УДК 656.61/004.056.5

Т.В. ЗАЙЦЕВА, О.М. БЕЗБАХ, Н.Г. КАМІНСЬКА
Херсонська державна морська академія

КІБЕРБЕЗПЕКА В МОРСЬКІЙ ГАЛУЗІ: ЗАГРОЗИ, РЕАГУВАННЯ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ

У статті розглядається проблема кібербезпеки в галузі судноплавства в умовах зростання цифровізації морської інфраструктури. Останні дослідження та публікації з кібербезпеки судноплавної галузі вказують на зростання загроз через цифровізацію морської галузі. Підкреслюється важливість упровадження ефективних планів реагування на кіберінциденти для забезпечення безперервності бізнесу та зниження ризиків, пов'язаних із кіберзагрозами. Упровадження міжнародних стандартів, тестування сценаріїв і гнучке управління процесами – усе це формує фундамент кіберстійкості морського сектору.

Метою дослідження є розроблення моделі для побудови ефективного плану дій і плану реагування на кіберінциденти із застосуванням сучасних технологій управління проєктами та на основі стандартів захисту даних. Як автори ми бачимо таки основні завдання, як: побудова плану дій із гарантування кібербезпеки судна на основі керівних документів, досвіду провідних спеціалістів, аналізу досягнень у сфері кібербезпеки на морських суднах; упровадження проєкту в систему освіти відповідного напряму та його апробація під час проходження курсантами плавальних практик; подальше його застосування для оперативного навчання членів екіпажів на суднах. Натепер уже отримано домовленість на включення побудованого плану у програму освітньої компоненти «Кібербезпека суднових комп'ютерних мереж та систем» конкретних навчальних закладів, як-от Херсонська державна морська академія.

Проаналізовано поширені підходи до реагування на інциденти, досліджено можливості адаптації проєктного управління для підвищення ефективності таких заходів. Іншою метою даного дослідження є вдосконалення плану ефективної підготовки майбутніх судноводіїв із гарантування кібербезпеки на морському судні завдяки осучасненню та зміні контенту освітньої компоненти.

Запропоновано структурований підхід до створення плану реагування на кіберінциденти, орієнтованого на специфіку загроз у судноплавстві. Практичне значення дослідження полягає в можливості використання отриманих результатів судноплавними компаніями, портовими адміністраціями та для навчання персоналу відповідно до вимог міжнародних стандартів.

Ключові слова: *кіберінцидент, кібербезпека, план реагування на кіберінцидент, управління проєктами.*

T.V. ZAITSEVA, O.M. BEZBAKH, N.H. KAMINSKA
Kherson State Maritime Academy

CYBERSECURITY IN THE MARITIME INDUSTRY: THREATS, RESPONSES, AND INCIDENT MANAGEMENT

This article addresses the issue of cybersecurity in the maritime sector amidst the increasing digitalization of maritime infrastructure. Recent research and publications on cybersecurity in the shipping industry indicate an increase in threats due to the digitalization of the maritime industry. It emphasizes the importance of implementing effective cyber incident response plans to ensure business continuity and reduce risks associated with cyber threats. The implementation of international standards, scenario testing, and agile process management all form the foundation for cyber resilience in the maritime sector.

The purpose of the study is to develop a model for building an effective action plan and response plan for cyber incidents using modern project management technologies and based on data protection standards. As authors, we see the following main tasks: building an action plan to ensure the cybersecurity of the ship based on governing documents, the experience of leading specialists, and an analysis of achievements in the field of cybersecurity on seagoing vessels; implementing the project into the education system of the relevant direction and testing it during the cadets' swimming practices; further using it for operational training of crew members on ships. Currently, an agreement has been reached to include the built plan in the program of the educational component "Cybersecurity of ship computer networks and systems" of specific educational institutions, such as the Kherson State Maritime Academy.

Existing approaches to incident response were analysed, and the possibilities of adapting project management to increase the effectiveness of such measures were investigated. Another goal of this study is to improve the plan for practical training of future shipowners in ensuring cybersecurity on a seagoing vessel by modernizing and changing the content of the educational component.

A structured approach to creating a cyber incident response plan focused on the specifics of threats in shipping is proposed. The study's practical significance lies in the possibility of using the results obtained by shipping companies and port authorities to train personnel by the requirements of international standards.

Key words: *cyber incident, cybersecurity, cyber-incident response plan, project management.*

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

Постановка проблеми

У сучасному світі морська інфраструктура відіграє ключову роль у глобальній торгівлі, обороні та міжнародних зв'язках. Водночас вона дедалі більше піддається загрозам у кіберпросторі. Відбуваються постійні оновлення в галузі інформаційних технологій, доступності даних, швидкості обробки та передачі даних із розширеними можливостями для оптимізації роботи, економії витрат, підвищення безпеки та стійкості бізнесу. Загальносвітовою тенденцією нині є цифровізація економіки, природно, що це стосується й морського транспорту. На морському транспорті використовується та розвивається електронна навігація, використання мережевого трафіку, автоматизація процесів експлуатації судна. Зростання цифровізації портів, навігаційних систем, систем управління суднами й інших компонентів морської галузі створює нові вектори атак для кіберзлочинців, що може мати катастрофічні наслідки як для окремих держав, так і для світової економіки загалом.

Питання розроблення кіберзахисту, стратегії управління захистом відповідно до правил і передової практики на борту судна з акцентом на робочі процеси, обладнання, навчання, реагування на інциденти й управління відновленням – невід'ємна частина системи управління безпекою судна як цілісної функціонуючої системи.

Кібербезпека – це не лише запобігання доступу хакерів до систем та інформації, що потенційно призводить до втрати конфіденційності та/або контролю. Це також стосується підтримки цілісності та доступності інформації та систем, забезпечення безперервності бізнесу та постійної корисності цифрових активів і систем. Судновласникам і операторам необхідно розуміти важливість кібербезпеки та підвищувати обізнаність про це співробітників, зокрема й персоналу на судні або в порту.

Аналіз останніх досліджень і публікацій

Ефективне реагування на кіберзагрози потребує не лише технічної підготовки, але й чіткої організаційної структури, планування і координації дій. Застосування технологій управління проєктами дозволяє структурувати процес реагування, встановити чіткі ролі, відповідальність і контроль за виконанням заходів. Саме тому дослідження можливостей поєднання кібербезпеки із проєктним менеджментом є одним із напрямів розроблення плану реагування на кіберінциденти як живого дієвого механізму [1–5].

