KAPITEL 3 / *CHAPTER 3* [3]
ENSURING MARITIME SECURITY AND MEASURES AGAINST CYBER THREATS AND CYBER PIRACY AT SEA

DOI: 10.30890/2709-2313.2023-16-01-017

Вступ

Сьогодні у сфері морського транспорту дедалі активніше йде процес цифровізації: розвивається електронна навігація, автоматизуються процеси управління, програмні продукти впроваджуються практично в усі суднові системи - зв'язку, обробки та управління вантажем, управління судном, судновою енергетично установкою, енергоживленням тощо. Розроблення та ухвалення нормативних актів, спрямованих на зниження вразливості суден від кібератак, дії шкідливого програмного забезпечення і, як наслідок, підвищення безпеки судноплавства - функція державного контролю в галузі морської індустрії, і, зокрема, на рівні капітана морського порту. Кіберзагрози - хоча й не нове явище для морської галузі, а нормативна база протидії перебуває у стадії формування, питання покращення кібербезпеки є нагальним. Завдання з 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.

3.1. Аналіз сучасного стану кіберпіратства в мореплавної галузі

Сучасне судно стає все більш технологічно залежним, і питання кібербезпеки є критично важливим оскільки кількість кіберзагроз стрімко зростає згідно даних аналітиків компанії McAfee, 2021 [12].

Пірати в морі були на заваді морякам і торговцям весь час. Паралельно з існуванням морського транспорту та морської торгівлі існує і піратство. Морське піратство поширилося глибоко у водах Європи, Південно-Східної Азії, Східної Азії, Південної Азії, Перської затоки, Мадагаскару, Канарських островів, Північної Америки та Карибського моря.

Сучасні пірати перетворилися з тих, хто просто хотів заробити на життя, на злочинців, які бажають отримати якнайбільше прибутку. Еволюція морських

[3] ***Authors:*** *Zayats Sergiy Valentynovysh*

піратів стала результатом змін економіки та технологій. В даний час пірати використовують сучасні технології для отримання своєї неправомірної вигоди.

Пандемією COVID-19 спричинила зростання піратства на 24%. Пандемія закрила багато підприємств і можливостей працевлаштування у всьому світі. Сучасні пірати схожі на хакерів, ніж на піратів старого ґатунку, кібер-піратство передбачає отримання доступу до інтернет-підключених систем судна чи морської інфраструктури.

Кількість кібератак в морській галузі з роками збільшується, що призводить до великих фінансових втрат для морських компаній, а також може спричинити репутаційні збитків, і втрату довіри клієнтів. У цьому відношенні морський сектор, який до цього часу вважався безпечним через нестачу IOT і ізольованості судна у морі, але останні статистичні дані свідчить про збільшення на 90% кібер інцидентів в морській галузі.

Сьогоднішні судна значною мірою залежать від цифрового з'єднання: навігаційні системи, маніфести, операції по швартуванню і завантаженню, контроль за навколишнім середовищем, відстеження вантажів. Цифровізації надає багато можливостей кібер-піратам отримати доступ до систем судна з метою підриву або відволікання для здійснення крадіжки або інших неправомірних дій.

Сучасний торговий флот налічує більші 118000 суден, і функціонує в 150 країнах, і налічує близько мільйона моряків, забезпечуючи кібер-піратів великою кількістю потенційних цілей. Високотехнологічні судна можуть коштувати понад 200 дол. млн в процесі будівництва, що робить їх самих вже цінним активом. З урахуванням того що вартість вантажу може бути високо вартісним, що може становити до 100 млн доларів сирої нафти, або 1,200 автомобілів класу люкс вартістю 53 млн доларів, легко побачити, чому кібер-піратство приваблює сучасних злочинців.

Сучасне кібер-піратство викликає величезне занепокоєння саме через збільшення кібер інцидентів. Кібератака 2017 року NotPetya довела, наскільки руйнівним може бути порушення для міжнародної судноплавної промисловості. Maersk, найбільша у світі контейнерна судноплавна компаній, яка транспортує 15% світового вантажу, зіткнулася з кібер атакою с залученням шкідливого програмного забезпечення, яке було поширено через бухгалтерське програмне забезпечення. Кібер атака спричинила величезні збитки: 50,000 персональних комп'ютерів і тисяча додатків і серверів були заражені крізь 600 сайтів в 130 країнах, Maersk був змушений працювати вручну протягом 10 днів, в той час як відбувалося інвестування в 4,000 нових серверів, 45,000 нових ПК і 2,500

додатків. Остаточний рахунок за збитками Maersk становив приблизно 300 мільйонів доларів США і спричинив великі затримки вантажу по всьому світу. Страхова компанія Lloyd's of London попередила, що серйозна кібератака в морській галузі може коштувати світовій економіці понад $120 млрд [27].

Морські компанії неохоче оприлюднюють дані про кібератаки через потенційну репутаційну шкоду, тому офіційної статистики за загальною кількістю кібератак на галузь не існує. Орієнтовно 47% моряків протягом переходу стали ціллю кібератаки. Завдяки інноваціям цифровим технологіям та при неухильно зростаючій вартості вантажу, спостерігається ще більше зростання кіберпіратства.

