АНАЛІЗ ВИПАДКІВ КІБЕРАТАК У СЕКТОРІ МОРСЬКОГО ТРАНСПОРТУ

Зайцева Т. В.
Херсонська державна морська академія
(Україна)

Вступ. Посилення цифровізації, автоматизації технологічних процесів, використання штучного інтелекту призводить до збільшення кількості та зміни якості кібератак на судноплавну галузь, яка за останні роки зазнала серйозних інцидентів кібербезпеки. Протягом багатьох років кількість кібератак стрімко зросла, що призвело до великих фінансових втрат для підприємств у зв'язку з відновленням, регулятивними санкціями, підвищенням страхової ставки, а також до побічних збитків, таких як, наприклад, репутаційна довіра. Морський сектор, який колись вважався безпечним через відсутність підключення до Інтернету та ізольованість суден у морі, показує 900% збільшення кількості порушень кібербезпеки операційних технологій. Незважаючи на те, що в цій галузі проводяться дослідження, питання кібербезпеки об'єктів сфери морських перевезень завжди будуть стояти на повістці дня.

Актуальність досліджень. Відповідно до звіту ENISA «Analysis of Cyber Security Aspects in the Maritime Sector», зацікавленність питаннями кібербезпеки в морському секторі знаходиться на низькому рівні [1].

Малу стурбованість питаннями, пов'язаними з кіберзагрозами, відзначають і аналітики компанії CyberKeel, що спеціалізується на безпеці морської індустрії. Вони наголошують на тому факті, що багато зайнятих у морській сфері звикли бути частиною «практично невидимої» галузі [1]. Разом із зростаючою опорою на автоматизацію, значно загострюється ризик зовнішнього втручання та зриву роботи технологічних систем; несанкціоновані дії можуть перешкодити управлінню судном або роботі навігаційних систем, вивести з ладу зовнішні комунікації судна або отримати конфіденційні дані. Бортові системи отримують оновлення під час плавання, команди мають вихід в інтернет. зміна даних про судно, включаючи його місцезнаходження, курс, інформацію про вантаж, швидкість та ім'я – все це, на жаль, сьогодні є реальністю, яку повинні враховувати всі зацікавлені сторони.

Постановка задачі. Міжнародна морська організація до вразливих суднових систем відносить майже всі бортові системи.

Технологія, яка необхідна для «підробки» судна, не дорога і відома вже на сьогодні, її даже можна знайти та завантажити з Інтернету. Інциденти спуфінгу вже були зареєстровані в Чорному морі, де кілька суден повідомили про аномалії свого GPS-положення. У тому ж районі судно було піддано фальсифікації GPS. Під час знаходження судна в морі, бортова система геолокації показувала, що воно було на суші. Крім того, неодноразово спостерігалися зіткнення суден і морські аварії через несправність навігаційних систем.

У травні 2017 року спуфінгова атака призвела до зіткнення корабля ВМС США та південнокорейського рибальського човна. У лютому 2017 року судно місткістю 8250 двадцятифутових еквівалентів (TEU) було повністю зламано на шляху з Кіпру до Джібуті. Приблизно на 10 годин зловмисник заволодів навігаційною системою судна, і капітан був безпорадний зробити що-небудь, щоб повернути судно в експлуатацію. Під час попередньої атаки з глушінням GPS Південна Корея повідомила, що понад 280 суден мали проблеми з навігаційною системою; сигнал GPS був заглушений хакерами, в результаті чого деякі сигнали GPS зникли, а інші отримували неправдиві дані. Коли GPS не працює належним чином, існує дуже високий ризик катастрофи з наслідками для екіпажу, судна та навколишнього середовища [2].

В останні роки галузь судноплавства стала привабливою мішенню для атак програм-вимагачів через відчутну відсутність інвестицій у кібербезпеку та потенційну можливість значних збоїв у роботі. Але на першому місці серед кібератак в морському секторі залишається фішинг.

У 2020 році два судна були заражені програмою-вимагачем Hermes 2.1 через троян AZORult. Зараження сталося через текстовий документ із підтримкою макросів, прикріплений до електронного листа. Після відкриття листа було вражено кілька робочих станцій у адміністративних мережах [3].

У 2021 році кілька грецьких транспортних компаній постраждали від атаки програм-вимагачів, яки поширилися через системи IT-консалтингової компанії. Цей інцидент показав реальний ризик ланцюга постачання інформаційних технологій для судновласників, менеджерів суден і судноплавної галузі. Через кілька днів одне судно було викрадено, а ще шість повідомили про втрату керування в Оманській затоці. Ці інциденти були розцінені як кіберпіратство.