Останні дослідження та публікації з кібербезпеки судноплавної галузі вказують на зростання загроз через зростання динамічним чином цифровізації морської галузі. Аналіз компаній *Positive Technologies, CyberOwl, Microsoft* та *Capgemini* (2017–2021 рр.) показав, що кібератаки на суднові системи типу NotPetya та WannaCry вразили контейнерні лінії (Maersk, COSCO, MSC), порти (Барселона, Сан-Дієго) та суднобудівні компанії (Austal) [6]. Атаки часто спрямовані на інформаційно-навігаційні системи в районах із високим трафіком, що підвищує ризик аварій.

Кібератаки можуть порушити роботу суднових систем, спричинити втрату керування, пошкодження вантажу чи екологічні катастрофи. Згадані дослідження акцентують на необхідності аналізу попередніх інцидентів для прогнозування загроз. Наприклад, атаки на системи GPS (Global Positioning System) чи ECDIS (Electronic Chart Display and Information System) можуть призвести до зіткнень через спотворення навігаційних даних. Саме тому із 2021 р. Міжнародна морська організація (далі – IMO) запровадила вимоги до кібербезпеки суден [2; 5]. Автори даної статті попередньо наголошують на потребі адаптації універсальних стандартів кібербезпеки саме для морських систем, тому що брак адаптованих стандартів ускладнює захист.

Актуальність запропонованих досліджень зумовлена тим, що в умовах сучасного судноплавства всі технічні засоби судноводіння функціонують у мережі як комбінація підсистем, які взаємопов'язані одна з одною, для забезпечення централізованого моніторингу різних навігаційних параметрів. Мережа таких технічних засобів судноводіння, які забезпечують вахтовому офіцеру централізований доступ до навігаційної інформації, силової установки, інформації управління і моніторингу тощо, дістала назву інтегрований місток, від англомовного терміна

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

“Integrated Bridge System” (далі – IBS). Метою IBS є підвищення безпечного й ефективного управління судном кваліфікованим персоналом. IBS дозволяє збирати й контролювати інформацію з датчиків про низку операцій, як-от виконання рейсу, зв’язок, управління технічними засобами, а також охорона й безпека, кібербезпека також.

Інтегрована система управління на містку – це різновид системи управління, яка об’єднує інші підсистеми для надання вахтовому офіцеру всіх подробиць, що стосуються навігації судна, в одному місці. Варто зазначити, що не всі типи суден мають однакові типові IBS. Такі системи будуть різнитися залежно від конструктивних особливостей суднового містка, різних типів обладнання, що використовується на судні, і загального розташування обладнання на містку.

Моніторинг останніх досліджень і публікацій, які стосуються зазначеної тематики, вказує на те, що безпека судноплавства значною мірою залежить, по-перше, від оснащеності судна, по-друге, від кваліфікації його офіцерського складу. Цим питанням приділяли увагу як іноземні дослідники, наприклад, Ф. Акпан, Г. Бендіаб [1], Дж. Алкаід, Р. Лаве [3], Г. Кесслер, С. Шепард [7], Г. Каваліраторс, С. Катсікас [16], С. Хопкінсон [9], Й. Челіч, М. Вукшич [4], так і вітчизняні науковці: В. Горбов, І. Ратушняк [20], О. Корнієнко [21]. Так, у своїй роботі «Система дипломування судноводіїв» О. Кочерєв [17] відзначив необхідність удосконалення системи підготовки моряків, акцентував увагу саме на їх комплексній підготовці.

Аналіз законодавчих баз європейських країн або нормативних актів, що стосуються безпекових питань морської галузі, доводить, що вони надають загальну інформацію за видами кіберзагроз, планом реагування на кіберінциденти. Але тільки група спеціалістів, у яку входять представники судноплавної галузі та компетентні особи з комп’ютерних технологій і питань кібербезпеки, може надати адаптований план реагування на кіберінциденти, який ураховує наявне обладнання та специфіку роботи саме операційних технологій, наприклад морського судна. На це спроможні великі судновласники чи великі порти. У малих портах і на невеликих суднах замість дієвого плану реагування на кіберінциденти ми спостерігаємо документи, де зазначені загальні положення, які не завжди стають у пригоді під час кіберінциденту. Тому завдання створення шаблону або алгоритму розроблення плану реагування залишається актуальним.

Автори даної статті вже кілька років приділяють увагу питанням комплексного підходу до підготовки фахівців морського профілю, акцентують увагу на питаннях забезпечення та підтримання безпечного робочого середовища, а саме на вирішенні питань управління кібербезпекою в судноплавстві [15; 22].

Мета дослідження

Морський транспорт дедалі більше покладається на цифрові системи: навігацію, зв’язок, управління вантажами, логістику. Натепер можна виділити такі основні вектори загроз (табл. 1):

Таблиця 1

Вектори загроз

Загроза	**Опис**
Вразливість навігаційних систем, як-от AIS (автоматична ідентифікація), ECDIS (електронна навігаційна карта), GMDSS (глобальна система морського зв’язку).	Порушення роботи систем призводить до аварій.
Атаки на інформаційні системи портів.	Крадіжка конфіденційної інформації, блокування операцій через програми-вимагачі.
Кібершпигунство та саботаж.	З боку держав або організованих угруповань.
Соціальна інженерія.	Фішингові листи, спрямовані на членів екіпажу або персонал, що мають доступ до критичних систем.
Спуфінг GPS.	Створення фальшивих навігаційних координат, які можуть спрямувати судно в неправильному напрямку або навіть створити аварійну ситуацію.
DoS/DDoS-атаки.	Виведення з ладу цифрової інфраструктури, яка забезпечує облік вантажів, координацію дій портових служб.

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

Серйозність таких загроз ілюструє низка інцидентів останніх років. Досить навести яскравий приклад, посилаючись на офіційні джерела або їх огляд [5], який показує важливість постійної уваги до кібербезпеки на морських суднах.

