УДК 004.056.5/946.5:656.61
DOI https://doi.org/10.32782/msd/2023.1.10

ПИТАННЯ ВДОСКОНАЛЕННЯ КІБЕРБЕЗПЕКИ МОРСЬКОГО ТРАНСПОРТУ: ЗАРУБІЖНИЙ ДОСВІД

Пядишев В. Г.
доктор юридичних наук, професор,
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
ORCID: 0000-0002-5174-1891

Анотація. *Аналіз сучасних вітчизняних публікацій показує, що хоча загальній організації безпеки морського транспорту в Україні приділяється значна увага, до такого нового важливого напряму, як кібербезпека морського транспорту, тут поки що не виявляється належного інтересу. Тому статтю присвячено закордонному досвіду щодо організації кібербезпеки морського судна.*

Твердження, що загальна небезпека морського транспорту останніми роками значно зростає, ґрунтується на фактах впровадження інформаційних технологій в операційні технології морського транспорту. Суть у тому, що інформаційні технології тісно пов'язані з Інтернетом, і саме це насамперед робить операційні технології морського транспорту відкритими для навмисного зовнішнього втручання, яке, за твердженням фахівців, може забезпечити зовнішнє керування судном з метою перекидання, зіткнення або заподіяння шкоди довкілля.

Загальне занепокоєння провідних морських держав ситуацією підтверджено низкою документів, таких як Резолюція комітету з морської безпеки MSC.428(98), що прийнята 16 червня 2017 р. і вимагає від держав-членів враховувати управління кіберризиками.

У роботі проаналізовано типовий підхід до розробки плану дій щодо організації морської кібербезпеки на борту судна. Розглянуто попередні кроки з підготовки, починаючи від оновлення паролів та програмного забезпечення та закінчуючи навчанням команди.

Вказано, що сьогодні у всьому світі безпосередню розробку такого плану рекомендується здійснювати на підставі «Посібника з кібербезпеки на борту суден», розробленого та підтримуваного провідними міжнародними організаціями, пов'язаними з операціями морського транспорту.

План, створюваний на підставі цього посібника, по суті полягає в управлінні кіберризиками і зводиться до такого: виявлення внутрішніх та зовнішніх загроз, внутрішніх та зовнішніх вразливостей; оцінки схильності до ризику; розроблення заходів щодо зменшення зазначених вразливостей; розроблення планів на випадок непередбачених обставин; розроблення планів заходів щодо відновлення після кіберінцидентів.

Необхідним елементом забезпечення кібербезпеки на морському транспорті вважається загальний підйом культури персоналу до сучасного рівня.

Ключові слова: *морський транспорт, кібербезпека, кіберзагрози, кібератакі, кіберризики, вразливості, заходи виявлення і захисту.*

Piadyshev V. H. THE ISSUES OF ENHANCEMENT OF MARITIME TRANSPORT CYBERSECURITY: FOREIGN EXPERIENCE

Abstract. *An analysis of modern national publications shows that, although in Ukraine considerable attention is being payed to the general organization of maritime transport security, the due interest has not yet been shown to the new important area, such as the maritime transport cybersecurity.*

Therefore, the article touches upon the best practices in organizing the cybersecurity of marine ships.

The assertion that the general danger of maritime transport has increased significantly in recent years is based on the facts of the introduction of information technology into the operational technologies of maritime transport. The bottom line is that information technology is closely linked to the Internet, and this is what, in the first place, makes the operational technologies of maritime transport open to deliberate external interference, which, according to experts, can provide external control of the vessel with the aim of capsizing, colliding or causing environment disaster.

The general concern of the leading maritime states about the situation is confirmed by a number of documents, such as Resolution of the Maritime Security Committee MSC.428 (98), adopted on June 16, 2017 and requiring member states to take into account the management of cyber risks.

The paper analyzes a typical approach to the development of an action plan for the organization of maritime cybersecurity on board a ship. The preliminary preparation steps are considered, ranging from updating passwords and software to training the team.

It is indicated that today, all over the world, the direct development of such a plan is recommended to be carried out on the basis of the "The Guidelines on Cyber Security onboard Ships", developed and supported by leading international organizations related to maritime transport operations.

The plan created on the basis of this guide, in essence, is to manage cyber risks and boils down to the following: identifying internal and external threats, internal and external vulnerabilities; risk exposure assessment; development of measures to reduce these vulnerabilities; developing contingency plans; developing plans for recovery measures after cyber incidents.

The general rise in the culture of personnel to a modern level is a necessary element of ensuring cybersecurity in maritime transport.