Під час іншого кіберінциденту був відкладений спуск на воду побудованого суховантажного судна на кілька днів через те, що його ECDIS було заражено невідомим вірусом. Джерело і шлях зараження не вдалося з'ясувати або виявити. За даними, затримка відпливу та витрати на ремонт склали сотні тисяч доларів США [3].

Мережа бортової системи керування американського судна була заражена шкідливим програмним забезпеченням. Ця мережа зазвичай використовується для оновлення електронних карт, керування даними про вантаж і зв’язку з береговими об’єктами. ФБР повідомило, що головною причиною такої атаки була відсутність стратегій безпеки на судні, що спричинило критичний захват облікових даних систем керування судна.

IT-системи портів також мали сплеск кіберінцидентів, які вплинули на морську інфраструктуру. Найпоширеніші види атак – це фішинг, шкідливе програмне забезпечення, соціальна інженерія, груба сила та відмова в обслуговуванні. У березні 2020 року порт Марселя був уражений програмою-вимагачем «Mespinoza/Pysa». У цьому інциденті морські інфраструктури постраждали від атаки через їх взаємозв’язок з інформаційними системами в Екс-Марсель-Прованс, який був головною метою атаки [4].

В іншому масштабному інциденті портова система Maersk стала жертвою великої кібератаки, спричиненої шкідливим програмним забезпеченням NotPetya, яка також вплинула на багато інших судноплавних компаній у всьому світі. На сьогодні це є класичним прикладом кібератаки на портову інфраструктуру, який описан в підручниках по кібербезпеці.

У 2020 році відбулася серйозна атака програмного забезпечення-вимагача на транспортну компанію CMA CGM SA, яка вплинула на деякі сервери в її мережі і завадила клієнтам мати зовнішній доступ до IT-додатків компанії та систем бронювання. Цього ж року порт Х’юстона став об’єктом кібератаки, яка включала програму керування паролями, що містила раніше невідому вразливість. Хакери використали це для встановлення шкідливого коду, який надавав доступ до мереж. Це було зроблено для викрадання облікових даних, необхідних для контролю доступу до мережі. На щастя, спроба злому була успішно захищена, і жодна система не постраждала [4].

Усі ці інциденти підтверджують, що сучасні кібератаки виходять за рамки маніпулювання навігацією чи підробки вантажу; вони можуть порушити локальні та глобальні ланцюжки поставок і навіть поставити під загрозу життя екіпажу чи пасажирів на борту судна. В таблиці 1 наведено приклади останніх кіберінцидентів у секторі морського транспорту, але слід враховувати, що тут представлені лише ті дані, які були висвітлені в засобах масової інформації. Але багато випадків кіберінцидентів так і залишаються не проаналізованими. Тому що судновласники не мають бажання нести репутаційні збитки та намагаються не давати розголосу кіберінцидентам.

Таблиця 1 – Приклади останніх кіберінцидентів у секторі морського транспорту

Рік	Інцидент	Наслідки
2016	Атака з глушінням GPS у Південній Кореї	Постраждало 280 суден
2017	Кібератака на навігаційну систему	Захоплення судна на 10 год
2017	Кібератака на навігаційну систему	Зіткнення корабля ВМС США з катером
2018	GPS-спуфінгова атака на кораблі в Чорному морі	Повернення 20 суден до порту
2018	Віддалена компрометація бортових комп'ютерів	Крадіжка конфіденційних даних
2018	Атака підробки GPS	Маніпулювання положенням судна
2018	Атака зловмисним програмним забезпеченням NotPetya	Постраждала інфраструктура судноплавства, великі економічні збитки
2018	Зараження ECDIS вірусом	Затримка відходу судна
2019	Атака зловмисного програмного забезпечення	Заволодіння критичними обліковими даними
2020	Програма-вимагач Hermes 2.1. напад на 2 судна	Зараження всієї мережі
2020	Атака програм-вимагачів "Mespinoza/Pysa"	Зараження морської інфраструктури
2021	Атака програм-вимагачів на транспортні компанії	Шифрування файлів
2022	Установка шкідливого коду	Проблеми доступу до мережі портів

Результати дослідження. Сучасні й автономні судна стали мішенями для кібератак через збільшення використання цифрових технологій. Таким чином, необхідно прийняти кілька контрзаходів і глибоких стратегій захисту, щоб створити стійкість до зовнішніх і внутрішніх загроз безпеці.