Однієї з найбільш значних і руйнівних кібератак останнього часу є NotPetya, яка завдала загального збитку на суму більш ніж 10 мільярдів доларів у червні 2017 р. Цікаво, що NotPetya був орієнтований передусім на українські компанії, але цей напад вийшов далеко за межі України, від нього постраждали багато великих організацій, зокрема й компанія з постачання "FedEx", данський судноплавний гігант "Maersk", який виконує доставку сьомої частки всіх контейнерів, що відправляють у світі. Ця компанія постраждала найсильніше, на суму 300 мільйонів доларів, втратила більшу частину своїх даних.

У 2021 р. порт Х'юстона у США став жертвою цільової атаки з використанням вразливостей у системах SCADA. Збільшення атак на українські морські об'єкти після початку повномасштабної війни також свідчить про стратегічну роль кібербезпеки в конфліктних регіонах.

У відповідь на зростання загрози постає потреба у створенні ефективних систем реагування на кіберінциденти. У морській індустрії це особливо критично, оскільки будь-яке зволікання може призвести до матеріальних збитків, небезпеки для екіпажу, екологічних катастроф або загроз національній безпеці.

Мета дослідження – побудова моделі або плану дій із гарантування кібербезпеки судна з урахуванням його специфіки, що охоплює всі основні компоненти оперативного реагування на кібератаки, та представлення цього плану в доступній наочній формі, яка б сприяла швидкому засвоєнню алгоритму його застосування.

Завдання дослідження:

1. Проаналізувати існуючі підходи до реагування на кіберінциденти.
2. Дослідити інструменти та методики управління проєктами, які можуть бути адаптовані для кібербезпеки.
3. Визначити ключові етапи створення плану реагування на кіберінциденти, розглядаючи типи загроз як окремі робочі пакети проєкту. Тобто спроєктувати структуру проєктного плану реагування з урахуванням специфіки загроз і типу судна.
4. Оцінити ефективність запропонованого підходу за допомогою моделювання реального процесу.

Об'єкт дослідження – процеси реагування на кіберінциденти в інформаційних системах судноплавства.

Предмет дослідження – інтеграція технологій управління проєктами із процесом розроблення та реалізації планів реагування на кіберінциденти.

Гіпотеза дослідження. Інтеграція методологій управління проєктами із процесом розроблення плану дій щодо реагування на кіберінциденти дозволить підвищити ефективність і оперативність реагування на загрози кібербезпеки в організації, дозволить ураховувати конкретні умови адаптації плану та надасть керівництву чіткий обсяг фінансування підтримки безпечних умов роботи.

Практичне значення. Розроблена модель і запропонований план дій можуть бути адаптовані:

– судноплавними компаніями для підвищення кіберстійкості завдяки розробці дієвого плану реагування на кіберінциденти та врахування конкретних вимог гарантування безпекового функціонування об'єктів;

– портовими адміністраціями для оптимізації дій під час кіберінцидентів;

– для навчання екіпажів та IT-персоналу згідно з вимогами ISM Code;

– для зміни контенту освітньої компоненти підготовки судноводіїв, що стосується проблематики кібербезпеки суднових комп'ютерних мереж і систем.

Виклад основного матеріалу дослідження

Відповідно до резолюції MSC.428 (98) Міжнародної морської організації (IMO), усі судна й оператори повинні інтегрувати кіберризики до існуючих систем управління безпекою. Це

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

означає не лише технологічні рішення, а й процедурні, організаційні й управлінські заходи та постійне навчання або тренінг персоналу. В основі цих заходів лежить план реагування на кіберінциденти. Він повинен поєднати всі відомі натепер засоби кіберзахисту та запропонувати як керівництву судноплавних компаній, так і екіпажам морських суден чіткий і зрозумілий план дій.

Система IBS повинна втілювати два або більше з таких аспектів: виконання рейсу, зв'язок, керування технічними засобами судноводіння, вантажні операції, а також охорона й безпека (кібербезпека). Критерії монтажу IBS і проєктування встановлюються класифікаційними товариствами, наприклад, клас NAV1 для LR, клас W1-OC від DNC є прикладами класів для IBS [13]. Чинники, що впливають на компонування, мають ураховувати конструкцію містка судна, характеристики електронавігаційного, радіонавігаційного й іншого обладнання, а також його розташування на містку. Підсистеми IBS можна поділити на чотири основні складники, як-от: технічна підсистема, людина-оператор (вахтовий офіцер), людино-машинний інтерфейс (далі – ЛМІ), інструкції з експлуатації та засоби фіксації активності (лог-буки).

IBS зазвичай складається з:

– авторульового;

– підсистеми радарів (ARPA), для якої передбачено дублювання функціоналу;

– гіроскопічного та магнітного компасів;

– підсистеми фіксації даних рейсу (VDR);

– ECDIS, для якої передбачено дублювання функціоналу (основна + резервна);

– центрального дисплея (Conning Display), який інтегрує важливі навігаційні дані, особливо на підходах до портів або виходах із них, забезпечує вахтового офіцера (OOW) центральним робочим місцем для моніторингу всіх датчиків і налаштувань;

– системи розподілу енергії;

– підсистеми стернового управління;

– GMDSS.

Згідно із Правилом 19 розділу V SOLAS, п. 6 [14], інтегровані системи управління на містку повинні бути влаштовані таким чином, щоб відмова однієї підсистеми негайно доводилася до відома офіцера, відповідального за навігаційну вахту, за допомогою звукової та візуальної сигналізації, і не спричиняла відмови будь-якої іншої підсистеми. У разі виходу з ладу однієї із частин інтегрованої навігаційної системи повинна бути забезпечена можливість експлуатації кожного окремого елемента обладнання або частини системи окремо.

Особливим напрямом розв'язування питання кібербезпеки морської галузі є зменшення ролі особистості в убезпеченні системи загалом. Недоліком сучасних систем управління морськими транспортними суднами є висока частка участі людини у процедурі ухвалення рішень. Тому важливо використовувати системний підхід до вирішення цієї проблеми.

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

Ключові елементи такого плану включають:

– класифікацію інцидентів за рівнем критичності;

– процедури виявлення, фіксації та ескалації інциденту;

– визначення відповідальних осіб і команд;

– порядок інформування керівництва, екіпажу, партнерів;

– юридичні аспекти, зокрема і звітування перед державними органами;

– післяінцидентний аналіз і оновлення політик.