Key words: *maritime transport, cyber security, cyber threats, cyber attacks, cyber risks, vulnerabilities, detection and protection measures.*

Вступ. Морські кібератаки є додатковою складністю порівняно з традиційними морськими загрозами, такими як піратство, незаконна діяльність, морський тероризм та аварії на морі. Глобальний морський сектор стає все більш цифровим, автоматизованим та взаємопов'язаним. Разом з цим приходить безліч кіберзагроз, кількість яких останніми роками значно зросла. Наприклад, кількість кібератак на берегові морські системи за останні кілька років зросла дев'ять разів. Україна є потужною морською державою, і все перелічене стосується її повною мірою.

Фахівці зазначили, що в управління кіберризиками морських компаній є суттєві прогалини, що створює небезпеку для ланцюгів постачання. Дослідники ретельно опитали понад 200 представників галузі та дійшли до висновку, що після вторгнення Росії в Україну питання кібербезпеки стали ще більш актуальними, оскільки атаки хакерів посилилися [1, с. 1]. Власники морських суден виплачують хакерам у середньому понад 3 млн. доларів викупу за припинення кібератаки та повернення контролю над власною цифровою системою. Близько 1000 морських суден постраждали в результаті атаки ransomware на компанію DNV [2, с. 23].

Можна стверджувати, що в Україні ведеться напружена наукова робота з розробки питань кібербезпеки. Але у фундаментальних роботах цього напряму питання кібербезпеки безпосередньо на морському транспорті тільки-но згадуються. Отже, роботу Ю. П. Лісовської «Кібербезпека: ризики та заходи» присвячено загальним питанням кібербезпеки як інноваційної системи віртуальності сучасного інформаційного простору. Автор навіть передбачає аерокосмічний тероризм. Але питанням організації кібербезпеки безпосередньо морського транспорту уваги не приділяється [3, с. 5]. У роботі В.Л. Бурячка, В.Б. Толубка, В.О. Хорошка, С.В. Толюпи «Інформаційна та кібербезпека: соціотехнічний аспект» морський транспорт згадується лише як одна зі сфер, де необхідно застосування кібербезпеки, без визначення її специфіки та конкретних заходів [4, с. 9, 67]. У сучасний монографії «Кібербезпека та інформаційні технології» «море» згадується лише у сенсі «е-Навігації» та не у плані захисту її від кібератак, але у сенсі «переходу е-Навігації зі стадії тестових перевірок в аспект впровадження» [5, с. 176]. У роботі В. А. Лахна «Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту» проводяться загальні фундаментальні дослідження, щодо підвищення кібербезпеки інформаційно-комунікаційних систем транспорту, але немає належної спеціалізації щодо проблем на морських суднах [6, с. 44 48].

Між тим морський транспорт, який донедавна вважався найбільш зручним та безпечним, сьогодні перестає бути таким: кіберпроникнення та подальше управління комерційним судном для перекидання, зіткнення або заподіяння шкоди навколишньому середовищу тепер цілком можливі. Це викликало потужну реакцію у науці розвинених морських держав. Саме через це вважаємо за доцільне ознайомитись з відповідним зарубіжним досвідом.

Матеріали.

Наскільки серйозною є проблема морської кібербезпеки?

Основними загальними мотивами кібератак на морі є отримання віддаленого контролю над кораблями та судами, крадіжка важливої та конфіденційної інформації, яка може бути використана для проведення подальших

атак або для порушення роботи корабля шляхом пошкодження важливих компонентів та виключення з роботи автоматизованих систем. Фактично більшість ІТ-систем на сучасних суднах небезпечні і вразливі для атак вже тому, що вони вважаються менш важливими для безпеки і продуктивності [7, с. 2].

Барометр ризиків. Кібербезпека на морі – це проблема, яка, незважаючи на зростаючу увагу, як і раніше, викликає серйозне занепокоєння. Величезний масштаб проблеми було наголошено у новому гучному звіті, в якому підкреслено витрати та потенційний вплив на репутацію та здатність працювати. Відповідно до звіту «Барометр ризиків» за 2019 рік від Allianz [8, с. 2] серед безлічі проблем, з якими стикаються компанії, кібербезпека сьогодні вважається найбільш неприємною.

Завдяки численним повідомленням у засобах масової інформації про вплив кібератак на низку відомих судноплавних компаній і портів по всьому світу стає все очевиднішим, що морська сфера не застрахована від атак.

Вказане вище видання називає кіберризик «основною проблемою для бізнесу в 2019 році і надалі», і це, можливо, посилюється для судноплавства. Так, у 2019 році кіберінциденти викликали побоювання, а збої роботи стали головним ризиком для корпорацій у всьому світі.