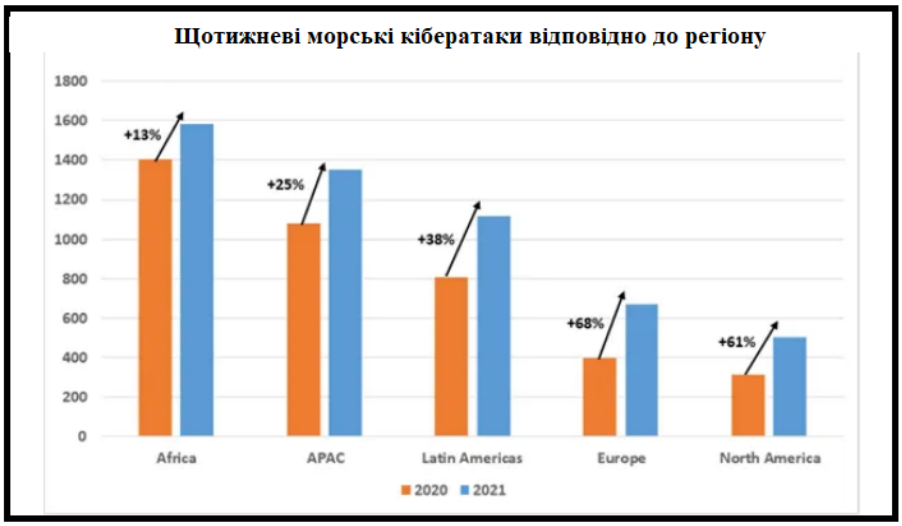

Рис 1 - Зростаючі тенденції кіберпіратства в морській галузі

Сучасний світовий морський сектор все більше залежить від діджиталізіції, операційної інтеграції, і автоматизації [9]. Провідні суднобудівні компанії та оператори прагнуть до залучення інновацій і використання найсучасніших технологій та систем, які виходять за рамки традиційного судна, і більш орієнтовані на створення судна з розширеним дистанційним керуванням, можливостями залучення цифрових технологій в оперативні системи судна та можливостями з'єднання з іншими суб'єктами морської галузі [10].

До 2030 року [7], автономні судна і сучасні судна будуть оснащенні різноманітними сенсорами, наприклад: сучасними радарами, технологіями отримання та обробки інформації про віддалені об'єкти за допомогою активних оптичних систем, що використовують явища відбиття світла і його розсіювання в прозорих і напівпрозорих середовищах LiDAR, камерами високої чіткості, тепловизирами, сонар і багатьома операційними технологіями (OT) системи, що взаємопов'язані між собою, щоб надати судну точне комбіноване зображення навколишнього середовища [5]. Їх рівні автоматизації будуть прогресувати від

повністю пілотованих суден до частково керованих, дистанційно керованих, частково автономних, і повністю автономних і безпілотних суден [22].

Морська промисловість складає 90% міжнародної торгівлі, та ринок судноплавства оцінюється в 720 мільярдів доларів у 2020 р. до 1,2 трлн дол. США у 2030 р. Морська галузь динамічно розвивається як промисловість за допомогою інвестицій і суднобудування. Інформаційні інновації як технології застосовуються до морської промисловість, так що різні навігаційні системи та технологічні операційні системі на суднах оцифровані. Це також допомагає для підключення пристроїв на судні один до одного, судно до судна, або судно з портом за допомогою мережі зв'язку. Ця зміна пов’язана з переходом до розумного судна з впровадженням інноваційних процесів IT- технологій згідно вимоги до виконання закону/нормативного акту розвитку морської галузі, а також підвищення вимог перевізника/ вантажовласника, інформації місця знаходження судна, аналіз продуктивності використання палива, застосування IT-технологій щодо виконання екологічних положень, застосування супутникового зв'язку з судном, особиста електронна пошта для благоустрою судна і популяризації користування інтернетом для операційних систем судна, наприклад контроль та керування пристроями судна, також залучення системи управління між судновласниками [5].

Згідно з даними обстеження з міжнародної морської ради (BIMCO) в 2016 року згідно з опитуванням кожен п’ятий респондент зазначив що став жертвою кібератаки і лише 40 відсотків респондентів сказали, що вжили профілактичні заходи в процесі реагування на загрози морській кібербезпеці. ENISA (The European Union Agency for Cybersecurity) [24] класифікував морську галузь як критичний сектор інфраструктури на ряду з (IPS SCADA) інтелектуальними енергосистемами, фінансами та здоров'ям. Міжнародна морська організація (ММО) комісія морської безпеки (МСК) запропонували план управління морськими кіберризиками, відповідно з підвищеним ризиком кібербезпеки і оприлюднив їх 1 січня 2021 року [12].

У цій роботі розглянуті випадки кібербезпеки, які носять глобальний характер та проаналізовані стандарти безпеки в морській галузі.