Розроблення плану реагування має розглядатись як окремий проєкт, що дозволяє структурувати процес і ефективно управляти ресурсами. Системний підхід до планування, реалізації

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

та контролю таких ініціатив базується на принципах класичного проєктного менеджменту (PMBOK) або гнучких методологіях (Agile/Scrum).

План реагування має складатися з декількох обов'язкових етапів (рис. 1), зазначення яких можна знайти як в законодавчих актах, так і в інструкціях із безпекових питань [8].

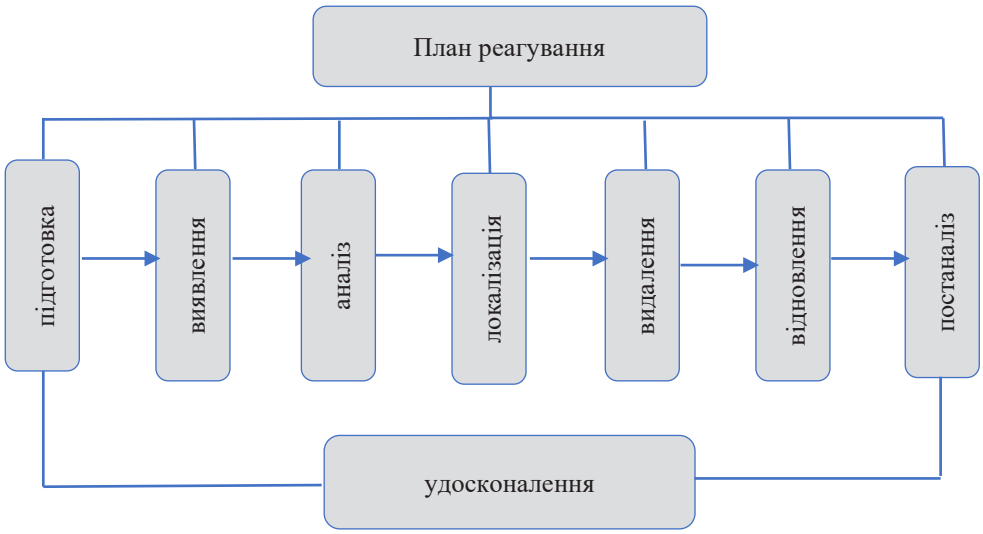

Рис. 1. План реагування на кіберінциденти

А так виглядатиме вдосконалена схема процесу управління кібербезпекою, яка охоплює всі етапи реагування на інциденти, відповідно до найкращих практик (наприклад, Міжнародного стандарту в області інформаційних технологій ISO/IEC 27035 [10; 11]):

1. Підготовчий етап (Preparation):
- розроблення політик безпеки та плану реагування на кіберінцидент;
- укладання та узгодження плану з керівництвом;
- побудова команди реагування (CSIRT / SOC), розподілення ролей;
- навчання співробітників, членів екіпажу;
- резервне копіювання даних;
- інвентаризація активів, їх класифікація та категоризація.

2. Виявлення кіберінциденту, його аналіз (Detection & Analysis):
- спостереження за технологічним процесом, роботою бортових систем;
- моніторинг логів, мережевого трафіка;
- виявлення індикаторів компрометації;
- класифікація та пріоритизація інциденту;
- визначення джерела й обсягу впливу.

3. Реагування на інцидент (Containment, Eradication & Recovery):
- повідомлення команди (внутрішнє інформування);
- локалізація інциденту (обмеження поширення);
- сегментація мереж;
- видалення шкідливого програмного забезпечення;
- відновлення систем (за можливості, до типового робочого стану);
- перевірка оновлень програмного забезпечення та злагодженої роботи всіх систем після оновлення.

4. Повідомлення та сповіщення (Notification):
- збір доказової бази;
- зовнішнє інформування (держоргани, судновласники, партнери, клієнти, ЗМІ);

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

– дотримання юридичних і регуляторних вимог.

5. Постаналіз (Post-Incident Activity):

– протоколювання дій команди реагування;

– аналіз причин кіберінциденту;

– оновлення політик, плану реагування;

– зворотний зв'язок для підвищення рівня готовності до запобігання кіберзагрозам.

6. Постійне вдосконалення:

– тестування оновленого плану реагування;

– оцінювання наявних ризиків;

– упровадження змін на основі висновків про попередні інциденти.

Такий підхід дозволяє розглядати план реагування не як статичний документ, а як живу систему, що постійно вдосконалюється відповідно до змін у середовищі загроз.

До того ж треба враховувати, що інформаційна безпека є фактично ключовим елементом стабільного розвитку як окремої компанії, так і всієї галузі загалом. Основним засобом комунікації учасників будь-яких бізнес-проєктів є обмін інформацією, який зазвичай здійснюється почтовими системами. Зазвичай це уніфікований протокол SMTP. Але їхня доступність з інтернету також підвищує ризик кібератак. Через почтові системи кіберзлочинці впроваджують вірусні файли, навіть якщо компанія має захищений внутрішній мережевий периметр. Вірусні електронні письма здатні розповсюдити шкідливе програмне забезпечення на тисячі комп'ютерів одночасно.

У зв'язку із ситуацією, яка склалася з навалою кіберзлочинів, IT-фахівці проводять глобальні дослідження з метою підвищення безпеки використання програмних продуктів. Натепер є досить дієвий спосіб зниження ризиків кіберзагроз. Це так званий харденінг – підхід, який останнім часом використовують саме IT-фахівці.

Харденінг (hardening) програмного забезпечення [19] – це процес підвищення безпеки системи завдяки видаленню або обмеженню потенційних вразливостей. Харденінг – комплекс дій і налаштувань, що спрямовані на суттєве зниження можливостей кіберзлочинців і захист даних. Можна коротко описати цілі харденінгу та засоби їх досягнення:

– зменшення поверхні атаки – скорочення числа шляхів і точок входу, які можуть бути доступні зловмисникам;

– посилення контролю та моніторингу – забезпечення контролю доступу та постійний нагляд за діями як користувачів, так і систем;

– забезпечення цілісності системи – запобігання несанкціонованим змінам налаштувань;

– підтримка відповідності стандартам безпеки – дотримання регуляторних вимог і стандартів, як-от ISO 27001, GDPR, ФЗ-152, PCI-DSS та інші.

Як бачимо, перелічені принципи є дуже простими та зрозумілими, але ефект від упровадження такого підходу є суттєвим.

