УДК 004.056:656.61

Т. В. ЗАЙЦЕВА
Херсонська державна морська академія

ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ У СУДНОПЛАВСТВІ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ

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) 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 недостатнє врахування впливу людського фактора на забезпечення сталої безпекової роботи морського сектору.

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 інші прояви кібератак [1]. *За результатами опитувань, 93 % членів екіпажів зізналися, що не відчувають здатність до розв'язування задач в області кібербезпеки, 70 % впевнені, що навчання та своєчасне тренування допомогло б покращити їх підготовку.*

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

T. V. ZAITSEVA
Kherson State Maritime Academy

CYBERSECURITY ASSESSMENT IN MARITIME SHIPPING BASED ON INTERNATIONAL STANDARDS

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), 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, 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

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

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 [1]*. 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.*

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

Постановка проблеми

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 оновленого 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.

Аналіз останніх досліджень і публікацій

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. [2] та інш. 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 [3]. У роботах ми знаходимо опис модульного підходу, який охоплює стратегічне планування системи кіберзахисту на основі двох факторів: соціальної інженерії та операційної стійкості.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

Питання, пов'язані з безпекою судноплавства часто стають головною тематикою міжнародних конференцій. Ці виклики привертають увагу іноземних дослідників, наприклад, таких як Ф. Акпан, Г. Бендіаб [4], Дж. Алкаід, Р. Лаве [5], Г. Кесслер, С. Шепард [6], А. Карас [7], Й. Челіч, М. Вукшич [8] і др. [9; 10], так і вітчизняних науковців: О. Кочерєв [11], О. Корнієнко [12], А. Вавіленкова [13]. Автори даної статті вже кілька років приділяють увагу питанням забезпечення та підтримання безпечного робочого середовища, а саме на розв'язуванні питань управління кібербезпекою в судноплавстві [14].

Мета дослідження

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 суднновому середовищі; застосування TRL-аналізу для оцінки готовності кібербезпекових рішень; формування основ інтегрованої аналітичної моделі плану реагування.

Виклад основного матеріалу дослідження

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 нагоді 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.

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 [15; 16; 17; 18].

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.

На завершальному етапі дослідження застосовано елементи TRL-аналізу для оцінки рівня готовності кібербезпекових рішень до впровадження в реальних умовах.

Аналіз вимог міжнародних стандартів кібербезпеки свідчить, що кожен із них орієнтований на окремий рівень управління ризиками. На наш погляд, розмежування зон застосування вимог стандартів створює низку практичних проблем. Судно функціонує як єдина

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

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.

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.

Міжнародний стандарт для системи управління інформаційною безпекою (ISO/IEC 27001) своєю чергою забезпечує системний підхід до управління 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 стандарту IEC 62443, який фокусується на безпеці промислових автоматизованих систем управління, і саме він є більш адаптованим до операційних технологій. Положення цього стандарту частково відповідають архітектурі суднових OT систем, зокрема електронній системі відображення навігаційних карт та інформації (ECDIS), систем управління енергетичними установками та автоматизованим системам контролю. Водночас практичне застосування цього стандарту у морській галузі залежить від налаштувань OT, від виробників обладнання, обмеженим доступом до електронних схем, неможливістю повної реалізації вимог безпеки без втручання сертифікованих сервісних інженерів [7].

Особливістю запропонованої нами 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.

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.

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 [19].

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 [20]. Для формалізації процесу оцінки ефективності покриття вимог стандартів у межах плану реагування будемо використати узагальнену математичну модель.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

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 (табл. 1). Вага кожного критерію (w_j) визначається з урахуванням його критичності для безпечної експлуатації судна:

$$\sum_{j=1}^{n} w_j = 1. \tag{1}$$

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. Інтегральний індекс морської придатності стандарту може бути визначений наступним чином:

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

де $MSI(S_i)$ – зведений показник ефективності стандарту в морських умовах.

Таблиця 1

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 [21]. Даний метод є структурованою процедурою прийняття рішень і широко використовується для багатокритеріального аналізу складних систем. Процес оцінювання було подано у вигляді трирівневої ієрархічної структури:

1. *Мета*: визначення інтегрального показника морської придатності стандартів кібербезпеки.
2. *Критерії*: набір критеріїв C_j, що охоплюють ключові аспекти морської кібербезпеки.
3. *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.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

Для перевірки надійності експертних оцінок обчислювався коефіцієнт узгодженості *CR* (Consistency Ratio). Значення оцінок вважалися прийнятними за умови $CR < 0.1$, відповідно до рекомендацій Сааті [21].