У MSC 94 [13], США і Канада запропонували посилити кібербезпеку в різних сферах морської галузі. Стверджувалося, що є термінова необхідність в розробці інтегрованих рекомендацій для кібербезпеки портів, морських об'єктів і оперативних систем судна.

Таблиця 1 - Тенденції морської кібербезпеки і інциденти з питань безпеки

Випадок	Дата	Зміст / суть
1	04. 2018	Нігерійська хакерська група атакувала судноплавні компанії Кореї, Японії і Норвегії. Використавши особисту інформацію офіцерів і співробітників 3 корейських судноплавних компаній, 280 суден були уражені для шахрайських дій BEC (Business Email Compromise)
2	03. 2018	Голландська система електронної пошти морської компанії зазнала кібератаку, яка тривала 11 місяців, виконувалась автоматична переадресація листів на хакерські носії і відбувся витік особистої та конференційної інформації.
3	12. 2020	Комп'ютерна система в Сінгапурській морській компанії BW Group вийшла з ладу через хакерську атаку.
2	07. 2019	Clarksons, Велика Британія, морській компанії погрожували оприлюдненням (витіком) конфіденційних даних через відмову виплати суми яку вимагали хакери.
3	10.2021	Maesk була виявлена серйозна вразливість у пов’язаній системі супутникових служб компанії.
4	08. 2017	Близько 10 членів екіпажу пропали безвісти або загинули у катастрофі військово-морського флоту США корабель Джона с.Маккейна. Існує версія що є ймовірність кібератаки.
5	06. 2017	Найбільша у світі судноплавна компанія, Maesk Line, перевстановила 4,000 серверів, 45,000 ПК і 2,500 програмних додатків через хакерську атаку вірус (N o t Pe t y a). Кошторис загальна шкоді склав приблизно 300 мільярдів дол.
6	02. 2019	Навігаційна система 8,250 суден TEU, що належить Німеччині зазнала кібератаку і була паралізована на 10 годин, що дорівнює переходу судна з Кіпра до Джибуті.
7	08. 2016	Вразливість системи т/х Навис, яка була виявлена і оприлюднена онлайн системою в Cargotech корпорація в США, цією системою користуються в США і використовується 13 портами по всьому світу.

Випадок	Дата	Зміст / суть
8	03. 2016	Пірати викрали судно міжнародної судноплавної компанії, вони забрали тільки контейнери завантажені с певні вантажем і втікли. В результаті цього факти що були викриті у системі укладення договорів морського перевезення компанія постраждала від піратський дій, зловмисний код було виявлено в системі документообороту компанії.
9	07.2021	World Fuel Services (WFS), найбільша бункерна компанія у світі, яка поставляє паливо до суден, зазнав втрат на 18 мільйонів доларів США через шахрайські дії електронною поштою - АФЕРА.
10	10. 2017	Наркодилери наняли хакерів, щоб зламати систему Бельгійського портового управління і ідентифікувати контейнери, в яких перевозили кокаїн і героїн, зловмисники видалили їх з системі до прибуття до законного власнику використаних контейнерів. Хакер заразив відповідний ПК за допомогою вірусу Троян, якій був прикріплений до листа e-mail, після активізації вірусу вторгся в офісну систему і заволодів паролем.
11	10. 2018	GPS spoofing атака проти суден у Чорному морі [25] 20 суден відхилилися від курсу. Маніпуляція положенням судна
12	11. 2020	Ransomware Hermes Атака на 2 судна [27] зараження всієї системи судна
13	07. 2020	Атака “Mespinoza/Psza” [27] заражена морська інфраструктура
14	05. 2021	Атака програмою-вимагач на судноплавні компанії [28] всі їхні файли були зашифровані
15	03. 2022	Встановлення зловмисного коду [28] що в свою чергу надав доступ до мережі портів

Судноплавство зробило багато кроків, і на додаток до рекомендацій Міжнародної морської організації (ММО), було видано безліч інструкцій від галузевих організацій, таких як BIMCO, Асоціація круїзної індустрії (CLIA), Міжнародна палата Shipping (ICS), INTERCARGO, INTERTANKO, Міжнародний морський форум нафтових компаній (OCIMF) і Міжнародний союз морського страхування (IUMI) [20].

3.2. Структура і послідовність кібератаки та аналіз кіберуразливості судна

Вразливими об'єктами судна з погляду кібербезпеки, є різні системи, які сьогодні, управляються та контролюються відповідним програмним забезпеченням, а саме інформаційними системами. Варто відзначити, що в різних джерелах наводяться різні погляди на склад цих систем, але здебільшого ці підходи збігаються. Так, основними системами вантажного судна, вразливими для кібератак, є:

- системи навігаційного містка;
- системи управління рухом та механізмами;
- електронні системи відображення карт та інформації (ECDIS);
- автоматична ідентифікаційна система (AIC);
- системи контролю доступу на судно;
- системи управління вантажними операціями;
- системи контрою суднової енергетичної установки;
- адміністративні системи та системи життєзабезпечення екіпажу;
- системи зв'язку.