Але сам собою харденінг не буде дієвим, якщо вся команда компанії не буде ставитися до цього максимально відповідально. Тому одним із найважливіших елементів запобігання кібератакам є постійна підготовка всього персоналу, як усього екіпажу кожного судна, так і берегових служб. Діяльність кіберзлочинців щодня вдосконалюється, на їхньому боці також працюють «просунуті» фахівці, тому і контроль за персоналом з боку структури, яка відповідальна за кібербезпеку всієї системи, має бути постійним.

Можна навести приклад, який свідчить про необхідність таких заходів. За даними звіту Thetius, CyberOwl і HFW, тільки у 2024 р. кожна п'ята суднoплавна компанія зазнала тих чи інших проявів кібератак [6]. За результатами опитувань, 93% членів екіпажів зізналися, що не відчувають здатності до вирішення завдань у сфері кібербезпеки, 70% упевнені, що навчання та своєчасне тренування допомогло б покращити їхню 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 р., 60% – зараження суднових систем шкідливим програмним забезпеченням, найгірше, що 77% із них здійснено через USB-накопичувачі й інші носії,

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

як-от ноутбуки персоналу. Своєчасне інформування персоналу, проходження співробітниками відповідних тренінгів, отримання сертифікатів, підписання актів відповідальності – ось шлях суттєвого зниження кіберризиків у цій сфері. Створення стандартів кібербезпеки та неухильне дотримання вимог є одним із головних шляхів підвищення рівня кібербезпеки.

Застосування методологій управління проєктами PMBOK або PRINCE2 дозволяє структуровано реалізувати цей процес: від ініціації та планування до контролю та закриття. PMBOK (Project Management Body of Knowledge) – це довідник з управління проєктами, який акумулює сукупність професійних знань з управління проєктами в різних галузях незалежно від організації, містить фундаментальні базові практики. PMBOK – це стандарт PMI (Project Management Institute), одна із провідних некомерційних світових організацій у галузі управління проєктами. Даний стандарт пропонує втілювати єдині глобальні стандарти роботи в галузі управляння проєктами (табл. 2).

Таблиця 2

Упровадження плану реагування в PMBOK

Етап	**Дія (що виконується)**	**Особливості застосування на судні або в порту**	**Конкретні приклади дій**
Ініціація	Визначення потреби в реагуванні. Формування команди та призначення відповідальних осіб.	Залежить від типу судна, наявності IT/OT-систем, ролей екіпажу.	Призначення координатора безпеки. Аналіз політик компанії.
Планування	Ідентифікація кіберризиків, аналіз загроз, розроблення плану реагування.	Залучення фахівців з кібербезпеки. Оцінювання критичних систем: ECDIS, AIS, IBS.	Розроблення сценаріїв інцидентів. Визначення ролей і процедур.
Виконання	Упровадження систем виявлення атак, навчання персоналу.	Інсталяція IDS/IPS на судні. Проведення тренувань для екіпажу.	Навчання реагування на інциденти. Запуск систем моніторингу.
Моніторинг і контроль	Аудит упроваджених заходів, моделювання інцидентів, перевірка ефективності плану.	Постійне оновлення інструкцій. Випробування реальних сценаріїв на практиці.	Імітація GPS-спуфінгу. Відпрацювання DDoS-атак.
Закриття	Аналіз інцидентів, оновлення документації, підготовка звіту про виконання плану.	Формування рекомендацій для майбутніх інцидентів. Архівування даних.	Створення звіту. Коригування процедур.

Але для втілення в життя цього проєкту необхідне залучення всієї команди, від судновласника або адміністрації порту до членів екіпажу або операторів порту. У команду реагування мають входити кіберфахівці, начальники служб безпеки, страхові компанії. А іноді навіть держоргани або представники ІМО.

Розглянемо процес реагування як програмно-керований інцидент із визначенням стадій, продуктів і ролей. PRINCE2 – це структурований підхід до управління проєктами, який спрямований на управління проєктами в рамках чітко визначеної організаційної структури. Цей підхід сприяє більш чіткому розумінню питань координації людей, розподілу обов'язків і відповідальності. Структурований підхід дозволяє кожний процес або напрям дії зазначати із ключовими вхідними та вихідними даними, описувати завдання, які необхідно виконати. І як будь-яка технологія управління проєктами, PRINCE2 надає можливість урахування ризиків, які можуть спричинити відхилення від початкового плану, та можливості стабілізації положення.

Стандарт PRINCE2 був застосований для контролю процесу та призначення відповідальних осіб (табл. 3). Даний підхід більше підходить малим суднам або портам через меншу кількість дій і необхідного документування.

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

Таблиця 3

Процес (надається англійською, щоб показати відповідність міжнародним стандартам)	**Опис реалізації в контексті реагування на кіберінциденти**
Starting Up a Project Ініціювання проєкту	Визначення проблеми (кіберзагроза), погодження цілей реагування, формування ініціативи.
Initiating a Project Запуск проєкту	Створення плану реагування, визначення обов'язків, розподіл ресурсів.
Directing a Project Управління проєктом	Затвердження дій вищим керівництвом: судновласником, Project Board.
Controlling a Stage Контроль етапу	Координація етапів реагування: виявлення, реагування, відновлення.
Managing Product Delivery Управління виконанням	Технічне впровадження заходів, навчання екіпажу, застосування систем.
Managing Stage Boundaries Управління переходами між етапами	Оцінка результатів, ухвалення рішень щодо продовження або зміни стратегії.
Closing a Project Закриття проєкту	Аналіз ефективності дій, документування висновків, оновлення планів реагування.
Organizational structure Організаційна структура	Executive (капітан), Project Board (судновласник), Team Manager (офіцер з безпеки).
Risk management Управління ризиками	Створення реєстру ризиків: фішинг, GPS-спуфінг, зловмисне ПЗ, вразливості в навігації.
Lessons and conclusions Уроки й висновки	Аналіз кожного інциденту з метою вдосконалення практики, оновлення навчання персоналу.

Основні результати дослідження

З 1 січня 2021 р. згідно з вимогами IMO (International Maritime Organization) усі судна мають інтегрувати питання кібербезпеки в систему управління безпекою (ISM Code). Також актуальними є стандарти [10; 11; 18]:

– ISO/IEC 27001 – система управління інформаційною безпекою;

– ISO/IEC 27035 – управління інцидентами інформаційної безпеки;

– NIST Cybersecurity Framework – посібник з побудови кіберзахисту.

