Технічні науки

УДК 656.6:629.067

Мельник Олексій Миколайович

кандидат технічних наук,

доцент кафедри судноводіння і морська безпека

Одеський національний морський університет

Melnyk Oleksiy

PhD, Associate Professor of the

Department of Navigation and Maritime Safety

Odesa National Maritime University

ORCID: 0000-0001-9228-8459

Волошин Андрій Олександрович

кандидат технічних наук, професор,

завідувач кафедри судноводіння і морської безпеки

Одеський національний морський університет

Voloshyn Andrii

PhD, Associate Professor,

Head of the Department of Navigation and Maritime Safety

Odesa National Maritime University

ORCID: 0000-0003-3993-5826

Пуляєв Ігор Олександрович

старший викладач кафедри судноводіння і морської безпеки

Одеський національний морський університет

Puliaev Igor

Senior Lecturer of the Department of Navigation and Maritime Safety

Odesa National Maritime University

ORCID: 0000-0002-0592-032X

Бурлаченко Дементій Анатолійович
старший викладач кафедри судноводіння і морська безпека
Одеський національний морський університет
Burlachenko Dementiy
Senior Lecturer of the Department of Navigation and Maritime Safety
Odesa National Maritime University
ORCID: 0000-0003-3749-4908

Щенявський Геннадій Сергійович
викладач кафедри судноводіння і морська безпека
Одеський національний морський університет
Shcheniavskyi Hennadii
Senior Lecturer of the Department of Navigation and Maritime Safety
Odesa National Maritime University
ORCID: 0000-0001-7803-978X

ОГЛЯД МІЖНАРОДНОЇ ПРАКТИКИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В МОРСЬКІЙ ГАЛУЗІ
REVIEW OF INTERNATIONAL PRACTICE OF ENSURING CYBERSECURITY IN THE MARITIME INDUSTRY

Анотація. *Науково-технічний прогрес є основоположним фактором і для торговельного судноплавства що розвивається у частині розмірів та швидкості сучасних суден та рівні їх технічного оснащення. Вантажні характеристики суден також збільшуються, а кількість членів екіпажу на борту скорочується, оскільки все більше робочих процесів автоматизується за рахунок впровадження IT-технологій, включаючи системи управління суднами. Незважаючи на багаторазові заклики з боку ІМО, з метою зосередження уваги на побудову ефективного захисту у сфері морської безпеки щодо протидії кібератакам, проблеми залишалися*

невирішеними. Власники судноплавного бізнесу не розголошують інформацію про спроби здійснення або випадки кібератак, що були спрямовані проти них, побоюючись комерційних збитків або наслідків, таких як втрата іміджу, претензії з боку клієнтів та страхових компаній, розслідування, що проводяться незалежними міжнародними організаціями та державними органами. Питання кібербезпеки систем управління в сучасному світі набули важливого значення, з приводу того що існуючі загрози стосується не лише безпеки технічних засобів та пристроїв, а також питань забезпечення екологічної безпеки та безпеки життя на морі. У статті проведено аналіз застосування рекомендацій щодо управління кіберризиками в морській галузі в межах систем управління безпекою для забезпечення безпеки функціонування суднових систем, що контролюються за допомогою комп'ютерного обладнання.

Ключові слова: *морський транспорт, безпека судноплавства, кібератаки, загрози судноплавству, міжнародна морська організація, кіберризики в морській галузі.*

Summary. *Scientific and technological progress is an underlying factor for merchant shipping as well, which is evolving in terms of the size and speed of modern ships and the level of their technical equipment. Vessel performance is also increasing and the number of crew members on board is decreasing as more and more work processes are automated through the introduction of IT technologies, including ship management systems. In spite of numerous requests by IMO to focus on effective maritime security protection against cyber-attacks, problems remain unresolved. Owners of the shipping business do not disclose information about attempts or incidents of cyber attacks directed against them, fearing commercial losses or consequences, such as loss of image, claims by clients and insurance companies, investigations by independent international bodies and public authorities. Cyber security issues of management systems in*

today's world have gained importance, due to the fact that the current threats are not only concerned with the safety of technical equipment and devices, but also issues of environmental and safety of life at sea. The article analyzes the application of recommendations on the control of cyber risks in the maritime sphere within safety management systems to ensure safe functioning of ship systems monitored with the help of computer equipment.

