org/10.3390/jmse8100776
6. BIMCO. (2024). *The guidelines on cyber security onboard ships* (Version 5). https://www.bimco.org/media/s4ddrsfe/2024-11-14-guidelines_on_cyber_security-v5-final.pdf
7. Bolbot, V., Kulkarni, K., Brunou, P., Banda, O., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International Journal of Critical Infrastructure Protection, 39, 100571. https://doi.org/10.1016/j.ijcip.2022.100571
8. Čelić, J., Vukšić, M., Baždarić, R., & Cuculić, A. (2025). The challenges of cyber resilience in the maritime sector: Addressing weak awareness of cyber threats. Journal of Marine Science and Engineering, 13(4), 762. https://doi.org/10.3390/jmse13040762
9. Čelić, J., & Vukšić, M. (2018). Cyber security in maritime systems: Risks and challenges. Pomorstvo, 32(1), 17-25.
10. International Electrotechnical Commission. (2021). IEC 62443-1-1:2021 Security for industrial automation and control systems. https://www.iec.ch
11. International Maritime Organization. (2017). Resolution MSC.428(98): Maritime cyber risk management in safety management systems. https://www.imo.org
12. International Organization for Standardization. (2013). ISO 16290:2013 Space systems: Definition of the technology readiness levels (TRLs) and their criteria of assessment. https://www.iso.org
13. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. https://www.iso.org/standard/27001
14. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023 Information security incident management. https://www.iso.org/standard/78973.html
15. Kaminska, N., Kravtsova, L., Kravtsov, H., & Zaytseva, T. (2023). Modeling ship cybersecurity using Markov chains: An educational approach. In Proceedings of the 11th Workshop on Cloud Technologies in Education. CEUR Workshop Proceedings. 22-35. http://ceur-ws.org/
16. Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2023). Cyberattacks against the autonomous ship. Computer Security. Springer. 20-36.
17. Karas, A. (2023). Maritime industry cybersecurity: A review of contemporary threats. European Research Studies Journal, 26, 921-935. https://doi.org/10.35808/ERSJ/3336
18. Kessler, G., & Shepard, S. (2020). Maritime cybersecurity: A guide for leaders and managers. Independently published.
19. Macdonald, F. (2025). The lifecycle dilemma: Navigating cybersecurity risks across designing, constructing and operating a vessel. Thetius, CyberOwl, & HFW. https://thetius.com/wp-content/uploads/2025/03/Thetius-CyberOwl-HFW-The-Lifecycle-Dilemma.pdf

20. Martínez, F., Sánchez, L., Santos-Olmo, A., Rosado, D., & Fernández-Medina, E. (2025). Poseidon: An integrated cybersecurity framework for maritime systems with empirical validation. Research Square. https://doi.org/10.21203/rs.3.rs-7490210/v1
21. Mission Secure. (n.d.). Complying with the IMO 2021 cyber risk management regulations. https://www.missionsecure.com/regulation-overview-imo-2021-cyber-risk-management-compliance
22. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. https://www.nist.gov
23. National Institute of Standards and Technology. (2024). Cybersecurity framework profile guidance (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
24. Oruc, A., Bauk, S., & Zhou, J. (2025). A National Maritime Cyber Security Operations Centre (M-SOC) Concept. Marine Science and Engineering, 14(1), 17-29. https://doi.org/10.3390/jmse14010017
25. Reason, J. (2020). Human error. Cambridge University Press.
26. Saaty, T. (1990). How to make a decision: The analytic hierarchy process. European Journal of Operational Research, 48(1), 9-26. https://doi.org/10.1016/0377-2217(90)90057-I)
27. Saaty, T. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1), 83-98.
28. Skladannyi, P., Kostiuk, Y., Zhyltsov, O., Savchenko, Y., & Antypin, Y. (2025). Intelligent modeling of personalized learning in cybersecurity training. In Proceedings of CPITS-II 2025. CEUR Workshop Proceedings. 95-119.
29. Вавіленкова, А. (2025). Процес управління кіберінцидентами як необхідний етап в організації кібербезпеки підприємства. Інформаційна безпека людини, суспільства, держави, 1(38), 64-71. https://journals.uran.ua/ispss/article/view/340022
30. Горбов, В., Ратушняк, І., & Горбова, Г. (2023). Стандарти компетентності персоналу морських суден та захисту його прав. Миколаїв: НУК.
31. Зайцева, Т., Безбах, О., & Камінська, Н. (2025). Кібербезпека в морській галузі: загрози, реагування та управління інцидентами. Прикладні питання математичного моделювання, 8(1), 65-78. https://doi.org/10.32782/mathematical-modelling/2025-8-1-6
32. Корнієнко, О. (2023). Тенденції цифрових технологій у морському менеджменті. Економіка та управління національним господарством, 81, 51-56. https://doi.org/10.32782/2521-666X/2023-81-6
33. Кочерєв, О. (2021). Система сертифікації судноводіїв у сфері морського, зокрема річкового, судноплавства в Україні. Південноукраїнський правничий журнал, 3(1), 77-81.
34. Кравцова, Л., Зайцева, Т., & Камінська, Н. (2023). Марковські процеси в дослідженні ймовірності кібератак на морському судні. Information Technologies in Education (ITE), 3(52), 20–32. https://doi.org/10.14308/ite000763
35. Новини про дослідження Thetius/CyberOwl/HFW. (2025). Центр транспортних стратегій. https://cfts.org.ua/news/2025/03/13/u_2024_rotsi_kozhna_pyata_sudnoplavna_kompaniya_zaznala_kiberataki_doslidzhennya_82248