У глобально взаємопов'язаній економіці потенційні сценарії збоїв роботи стають все більш різноманітними та складними. До них відносяться поломка основних ІТ-систем, проблеми з якістю, тероризм, політичні заворушення та забруднення довкілля. Вони неминуче включають елемент кібербезпеки, оскільки ризики стають все більш взаємопов'язаними.

Зростання кіберризиків. Атаки програм-вимагачів або випадкові збої в роботі ІТ часто призводять до порушення роботи та служб, що коштує сотні мільйонів доларів. Рік 2018 вважається переломним роком кіберактивності [9, с. 12]. Морські кібератаки є додатковою складністю порівняно з традиційними морськими загрозами, такими як піратство, незаконна діяльність, морський тероризм та аварії на морі. Глобальний морський сектор стає все більш цифровим, автоматизованим та взаємопов'язаним. Разом з цим приходить безліч кіберзагроз, кількість яких останніми роками значно зросла. Наприклад, кількість кібератак на берегові морські системи за останні кілька років зросла в дев'ять разів, часто спостерігалися випадки спуфінгу GPS і AIS. Проникнення та подальше управління комерційним судном для перекидання, зіткнення або заподіяння шкоди навколишньому середовищу тепер цілком можливо [10, с. 2].

Наразі кіберзлочинність коштує приблизно 600 мільярдів доларів на рік – порівняно з 445 мільярдами доларів у 2014 році. Це можна порівняти із середніми економічними втратами від стихійних лих за 10 років у розмірі 208 мільярдів доларів. У той час як злочинці використовують більш інноваційні методи для крадіжки даних, здійснення шахрайства або здирництва коштів, також зростає кількість кіберзагроз, націлених на постачальників критично важливої інфраструктури, які крадуть цінні дані та/або комерційну таємницю у компаній [11, с. 3].

Крім того, кіберінциденти все частіше призводять до судових розглядів, у тому числі з цінних паперів та колективних позовів споживачів. У той час як витік даних або збої в роботі ІТ можуть спричинити великі зобов'язання перед третіми особами, постраждалі клієнти або акціонери прагнуть відшкодувати збитки від компаній. Вони навіть звертаються до урядів із закликами виявити компанії, які роблять недостатньо для свого захисту. Згідно з новим звітом, вчені Королівського коледжу Лондона закликали до розгортання кампанії, щоб назвати та присоромити компанії з поганою кібербезпекою. Вони вважають, що такий крок підвищить прозорість кіберзахисту підприємств та змусить неефективні компанії покращити свій захист, що призведе до зниження рівня злочинності.

Найбільші проблеми. Сьогодні про кіберинциденти та збої в роботі говорять з погляду великомасштабних атак чи проблем. Насправді ж атаки меншого масштабу можуть викликати найбільше проблем. За даними Ernst & Young (EY) [12, с. 2], фішингові кампанії за допомогою електронної пошти продовжують домінувати на світовій арені кіберзлочинності.

У той час як такі проблеми, як програмиздирники, видобуток криптовалюти та атаки, спонсовані державами, потрапляють у заголовки ЗМІ, найбільші проблеми викликають кібератаки нижчого рівня, і морська доставка аж ніяк не захищена. Організації всіх розмірів стають мішенню та успішно піддаються шахрайству за допомогою фішингових кампаній та компрометації корпоративної електронної пошти. Проблеми від фішингу слід розглядати як поєднання соціальної інженерії з поганою кібергігієною. Це стосується практик та кроків, які користувачі комп'ютерів та інших пристроїв мають робити для підтримки працездатності системи та підвищення безпеки в Інтернеті.

Інтегрованість та незахищеність. Сучасні корабельні системи високо інтегровані, але погано захищені. Це створює величезні потенційні ризики. Оскільки судна все більше покладаються на автоматизацію та віддалений моніторинг, ключові системи, включаючи навігаційне обладнання, можуть бути виведені з ладу у разі атаки чи ненавмисного завантаження вірусу.

У боротьбі з цим судноплавство зробило багато кроків, і на додаток до настанов Міжнародної морської організації (IMO) було випущено безліч настанов галузевих організацій, таких як BIMCO, Асоціація круїзних компаній (CLIA), Міжнародна палата судноплавства. Судноплавство (ICS), ІНТЕРКАРГО, ІНТЕРТАНКО, Міжнародний морський форум нафтових компаній (OCIMF) та Міжнародний союз морського страхування (IUMI).