Перший контрзахід полягає у створенні системи безперервного моніторингу, яка може забезпечувати обізнаність про стан безпеки судна в режимі реального часу. Тобто план реагування судна на кіберінциденти та відповідальні особи повинні оновлювати та аналізувати нові технологічні та програмні засоби захисту. У цьому контексті технологія блокчейн була запропонована для покращення безпеки керування автономними суднами в багатьох дослідженнях [5]. Основна функція технології блокчейн, включаючи відстежуваність, прозорість, можливість аудиту, незмінність і децентралізацію, виявляється в реалізації безпечного зв'язку та безпечного зберігання даних, якими обмінюються судна та береговий центр управління. Використання цієї технології усуне деякі критичні загрози безпеці зв'язку на судні, такі як втрата даних, зміна даних зловмисниками або викрадення даних. Блокчейн відіграватиме головну роль в ідентифікації та сертифікації, забезпеченні цілісності даних та інформаційної безпеки в морській галузі.

Оскільки всі системи судна взаємопов'язані, лише одна скомпрометована система може дозволити атакам отримати доступ до всіх інших систем, від системи очищення води до системи керування двигуном. Таким чином, конфігурація самих інформаційних і операційних технологій та систем також може бути цінним активом для захисту від певних атак. Одним із механізмів, який може підвищити навігаційну безпеку, є система

автентифікації навігаційних повідомлень (NMA), яка розроблена для запобігання спуфінгу та забезпечення підвищеної безпеки. Схема NMA включає процес автентифікації в потік навігаційних повідомлень, автентифікуючи джерело, одночасно захищаючи криптографічну цілісність навігаційних даних. Приймач може виявити зловмисників, які намагаються створити або змінити навігаційні дані. Зловмисник не може імітувати повідомлення автентифікації, оскільки він не має ключа, необхідного для створення повідомлення автентифікації.

Враховуючи небезпеку збою ECDIS, IMO окреслила необхідність резервних заходів на борту суден. Оскільки ці резервні копії не забезпечують повної функціональності ECDIS, їх слід використовувати в поєднанні з поточними паперовими картами. Багато авторитетних судноплавних компаній вирішують встановити другу ECDIS на борту, щоб зменшити ризик відмови ECDIS.

Висновки. У політиці морської безпеки людський фактор відіграє значну роль, оскільки, з одного боку, це може бути найслабшою ланкою, але, з іншого боку, першим захистом у кіберланцюзі. Судна, порти та треті сторони часто працюють зі змінними екіпажами з різним рівнем розуміння кібербезпеки, які можуть бути не повністю знайомі з безпечною роботою відповідних систем і методами кібергігієни. Відсутність культури кібербезпеки може бути вигідною для будь-якого зловмисника, який хоче отримати доступ до судна та його систем, викрасти фактичну інформацію або порушити роботу судна.

Отже, у морській галузі існує критична потреба у підвищенні рівня обізнаності та розуміння, пов’язаного з реальними кіберризиками. Найефективнішим способом досягти цього є просування культури кібербезпеки, яка, включає навчання з питань кібербезпеки, освіту та сертифікацію для членів екіпажу, робітників портів, операторів та інш.

ЛІТЕРАТУРА

1. Gary C. Kessler, Steven D. Shepard. Maritime Cybersecurity: A Guide for Leaders and Managers. 2020, 252 p.

2. DiRenzo, J., Goward, D. A., Roberts, F. S. The little-known challenge of maritime cybersecurity. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 6–8 July 2015; pp. 1–5. Jensen, L. Challenges in maritime cyber-resilience. *Technol. Innov. Manag. Rev.* 2015, *5*, 35.

3. Alcaide J. I., Llave R. G. Critical infrastructures cybersecurity and the maritime sector. *Transp. Res. Procedia* 2020, *45*, 547–554.

4. Foundation N. Demonstration Test of World’s First Unmanned Operation of Small Tourism Boat Successfully Completed at Sarushima, Yokosuka. Available online: https://www.nippon-foundation.or.jp/en/news/articles/2022/20220111-67000.html.

5. Kavallieratos G., Katsikas S., Gkioulos V. Cyberattacks against the autonomous ship. In *Computer Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 20–36.