Деякі компоненти з наведеного вище списку виділені як окремі системи (наприклад, система контролю доступу, система управління сигналізацією, система управління підрулюючими пристроями). Візуальне уявлення розташування цих систем на борту судна показано на Рис 2.

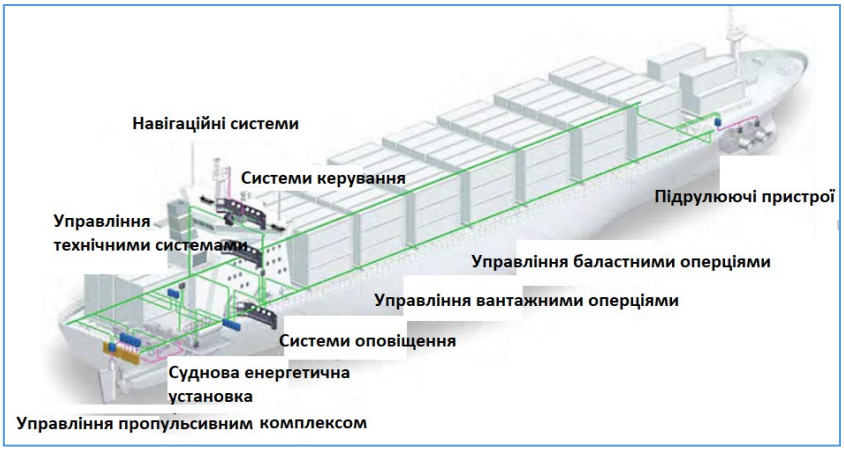

Рис. 2 – Основні системи судна

Сучасні суднові інформаційні системи представляють наступну інформацію:

- дані про власне судно (поточне місце, кінематичні параметри, минулий шлях, запланований маршрут та ряд інших елементів);
- радіолокаційне зображення та кінематичні параметри цілей с засобів

автоматичної радіолокаційної прокладки;

- дані з автоматичної ідентифікаційної системи про інші судна;

- відомості про навігаційні огорожі, про оптичні та радіотехнічні навігаційні засоби, настанови для плавання;

- інформацію берегових систем управління рухом;

- гідрометеорологічні відомості про поточний стан погоди, дані про льодову обстановку, прогноз, тощо.

Особливу небезпеку кібератаки можуть представляти для критичних систем судна або обладнання, раптова відмова якого може створювати небезпечні ситуації на судні, тому вони є життєво важливими для функціонування судна.

Сутність кіберризиків все більше ускладнюється через участь організованої злочинності, міжнародних санкцій та міжнародного регулювання. Судновласники та оператори тепер повинні орієнтуватися в цьому складному питанні на додаток до всіх інших навантажень, з якими стикається сектор. Відсутність належного кіберуправління підриває належну обачність.

Сьогодні кіберзлочинців 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.

Наслідком зараження систем шкідливим програмним забезпеченням може стати зміна даних про судно, включаючи його місцеположення, інформацію про рейс, порти, дані про вантаж. Шкідлива програма може конкретним суднам надсилати 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.

Інша проблема це вплив пандемії COVID-19 та нові виклики для судноплавної галузі, яка стала мішенню групи кіберпіратів, 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 ММО [21] 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.

Тенденція в морській кібербезпеці очевидна: масштаби та частота атак зростають, а кіберпірати все краще й краще вміють виявити слабкі місця кіберзахисту. Незалежно від того, викрадають вони конфіденційні дані з подальшим шантажуванням, порушують роботу критично важливих систем або і те, і інше, мореплавна галузь зазнає великих ризиків.

На відміну від інших галузей, морські та логістичні компанії, як правило, надають дуже обмежену інформацію про будь-яку атаку. Ось чому підготовка до кіберстійкості є більш важливою, ніж будь-коли.

Вразливі суднові системи можуть містити [5]:

1. Системи містку:

- інтегрована система навігації;
- системи позиціонування (GPS тощо);
- інформаційна система відображення електронних карт (ECDIS);
- системи динамічного позиціонування (DP);
- системи, які взаємодіють з електронними навігаційними системами та системами руху/маневрування;
- автоматична ідентифікаційна система (AIC);
- глобальна морська система зв'язку під час лиха (ГМССБ);
- радіолокаційне обладнання;

- реєстратори даних рейсу (РДР);
- система аварійної сигналізації на містку (BNWAS);
- суднові системи охоронної сигналізації (SSAS).

Все більш широке використання цифрових мережевих навігаційних систем з інтерфейсом до прибережних мереж для оновлення та надання послуг робить такі системи вразливими для кіберінцидентів. Системи містку, які не підключені до інших мереж, можуть бути настільки ж уразливі, оскільки знімні носії часто використовуються для оновлення таких систем з інших контрольованих або неконтрольованих мереж. Кіберінцидент може поширюватися і, отже, може вплинути на всі системи, пов'язані з навігацією, включаючи ECDIS, GNSS, AIS, VDR та Radar/ARPA.