Нещодавно до цього приєдналася нова стратегія Міністерства промисловості, бізнесу та фінансів Данії [13, с. 2] Цей державний орган запустив нову галузеву стратегію для суднoплавної галузі, яка містить кілька ініціатив, спрямованих на зміцнення IT-безпеки та запобігання кіберзагрозам у морському секторі. Мета стратегії – забезпечити, щоб безпека в данських водах і на борту данських суден не наражалася на ризик у результаті кібератак. Паралельно з цим Данське морське управління навіть створило спеціальний підрозділ Данської морської кібербезпеки для реалізації стратегії.

Пошук відповідей. Одним з особливо складних аспектів вирішення морських кіберпроблем є той факт, що морські правила щосили намагаються не відставати від швидкого темпу кіберзлочинів і загроз [14, с. 1]. Вони постійно розвиваються, і тому регулювання має супроводжуватись зміною мислення. Дійсно, поінформованість про кіберзагрози та способи їх пом'якшення життєво важлива і на борту суден, і в офісах на березі.

Незалежно від того, чи це доставлені людьми на борт їхні приватні проблемні гаджети (наприклад, дрони з пультами керування тощо), чи зловмисна кібератака, все це може поставити під загрозу навігаційну систему судна. У всіх таких умовах для забезпечення безпеки суден та всього логістичного ланцюжка поставок необхідні дії.

Реакція на ситуацію Комітету безпеки на морі (MSC). Оскільки підключення до Інтернету та залежність від нього в даний час є нормою для багатьох технологій, необхідних для експлуатації та управління суднами, безпека та надійність цих технологій мають першочергове значення. У зв'язку з цим морська галузь усвідомлює необхідність нагляду за кібербезпекою для забезпечення ефективного управління та пом'якшення кіберзагроз, що виникають. У своїй Резолюції MSC.428(98), ухваленій 16 червня 2017 р. [15, с. 1.], а саме, у додатку 10 (Управління морським кіберризиком у системах управління безпекою) Комітет з морської безпеки:

1. Підтверджує, що затверджена система управління безпекою в морі повинна враховувати управління кіберризиками відповідно до цілей та функціональних вимог Міжнародного кодексу з управління безпекою.

2. Закликає адміністрації забезпечити належний облік кіберризиків у системах управління безпекою не пізніше першої щорічної перевірки Документу про відповідність компанії після 1 січня 2021 року.

3. Визнає необхідні запобіжні заходи, які можуть знадобитися для збереження конфіденційності деяких аспектів управління кіберризиками.

4. Пропонує державам-членам довести цю резолюцію до всіх зацікавлених сторін.

Розробка плану дій щодо організації морської кібербезпеки на борту судна.

З чого почати?

Для складання плану дій з морської кібербезпеки знадобиться деякий час. Щоб прискорити результати своїх зусиль і встановити початковий базовий рівень кібербезпеки для суден, можна зробити кілька кроків у короткостроковій перспективі [16, с. 2–5].

Попередні кроки.

Розгляньте кожен пункт, щоб згодом викреслити його зі списку справ з морської кібербезпеки:

1. Оновіть пароль адміністратора на критично важливих системах та пристроях у мережі ОТ.

2. Регулярно оновлюйте свої паролі та по можливості використовуйте багатофакторну автентифікацію.

3. Переконайтеся, що критичні системи та пристрої недоступні через Інтернет.

4. Оновіть програмне забезпечення на критичних системах та пристроях

5. Захистіть порти USB на всіх суднових системах.

6. Сегментуйте свій місток, машинне відділення, екіпаж, Wi-Fi та ділові мережі на борту

7. Навчіть свою команду кібербезпеці

Початок роботи із планом дій.

При розробці плану безпеки на морі потрібно враховувати дуже багато. План повинен включати значний компонент кібербезпеки, щоб забезпечити безпеку ваших суден та морських операцій від зростаючого числа морських кіберзагроз. У міру того, як кораблі стають все більш складними в цифрову епоху, в той же час скорочуються екіпажі, а ресурсів, що виділяються на кібербезпеку, може не вистачати. Але кібербезпека не може бути другорядним завданням – вона має стати пріоритетним завданням на рівні ради директорів.