Дотримання цих стандартів дозволяє не лише забезпечити базовий рівень кіберзахисту, але й покращити репутацію компанії, підвищити довіру клієнтів і страхових агентств. PMBOK забезпечує гнучкий підхід, що дозволяє адаптувати процеси щодо запобігання кіберзагрозам до специфіки суднових систем, як-от сучасна концепція E-Navigation та ECDIS, а також до потреб екіпажу. PRINCE2 сприяє чіткому розподілу ролей і контролю етапів, що особливо корисно для координації між судновласниками, екіпажем і зовнішніми сторонами. Запропонований авторами даної статті План реагування на кіберінциденти та ризик-реєстри знижують вразливість до кібератак у судноплавній галузі. Як подальший розвиток пропонуються регулярні аудити, симуляції та навчання з метою підвищення готовності до інцидентів, а також післяінцидентний аналіз, який сприятиме вдосконаленню систем кібербезпеки.

Серед основних методів і підходів до управління кібербезпекою варто виділити:

– ризик-орієнтований підхід до оцінювання загроз;

– проведення регулярних аудитів інформаційної безпеки;

– створення центру моніторингу безпеки (SOC) у великих портах;

– упровадження міжвідомчої взаємодії, зокрема зі спецслужбами, кіберполіцією;

– проведення навчань екіпажів і операторів портів щодо реагування на інциденти.

Також велику роль відіграє міжнародна кооперація: кіберзлочинність не має кордонів, тому ефективне реагування можливе лише за умови спільних дій. Тобто гарантування кібербезпеки не має обмежуватися лише ІТ-відділом. Необхідні:

– міжвідомче співробітництво між морськими адміністраціями, службами безпеки, військово-морськими силами;

– правове регулювання: гармонізація з нормами ЄС, IMO, національне законодавство;

– інвестиції в персонал: навчання екіпажу, проведення симуляцій, сертифікації;

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

– інформаційний обмін: участь у глобальних ініціативах, як-от Maritime ISAC, обмін кейсами атак і контрзаходів.

Оцінювання ефективності запропонованої моделі:

– здійснюється шляхом експертного опитування та сценарного моделювання можливих інцидентів під час викладання освітньої компоненти Кібербезпека суднових комп'ютерних систем та мереж;

– методологія спрямована на практичну реалізацію та враховує специфіку галузі – складність інформаційних систем, розподіленість інфраструктури та високі вимоги до безпеки;

– інтегрування обох методологій для комплексного підходу, PMBOK для процесів, а PRINCE2 для структуризації ролей, дозволить покращити якість підготовки здобувачів вищої освіти, наприклад Херсонської державної морської академії, у якій уже впроваджується цей проєкт, упродовж вивчення освітньої компоненти Радіонавігаційні прилади і системи. Імерсійні технології (VR/AR) також матимуть позитивний ефект на навчання майбутніх судноводіїв у рамках запропонованих методологій. Отже, ці методології дозволяють системно підійти до управління кібербезпекою судноводіння, забезпечують стійкість до загроз і ефективну координацію всіх учасників процесу.

Упровадження проєкту в систему підготовки плавскладу морських суден можна здійснити так: по-перше, залученням до проєкту студентів заочної форми навчання морських навчальних закладів, які зазвичай є вже моряками-практиками – судноводіями, механіками, електромеханіками; по-друге, шляхом домовленостей з морськими компаніями, такими, наприклад, як Marlow Navigation, які опікуються відповідними навчальними закладами.

Зауважимо, що будь-яка програма дій у такій сфері, як кібербезпека, має регулярно оновлюватися та проходити тестування, щоб ураховувати нові методи й цілі кібератак, покращувати як окремі кроки алгоритму, так і весь процес загалом, виявляти будь-які недоліки та визначати дії з ліквідації наслідків кіберінцидентів.

Наступна схема наочно представляє план дій із гарантування кібербезпеки судна (рис. 2).

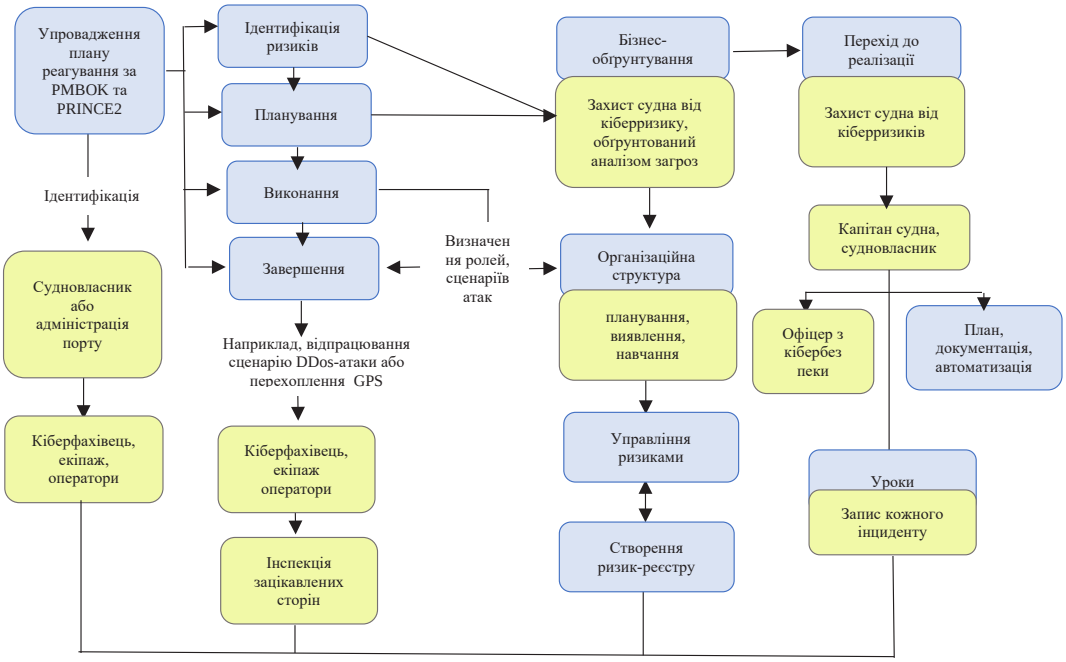

Рис. 2. Модель плану реагування на кіберінциденти

Висновки

Інтегровані системи управління на містках суден є складними комплексами, що об'єднують навігаційні, комунікаційні та керівні системи для гарантування безпеки й ефективності

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

судноводіння. Оскільки ці системи дедалі більше покладаються на цифрові технології, автоматизацію та підключення до мереж, вони стають вразливими до кіберзагроз. Заходи кібербезпеки для IBS мають бути спрямовані на захист від несанкціонованого доступу, атак, збоїв, на забезпечення надійного функціонування.