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. 2).

Таблиця 2

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. 3).

Таблиця 3

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.

Результати дослідження. 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).

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

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, відсутнє 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 [9].

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.

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.

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.

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. Проте під час перенесення цих вимог у морське середовище виникає низка обмежувальних факторів.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

Фактор I (інтеграція IT/OT) проявляється через фрагментарність 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, 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:

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

Це пояснює розрив між формальним впровадженням стандартів кібербезпеки та їх реальною ефективністю в умовах експлуатації суден.

Покажемо, як це працює на прикладі двох факторів.

1. *Критерій C2 – Інтеграція IT- / OT-систем*.

Для забезпечення критерію C2 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.

2. *Критерій C7 – 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. 1).

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.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-11 ISSN 2618-0332 (print), 2618-0340 (online)

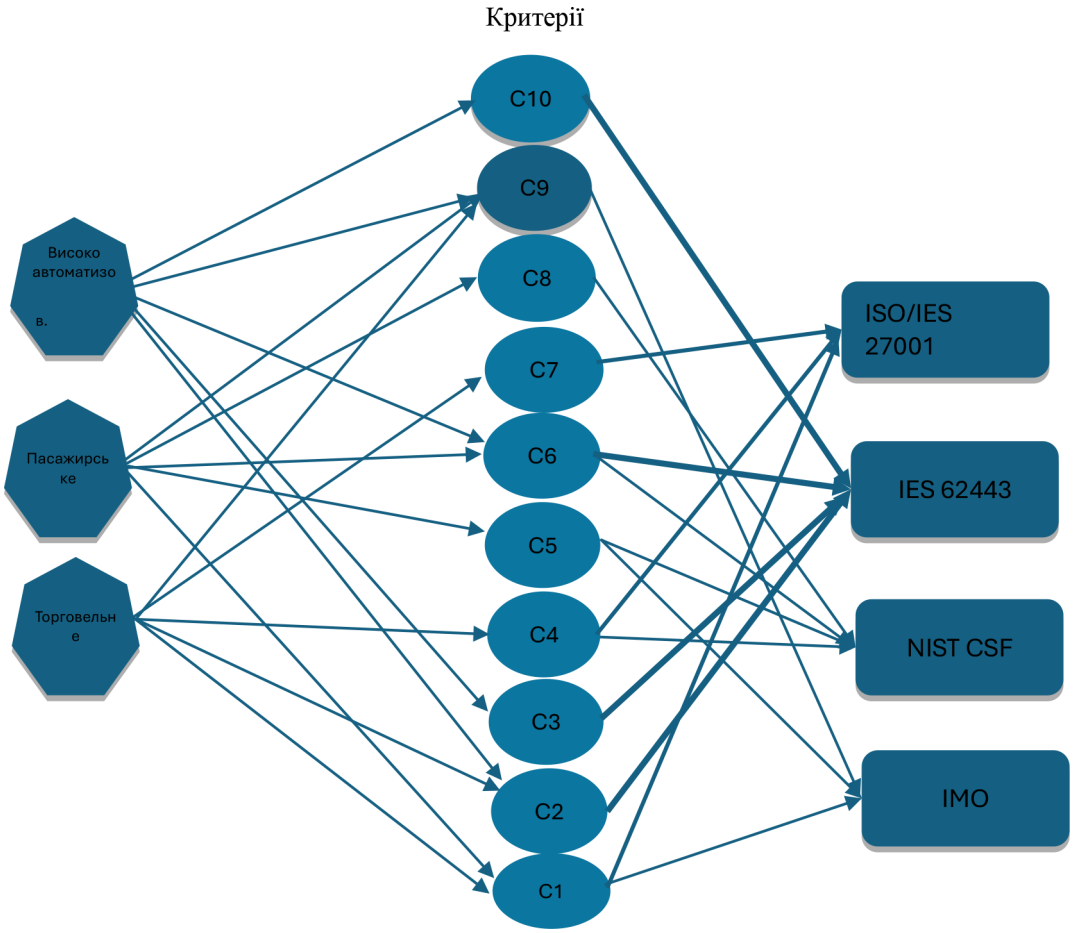

Рис. 1. Тришаровий граф з урахуванням індексу MSI стандартів

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.