2. Системи обробки вантажів та управління:

- пункт управління вантажами (CCR) та його обладнання;
- бортові комп'ютери, які використовуються для обміну інформацією про навантаження та оновлення плану навантаження з морським терміналом та стивідорною компанією;
- дистанційні системи відстеження та виявлення вантажів та контейнерів;
- система індикації рівня;
- система дистанційного керування клапанами;
- системи водяного баласту;
- системи моніторингу рефрижераторів;
- система сигналізації попадання води.

Цифрові системи, що використовуються для навантаження, керування та контролю вантажів, включаючи небезпечні вантажі можуть взаємодіяти з різними системами на березі, включаючи порти, морські термінали та стивідорів. Такі системи можуть містити інструменти відстеження відвантаження, доступні для відправників вантажів через мережу інтернет. Подібні інтерфейси роблять системи управління вантажами та дані у вантажних маніфестах та списках навантаження вразливими для кіберінцидентів.

3. Системи управління рухом та механізмами, управління потужністю:

− регулятор обертів головного двигуна;
− управління живлення;
− інтегрована система управління;
− сигналізація;
− система контролю трюмних вод;
− система очищення води;
− моніторинг викидів;

− моніторинг опалення, вентиляції та кондиціювання;

− системи контролю ушкоджень;

- інші системи моніторингу та збору даних, наприклад пожежна сигналізація.

Використання цифрових систем для моніторингу та управління бортовим обладнанням, рухом та кермовим управлінням робить такі системи вразливими для кіберінцидентів. Вразливість цих систем може зрости при використанні в поєднанні з дистанційним моніторингом на основі стану та/або інтеграції з навігаційним та комунікаційним обладнанням на суднах, які використовують інтегровані системи містка.

4. Системи контролю доступу на судно:

− системи спостереження, такі як мережа відеоспостереження;

− електронні системи бортового персоналу.

Цифрові системи, що використовуються для підтримки контролю доступу для забезпечення фізичної безпеки та захисту судна та його вантажу, включаючи спостереження, суднову охоронну сигналізацію та електронні системи «персонал на борту», вразливі для кіберінцидентів.

5. Системи обслуговування пасажирів та керування ними:

− система управління пасажирами (PMS);

− системи управління судном

− системи, пов'язані з фінансами;

− системи доступу пасажирів/відвідувачів/моряків на борт судна;

− системи підтримки інфраструктури, такі як система доменних імен (DNS) та системи автентифікації/авторизації користувачів;

− системи управління інцидентами.

Цифрові системи, що використовуються для управління майном, посадки та контролю доступу, можуть містити цінні дані про пасажирів. Інтелектуальні пристрої (планшети, портативні сканери і т. д.) самі по собі є вектором атаки, оскільки в результаті зібрані дані передаються в інші системи.

6. Мережі загального користування, обслуговування пасажирів та керування ними:

− пасажирський Wi-Fi та доступ до мережі інтернет по локальній мережі (LAN) з можливістю підключати власні пристрої;

− гостьові розважальні системи.

Фіксовані або бездротові мережі, підключені до інтернету, встановлені на борту для зручності пасажирів, наприклад гостьові розважальні системи, повинні вважатися неконтрольованими і не повинні бути підключені до будь-якої

критично важливої інформаційної системи на борту.

Адміністративні системи та системи соціального забезпечення екіпажу:

− адміністративні системи;

− системи доступу до мережі Wi-Fi або LAN для екіпажу з можливістю підключення особистих пристроїв.

Бортові комп'ютерні мережі, що використовуються для керування судном або забезпечення безпеки екіпажу, особливо вразливі при наданні доступу до мережі інтернет та електронної пошти. Вони можуть бути використані кіберзлочинцями для отримання доступу до бортових систем та даних. Ці системи слід розглядати як неконтрольовані, їх не слід підключати до будь-якої бортової системи, критично важливої для безпеки. Програмне забезпечення, надане керуючими компаніями або власниками суден, також входить до цієї категорії.

Системи зв'язку:

− інтегровані системи зв'язку;

− обладнання супутникового зв'язку;

− обладнання для передачі голосу через інтернет (VOIP);

− бездротові мережі (WLAN);

− системи гучного зв'язку та загальної сигналізації;

Доступність підключення до мережі інтернет через супутник та/або інший бездротовий зв'язок збільшує вразливість судна [23]. Нещодавні дослідження свідчать, що, наприклад, сигнали VSAT уразливі для використання з недорогих мобільних пристроїв, здатних приймати супутниковий сигнал. Слід враховувати системи зв'язку із шифруванням та ретельно вивчити механізми кіберзахисту, впроваджені постачальником послуг, але слід покладатися виключно на них для захисту кожної бортової системи та даних. У ці системи включено канали зв'язку з державними органами для передачі необхідної звітної інформації про судно та вантаж. Застосовані вимоги до управління автентифікацією та контролем доступу з боку цих органів повинні суворо дотримуватися. Також включені суднові можливості для збору даних та моніторинг пристроїв та реєстраторів даних, прикріплених до вантажів, для подальшої передачі призначеним отримувачам на березі.