Key words: *cyber risks, maritime transport, international maritime organization, cyber security, maritime industry.*

Вступ. Загальносвітовою тенденцією є прогресуюча цифровізація в усіх галузях промисловості, не винятком є морський транспорт де активно розвивається електронна навігація, автоматизація процесів керування судном, технології зв'язку та безпеки поряд зі збільшенням розмірів суден, їх швидкісних за рахунок зменшення кількості членів екіпажу Разом з цим суднові системи та програми оновлюються шляхом відкритого доступу до інтернету під час плавання, що безпосередньо пов'язане з питаннями забезпечення безпечної експлуатації судна.

Міжнародна морська організація (IMO) відносіть наступні системи судна до найбільш вразливих суднових систем, з боку суб'єктів кібератак [1]:

- системи ходового містка;
- системи обробки та управління вантажем;
- системи управління двигунами, машинами та енергоживленням;
- системи контролю доступу на судно;
- системи обслуговування пасажирів та екіпажу;
- публічні інтернет-мережі судна, призначені для використання пасажирами;
- адміністративні системи та мережі;
- системи зв'язку.

Як безпека судна, так і кібербезпека є важливими складовими через їх потенційний вплив на екіпаж, судно, довкілля, компанію та вантаж. Забезпечення кібербезпеки судна відноситься до захисту інформаційних технологій судна (IT-information technologies) та його операційних технологій (OT-operational technologies), перш за все це захист інформації та даних від несанкціонованого доступу, маніпуляцій або порушення. Кібербезпека охоплює ризики, пов'язані з втратою доступності або цілісності важливих для безпеки даних. Відповідно порушення кібербезпеки судна може статися внаслідок інциденту, що впливає на доступність та цілісність операційних технологій, наприклад, пошкодження картографічних даних, що зберігаються в електронній системі відображення карт та інформації (ECDIS), збій під час технічного обслуговування та оновлення програмного забезпечення, втрата або маніпуляція даними із зовнішніх датчиків, що критично важливі для роботи судна - сюди входять також глобальні навігаційні супутникові системи (GNSS).

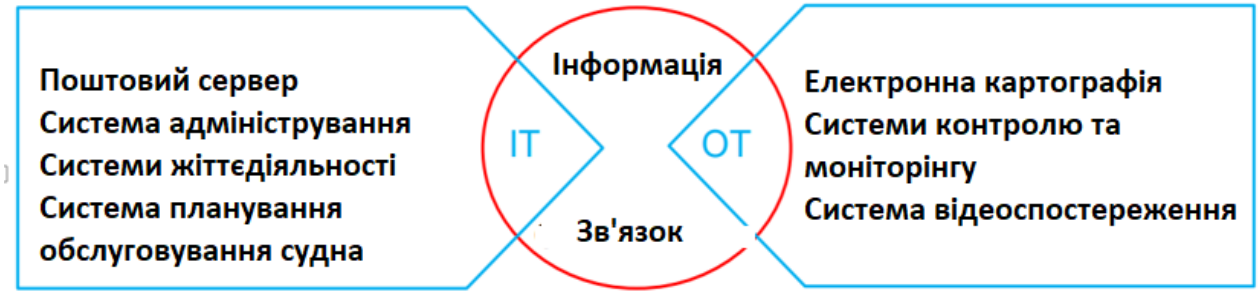

Рис. 1. Конвергенція інформаційних та операційних технологій [6]

Виходячи з цього, можна зробити висновок, що сучасне морське судно є вкрай уразливим перед спланованою кібератакою. Тому враховуючі думки науковців та експертів з морської галузі, необхідно дослідити поточний стан морської кібербезпеки та нормативні документи. Під час 98-ї сесії Комітет з безпеки на морі Міжнародної морської організації (IMO) схвалив Циркуляр MSC-FAL.1/Circ.3 "Посібник з