Приступаючи до ретельного планування кібербезпеки, доцільно використовувати підхід до управління кіберрисками, наведений у «Посібнику з кібербезпеки на борту суден», розробленому та підтримуваному BIMCO, Міжнародною асоціацією круїзних ліній (CLIA), Міжнародною палатою судноплавства (ICS), Міжнародною асоціацією (INTERCARGO), InterManager, INTERTANKO, Міжнародним союзом морського страхування (IUMI), Міжнародним морським форумом нафтових компаній (OCIMF) та Всесвітньою радою судноплавства (WSC) [17, с. 32]. Зазначена настанова консультує судновласників та операторів щодо процедур та дій щодо підтримки безпеки кіберсистем у їх організації та на борту їх суден.

Підхід до керування кіберрисками.

Виявити загрози. Виявити зовнішні загрози кібербезпеці для корабля.

Виявити внутрішню загрозу кібербезпеці, пов'язану з неналежним використанням та відсутністю обізнаності.

Виявити вразливості. Розробити перелік бортових систем із прямими та непрямими каналами зв'язку.

Зрозуміти наслідки загрози кібербезпеці цих систем.

Зрозуміти можливості та обмеження існуючих заходів захисту.

Оцінити схильність до ризику. Визначити можливість використання вразливостей зовнішніми загрозами.

Визначити можливість розкриття вразливостей при неналежному використанні.

Визначити вплив на безпеку та безпеку будь-якого окремого або комбінації вразливостей, що використовуються.

Розробити заходи захисту та виявлення. Зменшити ймовірність використання вразливостей за допомогою захисних заходів.

Зменшити потенційний вплив експлуатаційної вразливості.

Розробити плани на випадок непередбачених обставин. Розробите пріоритетний план на випадок непередбачених обставин, щоб знизити будь-який потенційний кіберриск.

Відреагувати та відновити. Реагуйте на інциденти кібербезпеки та відновлюйтесь після них, використовуючи план дій у надзвичайних ситуаціях.

Оцініть вплив ефективності плану реагування та повторно, більш детально, оцініть загрози та вразливості.

Виявити загрози. Кібер-ризик специфічний для компанії, корабля, операції та/або торгівлі. При оцінці ризику організації слід враховувати будь-які конкретні аспекти своєї діяль-

ності, які можуть підвищити їхню вразливість до кіберінцидентів.

Організації та приватні особи мають мотиви для використання кіберуразливостей. Існує ймовірність того, що персонал компанії на борту та на березі може поставити під загрозу кіберсистеми та дані [18, с. 2].

Загалом організація повинна усвідомлювати, що це може бути ненавмисним і викликано помилкою людини під час експлуатації та управління системами ІТ та операційними технологіями (ОТ) або недотриманням технічних та процедурних заходів захисту. Однак існує ймовірність того, що дії можуть бути зловмисними і являти собою навмисну спробу незадоволеного працівника завдати шкоди компанії або судну.

Виявити вразливості. Судноплавній компанії рекомендується здійснити оцінку потенційних загроз, з якими можна зіткнутися. Після має бути здійснена оцінка систем і бортових процедур для визначення їх стійкості до поточного рівня загроз. В результаті має вийти стратегія, орієнтована на ключові ризики.

Автономні системи будуть менш уразливими для зовнішніх кібератак у порівнянні з системами, підключеними до неконтрольованих мереж або безпосередньо до Інтернету. Слід з обережністю підійти до процесу з'ясування, якими чином критично важливі бортові системи можуть бути підключені до неконтрольованих мереж.

Оцінити схильність до ризику. Оцінка кіберрисків має починатися на рівні вищого керівництва компанії, а не одразу делегуватися офіцеру служби безпеки корабля або голові ІТ-відділу:

1. Ініціативи щодо підвищення кібербезпеки можуть також вплинути на стандартні бізнес-процедури та операції, роблячи їх більш трудомісткими та дорогими. Оцінка та ухвалення рішення про зниження ризику зазвичай стає рішенням на рівні вищого керівництва.

2. Деякі ініціативи, спрямовані на покращення управління кіберрисками, пов'язані з бізнес-процесами, навчанням, безпекою судна та навколишнім середовищем, а не з ІТ-системами, і мають бути організаційно закріплені за межами ІТ-відділу.

3. Ініціативи, спрямовані на підвищення обізнаності щодо кібербезпеки, можуть змінити спосіб взаємодії компанії з клієнтами, постачальниками і владою та накласти нові вимоги на співпрацю між сторонами. Рішення про те, чи слід і як стимулювати ці зміни у відносинах, приймається лише на рівні вищого керівництва.

Розробити заходи захисту та виявлення. Результатом оцінки ризику компанії та подальшої стратегії кібербезпеки має бути зниження ризику до розумно можливого низького рівня. На технічному рівні це буде включати необхідні дії, які мають бути реалізовані для встановлення та підтримання узгодженого рівня кібербезпеки. Вкрай важливо визначити, як керувати кібербезпекою на борту і делегувати обов'язки капітану, відповідальним співробітникам і, при необхідності, співробітнику служби безпеки компанії [19 , с. 27].