Крім вищезгаданих категорій, можна виділити в окрему категорію системи базової інфраструктури та системи захисту, що включають:

− шлюзи безпеки;

− маршрутизатори;

− перемикачі;

− міжмережові екрани;

− віртуальні приватні мережі (VPN);

− віртуальну мережу LAN (VLAN);

− системи запобігання вторгненням;

− системи реєстрації подій безпеки.

Кіберуразливості як передумови для реалізації кіберзагроз слід розглянути більш детально. Наявність вразливих суднових систем не гарантує безпосередню кіберзлочинцям реалізацію кіберзагрози та виникнення кіберінциденту. Але існують уразливості, які є передумовами для можливої реалізації задуманого кіберзлочинцями. Дані вразливості можуть бути використані, у тому числі через розглянуті вище вразливі системи судна.

Нижче наведено деякі поширені кіберуразливості, які можуть бути виявлені на борту нових та існуючих суден [26]:

− застарілі та непідтримувані операційні системи;

− неактуальні (неоновлені) версії системного програмного забезпечення;

− застаріле або відсутнє антивірусне програмне забезпечення та захист від шкідливих програм;

− неадекватні конфігурації безпеки, включаючи неефективне керування мережею та використання облікових записів та паролів адміністраторів за замовчуванням;

− суднові комп'ютерні мережі, в яких відсутні заходи захисту та сегментація мереж;

− критично важливе для безпеки обладнання або системи, завжди підключені до берега;

− недостатній контроль доступу до кіберактивів, мереж тощо для третіх сторін, включаючи підрядників та постачальників послуг;

− недостатньо навчений та/або кваліфікований персонал для управління кібер ризиками;

− відсутні, неадекватні чи неперевірені плани та процедури на випадок непередбачуваних обставин.

Кіберуразливості на борту судна можна віднести до однієї з наступних категорій:

− тимчасові вразливості, такі як дефекти програмного забезпечення, застарілі або невиправлені системи;

− помилки технічного проектування, такі як керування доступом або некеровані мережеві з'єднання;

− помилки реалізації, наприклад неправильно налаштовані міжмережові

екрани;

− процедурні або інші помилки користувача.

Зазначимо, що автономні системи будуть менш уразливими для зовнішніх кіберінцидентів, в порівнянні з системами, підключеними до неконтрольованих мереж або безпосередньо підключені до інтернету. Слід розуміти, які важливі суднові системи та яким чином підключені до неконтрольованих мереж, і враховувати людський фактор, тому що багато інцидентів ініціюються діями екіпажу чи береговим персоналом.

Типи кіберзагроз, існують дві категорії кіберзагроз, які можуть торкнутися компанії та судна [3]:

− нецільові атаки, коли системи та дані компанії чи судна є однією з багатьох потенційних цілей;

− цільові атаки, коли системи та дані компанії чи судна є передбачуваною метою або однією з кількох цілей.

Нецільові атаки можуть використовувати інструменти та методи, доступні в Інтернеті, для виявлення та використання широко поширених уразливостей, які можуть існувати в компанії та на борту судна. Приклади деяких інструментів і методів, які можуть використовуватися в цих обставинах, включають:

− шкідливе програмне забезпечення, призначене для доступу до комп'ютера або його пошкодження, модифікації несанкціонованого доступу до файлів без відома власника. Існують різні типи шкідливих програм, включаючи трояни, програми здирники, шпигунське програмне забезпечення, віруси та черв'яки;

− експлойти. Термін «експлойт» означає комп'ютерну програму, фрагмент програмного коду або послідовність команд, що використовує вразливості в програмному забезпеченні та застосовувані для проведення атаки на систему [6]. Цими вразливостями можуть бути, наприклад, помилка коду, несправність обладнання та/або помилка в реалізації протоколу. Дані вразливості можуть використовуватися віддалено або запускатися локально, наприклад частина шкідливого коду може виконуватися користувачем через посилання, що розповсюджуються у додатках до електронної пошти або через шкідливі веб-сайти;

− «водопою» – створення підробленого веб-сайту або злом справжнього веб-сайту для використання відвідувачами, які нічого не підозрюють;

− сканування – довільний пошук у великих частинах інтернету вразливостей, які можна використовувати для кібератаки;

− тайпсквоттінг, або перехоплення URL-адрес, підроблена URL-адреса. ґрунтується на помилках, такі як помилки зроблені інтернет-користувачами під

час введення адреси веб-сайту у веб-браузер. Якщо користувач випадково введе неправильну адресу веб-сайту, він може потрапити на альтернативний і часто шкідливий веб-сайт.