управління кіберризиками в морській галузі" та Резолюцію MSC.428(98) — Управління кіберризиками в морській галузі у межах систем управління безпекою. Ця резолюція передбачає необхідність підвищення рівню обізнаності персоналу судноплавних компаній та членів екіпажу щодо існуючих загроз і кіберризиків для забезпечення безпеки судна та захисту судноплавства в цілому. У циркулярі наголошується на необхідності врахування кіберзагроз на борту суден за аналогією з іншими експлуатаційними ризиками, зокрема, через застосування системи управління безпекою, яка відповідає вимогам МКУБ (Міжнародний кодекс управління безпекою). Державам-членам пропонується забезпечити належну увагу щодо кіберзагроз у системах управління безпекою під час першої щорічної перевірки ступеню відповідності щодо вимог всіх судноплавних компанії після 1 січня 2021 року.

Відзначимо, що загрози для кібербезпеки морських суден, терміналів та логістичних компаній цілком реальні. Сумнозвісний вірус-шифрувальник NotPetya (аналог «Petya») в 2017 році заразив 17 з 76 вантажних терміналів компанії Maersk [2], що вилилося в 300 млн євро збитків. У 2018 році фіксувалися кібератаки на порти Барселони, Сан-Дієго [3].

У період з вересня 2020 року, до цього часу судноплавні компанії, організації та порти, як і раніше, були ціллю кібератак. Так, у зазначений період від них потерпали Міжнародна морська організація (IMO) та Італійське класифікаційне товариство RINA; французька контейнерна судноплавна компанія CMA CGM, британська поромна компанія Red Funnel, норвезька круїзна компанія Hurtigruten, оператор поромної переправи Steamship Authority в Массачусетсі, флагманський контейнерний перевізник Південної Кореї HMM і японська судноплавна компанія Kawasaki Kisen Kaisha; не названі іранський та індійський порти, а також річковий порт Кенневік у штаті Вашингтон, США [4].

Сьогодні цифрових піратів найбільше цікавлять можливості взяти під контроль виробничі комунікаційні мережі та інформаційні системи суден. До бортових IT- і OT-систем, що схильні до кіберризиків, в першу чергу, слід віднести електронну картографічну навігаційну інформаційну систему (ECDIS), реєстратор даних маршруту (VDR), системи управління вантажними операціями, силовими установками та енергозабезпеченням, а також системи радіозв'язку та передачі даних.

Реальним наслідком зараження систем шкідливим програмним забезпеченням може стати зміна даних про судно, включаючи його місцеположення, інформацію про рейс, порти, дані про вантаж. Під впливом шкідливої програми конкретним суднам може бути надіслано неправдиву інформацію про хибні метеоумови, штормові попередження, з метою примусової зміни курсу. В результаті викрадення інформації з реєстратора даних маршруту можна змінити поточні параметри судна, наприклад, швидкість, та всі дані, що відображаються на радіолокаційних системах (РЛС) та інших технічних пристроях пов'язаних із навігацією судна. Кіберзлочинці можуть видалити аудіозаписи та інформацію з систем керування курсом судна, рульовою машиною, дані про стан герметизації відсіків, перебірок, дверей та люків [5].

Інша проблема це вплив пандемії COVID-19 та нові виклики для судноплавної галузі, яка стала мішенню групи хакерів, які розсилають на електронні скриньки листи з файлами з нібито важливою інформацією про коронавірус і тим самим заносять вірус до комп'ютерних користувачів. За даними американських фахівців з кібербезпеки Proofpoint, у листах міститься шкідливий документ Microsoft Word. Коли одержувач відкриває файл, на його комп'ютер встановлюється AZORult – шкідливе програмне забезпечення. Воно запрограмоване для викрадання різних даних користувачів (інформацію з різних файлів, паролі, куки, історію браузерів, банківські облікові дані та інформацію про криптовалютні гаманці). Тому

всім компаніям та екіпажам торгових суден рекомендують з підвищеною обережністю ставитися до будь-яких електронних повідомлень, посилань та веб-сайтів, які стосуються коронавірусу тому що зловмисники розуміють економічні проблеми, що пов'язані з спалахом пандемії тому винаходять різні схеми обману. Зриви процесів перевезень вантажів у зв'язку з поширенням хвороби безумовно мають вплив на перевізників, судноплавні компанії, і ті, хто стоїть за атаками, добре знають, які побічні наслідки це матиме для індустрії, що демонструє не лише їхню технічну, а й економічну досвідченість.

