Section: Information Technology, Cyber Security and Computer Engineering

УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ В МОРСЬКІЙ ГАЛУЗІ КРІЗЬ ПРИЗМУ ТЕХНОЛОГІЙ ПРОЄКТНОГО МЕНЕДЖМЕНТУ

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

У сучасному світі морська інфраструктура має критичне значення для забезпечення глобальної торгівлі, оборони та міжнародного співробітництва. Проте стрімке впровадження цифрових технологій у морському секторі призводить до зростання кіберзагроз. Розвиток інформаційних систем, автоматизації, електронної навігації, мережевого зв'язку, систем дистанційного управління та цифрового обміну даними відкриває нові можливості для підвищення ефективності та безпеки морських операцій. Водночас ці ж інновації створюють потенційні вектори для кібератак, які можуть мати серйозні наслідки для економіки та безпеки національного й міжнародного рівня.

Актуальність теми дослідження обумовлена необхідністю комплексного підходу до забезпечення кіберзахисту морської інфраструктури. Зокрема, актуальним є питання формування системи кібербезпеки судна, яка включає організацію технічного захисту, навчання персоналу, алгоритми реагування на інциденти та плани відновлення. Кібербезпека охоплює не лише захист від несанкціонованого доступу до систем, а й забезпечення цілісності, доступності та стійкості цифрових сервісів. Судновласники, оператори, екіпаж і портовий персонал повинні усвідомлювати значення цифрової безпеки та бути готовими до реагування на загрози.

Оскільки ефективне реагування вимагає не лише технічних засобів, але й структурованої організації процесу, все більшої актуальності набуває застосування підходів з управління проєктами. Використання сучасних методик, таких як BPMN, дозволяє візуалізувати й формалізувати процеси реагування, визначити ролі та відповідальність учасників, забезпечити контроль та гнучке управління у випадку інцидентів.

Огляд літератури. Останніми роками науковці й фахівці в галузі морського транспорту та інформаційної безпеки звертають дедалі більшу увагу на питання кіберзахисту в морському середовищі. Згідно зі стандартами Міжнародної морської організації IMO [1, 2, 3], впровадження кібербезпеки є обов'язковим елементом системи управління безпекою судна (ISM Code). У звітах таких

організацій, як BIMCO та ENISA, наголошується на необхідності розвитку стратегій цифрової безпеки на рівні компаній та портів.

Дослідження [4, 5, 6] вказують на зростання кількості інцидентів у морській галузі, зокрема на системах навігації, контейнерного управління та автоматизації. Автори пропонують запровадження структурованих підходів до оцінки ризиків та інцидент-менеджменту. Водночас у працях [7] обговорюється необхідність інтеграції методів управління проєктами, таких як PMBOK і PRINCE2, для побудови ефективних планів реагування та підвищення стійкості систем.

Таким чином, актуальність дослідження обумовлюється наявністю реальних загроз, необхідністю узгодженого управління кіберінцидентами та використанням сучасних проєктних підходів для побудови ефективної системи реагування

Постановка задачі. Відповідно до резолюції MSC.428(98) Міжнародної морської організації (IMO), усі судна та оператори повинні інтегрувати кіберризики до існуючих систем управління безпекою. Це означає не лише технологічні рішення, а й процедурні, організаційні та управлінські заходи та постійне навчання або тренінг персоналу. В основі цих заходів лежить план реагування. Він повинен поєднати всі відомі на сьогодні засоби кіберзахисту та запропонувати як керівництву судноплавних компаній, так і екіпажам морських суден чіткий й зрозумілий план дій.

Серйозність кіберзагроз ілюструє низка інцидентів останніх років, зокрема атака на Maersk у 2017 році, яка завдала збитків на сотні мільйонів доларів. У 2021 році порт Х'юстона в США став жертвою цільової атаки з використанням уразливостей у системах SCADA. Збільшення атак на українські морські об’єкти після початку повномасштабної війни також свідчить про стратегічну роль кібербезпеки у конфліктних регіонах.