Розробити плани реагування на непередбачені обставини/інциденти. При розробці планів на випадок непередбачених обставин для реалізації на борту суден важливо розуміти значення будь-якого кіберінциденту та відповідним чином розставляти пріоритети у діях у відповідь.

Будь-який кіберінцидент повинен оцінюватися для оцінки впливу на операції, активи тощо. У більшості випадків, за винятком систем планування та управління навантаженням, втрата бортових ІТ-систем, включаючи витік конфіденційної інформації, буде проблемою безперервності бізнесу, але вона не повинна впливати на безпечну експлуатацію судна.

Вихід з ладу систем ОТ може мати суттєвий і безпосередній вплив на безпечну експлуатацію судна. Якщо кіберінцидент призведе до втрати або збою в роботі систем ОТ, важливо вжити ефективних дій для забезпечення безпосередньої безпеки екіпажу, судна, вантажу та захисту морського середовища. Команди повинні регулярно навчатись планам реагування. Ці плани повинні регулярно відпрацьовуватись екіпажами судів, офіцерами, а також керівництвом та персоналом ІТ-підтримки – аналогічно до навчань з реагування на загрози безпеці, які зазвичай проводяться сьогодні. Сторонні постачальники систем на борту суден повинні бути включені та зобов'язані

брати участь у цих заходах та плануванні реагування на непередбачені обставини/інциденти.

Реагувати на інциденти кібербезпеки та відновитись після них. Важливо розуміти, що кіберінциденти не можуть зникнути самі по собі Якщо, наприклад, система відображення карт та інформації про надзвичайні ситуації (ECDIS) була заражена шкідливим програмним забезпеченням, запуск резервної ECDIS може призвести до іншого кібер-інциденту. Тому рекомендується планувати, як проводити очищення та відновлення заражених систем.

Плани аварійного відновлення мають бути невід'ємною частиною будь-якого плану морської кібербезпеки [20, с. 15]. Вони передбачають збереження кіберданих для криміналістичних цілей на додаток до відновлення та захисту процесів ОТ та засобів управління судном. Ці плани також слід регулярно перевіряти та оновлювати при необхідності як у морі, так і на березі. Будь-які сторонні системні постачальники, з якими ви співпрацюєте, повинні бути включені та зобов'язані брати участь у плануванні та виконанні цих заходів щодо аварійного відновлення. Будь-які відомості, які ви отримуєте про раніше виявлені кіберінциденти, повинні використовуватися для покращення планів реагування всіх суден флоту вашої компанії, і вам слід продумати інформаційну стратегію для таких інцидентів.

Тут згадано деякі з середовищ безпеки та міркувань відповідності, які можна використовувати при плануванні. Створення плану кібербезпеки не відбудеться відразу. Розробка заходів та відповідальність за кібербезпеку лягають на всіх. Щоб гарантувати успіх у розробці ефективного плану кібербезпеки, необхідно зробити зміни і в самому процесі, і в плані відповідної культури.

Висновки. Морський транспорт залишається величезною перевагою морських держав, оскільки за його допомогою у світі досі пересувається левова частка товарів. Не можна обминути згадкою сферу пересування пасажирів, зокрема туристичну. Однак при цьому через недавнє злиття операційних технологій морського транспорту з інформаційними технологіями значно виріс ризик небезпеки морського транспорту через зовнішнє втручання. Останнє підтверджується низкою публікацій з хронологією подій та описом втрат.

Питанням кібербезпеки взагалі в усьому світі та в Україні зокрема присвячено багато робіт. Є практичні напрацювання у галузі кіберзахисту критичної інфраструктури. На жаль, питання кіберзахисту морського транспорту в українській науковій літературі належним чином не відстежуються.

Світова ж спільнота у цій галузі швидко робить відповідні кроки. Відповідні документи зі зверненням до держав-членів випускає Комітет з морської безпеки.

Напрацьовуються навіть певні стандарти, випускаються посібники та настанови. В них, зокрема, вказується на вірогідність кібератак як ззовні, так і з середини компанії, установи, організації, судна, наголошується на необхідність ретельного створення та неухильного виконання плану з кіберзахисту. Висвітлюються особливості організації здійснення кіберзахисту саме морського транспорту.

Необхідним елементом забезпечення кібербезпеки на морському транспорті вважається також загальний підйом культури персоналу до сучасного рівня.

