5. Chuan-jin OU, Bing-tao LI (2020). Research and application of new multimodal transport equipment-swap bodies in China. *E3S Web of Conferences*, 145. https://doi.org/10.1051/e3sconf/202014 [In English].

АНАЛІТИЧНИЙ ПІДХІД ДО ОЦІНКИ РІВНЯ КІБЕРБЕЗПЕКИ ПРОЦЕСІВ ІНТЕЛЕКТУАЛІЗАЦІЇ ПОРТУ

Безбах Олег Михайлович
кандидат технічних наук, доцент,
доцент кафедри інноваційних технологій
та технічних засобів судноводіння
Херсонської державної морської академії
місто Херсон, Україна
ombezb@gmail.com
ORCID: 0000-0003-1030-7586/
Безуглова Ірина Василівна
кандидат економічних наук, доцент,
завідувач кафедри економіки та морського права
Херсонської державної морської академії,
місто Херсон, Україна
ibezuhlova@gmail.com
ORCID: 0000-0001-9796-1980/

Анотація. Автори даних тез систематизують випадки кібератак на інтелектуальні портові системи з метою визначитися, який саме математичний апарат використовувати. Заначений математичний апарат має дозволяти на підставі досліджень та розрахунків, визначать ймовірність наступного втручання зловмисників та заздалегідь передбачити відповідні заходи запобігання цим негативним факторам. На думку авторів даних тез найбільшу загрозу процесам інтелектуалізації портів несуть такі факти неправомірного

використання кіберпростору, що містять злочинну діяльність відносно низького рівня, тобто несанкціонований доступ або порушення роботи операційних систем, пошкодження веб-порталів, крадіжки даних аккаунтів користувачів інтелектуальних систем портів тощо.

Ключові слова. Кібератаки, централізовані інформаційно-обчислювальні центри, кібербезпека, цифрові технології, митниця, оператори терміналів, судновласники, суднові брокери, логістика.

Вступ. Кібербезпека на сьогодні є одним із пріоритетів діджиталізації та інтелектуалізації будь-якої галузі, не тільки портової. Усі без виключення оператори сучасних портових послуг використовують цифрові технології, що є надзвичайно вразливими для кіберзагроз, для навігації, зв'язку, планування транспортування вантажів, забезпечення безпеки, екологічного контролю тощо. Саме тому частка кіберзагроз у загальному обсязі вразливостей, з якими стикається сучасна портова галузь, постійно підвищується [1].

З метою кращої систематизації випадків кібератак на інтелектуальні портові системи автори даних тез пропонують використовувати математичний апарат, що дозволить на підставі досліджень та розрахунків, визначити ймовірність наступного втручання зловмисників та заздалегідь передбачити відповідні заходи запобігання цим негативним факторам. На думку авторів даних тез найбільшу загрозу процесам інтелектуалізації портів несуть такі факти неправомірного використання кіберпростору, що містять злочинну діяльність відносно низького рівня, тобто несанкціонований доступ або порушення роботи операційних систем, пошкодження веб-порталів, крадіжки даних аккаунтів користувачів інтелектуальних систем портів тощо.

Виклад основного матеріалу дослідження. У сучасних портах вся система перевалки вантажів базується на комп'ютерних системах, а обмін даними між великою кількістю залучених партнерів організовується централізовано. Отже, відповідні інформаційні та комунікаційні системи є привабливою мішенню для кібератак [2, 3]. Різниця між звичайними

фізичними атаками, які ще кілька років тому були основним напрямком заходів безпеки, і кібератаками полягає в тому, що останні можуть бути здійснені з безпечної відстані з відносно невеликим ризиком. Крім того, набагато складніше виявити кібератаки, ніж звичайні фізичні атаки [4, 5].