У січні 2021 року в морському судноплавстві набули чинності оновлені глобальні вимоги щодо кібербезпеки. Тепер судновласники відповідно до резолюції ІМО MSC.428(98) повинні враховувати кіберризики у системі управління безпекою (СУБ) судна. Відсутність цієї інформації може бути розцінена як порушення процесу ведення документації СУБ. Як результат, судновласники можуть зіткнутися з адміністративними стягненнями аж до заборони на вихід судна з порту.

Забезпечення кібербезпеки на морському транспорті не закінчується тим, що необхідно вписати кілька нових рядків в існуючу систему управління безпекою судна, адже рекомендований ІМО «Посібник з кібербезпеки на борту суден» визначає наступне коло суб'єктів кібератак:

- активісти (включаючи незадоволених працівників);
- злочинці;
- опортуністи;
- держави;
- організації, що фінансуються державою;
- терористи.

Провідні керівні та консультаційні документи про морську кібербезпеку, розроблені владою таких країн як США, Великої Британії, Євросоюзу, Данії та Норвегії. За підсумками 103 сесії, Комітет з безпеки на

морі Міжнародної морської організації 14 червня 2021 випустив циркуляр MSC.1/Circ.1639. У документі державам-членам пропонується взяти до уваги рекомендації, що містяться у четвертій версії «Керівництва з кібербезпеки на суднах», підготовленій галузевими асоціаціями. Рекомендувати відповідним заінтересованим сторонам, включаючи судновласників, операторів та менеджерів, враховувати при необхідності цей посібник при розгляді кіберризиків на суднах відповідно до цілей та функціональних вимог Міжнародного кодексу управління безпекою, як це рекомендовано Резолюцією MSC.428(98).

Також 14 червня 2021 року комітетами з безпеки на морі для спрощення формальностей було випущено першу редакцію циркуляру MSC-FAL.1/Circ.3/Rev.1 «Методичні рекомендації з управління кіберризиками в морській сфері», яким було схвалено оновлення додаткових рекомендацій та стандартів , включених до пункту 4.2 цих рекомендацій. Вказаний пункт був доповнений новою редакцією «Посібника з кібербезпеки на суднах», підготовленого галузевими організаціями, та зведеною Рекомендацією Міжнародної асоціації класифікаційних товариств (МАКО) з кіберзахисту (відомої як Рекомендація № 166).

Четверта версія «Посібника з кібербезпеки на суднах» містить загальні оновлення найкращих практик у галузі управління кіберризиками і як ключову функцію включає розділ з покращеним керівництвом з концепції ризику та управління ризиками. До найважливіших відмінностей четвертої версії можна віднести включення розділів, присвячених участі вищого керівництва в управлінні кіберризиками; розподілу обов'язків та завдань у між працівниками компанії; кількісної оцінки загрози; виявлення вразливостей, у тому числі при фізичному відвідуванні суден та віддаленому доступі; оцінки ймовірності, оцінки впливу та взаємозв'язку

чинників, які впливають на ризики; розробленні заходів щодо їх виявлення, етапи реагування на інциденти.

У Європейському Союзі 17 грудня 2020 року Агентство Європейського Союзу з кібербезпеки (ENISA) випустило Керівництво для європейських портових операторів з управління кіберризиками в умовах цифрової трансформації. Керівництво засноване на доповіді ENISA про кібербезпеку портів за 2019 рік, та надає практичні рекомендації, які розповідають про поточні загрози кібербезпеці та змінному цифровому ландшафту, з яким стикається морський сектор Європи. У керівництві наголошується, що морський сектор ЄС має ферментований підхід до оцінки кіберзагроз.