Література:

1. Судноплавна галузь виявилася беззахисною перед кіберзлочинцями. *Logist.Fm. 23.03.2022*. Сайт. URL: https://logist.fm/news/sudnoplavna-galuz-viyavilasya-bezzahisnoyu-pered-kiberzlochincyami (дата звернення: 26.03.2023).

2. Огляд подій в сфері кібербезпеки, Національний координаційних центр кібербезпеки. *Cyber Digest.* січень 2023. Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України». 2023. 42 с. URL: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf (дата звернення: 26.03.2023).

3. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. д-ра техн. наук, професора В.Б. Толубка. Київ : ДУТ, 2015. 288 с.

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.

5. Кібербезпека та інформаційні технології : монографія. Харків : ТОВ «ДІСА ПЛЮС», 2020. 380 с. URL: http://nauka.kntu.kr.ua/files/monograf_pz.pdf (дата звернення: 23.03.2023).

6. Лахно В.А. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту. *Український науковий журнал з інформаційної безпеки*. 2016, том. 22, випуск 1. С. 44–50. URL: file:///C:/Users/Admin/Downloads/cyril,+9.pdf (дата звернення: 23.03.2023).

7. Akpan, F., Bendiab, G., Shiaeles, S. ,Karamperidis, S., Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. *MDPI*. 7 March 2022. Site. URL: https://www.mdpi.com/2673-8732/2/1/9 (дата звернення: 26.03.2023).

8. Allianz Risk Barometer. Top Business Risks for 2019. Allianz Global Corporate & Specialty. Site. URL: https://www.assiteca.it/wp-content/uploads/2019/10/Allianz-Risk-Barometer-2019-1.pdf (дата звернення: 25.03.2023).

9. Coburn, A.W.; Daffron, J.; Smith, A.; Bordeau, J.; Leverett, É.; Sweeney, S.; Harvey, T.; 2018. Cyber Risk Outlook; Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. 2018. P. 33. URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2018.pdf (дата звернення: 25.03.2023).

10. Neo, M. The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore. Royal Australian Navy Sea Power. Issue 42, 2021. P. 38. Site. URL: https://www.navy.gov.au/sites/default/files/documents/Soundings_Papers_42_2021.pdf (дата звернення: 26.03.2023).

11. Harris, R. How Big a Problem is Maritime Cyber Security? Ocean Technology group. Сайт. URL: https://oceantg.com/blog/the-problem-of-maritime-cyber-security/ (дата звернення: 25.23.2023).

12. Cybercrime. What does the most damage, losing data or trust? *Ernst & Young. S*ite. URL: https://www.ey.com/en_gl/financial-services/cybercrime-what-does-the-most-damage-losing-data-or-trust (дата звернення 23.03.2023).

13. The Government launches new Digitalisation Strategy. Ministry of Foreign Affairs of Denmark. *InvestInDK* 05.05.2022. Site. URL: https://investindk.com/insights/digitization-strategy (дата звернення: 23.03.2023).

14. The Principal Regulations Governing Maritime Safety. International Chamber of Shipping, Site, URL: https://www.ics-shipping.org/shipping-fact/safety-and-regulation-the-principal-regulations-governing-maritime-safety/. (дата звернення: 23.03.2023).

15. Maritime Cyber Risk Management in Safety Management Systems. Resolution MSC.428(98) Annex 10 (adopted on 16 June 2017). URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. (дата звернення: 23.03.2023).

16. A Comprehensive Guide to Maritime Cybersecurity. *MissionSecure.Com*. Сайт. URL: https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach (дата звернення: 25.23.2023).

17. The Guidelines on Cyber Security onboard Ships – Version 4. *BIMCO*. Site. URL: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (дата звернення: 23.03.2023).

18. 6 Common Ways Employees Compromise Enterprise Data Security (And What You Can Do About It). *VIRTRU*. Site. URL: https://www.virtru.com/blog/enterprise-data-security (дата звернення: 23.03.2023).

19. Boyes, H., Isbell, R. Code of Practice. Cyber Security for Ships. London : Institution of Engineering and Technology, 2017. P. 73

20. Cybersecurity and Disaster Recovery Plan by Marine Digital. Marine Digital. Site. URL: https://marine-digital.com/article_cybersecurity (дата звернення: 23.03.2023).

References:

1. Sudoplavna galuz vyiavylasia bezzakhysnoiu pered kiberzlochyntsiamy [The shipping industry proved to be defenseless against cybercriminals] *Logist.Fm. 23.03.2022*. Site. URL: https://logist.fm/news/sudnoplavna-galuz-viyavilasya-bezzahisnoyu-pered-kiberzlochincyami [accessed 23 March 2023] [in Ukrainian].