Цільові атаки можуть бути більш витонченими та використовувати інструменти та методи, спеціально створені для націлювання на певну компанію чи судно. Приклади інструментів та методів, які можуть використовуватися в цих обставинах, включають:

− соціальну інженерію – нетехнічний метод, який використовується для маніпулювання інсайдерами з метою порушення процедур безпеки та отримання інформації, зазвичай за допомогою взаємодії через соціальні мережі та електронну пошту;

− брутфорс – атака з перебором безлічі паролів, сподіваючись вгадати їх правильно. Зловмисник систематично перевіряє всі можливі паролі, доки не буде знайдено правильний;

− credential stuffing – використання раніше скомпрометованих облікових даних або певних часто використовуваних паролів для спроби несанкціонованого доступу до системи або додатка;

− відмова в обслуговуванні (DoS, DDoS), яка не дозволяє законним та авторизованим користувачам отримати доступ до інформації, зазвичай шляхом наповнення мережі даних. Розподілена атака типу «відмова в обслуговуванні» (DDoS) бере під контроль кілька комп'ютерів та/або серверів для реалізації DoS-атаки;

− фішинг – відправка електронних листів великої кількості потенційним цілям із проханням надати певні фрагменти конфіденційної інформації. Електронний лист також може містити шкідливе вкладення або запит на відвідування людиною підробленого веб-сайту з використанням гіперпосилання, що міститься в електронному листі;

− цільовий фішинг, коли жертвами стають особисті електронні листи, які часто містять шкідливе програмне забезпечення або посилання, які автоматично завантажують шкідливе програмне забезпечення;

− підрив ланцюжка поставок – кібератака на компанію чи судно шляхом компрометації обладнання, програмного забезпечення або допоміжних послуг, що надаються компанії або судну.

Наведені вище приклади не є вичерпними, розвиваються й інші методи кібератак. З урахуванням прогресу в галузі автономного судноплавства слід очікувати появи нових кіберзагроз, націлених на цей напрямок. Можлива кількість і витонченість інструментів і методів, що використовуються в

кібератаках, продовжують розвиватися та обмежуються лише винахідливістю тих організацій та окремих осіб, які їх розробляють.

Сучасні технології можуть додати судну уразливості, особливо якщо є незахищені мережі та вільний доступ до інтернету. Крім того, береговий і бортовий персонал може не знати, що деякі виробники обладнання підтримують віддалений доступ до суднового обладнання та його мережевої системи. Невідомий та неузгоджений віддалений доступ до діючого судна слід враховувати як важливу частину оцінки ризику.

До деяких IT- та OT-систем можна отримати віддалений доступ і вони можуть мати безперервне підключення до інтернету для віддаленого моніторингу, збору даних, обслуговування, безпеки. Це можуть бути «сторонні системи», за допомогою яких підрядник відстежує та обслуговує системи з віддаленого місця, і вони можуть мати як двосторонній потік даних, так і лише завантаження.

Таким чином, ще раз необхідне підкреслити, що будь-які заходи не можуть гарантувати абсолютну кібербезпеку. З цієї причини слід досягати такого співвідношення складності системи забезпечення безпеки та реальних умов функціонування інформаційних систем, яке не призводило до перевищення вартості розробки, впровадження, експлуатації та обслуговування системи забезпечення безпеки над масштабами можливої шкоди у разі її порушення [11]. Сьогодні найслабшою ланкою, коли йдеться про кібербезпеку, є людський фактор. Тому важливо, щоб моряки проходили належну підготовку, яка допоможе їм виявляти кіберінциденти та повідомляти про них.

3.3. Визначення передумов кібератаки і етапів інциденту та прогнозування кіберзагроз на судні

На жаль, проблеми інформаційної безпеки судна найчастіше відносять до другорядних, або взагалі змішують їх із загальними проблемами безпеки та автоматизації. При цьому передбачається, що у разі виникнення проблем, пов'язаних з порушенням конфіденційності, цілісності інформації, вдасться вжити своєчасних і адекватних заходів, однак як свідчить практика, такий підхід не є виправданим та ефективним в протидії кіберпіратству.

Етапи кібератаки: тривалість часу для підготовки кібератаки може визначатися мотивами та цілями зловмисника, а також стійкістю технічних та процедурних засобів захисту, що реалізуються компанією, у тому числі на судні та в компанії. При розгляді цільових кібератак зазвичай спостерігаються такі

стадії:

1. Обстеження/розвідка. Відкриті та загальнодоступні джерела, такі як соціальні мережі, що використовуються для отримання інформації про потенційну мету (наприклад: компанія, судно або члена екіпажу) під час підготовки до кібератаки. Соціальні мережі, технічні форуми та приховані властивості веб-сайтів, документів та публікацій можуть використовуватися для виявлення технічних, процедурних та фізичних уразливостей. Використання відкритих/загальнодоступних джерел може бути доповнено моніторингом (сніффінгом) фактичних даних, що надходять з або до компанії чи судна;

2. Доставка. Кіберзлочинці можуть спробувати отримати доступ до систем та даних компанії та судна. Це може бути зроблено або всередині компанії, або на судні, або видалено через підключення до мережі інтернет. Приклади методів, які використовуються для отримання доступу:

1. − онлайн-сервіси компанії, включаючи системи відстеження вантажів чи контейнерів;

2. − надсилання співробітникам електронних листів, які містять шкідливі файли або посилання на шкідливі веб-сайти;

3. − надання заражених знімних носіїв, наприклад як частина оновлення програмного забезпечення бортової системи;

4. − створення помилкових або хибних веб-сайтів, які заохочують розкриття персоналом інформації про обліковий запис користувача;