У відповідь на зростаючу загрозу постає потреба у створенні ефективних систем реагування на кіберінциденти. В 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. Розробити ефективний план реагування на кіберінциденти із застосуванням сучасних технологій управління проектами для підвищення рівня кібербезпеки судноплавства та з врахуванням особливостей об’єкта захисту.

Практичне значення. Розроблений план реагування може бути адаптований:

- судноплавними компаніями для підвищення кіберстійкості;
- портовими адміністраціями для оптимізації дій під час інцидентів;
- для навчання екіпажів та IT-персоналу згідно з вимогами ISM Code.

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 вирішення цієї проблеми.

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

Ключові елементи такого плану включають:

- класифікацію інцидентів за рівнем критичності;
- процедури виявлення, фіксації та ескалації інциденту;
- визначення відповідальних осіб та команд;
- порядок інформування керівництва, екіпажу, партнерів;
- юридичні аспекти, включаючи звітування до державних органів;
- післяінцидентний аналіз та оновлення політик.

Розробка плану реагування має розглядатись як окремий проєкт, що дозволяє структурувати процес та ефективно управляти ресурсами. Системний підхід до планування, реалізації та контролю таких ініціатив базується на принципах класичного проєктного менеджменту (PMBOK) або гнучких методологіях (Agile/Scrum). Такий підхід дозволяє розглядати план реагування не як статичний документ, а як живу систему, що постійно вдосконалюється відповідно до змін у середовищі загроз.

Основні результати дослідження:

Застосування методології BPMN (Business Process Model and Notation) дозволяє чітко візуалізувати послідовність дій та взаємодію між учасниками процесу реагування на інциденти. BPMN є стандартом моделювання бізнес-процесів, який використовується для створення графічних схем, що відображають логіку та структуру операцій. Це особливо корисно у складних ситуаціях, таких як кіберінциденти на суднах або в портах, де важливо узгодити дії різних команд: навігаційної, IT, кібербезпеки та зовнішніх служб. За допомогою BPMN можливо структурувати процес виявлення інциденту до його вирішення, включаючи етапи комунікації, аналізу ризиків, мобілізації підтримки. Такий підхід забезпечує прозорість, керованість і відтворюваність дій, що критично важливо для морських операцій.

Основні компоненти моделі:

1. Пул (Pool): Визначає ключовий об’єкт (судно або порт). Якщо потрібно моделювати взаємодію, наприклад, інтерфейс судно-судно або судно-порт, тоді додаємо до моделі окремий пул для кожного об’єкту.

2. Лейни (Lane): Відображають команди або підрозділи, наприклад, група реагування на кіберінциденти, IT-відділ, офіцери з кібербезпеки чи адміністрація.

3. Події (Events): Початкові та кінцеві маркери, такі як виявлення атаки (Start Event), сигнал тривоги (Intermediate Event), інцидент завершено (End Event).

4. Задачі (Task), які потребують не тільки обов'язкового виконання, а й визначенної послідовності дій: виявлення загрози (автоматизовано або вручну) → повідомлення ключовим особам → ізоляція скомпрометованого елементу системи → відновлення або активування резервів → аналіз події та звіт.

При побудові моделі ми враховували тип судна, щоб моделі мали змогу адаптуватися чи то до танкера, наприклад, чи то до яхти тощо. Ми враховували логіку реагування, наприклад, для малих суден використовуються лише базові засоби захисту (антивірус, брандмауер, ручне резервне копіювання). Якщо створювати модель плану реагування для портів, то тут повинні з'явитися додаткові зовнішні ролі - митниця, провайдери IT, оператори зв'язку.