Список використаної літератури

1. Новини про дослідження Thetius/CyberOwl/HFW. Центр транспортних стратегій. 2025. URL: https://cfts.org.ua/news/2025/03/13/u_2024_rotsi_kozhna_pyata_sudnoplavna_kompaniya_zaznala_kiberataki_doslidzhennya_82248 (дата звернення 10.01.2026).
2. Skladannyi P., Kostiuk Y., Zhyltsov O., Savchenko Y., Antypin Y. Intelligent modelling of personalized learning in cybersecurity training. (*In Proceedings of CPITS-II 2025. CEUR Workshop Proceedings*) 2025. Vol. 4145. P. 95–119. URL: https://ceur-ws.org/Vol-4145/
3. Oruc A., Bauk S., Zhou J. A National Maritime Cyber Security Operations Centre (M-SOC) Concept. *Marine Science and Engineering*. 2025. Vol. 14(1). P. 17–29. doi: https://doi.org/10.3390/jmse14010017

4. Akpan F., Bendiab G., Shiaeles S., Karamperidis S., Michaloliakos M. Cybersecurity Challenges in the Maritime Sector. *Network*. 2022. Vol. 2(1). P. 123–138. doi: https://doi.org/10.3390/network2010009.
5. Alcaide J. I., Llave R. G. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. 2020. Vol. 45. P. 547–554. doi: https://doi.org/10.1016/j.trpro.2020.03.058
6. Kessler, G., & Shepard, S. (2020). Maritime cybersecurity: A guide for leaders and managers. Independently published, 2022. 270 p.
7. Karas A. Maritime industry cybersecurity: A review of contemporary threats. *European Research Studies Journal*. 2023. Vol. 26. P. 921–935. doi: https://ersj.eu/journal/3336
8. Čelić J., Vukšić M., Baždarić R., Cuculić A. The Challenges of Cyber Resilience in the Maritime Sector: Addressing the Weak Awareness of the Dangers Caused by Cyber Threats. *J. Mar. Sci. Eng*. 2025. Vol. 13(4). P. 762. doi: https://doi.org/10.3390/jmse13040762
9. Androjna A., Brcko T., Pavic I., Greidanus H. Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*. 2020. Vol. 8(10). P. 776. doi: https://doi.org/10.3390/jmse8100776
10. Bolbot V., Kulkarni K., Brunou P., Banda O., Musharraf M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*. 2020. Vol. 39. P. 100571. doi: https://doi.org/10.1016/j.ijcip.2022.100571
11. Кочерєв О. Система дипломування судноводіїв у галузі морського, зокрема річкового, судноплавства України. *Південноукраїнський правничий часопис*. 2021. № 3(1). С. 77–81. https://doi.org/10.32850/sulj.2021.3.1.13
12. Корнієнко О. Тренди цифрових технологій в морегосподарюванні. *Економіка та управління національним господарством*. 2023. № 81, С. 51–56. https://doi.org/10.32782/2521-666X/2023-81-6
13. Вавіленкова А. Процес управління кіберінцидентами як необхідний етап в організації кібербезпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1(38), С. 64–71. URL: https://journals.uran.ua/ispss/article/view/340022 (дата звернення 21.12.2025).
14. Зайцева Т., Безбах О., Камінська Н. Кібербезпека в морській галузі: загрози, реагування та управління інцидентами. *Прикладні питання математичного моделювання*. 2025. № 8(1). С. 65–78. doi: https://doi.org/10.32782/mathematical-modelling/2025-8-1-6
15. International Electrotechnical Commission. IEC 62443-1-1:2021 – Security for industrial automation and control systems. 2021. URL: https://www.iec.ch/homepage (дата звернення 20.01.2026).
16. International Maritime Organization. Resolution MSC.428(98): Maritime cyber risk management in safety management systems. 2017. URL: https://www.imo.org/ (дата звернення 27.02.2026).
17. International Organization for Standardization. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. 2022. URL: https://www.iso.org/standard/27001 (дата звернення 12.01.2026).
18. National Institute of Standards and Technology. Cybersecurity framework profile guidance (NIST CSWP 29). 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення 26.01.2026). doi: https://doi.org/10.6028/NIST.CSWP.29
19. International Organization for Standardization. ISO 16290:2013 – Space systems: Definition of the technology readiness levels (TRLs) and their criteria of assessment. 2013. URL: https://www.iso.org/home.html (дата звернення 05.02.2026).
20. Martínez F., Sánchez L., Santos-Olmo A., Rosado D., Fernández-Medina E. Poseidon: An integrated cybersecurity framework for maritime systems with empirical validation. *Research*