Упровадження принципу «кібербезпека за дизайном» (Cybersecurity by Design) під час розроблення нових IBS дозволить передбачити захист від кіберзагроз на всіх етапах життєвого циклу системи. Із цією метою корисним буде також використання безпечних промислових протоколів, наприклад IEC 61162-460, для зв'язку між підсистемами IBS [12]. Перевірка ланцюгів постачання є одним із головних заходів кібербезпеки, бо необхідна впевненість, що постачальники обладнання та спеціалізованого програмного забезпечення для IBS дотримуються відповідних стандартів кібербезпеки, як-от ISO / IEC 27001 «Стандарт управління інформаційною безпекою» [10; 11]. Нагальною необхідністю є укладання угод, що зобов'язують постачальників надавати оновлення безпеки та підтримку, комунікації IBS із береговими центрами, що потребує захищених каналів зв'язку й обмеження віддаленого доступу.

Кібербезпека в морській індустрії нині – не опція, а необхідність. Без адекватного захисту кіберпростору морські перевезення та порти можуть стати вразливими до загроз, що виходять за рамки фінансових збитків. Інтеграція планів реагування із системою безпеки підприємства, використання сучасних підходів до управління та постійне навчання персоналу є запорукою кіберстійкості галузі.

Розроблення ефективного плану реагування на інциденти – ключова умова стійкості до загроз. Розгляд такого плану як проєкту, із чітким управлінням, дозволяє досягти більшої узгодженості, ефективності й адаптивності. Упровадження міжнародних стандартів, тестування сценаріїв і гнучке управління процесами – усе це формує фундамент кіберстійкості морського сектору.

Кібербезпека IBS потребує комплексного підходу, що поєднує технічні заходи, організаційні політики та навчання екіпажу. Регулярний аудит, сегментація мереж, шифрування, контроль доступу та відповідність стандартам є основою для захисту суднових систем від кіберзагроз. Постійне оновлення знань і технологій допоможе убезпечити судна в умовах зростання цифровізації морської галузі.

Список використаної літератури

1. Akpan F., Bendiab G., Shiaeles S., Karamperidis S., Michaloliakos M. Cybersecurity Challenges in the Maritime Sector. *Network.* 2022. № 2 (1). P. 123–138. https://doi.org/10.3390/network2010009
2. A Primer on IMO Cyber Risk Management Guidelines. URL: https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf
3. Alcaide J.I., Llave R.G. Critical infrastructures cybersecurity and the maritime sector. *Transp. Res. Procedia.* 2020. № 45. P. 547–554. https://doi.org/10.1016/j.trpro.2020.03.058
4. C´elic´ J., Vukšic´ M., Baždaric´ R., Cuculic´ A. The Challenges of Cyber Resilience in the Maritime Sector. *Addressing the Weak Awareness of the Dangers Caused by Cyber Threats.* 2025. Vol. 13. P. 762. https://doi.org/10.3390/jmse13040762
5. Complying with the IMO 2021. URL: https://www.missionsecure.com/regulation-overview-imo-2021-cyber-risk-management-compliance
6. Macdonald F. The lifecycle dilemma Navigating cybersecurity risks across designing, constructing and operating a vessel. *Thetius, CyberOwl, and HFW.* 2025. URL: https://thetius.com/wp-content/uploads/2025/03/Thetius-CyberOwl-HFW-The-Lifecycle-Dilemma.pdf
7. Kessler G.C., Shepard S.D. Maritime Cybersecurity. Independently published, 2020. 270 p.
8. Guidelines on Cyber Security Onboard Ships. 2021. URL: https://www.bimco.org/products/publications/titles/the-guidelines-on-cyber-security-nboard-ships/

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

9. Hopkinson S. Navigation: Learn How to Navigate at Sea Paperback (4th ed.). England : Fernhurst Books Limited, 2023. 96 p.
10. International standard. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Ed. 3 (ISO/IEC 27001:2022). 2022. URL: https://www.iso.org/standard/27001
11. International standard. Information technology – Information security incident management. Ed. 2 (ISO/IEC 27035-1:2023). 2023. URL: https://www.iso.org/standard/78973.html
12. International standard. Maritime navigation and radiocommunication equipment and systems. Ed. 3 (IEC 61162-460), 2024. URL: https://cdn.standards.iteh.ai/samples/108137/f09eb4a33df343f6aee8acb807227f16/IEC-61162-460-2024.pdf.
13. International standard. SOLAS Consolidated Edition. London : International Maritime Organization Publications, 2020. 574 p.
14. International standard. STCW Including 2010 Manila Amendments. London : International.
15. Kaminska N., Kravtsova L., Kravtsov H., Zaytseva T. Modeling ship cyber-security using Markov chains: an educational approach. *Proceedings of the 11th Workshop on Cloud Technologies in Education.* 2023. Vol. 3679. P. 22–35. URL: http://ceur-ws.org/
16. Kavallieratos G., Katsikas S., Gkioulos V. Cyberattacks Against the Autonomous Ship. *In Computer Security: Springer*. Berlin ; Heidelberg, Germany, 2023. P. 20–36.
17. Кочерєв О. С. Система дипломування судноводіїв у галузі морського, зокрема річкового, судноплавства України. *Південноукраїнський правничий часопис*. 2021. № 3 (1). P. 77–81. DOI https://doi.org/10.32850/sulj.2021.3.1.13.
18. NIST Cybersecurity Framework : посібник з побудови кіберзахисту. URL: https://www.nist.gov/cyberframework
19. Systems Hardening. URL: https://www.beyondtrust.com/resources/glossary/systems-hardening
20. Горбов В., Ратушняк І., Горбова Г. Стандарти компетентності персоналу морських суден та захисту його прав. Миколаїв : НУК, 2023. 180 с.
21. Корнієнко О. Тенденції цифрових технологій у морському менеджменті. *Економіка та управління національним господарством.* 2023. № 81. С. 51–56. https://doi.org/10.32782/2521-666X/2023-81-6
22. Кравцова Л., Зайцева Т., Камінська Н. Марковські процеси в дослідженні ймовірності кібератак на морському судні. *Information Technologies in Education (ITE).* 2023. № 3 (52). С. 20–32. https://doi.org/10.14308/ite000763