Особливості реалізації процесів реагування на кіберінциденти значно залежать від типу судна або порту. У великих морських суднах та портах зазвичай застосовуються комплексні системи кібербезпеки з розвиненою інфраструктурою, тоді як у малих — переважають спрощені процедури з мінімальним технічним забезпеченням.

Висновки

Без адекватного захисту кіберпростору морські перевезення та порти можуть стати вразливими до загроз, що виходять за рамки фінансових збитків. Інтеграція планів реагування в систему безпеки об'єкту, використання сучасних підходів до управління та постійне навчання персоналу є запорукою кіберстійкості будь-якої галузі. Розробка ефективного плану реагування на інциденти — ключова умова стійкості до загроз. Розгляд такого плану як проєкту, з чітким управлінням, дозволяє досягти більшої узгодженості, ефективності та адаптивності. Впровадження міжнародних стандартів, тестування сценаріїв та гнучке управління процесами — усе це формує фундамент кіберстійкості морського сектору.

У морському середовищі реагування на кіберінциденти має враховувати тип судна, склад екіпажу, наявність IT-інфраструктури, а також взаємодію з портовими службами. Для великих суден актуальною є гнучка система ролей, чітко окреслені обов'язки й висока автоматизація. Натомість малі судна потребують спрощених моделей реагування, зручних для застосування непрофільним персоналом. Крім того, порти як важливі логістичні вузли вимагають окремого врахування зовнішніх учасників — митниці, IT-команд провайдерів тощо.

BPMN (Business Process Model and Notation) забезпечує зручний графічний інструмент для моделювання бізнес-процесів, зокрема — процесів реагування на

кіберінциденти в морській галузі. Його використання дозволяє чітко візуалізувати послідовність дій, залучених осіб і відповідальність кожного етапу.

Список використаних джерел

1. Model Course 7.03: Officer in Charge of a Navigational Watch. - London: International Maritime Organization Publications, 1999. - 248 p.
2. Model Course 1.07: Radar Navigation at Operational Level. - London: International Maritime Organization Publications, 2017. - 232 p.
3. Model Course 7.08. Electro-Technical Officer. London: International Maritime Organization, 2014. - 190 p.
4. Akpan F. Cybersecurity Challenges in the Maritime Sector / F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos // Network. - 2022. - № 2(1), P. 123–138. https://doi.org/10.3390/network2010009.
5. Alcaide J.I. Critical infrastructures cybersecurity and the maritime sector / J.I. Alcaide, R.G. Llave // Transp. Res. Procedia. – 2020. – №45. – P. 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.
6. Корнієнко О. Тенденції цифрових технологій у морському менеджменті / О. Корнієнко // Економіка та управління національним господарством. - 2023. - №81. - С. 51–56. https://doi.org/10.32782/2521-666X/2023-81-6.
7. Matos S. Prince2 or PMBOK – A Question of Choice /Santa Matos, Eurico Lopes // Procedia Technology. – 2013. – V. 9. – P. 787-794. https://doi.org/10.1016/j.protcy.2013.12.087.

ПОБУДОВА ДВОРІВНЕВОЇ ТЕОРЕТИКО-ІГРОВОЇ МОДЕЛІ РОЗДРІБНОГО РИНКУ ЕЛЕКТРОЕНЕРГІЇ УКРАЇНИ У ПРОЦЕСІ УПРАВЛІННЯ ПОПИТОМ

Борукаєв Зелімхан Харитонович
доктор техн. наук, ст. наук. співр.
Інститут проблем моделювання в енергетиці
імені Г.Є.Пухова Національної академії наук України, Україна
Остапченко Костянтин Борисович
канд. техн. наук, доцент
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Україна

Анотація. Відомо, що багато країн активно займаються пошуком, розробкою та впровадженням механізмів участі розподілених енергетичних ресурсів споживачів у програмах розвитку електроенергетики з метою розбудови їх потенціалу та більш масштабного використання цього ресурсу, а також пошуком нових технічних рішень для автоматизації участі, в тому числі в рамках