2. Ohliad podiy v sferi kiberbezpeky. Natsionalnyi koordynatsiynyi tsentr kiberbezpeky [Overview of events in the field of cyber security]. *Cyber Digest. January 2023.* Pidhotovleno za pidtrymky Proektu USAID “Kiberbezpeka krytychno vazhlyvoi infrastruktury Ukrainy”. 2023. P. 42. URL: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf [accessed 23 March 2023] [in Ukrainian].

3. Lisovska Yu. P. (2019). Kiberbezpeka: ryzyky to zakhody: navchal’nyi pisibnyk [Cyber security: risks and measures: education. Manual]. Kyiv: Vydavnychyi dim “Kondor”. P. 272 [in Ukrainian].

4. Buriachok V. L. (2015). Informatsiyna ta kiberbezpeka: sotsiotekhnichnyi aspect: pidruchnyk [Information and cyber security: socio-technical aspect: Manual]. DUT. P. 288 [in Ukrainian].

5. Kiberbezpeka ta informatsiyni tekhnologii: monografia [Cyber security and information technologies: monograph]. Kharkiv. TOV “DISA PLUS”. 2020. P. 380. URL: http://nauka.kntu.kr.ua/files/monograf_pz.pdf [accessed 23 March 2023]. [in Ukrainian].

6. Lakhno V. A. (2016). Pidvyshchennia iberbeszpeky informatsiyno-komunikatsiynykh system transporut [Increasing the cyber security of information and communication systems of transport]. *Ukrainskyi naukovyi zhurnal z informatsiynoi bezpeky.* Vol. 22. Issue 1. P. 44–50 [in Ukrainian].

7. Akpan F., Bendiab G., Shiaeles S., Karamperidis, S., Michaloliakos M. (2022). Cybersecurity Challenges in the Maritime Sector. *MDPI*. 7 March 2022. Site. URL: https://www.mdpi.com/2673-8732/2/1/9 [in English].

8. Allianz Risk Barometer. Top Business Risks for 2019. Allianz Global Corporate & Specialty. URL: https://www.assiteca.it/wp-content/uploads/2019/10/Allianz-Risk-Barometer-2019-1.pdf [in English].

9. Coburn, A.W.; Daffron, J.; Smith, A.; Bordeau, J.; Leverett, É.; Sweeney, S.; Harvey, T. (2018). Cyber Risk Outlook; Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. 2018. P. 33. URL: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2018.pdf [in English].

10. Neo M. (2021). The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore. Royal Australian Navy Sea Power. Issue 42. P. 38. URL: https://www.navy.gov.au/sites/default/files/documents/Soundings_Papers_42_2021.pdf [in English].

11. Harris R. (2019). How Big a Problem is Maritime Cyber Security? Ocean Technology group. URL: https://oceantg.com/blog/the-problem-of-maritime-cyber-security/ [in English].

12. EY Global (2019). Cybercrime. What does the most damage, losing data or trust? *Ernst & Young.* URL: https://www.ey.com/en_gl/financial-services/cybercrime-what-does-the-most-damage-losing-data-or-trust [in English].

13. The Government launches new Digitalisation Strategy. Ministry of Foreign Affairs of Denmark. *InvestInDK* 05.05.2022. URL: https://investindk.com/insights/digitization-strategy [in English].

14. The Principal Regulations Governing Maritime Safety. International Chamber of Shipping. URL: https://www.ics-shipping.org/shipping-fact/safety-and-regulation-the-principal-regulations-governing-maritime-safety/. [in English].

15. Maritime Cyber Risk Management in Safety Management Systems. Resolution MSC.428(98) Annex 10 (adopted on 16 June 2017). URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. [in English].

16. A Comprehensive Guide to Maritime Cybersecurity. *MissionSecure.Com*. URL: https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach [in English].

17. The Guidelines on Cyber Security onboard Ships – Version 4. *BIMCO*. URL: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships [in English].

18. 6 Common Ways Employees Compromise Enterprise Data Security (And What You Can Do About It). *VIRTRU*. URL: https://www.virtru.com/blog/enterprise-data-security [in English].

19. Boyes, H., Isbell, R. (2017). Code of Practice. Cyber Security for Ships. London : Institution of Engineering and Technology. P. 73 [in English].

20. Cybersecurity and Disaster Recovery Plan by Marine Digital. Marine Digital. URL: https://marine-digital.com/article_cybersecurity [in English].