МІЖНАРОДНО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ НА МОРСЬКОМУ ТРАНСПОРТІ

Веремчук Владислав Сергійович,
викладач кафедри загальноправових дисциплін та міжнародного права економіко-правового факультету Одеського національного університету ім. І.І. Мечникова

Інформаційні технології є невід'ємним засобом сучасного обміну інформацією, навчання, автоматизації виробничих процесів, а цифровізація торкнулась усіх сфер світової економіки, у тому числі морського транспорту.

Важко уявити сучасне торговельне судно без точних локаторів, систем електронної навігації, супутникового зв'язку та систем контролю параметрів роботи силової установки, які роблять експлуатацію такого судна більш безпечною та автономною.

Більш того, стрімкий технологічний прогрес призвів до виникнення

концепції автономних морських торговельних суден (Maritime autonomous surface ships, MASS), які, за аналогією із безпілотною авіацією, не потребують наявності екіпажу на борту та можуть керуватися віддалено з берегового центру управління.

Окрім підвищення ролі цифрових технологій та мінімізації участі людини на морському транспорті актуалізується проблема захисту інформації (кібербезпеки, управління кіберризиками) у портах та на торговельних суднах з метою запобігання випадків несанкціонованого доступу до систем зв'язку та автоматизованого управління морським судном.

Проблема захисту морського транспорту від кіберризиків не є новою. Так, Дж. Сол вказує, що ще у 2016 році Південна Корея повідомила, що 280 торговельних суден зіткнулися із проблемами експлуатації навігаційних систем. Внаслідок кібератаки GPS-сигнал було перехоплено зловмисниками, що спричинило переривання сигналу та отримання хибної інформації щодо місцезнаходження судна [1].

Експерти «The North of England P&I Association», морського страхувальника взаємної відповідальності, визначають кібербезпеку як «сукупність технологій, процесів і практики, призначених для захисту електронних мереж, комп'ютерів, програм та даних від нападу, пошкодження або несанкціонованого доступу». Вказується, що у контексті судноплавства «кіберризик може полягати у виході з ладу електронного обладнання, ризик якого загалом розглядається як високий, що призводить до необхідності мати резервне обладнання та запчастини до нього задля забезпечення можливості переходу на ручне управління судном у разі відмови електроніки» [2].

Так, Д. Дімітріос наголошує, що «чим вищим буде ступінь автоматизації морського судна, тим вищим буде й ризик кібератак» [3].

В.С. Веремчук визначає кібербезпеку при експлуатації морських суден як один із основних аспектів потенційних змін у морському праві у процесі його адаптації до технологічних викликів [4, с. 77].

Слід зазначити, що чинні станом на 2023 рік «морські» конвенції не закріплюють положень щодо кібербезпеки у світовому мореплавстві, проте значну роль у розробці правового регулювання із вказаної проблеми посідає діяльність Міжнародної морської організації (далі - ІМО).

ІМО визначає морський кіберризик одним із найважливіших елементів морської безпеки, який «означає міру, до якої технологічний актив може бути під загрозою через потенційну обставину чи подію, яка може призвести до збоїв у роботі судна, безпеці судноплавства внаслідок пошкодження та втрати інформації або систем управління» [5].

У 2017 році ІМО ухвалила Резолюцію MSC.428(98) «Управління морськими кіберризиками у системах управління безпекою».

Вказана резолюція визначає наступні типи кіберризиків:

- зовнішні чинники, такі як спам, фішинг, вірусне програмне забезпечення, несанкціонований доступ та злам системи;

- внутрішні чинники, такі як наявність помилок у роботі та загальний збій системи [6].

Додатково слід відзначити що ІМО відносить до вразливих до кіберризику наступні системи судна: системи навігаційного містка; вантажні системи; системи руху та машинного відділення; системи керування доступом на судно; системи обслуговування пасажирів; мережі загального користування; системи соціального забезпечення екіпажу; системи радіозв'язку та комунікації [6].

Окрім того, у резолюції MSC.428(98) ІМО вимагає, щоб судновласники та менеджери включили управління кіберризиками до системи безпеки суден. Недотримання цих вимог може призвести до здорожчання страхування, відмови у доступі до порта і навіть арешту суден [6].

Важливим кроком для забезпечення кібербезпеки на морі стало ухвалення у 2022 році Міжнародною морською організацією Керівництва з управління морськими кіберризиками (MSC-FAL.1-Circ.3-Rev.2), яке «містить рекомендації високого рівня щодо управління морськими кіберризиками для захисту судноплавства від існуючих та потенційних кіберзагроз і вразливостей та включає функціональні елементи, що підтримують ефективне управління кіберризиками» [7].

Керівництво з кібербезпеки на борту суден, видане ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC та SYBAss (четверта версія 2021 року) містить здебільшого технічні норми, які сприятимуть оцінці кіберризику та забезпеченню кібердисципліни на борту суден. Метою Керівництва є «покращення безпеки моряків, навколишнього середовища, вантажів та суден. Рекомендації спрямовані на допомогу в розробці належної стратегії управління кіберризиками, згідно з відповідними правилами та передовою практикою на борту судна, з акцентом на робочих процесах, обладнанні, навчанні, реагуванні на інциденти та управлінні відновленням» [8].

Таким чином, можемо констатувати зростання занепокоєння проблемою захисту інформації (управління кіберризиками) стейкхолдерами морської галузі. Несанкціонований доступ до систем управління торговельними суднами є загрозою безпеці мореплавства та експлуатації судна, а також визнається страховим ризиком з боку морських страхувальників взаємної відповідальності.

Хоча на сьогоднішній день відсутній універсальний міжнародний договір, який врегулював би питання управління кіберризиками у морській індустрії, помітну роль відіграють міжнародні організації, зокрема ІМО, які розробляють міжнародні стандарти управління кібербезпекою на морському транспорті. Вказані стандарти можуть розглядатися як основа

для запровадження уніфікованих загальнообов'язкових норм, які регулюватимуть безпеку автоматизованих систем управління морським судном.

Список використаних джерел:

1. Saul J. Cyber threats prompt return of radio for ship navigation. *Reuters*, 2017. URL: https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT (дата звернення: 23.10.2023).

2. Cyber Risks in Shipping. Loss prevention briefing for north members ships. July, 2017. URL: https://www.nepia.com/cyber-risks-in-shipping-lp-briefing (дата звернення: 23.10.2023).

3. Dimitrios D. Exploring the Issue of Technology Trends in the «Era of Digitalisation». *World Maritime Day Parallel Event*. At: Szczecin-Poland, 2018. URL: https://www.researchgate.net/publication/325877588_ Exploring_the_ Issue_of_Technology_Trends_in_the_Era_of_Digitalisation (дата звернення: 23.10.2023).

4. Веремчук В.С. Міжнародно-правові аспекти експлуатації автономного морського судна: постановка питання. *Правова держава*. № 50. 2023. С. 72-80.

5. Maritime cyber risk. *International maritime organization*. URL: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

6. Maritime cyber risk management in safety management systems. MSC 98/23/Add.1 Annex 10. URL: https://wwwcdn.imo.org/localresources/en/ OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (дата звернення: 23.10.2023).

7. Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3/Rev.2 (7 June 2022). URL: https://www.imo.org/en/OurWork/ Security/Pages/Cyber-security.aspx (дата звернення: 23.10.2023).

8. The Guidelines on Cyber Security Onboard Ships. Version 4 (2019). Produced and supported by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf (дата звернення: 23.10.2023).