References

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 [in English].
2. A Primer on IMO Cyber Risk Management Guidelines. Retrieved from: https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf [in English].
3. Alcaide, J.I., & Llave, R.G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transp. Res. Procedia*, 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058 [in English].
4. C´elic´, J., Vukšic´, M., Baždaric´, R., & Cuculic´, A. (2025). The Challenges of Cyber Resilience in the Maritime Sector: Addressing the Weak Awareness of the Dangers Caused by Cyber Threats. https://doi.org/10.3390/jmse13040762 [in English].
5. Complying with the IMO 2021. Retrieved from: https://www.missionsecure.com/regulation-overview-imo-2021-cyber-risk-management-compliance [in English].
6. Macdonald, F. (2025). The lifecycle dilemma Navigating cybersecurity risks across designing, constructing and operating a vessel. Thetius, CyberOwl, and HFW. Retrieved from:

https://thetius.com/wp-content/uploads/2025/03/Thetius-CyberOwl-HFW-The-Lifecycle-Dilemma.pdf [in English].
7. Kessler, G.C., & Shepard, S.D. (2020). Maritime Cybersecurity. Independently published. 270 p. [in English].
8. Guidelines on Cyber Security Onboard Ships. 2021. Retrieved from: https://www.bimco.org/products/publications/titles/the-guidelines-on-cyber-security-onboard-ships/ [in English].
9. Hopkinson, S. (2024). Navigation: Learn How to Navigate at Sea Paperback. Fernhurst Books Limited [in English].
10. International standard (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC № 27001:2022). Retrieved from: https://www.iso.org/standard/27001 [in English].
11. International standard (2023). Information technology – Information security incident management (ISO/IEC Standard № 27035-1:2023). Retrieved from: https://www.iso.org/standard/78973.html [in English].
12. International standard (2024). Maritime navigation and radiocommunication equipment and systems (IEC 61162-460). Retrieved from: https://cdn.standards.iteh.ai/samples/108137/f09eb4a33df343f6aee8acb807227f16/IEC-61162-460-2024.pdf [in English].
13. International standard (2020). SOLAS Consolidated Edition. London: International Maritime Organization Publications NIST Cybersecurity Framework – Cybersecurity building guide.
14. International standard (2017). STCW Including 2010 Manila Amendments. London: International Maritime Organization Publications [in English].
15. Kaminska, N., Kravtsova, L., Kravtsov, H., & Zaytseva, T. (2023). Modeling ship cyber-security using Markov chains: an educational approach. *Proceedings of the 11th Workshop on Cloud Technologies in Education* (CTE 2023), 3679, 22–35 [in English].
16. Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2023). Cyberattacks Against the Autonomous Ship. In *Computer Security*. Springer: Berlin/Heidelberg, Germany. 20–36 [in English].
17. Kocheriev, O.S. (2021). Systema dyplomuvannia sudnovodiiv u haluzi morskoho, zokrema richkovoho, sudnoplavstva Ukrainy [The system of certification of shipmasters in the field of maritime, in particular river, shipping of Ukraine]. *Pivdennoukrainskyi pravnychyi chasopys*, 3 (1), 77–81. https://doi.org/10.32850/sulj.2021.3.1.13 [in Ukrainian].
18. NIST Cybersecurity Framework – Cybersecurity building guide (2024). Retrieved from: https://www.nist.gov/cyberframework [in English].
19. Systems Hardening. Retrieved from: https://www.beyondtrust.com/resources/glossary/systems-hardening [in English].
20. 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].
21. Korniienko, O. (2023). Tendentsii tsyfrovykh tekhnolohii u morskomu menedzhmenti [Trends of digital technologies in maritime management]. *Ekonomika ta upravlinnya natsional'nym hospodarstvom – Economics and management of the national economy,* 81, 51–56. https://doi.org/10.32782/2521-666X/2023-81-6 [in Ukrainian].
22. Kravtsova, L., Zaitseva, T., & Kaminska, N. (2023). Markovski protsesy v doslidzhenni ymovirnosti kiberatak na morskomu sudni [Markov processes in the study of the probability of cyberattacks on a marine vessel]. *Information Technologies in Education* (ITE), 3 (52), 20–32. DOI: 10.14308/ite000763 [in Ukrainian].

Зайцева Тетяна Василівна – к.пед.н., доцент, доцент кафедри суднових комп'ютерних систем та мереж Херсонської державної морської академії. E-mail: zaytseva1966sunny@gmail.com, ORCID: 0000-0001-6780-719X.

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6

Безбах Олег Михайлович – к.т.н., доцент кафедри суднових комп'ютерних систем та мереж Херсонської державної морської академії. E-mail: ombezb@gmail.com, ORCID: 0000-0003-1030-7586.

Камінська Наталія Геннадіївна – викладач кафедри суднових комп'ютерних систем та мереж Херсонської державної морської академії. E-mail: kam_natali @gmail.com, ORCID: 0000-0002-9975-7403.

Zaytseva Tatyana Vasylivna – Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Shipboard Computer Systems and Networks of the Kherson State Maritime Academy. E-mail: zaytseva1966sunny@gmail.com, ORCID: 0000-0001-6780-719X.

Bezbakh Oleh Mykhailovych – Candidate of Technical Sciences, Associate Professor at the Department of Shipboard Computer Systems and Networks of the Kherson State Maritime Academy. E-mail: ombezb@gmail.com, ORCID: 0000-0003-1030-7586.

Kaminskaya Natalia Hennadiivna – Lecturer at the Department of Shipboard Computer Systems and Networks of the 6Kherson State Maritime Academy. E-mail: kam_natali @gmail.com, ORCID: 0000-0002-9975-7403.

https://doi.org/10.32782/mathematical-modelling/2025-8-1-6