У США 5 січня 2021 року Радою національної безпеки США прийнято Національний план морської кібербезпеки США. Цей документ розробляється у рамках Національної стратегії морської безпеки США. Новий п'ятирічний план фокусується на нових стандартах для власників портів, відправників вантажів та операторів, а також на майбутніх мандатах, що дозволяють підрядникам відповідати кіберстандартам. Офіційні особи США заявили, що Національний план морської кібербезпеки випускається у рамках визнання того, що існують прогалини у морській безпеці США. Головна проблема полягає в тому, що збої в роботі портів та судноплавстві можуть спричинити шокові хвилі в економіці США. Відповідно до плану, одним із пріоритетів уряду США у просуванні вперед має стати розробка структури ризиків для систем портових операційних технологій (ОТ), щоб страховики, судновласники та вантажовідправники мали спільну мову щодо управління ризиками. Крім того, у 2020 році Управління Берегової охорони США щодо дотримання вимог до комерційних суден випустило робочу інструкцію CVC-WI-027 «Управління кіберризиками суден», яка містить керівництво для інспекторів та посадових осіб портового контролю з оцінки кібергігієни на

борту суден, а також варіанти дотримання вимог щодо виявлення недоліків.

Згідно з інструкцією, якщо управління кіберризиками не було включено до системи управління безпекою судна до першої щорічної перевірки судноплавних компаній після 1 січня 2021 року, судно може бути затримане з вимогою зовнішнього аудиту протягом трьох місяців.

Також коли об'єктивні докази вказують на наявність серйозного збою в реалізації системи управління безпекою судна щодо управління кіберризиками, який безпосередньо призвів до інциденту кібербезпеки, що впливає на роботу судна (наприклад, зниження безпеки судна або підвищення ризику для навколишнього середовища), то судно також може бути затримане із вимогою зовнішнього аудиту протягом трьох місяців.

У листопаді 2020 року Міжнародна палата судноплавства у співпраці з BIMCO та Witherbys випустила друге видання «Робочого зошита з кібербезпеки для використання на борту судна». Робочий зошит надає екіпажам суден практичні засоби виявлення кіберзагроз та захисту вразливих бортових систем. Міжнародна палата судноплавства в робочому зошиті вважає, що на операційному рівні недоліком цифрової революції є зростаюча вразливість оператора до кібератак. Оскільки підключення до інтернету на борту стає все більш поширеним явищем, а суднові системи дедалі більше оцифровуються та інтегруються, і судна тепер є мішенню для хакерів у всьому світі, дуже важливо, щоб весь екіпаж мав уявлення про те, як і коли можуть статися кібератаки.

Класифікаційне товариство «Корейський регістр судноплавства» 18 вересня 2020 провело перше у світі присвоєння класу кібербезпеки (CS Ready) судну газовозу з компанії Hyundai Heavy Industries. Клас кібербезпеки було присвоєно після завершення успішних неодноразових інспекцій. Клас CS Ready присвоюється новозбудованим суднам і для його отримання необхідно успішно пройти 49 пунктів інспекції загалом за 12

категоріями, включаючи управління ризиками та активами, реагування на кіберінциденти та відновлення після них. Також Корейський регістр судноплавства проводить сертифікацію з морської кібербезпеки щодо компанії або судна із системою менеджменту кібербезпеки, за результатами якої видається сертифікат відповідності та засвідчення обладнання на відповідність вимогам кібербезпеки [4].

Висновки. Виходячи з викладеного, можна зробити висновок, що сучасне морське судно залишаться вразливим перед новими загрозами такими як сплановані кібератаки. Порти також потребують захисту від інформаційних загроз. Тому однією з рекомендацій з боку Міжнародної морської організації є практика управління кіберризиками що досягається через природне розширення існуючих методів управління безпекою мореплавання та безпекою судна. ІМО розглядає кібербезпеку як частину морської безпеки. Додатково існує низка рекомендацій щодо забезпечення морської кібербезпеки, розроблених провідними міжнародними морськими спільнотами. При цьому слід зауважити що немає єдиного затвердженого підходу щодо визначення конкретних кіберзагроз та їхньої оцінки тому кожна компанія-судновласник змушена самостійно визначати рівень цих небезпек і засоби їх запобігання.

