КІБЕРБЕЗПЕКА СУДЕН: ІНТЕГРОВАНЕ ОЦІНЮВАННЯ

Зайцева Тетяна
к.п.н., доцент
Кафедра загальнофахової підготовки та морської безпеки
Херсонська державна морська академія, Україна

Морський сектор стикається зі зростаючими кіберзагрозами, які ставлять під сумнів експлуатаційну безпеку суден і портів. Запровадження міжнародних стандартів кібербезпеки (ISO/IEC 27001, NIST CSF, IEC 62443, рекомендації IMO) є обов'язковим, однак їх ефективність обмежується неповним охопленням життєвого циклу систем, складністю інтеграції інформаційних та операційних технологій, а також недостатнім врахуванням людського фактора.

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.

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 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.

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. [1] 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 [2]. У роботах ми знаходимо опис модульного підходу, який охоплює стратегічне планування системи кіберзахисту на основі двох факторів: соціальної інженерії та операційної стійкості.

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 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. 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.

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 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 [3], 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.

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.

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 [4].

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:

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

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:

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

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 [5]. Даний метод є структурованою процедурою прийняття рішень і широко використовується для багатокритеріального аналізу складних систем.

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 [5].

Більш детально розглянемо процес розрахунку для одного конкретного критерію: 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 «Інтергація 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. 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.

Висновки. Аналіз міжнародних стандартів показав, що кожен із них орієнтований на окремий рівень управління ризиками та не забезпечує цілісного підходу. Судно функціонує як єдина кіберфізична система, тому роздільне застосування стандартів не дозволяє ефективно реагувати на інциденти. Запропоновано інтегровану модель реагування, яка поєднує:

- стратегічний рівень (IMO);
- тактичний рівень (NIST CSF: Identify–Protect–Detect–Respond–Recover);
- технічний рівень (IEC 62443).

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. Запропонований інтегрований підхід дозволяє перейти від формального виконання стандартів до практично орієнтованої системи управління кіберризиками. Більш детально результати дослідження представлені в статтях автора.

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 використаних джерел

1. Skladannyi P., Kostiuk Y., Zhyltsov O., Savchenko Y., Antypin Y. Intelligent modeling of personalized learning in cybersecurity training // Proceedings of CPITS-II 2025. – CEUR Workshop Proceedings. – 2025. – Vol. 4145. – P. 95–119.
2. Oruc A., Bauk S., Zhou J. A National Maritime Cyber Security Operations Centre (M-SOC) Concept // Journal of Marine Science and Engineering. – 2025. – Vol. 14(1). – P. 17–29. – DOI: 10.3390/jmse14010017.
3. International Electrotechnical Commission. IEC 62443-1-1:2021 – Security for industrial automation and control systems [Електронний ресурс]. – 2021. – Режим доступу: https://www.iec.ch (дата звернення: 26.05.2026).
4. International Organization for Standardization. ISO 16290:2013 – Space systems: Definition of the technology readiness levels (TRLs) and their criteria of assessment [Електронний ресурс]. – 2013. – Режим доступу: https://www.iso.org (дата звернення: 26.05.2026).
5. Saaty T. Decision making with the analytic hierarchy process // International Journal of Services Sciences. – 2008. – Vol. 1(1). – P. 83–98.

СУЧАСНІ ЗАГРОЗИ КІБЕРБЕЗПЕЦІ ТА МЕТОДИ ЇХНЬОГО ЗАПОБІГАННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сухосьян Олександра Борисівна
Студентка 3 курсу
Інженерія програмного забезпечення
Відокремлений структурний підрозділ «Економіко-технологічний фаховий коледж Херсонського національного технічного університету», Україна

Анотація.

У статті розглядаються сучасні загрози кібербезпеці, які виникають у зв'язку з розвитком інформаційних технологій. Проаналізовано основні види кібератак: фішинг, DDoS-атаки, програми-вимагачі (ransomware), а також методи соціальної інженерії. Запропоновано комплексний підхід до захисту інформаційних систем, який включає шифрування даних, багатофакторну автентифікацію, моніторинг мережевої активності та навчання персоналу. Особливу увагу приділено європейським стандартам кібербезпеки (NIS2, GDPR) та їх впровадженню в Україні [1-5].

Ключові слова: кібербезпека, інформаційні технології, кібератаки, фішинг, DDoS, ransomware, NIS2, GDPR, захист інформації.

1. Вступ

Стрімкий розвиток інформаційних технологій створює не лише нові можливості для бізнесу та суспільства, але й породжує серйозні загрози кібербезпеці. За даними Європейського агентства з кібербезпеці (ENISA),