Square. 2025. URL: https://www.researchsquare.com/article/rs-7490210/v1 (дата звернення 14.01.2026). doi: https://doi.org/10.21203/rs.3.rs-7490210/v1

21. Saaty T. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*. 2008. Vol. 1(1). P. 83–98.

References

1. Novyny pro doslidzhennia Thetius/CyberOwl/HFW. Tsentr transportnykh stratehii [Research news of Thetius/CyberOwl/HFW. Centre for Transport Strategies]. (2025). Retrieved from https://cfts.org.ua/news/2025/03/13/u_2024_rotsi_kozhna_pyata_sudnoplavna_kompaniya_zaznala_kiberataki_doslidzhennya_82248 [in English].
2. Skladannyi, P., Kostiuk, Y., Zhyltsov, O., Savchenko, Y., & Antypin, Y. (2025). Intelligent modelling of personalized learning in cybersecurity training. In Proceedings of CPITS-II 2025. *CEUR Workshop Proceedings*, 4145, 95–119. Retrieved from https://ceur-ws.org/Vol-4145/ [in English].
3. 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. doi: https://doi.org/10.3390/jmse14010017 [in English].
4. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123–138. doi: https://doi.org/10.3390/network2010009 [in English].
5. Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. doi: https://doi.org/10.1016/j.trpro.2020.03.058 [in English].
6. Kessler, G., & Shepard, S. (2020). *Maritime cybersecurity: A guide for leaders and managers*. Independently published. [in English].
7. Karas, A. (2023). Maritime industry cybersecurity: A review of contemporary threats. *European Research Studies Journal*, 26, 921–935. doi: https://ersj.eu/journal/3336 [in English].
8. Čelić J., Vukšić M., Baždarić R., Cuculić A. (2025). The Challenges of Cyber Resilience in the Maritime Sector: Addressing the Weak Awareness of the Dangers Caused by Cyber Threats. *J. Mar. Sci. Eng*. *13*(4), 762. doi: https://doi.org/10.3390/jmse13040762 [in English].
9. Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), 776. doi: https://doi.org/10.3390/jmse8100776 [in English].
10. Bolbot V., Kulkarni K., Brunou P., Banda O., Musharraf M. (2020). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, 100571. doi: https://doi.org/10.1016/j.ijcip.2022.100571 [in English].
11. 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. doi : https://doi.org/10.32850/sulj.2021.3.1.13 [In Ukrainian].
12. 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. doi: https://doi.org/10.32782/2521-666X/2023-81-6 [in Ukrainian].
13. 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. Retrieved from https://journals.uran.ua/ispss/article/view/340022 [in Ukrainian].

14. 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. doi: https://doi.org/10.32782/mathematical-modelling/2025-8-1-6 [in Ukrainian].
15. International Electrotechnical Commission. IEC 62443-1-1:2021 – Security for industrial automation and control systems. 2021. URL: https://www.iec.ch/homepage (дата звернення 20.01.2026) [in English].
16. International Maritime Organization. Resolution MSC.428(98): Maritime cyber risk management in safety management systems. 2017. URL: https://www.imo.org/ (дата звернення 27.11.2025) [in English].
17. International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Retrieved from https://www.iso.org/standard/27001 [in English].
18. National Institute of Standards and Technology. Cybersecurity framework profile guidance (NIST CSWP 29). (2024). doi: https://doi.org/10.6028/NIST.CSWP.29 [in English].
19. International Organization for Standardization. (2013). ISO 16290:2013 – Space systems: Definition of the technology readiness levels (TRLs) and their criteria of assessment. Retrieved from https://www.iso.org/home.html [in English].
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. doi: https://doi.org/10.21203/rs.3.rs-7490210/v1 [in English].
21. Saaty, T. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1*(1), 83-98. [in English].

Зайцева Тетяна Василівна – к.пед.н., доцент, доцент кафедри загальнофахової підготовки та морської безпеки Херсонської державної морської академії. E-mail: tetiananovitskawork@gmail.com, ORCID: 0000-0001-6780-719X.

Zaitseva Tetiana Vasylivna – Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of General Training and Maritime Safety of the Kherson State Maritime Academy. E-mail: tetiananovitskawork@gmail.com, ORCID: 0000-0001-6780-719X.

Дата першого надходження статті до видання: 09.03.2026
Дата прийняття статті до друку після рецензування: 21.04.2026
Дата публікації (оприлюднення) статті: 01.07.2026