Література

1. Міжнародна морська організація. URL: http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL 41–17. Table of contents (Secretariat).pdf (дата звернення 03.12.21).
2. The Untold Story of NotPetya, the Most Devastating Cyberattack in History // Wired. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russiacode-crashed-the-world/?src=longreads (дата звернення 03.12.21).

3. За один тиждень жертвами кібератак стали одразу два морські порти // Securitylab.ru by Positive Technologies. URL: https://www.securitylab.ru/news/495727.php (Дата звернення 03.12.21).
4. Семенов С. А. Морська кібербезпека // Держава і транспорт. 2019 № 3. С. 11-14.
5. Кібербезпека у судноплавстві. Актуальні виклики. URL: https://www.korabel.ru/news/comments/kiberbezopasnost_v_sudohodstve_aktualnye_vyzovy.html (дата звернення 03.12.21).
6. Мельник О.М., Окулов В.І., Пуляєв І.О. Захоплення заручників / В. І. Окулов, І. О. Пуляєв, О. М. Мельник // Логос. ONLINE. 2020. №15. С. 1–7.
7. Melnyk O., Okulov V., Pulyayev I., Koryakin K. Crew change problems under global pandemic conditions of COVID-19 / O. Melnyk, V. Okulov, I. Pulyayev, K. Koryakin // The scientific heritage. 2021. P. 54–57.
8. Practice of Cyber Security Management System on Cargo Ship (2018). China Classification Society, IMO: Guidelines On Maritime Cyber Risk Management (MSC-FAL.1-Circ.3).
9. Melnyk O., Onyshchenko S., Pavlova N., Kravchenko O., Borovyk S. Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. International Journal of Computer Science and Network Security. 2022. Vol. 22 (03). P. 135-140. doi: https://doi.org/10.22937/IJCSNS.2022.22.3.18
10. Мельник О.М., Бичковський Ю.В. Сучасна методика оцінки рівню безпеки судна та шляхи його підвищення / О.М. Мельник, Ю.В. Бичковський // Розвиток транспорту. 2021. № 2 (9). С. 37-46. doi: https://doi.org/10.33082/td.2021.2-9.03

References

1. International Maritime Organization. (2021). Retrieved from: http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL41-17. Table of contents (Secretariat).pdf (date of appeal 03.12.21)
2. The Untold Story of NotPetya, the Most Devastating Cyberattack in History *Wired*. (2021). Retrieved from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russiacode-crashed-the-world/?src=longreads (date of appeal 03.12.21)
3. Two seaports became victims of cyber-attacks in one week. (2021). *Securitylab.ru by Positive Technologies*. Retrieved from: https://www.securitylab.ru/news/495727.php (date of appeal 03.12.21)
4. Semenov S. A. (2019) Mors`ka kiberbezpeka. *Derzhava i transport*, 3, pp. 11-14.
5. Cyber-security in ship navigation. (2021). Actual vision. Retrieved from: https://www.korabel.ru/news/comments/kiberbezopasnost_v_sudohodstve_aktualnye_vyzovy.html (date of appeal 03.12.21)
6. Melnyk O.M., Okulov V.I., Pulyaev I.O. (2020). Zahoplennya zaruchnikiv. *Logos. ONLINE*, 15, pp. 1-7.
7. Melnyk O., Okulov V., Pulyayev I., Koryakin K. (2021). Crew change problems under global pandemic conditions of COVID-19. *The scientific heritage*, pp. 54-57.
8. Practice of Cyber Security Management System on Cargo Ship (2018). China Classification Society, IMO: Guidelines on Maritime Cyber Risk Management (MSC-FAL.1-Circ.3).
9. Melnyk O., Onyshchenko S., Pavlova N., Kravchenko O., Borovyk S. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. International Journal of Computer Science and Network Security, vol. 22 (03), pp. 135-140. doi: https://doi.org/10.22937/IJCSNS.2022.22.3.18

10. Melnyk O., Bychkovsky Yu. (2021). Modern methods of assessing the level of vessel safety and ways to its improvement. Transport Development, No. 2 (9). P. 37-46. doi: https://doi.org/10.33082/td.2021.2-9.03