Насправді, інтелектуальні порти є особливо складними об’єктами з точки зору безпеки, оскільки вони є складними організаціями з великою кількістю залучених гравців і безліччю різних функцій, що перетинають кілька рівнів, які фактично є централізованими інформаційно-обчислювальними центрами, що забезпечують функціональність обміну даними в межах портової комунікаційної мережі [6, 7]. Вони мають велику кількість технічно різнорідних інтерфейсів з багатьма різними підсистемами в порту, такими як митниця, оператори терміналів, судновласники, суднові брокери, оператори вантажних автомобілів, залізничні оператори, портові залізниці, оператори внутрішніх водних шляхів, експедиторські агентства, портові адміністрації та інші органи влади, а також інші компанії.

Кібератаки на зазначені підсистеми інтелектуального порту можуть здійснювати як не дуже досвідчені хакери, так й навіть інсайдери, тобто співробітники підрозділів цих портів, які мають право доступу до конфіденціальної інформації, та наприклад, незадоволені колегами, політикою компанії, підрядниками тощо. Але у будь-якому випадку ці зловмисники отримують доступ до підсистем інтелектуального порту без санкції адміністраторів систем [8, 9]. Однак, описане неправомірне використання кіберпростору може й не нести заздалегідь глибоких злочинних намірів, це можуть бути відсутність необхідних правових знань або звичайна цікавість, але згідно законодавств усіх країн Європейського Союзу, такі дії вважаються кримінальною злочинністю [10, с. 205].

Треба зазначити, що кібератаки, як правило, здійснюються поетапно. Підготовка кібератак потребує деякого часу, який визначається метою зловмисника, надійністю технічних засобів контролю кібербезпеки відповідної інтелектуальної системи, ступенем оновленості програмного

забезпечення відповідних підсистем тощо [4, с. 4]. Досвідчений, підготовлений фахівець, однак який не є професійним системним адміністратором, тим не менш здатний виявити неправомірне використання кіберпростору, відстежити найбільш уразливі ключові позиції, та на підставі аналізу отриманої інформації, зробити висновки про певну злочинну активність щодо підсистем навігації, зв'язку, планування транспортування вантажів, забезпечення безпеки, екологічного контролю тощо інтелектуального порту. Саме вчасна реакція такого фахівця дозволить заздалегідь запобігти більш серйозним кібератакам та зберегти час і витрати на відновлення роботи зазначених підсистем інтелектуального порту.

Ретельний аналіз джерел кібератак, які здійснюються найбільш часто, надає змогу припустити, що це випадковий процес, який підпорядковується законам, що в теорії ймовірностей або, точніше, у теорії стохастичних процесів, називають марковськими процесами. Найбільш поширене визначення цих процесів таке, марковські процеси – це випадкові процеси, для яких «майбутнє» залежить лише від «сьогодні» та не залежить від «вчора» [10, с. 206]. Тобто марковською є будь-яка система, для кожного моменту часу якою ймовірність будь-якого стану даної системи в майбутньому залежить тільки від її стану в теперішньому, і не залежить від того, як зазначена система прийшла до цього стану.

Отже, випадковою величиною X вважають величину, що визначається як результат випадкового явища [10, с. 207]. Отже, автори даних тез зазначають, що результатом події неправомірного використання кіберпростору, із врахуванням теорії марковських систем, може бути виявлення втручання у підсистеми інтелектуального порту, втрата даних (повна або часткова), відмова підсистем тощо. Взагалі простір можливих наслідків неправомірного використання кіберпростору, як простір випадкових величин, може бути дискретним або неперервним, в залежності від цього його поведінка відповідає тим чи іншим законам розподілу. Наприклад,

нормальному (неперервні випадкові величини) або розподілу Пуассона (дискретні випадкові величини) [9, с. 208].

