3. Конституція України: Закон України від 28.06.1996р. № 254к/96. Дата оновлення: 21.02.2019. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4976.

4. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23.02.2006. № 3477-IV. Дата оновлення 02.12.2012. URL: https://zakon.rada.gov.ua/laws/show/3477-15#undefined.

5. Про застосування судами міжнародних договорів України при здійсненні правосуддя: Постанова Пленуму Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 19.12.2014 № 13. URL: https://zakon.rada.gov.ua/laws/show/v0013740-14.

6. Про судове рішення в адміністративній справі: Постанова Пленуму Вищого адміністративного суду України від 20.05.2013 № 7. URL: https://zakon.rada.gov.ua/laws/show/v0007760-13.

Степаненко М.В.

студент,

Національний університет «Одеська морська академія»

ЗАГАЛЬНЕ ПОНЯТТЯ ТА ЗМІСТ БЕЗПЕКИ МОРЕПЛАВСТВА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Цифрова трансформація, яка приголомшує морську область, приносить революційні інновації, які повністю змінять роботу суден. Щоб отримати вигоду з цих активів, галузь повинна зіткнутися з проблемами і усунути потенційні ризики. В майбутньому кіберзагрози стануть більш поширеними, що зробить інформаційну безпеку мореплавства обов'язковою вимогою і конкурентною перевагою серед суб'єктів галузі.

Останнім часом інформаційна безпека та її окремі аспекти стали предметом численних праць російських та українських дослідників. Проте не зважаючи на стрімкий розвиток інформаційних відносин, досі немає повноцінного уявлення про таке явище як інформаційна безпека взагалі, а тим паче у сфері мореплавства.

Відомий український дослідник Калюжний Р.А., вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані з створенням, зберіганням, поширенням і використанням інформації [1, с. 18].

За українським законодавством, інформаційна безпека − стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через неповноту, невчасність та недостовірність інформації, що використовується; негативний інформаційний вплив; негативні насідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Безпека судноплавства є станом збереження (захищеності) людського здоров'я і життя, довкілля та майна на морі й на внутрішніх водних шляхах; відсутністю непростимого ризику, пов'язаного з загибеллю або травмуванням людей, заподіянням шкоди довкіллю або матеріальних збитків [3].

У 2017 ІМО видала "Рекомендації з управління кібер ризиками в морській галузі», та вперше дала визначення цьому поняттю в морській сфері:

морські кіберзагрози це ризики технологічного ресурсу з боку потенційних обставин або подій, які можуть призвести до збоїв у перевезенні вантажів і пасажирів, безпеки мореплавства або безпеки судна, у зв'язку з пошкодженням, втратою або компрометацією пов'язаних із судноплавством інформації або систем [4].

Шляхом вивчення різних джерел таких як нормативно – правові акти національного та міжнародного характеру та праць вчених, співставлення різних понять таких як інформаційна безпека, кібербезпека, безпека мореплавства вдалось створити власне визначення інформаційної безпеки мореплавства. Під інформаційною безпекою в області забезпечення безпеки мореплавання розуміються врегульовані інформаційно-правовими нормами інформаційні суспільні відносини з приводу збереження людського життя, захисту морських суден від небезпеки на морі та захисту морського середовища від забруднення з суден.

Також необхідно врахувати, що до інформаційної безпеки мореплавства входять інформаційні технології (ІТ) і експлуатаційні технології (ЕТ) [5].

Системи експлуатаційних технологій керують фізичним світом, а системи інформаційних технологій управляють даними. Експлуатаційні технології і системи відрізняються від традиційних ІТ-систем. Експлуатаційні технології – це апаратне і програмне забезпечення, яке безпосередньо контролює фізичні пристрої та процеси. Інформаційні технології охоплюють спектр технологій обробки інформації, включаючи програмне забезпечення, обладнання і технології зв'язку [5].

Інформаційна безпека мореплавства має широке коло суб'єктів які можна поділити на дві групи. До першої групи можна віднести всіх учасників морського підприємства (уряди, портову владу, судноплавні

компанії, логістичні компанії, постачальників телекомунікаційних послуг, екіпаж судна і т.д.), також є і інша група суб'єктів. Це так би мовити інша сторона медалі, а саме зловмисники які посягають на інформацію та данні.

До другої групи суб'єктів відносяться національні уряди, промислові шпигуни та угруповання організованої злочинності, хактивісти та хакери.

Об'єктами інформаційної безпеки постає власне інформація (особиста, комерційна, державна), інформаційні системи, данні та бази даних, автоматизовані системи і технології на морському транспорті і т.д.

Кібер ризики є відносно новим питанням у галузі мореплавства. Однак збиток, який він може завдати – величезний і може розглядатися як економічна шкода, так і шкода безпеці судноплавства. Зважаючи на той факт, що у світі дуже мало нормативно – правових актів, які могли б освітити дану проблему, то було б корисно, щоб міжнародна спільнота погодила спільну стратегію і створила спеціалізовану робочу групу для роботи над розробкою детального набору керівних вказівок з кібер-безпеки і передового досвіду для розробки технологій і впровадження інформаційних систем в морському секторі.

Список використаних джерел:

1. Калюжний Р. Питання щодо реформування інформаційного законодавства України. *Збірник «Правові, діючі та метрологічні системи інформації, що містяться в Україні».* Київ : НТУУ «КПІ», Міністерське навчання і науки України, СБУ. С. 17-21.

2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки : Закон України від 09.01.2007 № 537-V. URL: http://zakon.rada.gov.ua

3. Про затвердження Правил авіаційного пошуку та рятування в Україні: Наказ міністерства Юстицій від 17.05.2006. № 297. URL: https://zakon.rada.gov.ua/laws/show/z0772-06/ed20070730/find?text=%D1%E8%F1%F2%E5%EC%E0+%CA%CE%D1%CF%C0%D1-%D1%C0%D0%D1%C0%D2

4. IMO guidelines on maritime cyber risk management MSC-FAL.1/Circ.3. 2017. URL: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

5. IT Security vs OT Security: The OT Guide for Industrial IT Professionals. URL: https://www.otorio.com/blog/posts/the-ot-guide-for-industrial-it-professionals