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, 2(1), 123-138. https://doi.org/10.3390/network2010009
2. Alcaide, J., & Llave, R. (2020). Maritime cyber risk: A review of incidents and mitigation strategies. *Safety Science*, 130, 104821. https://doi.org/10.1016/j.ssci.2020.104821
3. Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, 45, 547-554. https://doi.org/10.1016/j.trpro.2020.03.058

4. American Club. (n.d.). *A primer on IMO cyber risk management guidelines*. https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf
5. Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10), 776. https://doi.org/10.3390/jmse8100776
6. BIMCO. (2024). *The guidelines on cyber security onboard ships* (Version 5). https://www.bimco.org/media/s4ddrsfe/2024-11-14-guidelines_on_cyber_security-v5-final.pdf
7. Bolbot, V., Kulkarni, K., Brunou, P., Banda, O., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 39, 100571. https://doi.org/10.1016/j.ijcip.2022.100571
8. Čelić, J., Vukšić, M., Baždarić, R., & Cuculić, A. (2025). The challenges of cyber resilience in the maritime sector: Addressing weak awareness of cyber threats. *Journal of Marine Science and Engineering*, 13(4), 762. https://doi.org/10.3390/jmse13040762
9. Čelić, J., & Vukšić, M. (2018). Cyber security in maritime systems: Risks and challenges. *Pomorstvo*, 32(1), 17-25.
10. International Electrotechnical Commission. (2021). IEC 62443-1-1:2021—Security for industrial automation and control systems. https://www.iec.ch
11. International Maritime Organization. (2017). Resolution MSC.428(98): Maritime cyber risk management in safety management systems. https://www.imo.org
12. International Organization for Standardization. (2013). ISO 16290:2013 Space systems: Definition of the technology readiness levels (TRLs) and their criteria of assessment. https://www.iso.org
13. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. https://www.iso.org/standard/27001
14. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023 Information security incident management. https://www.iso.org/standard/78973.html
15. Kaminska, N., Kravtsova, L., Kravtsov, H., & Zaytseva, T. (2023). Modeling ship cybersecurity using Markov chains: An educational approach. *In Proceedings of the 11th Workshop on Cloud Technologies in Education*. *CEUR Workshop Proceedings*. 22-35. http://ceur-ws.org/
16. Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2023). Cyberattacks against the autonomous ship. *Computer Security*. *Springer*. 20-36.
17. Karas, A. (2023). Maritime industry cybersecurity: A review of contemporary threats. *European Research Studies Journal*, 26, 921-935. https://doi.org/10.35808/ERSJ/3336
18. Kessler, G., & Shepard, S. (2020). *Maritime cybersecurity: A guide for leaders and managers.* Independently published.
19. Macdonald, F. (2025). The lifecycle dilemma: Navigating cybersecurity risks across designing, constructing and operating a vessel. *Thetius, CyberOwl, & HFW*. https://thetius.com/wp-content/uploads/2025/03/Thetius-CyberOwl-HFW-The-Lifecycle-Dilemma.pdf
20. Martínez, F., Sánchez, L., Santos-Olmo, A., Rosado, D., & Fernández-Medina, E. (2025). Poseidon: An integrated cybersecurity framework for maritime systems with empirical validation. *Research Square.* https://doi.org/10.21203/rs.3.rs-7490210/v1
21. Mission Secure. (n.d.). *Complying with the IMO 2021 cyber risk management regulations.* https://www.missionsecure.com/regulation-overview-imo-2021-cyber-risk-management-compliance
22. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. https://www.nist.gov

