СЕКЦІЯ XIII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

ІНТЕГРАЦІЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ В СУДНОПЛАВСТВІ

Зайцева Тетяна Василівна
ORCID ID: 0000-0001-6780-719X
Херсонська державна морська академія, Херсон, Україна

Морський сектор стикається зі зростаючими кіберзагрозами, які ставлять під сумнів експлуатаційну безпеку суден, портів. Запровадження в практику кіберзахисту міжнародних стандартів ISO/IEC 27001, NIST CSF, IEC 62443 та рекомендацій міжнародної морської організації (IMO) [3] 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 складнощі технічної інтеграції інформаційних та операційних технологій, через неповне врахування особливостей взаємодії бортових систем суден різного типу, через недостатнє врахування впливу людського фактора на забезпечення 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.

Аналіз наукових публікацій [1, 2, 6] 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 [2]. Особливо небезпечними є атаки на навігаційні системи GPS та ECDIS, наслідками яких можуть стати аварії та екологічні катастрофи.

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.

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 завершальному етапі дослідження застосовано елементи TRL-аналізу для оцінки рівня готовності кібербезпекових рішень до впровадження в реальних суднових умовах [4].

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.

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, включаючи життєвий цикл цифрових активів, інтеграцію IT/OT, людський фактор та операційну стійкість (табл. 1). Вага кожного критерію (w_j) визначається з урахуванням його критичності для безпечної експлуатації судна за формулою *(1).*

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

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 за формулою *(2):*

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

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

Продовження табл. 1

Критерій	C_j	w_j	p_{ij}	$w_j \cdot p_{ij}$
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**

[авторська розробка]

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.

Процес оцінювання було подано у вигляді трирівневої ієрархічної структури:

1. *Мета*: визначення інтегрального показника морської придатності стандартів кібербезпеки.

2. *Критерії*: набір критеріїв, що охоплюють ключові аспекти морської кібербезпеки.

3. *Альтернативи*: стандарти кібербезпеки, зокрема ISO/IEC 27001, NIST Cybersecurity Framework та IEC 62443.

Висновки. 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 ІМО 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.

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. 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
3. International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Вилучено з https://www.iso.org/standard/27001
4. International Organization for Standardization. (2013). ISO 16290:2013 - Space systems: Definition of the technology readiness levels (TRLs) and their criteria of assessment. Вилучено з https://www.iso.org
5. Saaty, T. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1), 83-98.
6. 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