Випадковий процес (стохастичний), у цьому випадку, визначають як набір випадкових величин, які можна представити у вигляді індексованого одномірного масиву, елементами якого є моменти часу прояви подій неправомірного використання кіберпростору. Якщо цей масив є множиною натуральних чисел, тоді це випадковий процес з дискретним часом, інакше це буде випадковим процесом з неперервним часом [9, с. 208]. Вибір моделі оцінки рівня кібербезпеки процесів інтелектуалізації порту обов'язково має відповідати сутності досліджуваних явищ неправомірного використання кіберпростору, глибокому аналізу їх характерних рис, статистичному аналізу числових результатів тощо.

Висновки. Насправді, інтелектуальні порти є особливо складними об'єктами з точки зору безпеки, оскільки вони є складними організаціями з великою кількістю залучених гравців і безліччю різних функцій, що перетинають кілька рівнів, які фактично є централізованими інформаційно-обчислювальними центрами, що забезпечують функціональність обміну даними в межах портової комунікаційної мережі. Вони мають велику кількість технічно різнорідних інтерфейсів з багатьма різними підсистемами в такому порту.

Ретельний аналіз джерел кібератак, які здійснюються найбільш часто, надає змогу припустити, що це випадковий процес, який підпорядковується законам, що в теорії ймовірностей або, точніше, у теорії стохастичних процесів, називають марковськими процесами. Автори даних тез зазначають, що результатом події неправомірного використання кіберпростору, із врахуванням теорії марковських систем, може бути виявлення втручання у підсистеми інтелектуального порту, втрата даних (повна або часткова), відмова його розглянутих підсистем тощо. Вибір моделі оцінки рівня кібербезпеки процесів інтелектуалізації порту обов'язково має відповідати сутності досліджуваних явищ неправомірного використання кіберпростору,

глибокому аналізу їх характерних рис, статистичному аналізу числових результатів тощо.

List of References

1. Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493. [in English]

2. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123-138. [in English]

3. Amro, A., & Gkioulos, V. (2022). From click to sink: Utilizing ais for command and control in maritime cyber attacks. In European Symposium on Research in Computer Security. Cham: Springer Nature Switzerland. [in English]

4. IAPH (2020). Port Community Cyber Security Report. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf[in English]

5. Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat. Marine Policy, 143, 105138. [in English]

6. Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526. [in English]

7. Longo, G., Merlo, A., Armando, A., & Russo, E. (2023). Electronic Attacks as a Cyber False Flag against Maritime Radars Systems. In 2023 IEEE 48th Conference on Local Computer Networks (LCN), 1-6. [in English]

8. 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, 22(03), 135-140. [in English]

9. Bezuglova, I. V., & Bezbakh, O. M. (2021). Innovative technical means of navigation as the main method of increasing the economic efficiency of maritime enterprises. Materials of the XIII International Scientific and Practical Conference "Modern Information and Innovative Technologies in Transport" (MINTT-2021). Kherson: KhDMA. 7-10. [in Ukrainian]

10. Kravtsova, L. V., Zaitseva, T. V., & Kaminska, N. G. (2023). Investigation of the probability of a cyber incident in flight conditions. Materials of the 5th International Scientific Conference "Technologies, Tools and Strategies for the Implementation of Scientific Research". Vinnytsia: European Scientific Platform. 204 207. [in Ukrainian]

АНАЛІЗ ВПЛИВУ ТЕХНОЛОГІЙ, ЩО ВИКОРИСТОВУЮТЬ БЛОКЧЕЙН, НА ІНТЕЛЕКТУАЛІЗАЦІЮ ПОРТОВОЇ ГАЛУЗІ

Безбах Олег Михайлович,
кандидат технічних наук, доцент,
доцент кафедри інноваційних технологій
та технічних засобів судноводіння
Херсонської державної морської академії,
місто Херсон, Україна,
ombezb@gmail.com
ORCID: 0000-0003-1030-7586
Кириченко Костянтин Володимирович,
кандидат технічнх наук, доцент,
доцент кафедри безпеки життєдіяльності
та професійно-прикладної фізичної підготовки
Херсонської державної морської академії,
місто Херсон, Україна
kvklecturer@gmail.com
ORCID:0000-0002-0974-6904