23. National Institute of Standards and Technology. (2024). Cybersecurity framework profile guidance (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
24. Oruc, A., Bauk, S., & Zhou, J. (2025). A National Maritime Cyber Security Operations Centre (M-SOC) Concept. *Marine Science and Engineering*, 14(1), 17-29. https://doi.org/10.3390/jmse14010017
25. Reason, J. (2020). *Human error*. Cambridge University Press.
26. Saaty, T. (1990). How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48(1), 9-26. https://doi.org/10.1016/0377-2217(90)90057-I)
27. Saaty, T. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, 1(1), 83-98.
28. Skladannyi, P., Kostiuk, Y., Zhyltsov, O., Savchenko, Y., & Antypin, Y. (2025). Intelligent modeling of personalized learning in cybersecurity training. *In Proceedings of CPITS-II 2025. CEUR Workshop Proceedings.* 95-119.
29. Vavilenkova, A. (2025). Protses upravlinnia kiberintsydentamy yak neobkhidnyi etap v orhanizatsii kiberbezpeky pidpryiemstva [The cyberincident management process as a necessary stage in the organisation of enterprise cybersecurity]. Information security of individuals, society, and the state, 1(38), 64-71. https://journals.uran.ua/ispss/article/view/340022 [in Ukrainian]
30. Horbov, V., Ratushniak, I., & Horbova, H. (2023). Standarty kompetentnosti personalu morskykh suden ta zakhystu yoho prav [Standards of competence of seafarers and protection of their rights]. Mykolaiv: NUK. [in Ukrainian]
31. Zaitseva, T., Bezbakh, O., & Kaminska, N. (2025). Kiberbezpeka v morskii haluzi: zahrozy, reahuvannia ta upravlinnia intsydentamy [Cybersecurity in the maritime industry: threats, responses, and incident management]. Applied questions of mathematical modeling, 8(1), 65-78. https://doi.org/10.32782/mathematical-modelling/2025-8-1-6 [in Ukrainian]
32. Korniienko, O. (2023). Tendentsii tsyfrovykh tekhnolohii u morskomu menedzhmenti [Trends of digital technologies in maritime management]. Economics and management of the national economy, 81, 51-56. https://doi.org/10.32782/2521-666X/2023-81-6 [in Ukrainian]
33. Kocheriev, O. (2021). Systema sertyfikatsii sudnovodiiv u sferi morskoho, zokrema richkovoho, sudnoplavstva v Ukraini [Certification system of navigators in the field of maritime, including river, navigation in Ukraine]. South Ukrainian Law Journal, 3(1), 77-81. [in Ukrainian]
34. Kravtsova, L., Zaitseva, T., & Kaminska, N. (2023). Markovski protsesy v doslidzhenni ymovirnosti kiberatak na morskomу sudni [Markov processes in researching the probability of cyberattacks on marine vessels]. Information Technologies in Education (ITE), 3(52), 20-32. https://doi.org/10.14308/ite000763 [in Ukrainian]
35. Research news of Thetius/CyberOwl/HFW. (2025). *Centre for Transport Strategies*. https://cfts.org.ua/news/2025/03/13/u_2024_rotsi_kozhna_pyata_sudnoplavna_kompaniya_za znala_kiberataki_doslidzhennya_82248

UDC 004.056:656.61
Tetiana Zaitseva
Kherson State Maritime Academy, Kherson, Ukraine
ORCID ID: 0000-0001-6780-719X

AN INTEGRATED APPROACH TO ASSESSING AND APPLYING INTERNATIONAL CYBERSECURITY STANDARDS IN THE MARITIME SECTOR

Abstract. *The maritime sector is facing a growing number of cyber threats that challenge the operational safety of vessels and ports. This study analyses cyber incident detection operations and standards, examines current challenges in maritime cybersecurity, and based on this analysis, proposes a new approach to the development of a cyber incident response plan.*

The implementation of international cybersecurity standards ISO/IEC 27001, NIST CSF, IEC 62443, as well as the guidelines of the International Maritime Organization (IMO) [12, 13, 14, 22],

has become mandatory in modern maritime cybersecurity practice. However, a detailed analysis of regulatory documents, scientific publications, and the conducted preliminary study indicates that the effectiveness of these standards is limited due to incomplete coverage of the system life cycle, technical challenges related to the integration of information and operational technologies, insufficient consideration of the interaction between onboard systems of different vessel types, and inadequate attention to the impact of the human factor on ensuring sustainable and secure maritime operations. Therefore, the development of a methodological approach to creating an adaptive cyber incident response plan for different vessel types, considering international standards and the specifics of shipboard operational technologies, remains a relevant and urgent task.

The aim of this study is to substantiate and develop an integrated approach to assessment and recommendations for the application of international cybersecurity standards under real vessel operating conditions. The proposed approach combines multicriteria analysis of standards, technological, organizational, and human factors, and considers modern cyber threats specific to the maritime industry.

To reduce the impact of the human factor and to validate the proposed model, the next step involves implementing the project within the educational system of the relevant specialization and its practical application during cadets' sea training. Further application is envisaged for operational training of ship crew members onboard vessels. The practical significance of the study lies in the possibility of using the obtained results by shipping companies, port authorities, and for personnel training in accordance with international standard requirements.

According to a report by Thetius, CyberOwl, and HFW, in 2024 alone, one in five shipping companies experienced some form of cyberattack [35]. Survey results indicate that 93% of crew members admitted they do not feel capable of solving cybersecurity-related tasks, while 70% believe that proper training and timely exercises would significantly improve their preparedness. These findings are supported by recent CyberOwl studies, which show that out of more than 12,000 cyber incidents recorded on vessels in 2024, 60% involved malware infections. Alarmingly, 77% of these incidents were caused through USB storage devices and other removable media, such as personnel laptops. Timely awareness, specialized training, certification, and the signing of responsibility agreements by personnel represent an effective path toward significantly reducing cyber risks in the maritime sector. The development of cybersecurity standards and strict compliance with their requirements remains one of the key measures for enhancing maritime cybersecurity.

Keywords*: cyber incident, cybersecurity of ship systems, security standards, information technology, operational technology, human factor, TRL analysis.*

Стаття надійшла до редакції 26.12.2025
The article was received 26 December 2025