3. Порушення. Ступінь, в якій кіберзлочинець може зламати систему компанії або судна, залежатиме від значущості виявленої вразливості та обраного методу атаки. Слід зазначити, що порушення може не призвести до будь-яких очевидних змін у стані обладнання. Залежно від серйозності порушення кіберзлочинець може:

− вносити зміни, що впливають на роботу системи, наприклад переривати або змінювати інформацію, що використовується навігаційним обладнанням;

− отримувати доступ, робити копії або змінювати оперативно важливу інформацію, таку як списки вантажів, або комерційно конфіденційні дані, такі як вантажні маніфести та/або списки членів екіпажу та пасажирів/відвідувачів;

− досягти повного контролю над системою, наприклад, системою управління обладнанням;

4. Поворот. Це метод використання вже скомпрометованої системи для атаки на інші системи у тій самій мережі. На цьому етапі атаки кіберзлочинець використовує першу скомпрометовану систему для атаки на інші недоступні системи. Як правило, атаці піддається найбільш вразлива частина системи

жертви з найнижчим рівнем захисту. Після отримання доступу кіберзлочинець спробує зламати решту системи. Зазвичай на етапі повороту кіберзлочинець може спробувати:

− завантажувати в систему інструменти, експлойти та скрипти для полегшення нового етапу атаки;

− виконувати виявлення сусідніх систем за допомогою інструментів сканування або відображення мережі;

− встановити постійні інструменти або реєстратор ключів для збереження та підтримання доступу до системи;

− виконувати нові атаки на систему

Суб'єкти кіберзагроз мають різний ступінь навичок і ресурсів, щоб потенційно загрожувати безпеці судна і морським компаніям.

Приклади основних суб'єктів кіберзагроз [12]:

− випадкові суб'єкти;

− власні співробітники;

− ідеологічно мотивовані особистості (наприклад, активісти, опортуністи та ін.);

− злочинці та організовані злочинні спільноти (у тому числі піратські/ хакерські);

− особи або компанії-конкуренти;

− держави / державні спонсоровані організації;

− терористи / терористичні угруповання.

Мотиви кіберзлочинців можуть бути різноманітними. На відміну від суб'єктів які є співробітниками морської компанії, які ненавмисно створили кіберінцидент, не маючи на це мотиву, більшість суб'єктів має конкретну причину для організації та проведення кібератаки. Основні мотиви для умисної кібератаки на компанії та судна можуть бути поділені на наступні категорії [28]:

- кібервандалізм – злочинна діяльність технічно-інформаційного рівня, включаючи порушення роботи систем, пошкодження веб-сайтів і несанкціонований доступ до систем, дані дії можуть бути скоєні, наприклад, початківцями хакерами;

- інсайдерська діяльність, що здійснюється, наприклад, незадоволеним персоналом або підрядниками з метою помсти;

- активізм – прагнення до розголосу, наприклад, засобами масової інформації, або надання тиску на користь конкретної мети чи причини;

- конкурентна діяльність – прагнення створити конкурентну перевагу з метою завдати шкоди опоненту, заподіяти фінансові чи репутаційні втрати,

наприклад, шляхом збору бізнес-інформації, крадіжки інтелектуальної власності, збору конфіденційної конкурентної інформації направленої на зрив бізнес-операцій;

- шпигунство (у тому числі промислове та комерційне шпигунство) це пошук несанкціонованого доступу до конфіденційної інформації (інтелектуальна власність, комерційна інформація, корпоративні стратегії, особисті дані) та порушення у державних чи комерційних цілях;
- організована злочинність – переважно обумовлена фінансовою вигодою, може включати злочинні збитки, крадіжку вантажу, контрабанду товарів і людей, а також спроби ухилитися від сплати податків та акцизів;
- тероризм – використання судна для заподіяння фізичних та економічних потрясінь;
- конфлікт між національними державами, метою якого є порушення перевантажувальних систем, інфраструктури, порушення оперативного використання і виведення з ладу судна.

Завдання та цілі кіберзлочинців можуть бути охарактеризовані слідуючи чином. Мотиви зловмисників визначають конкретні завдання та цілі при кібератаці, яких вони хочуть досягти і які будуть визначати вплив, що чиниться на систему та дані компанії чи судна. Перелічимо загальні приклади завдань та цілей при кібератаці [15]:

- доступ до комерційних або конфіденційних даних про вантаж, екіпаж, відвідувачів;
- маніпулювання списками екіпажу або пасажирів/відвідувачів, вантажними маніфестами, планами розміщення або вантажними листами;
- повна відмова в обслуговуванні в бізнес-системах, операційних та IT-системах судна;
- видалення критично важливої інформації про рейс/вантаж/пасажирів або іншу службову інформацію;
- шахрайське перевезення незаконних вантажів або полегшення крадіжок;
- порушення нормальної роботи компанії, суднових систем та судна в цілому;
- перешкоджання обробці певних вантажів;
- вимога викупу (шантаж) за службову чи особисту інформацію;
- інші.

3.4. Розроблення способів ефективної протидії кіберпіратству та кіберзагрозам на морі

Кіберпірати продовжують функціонувати на ринку морського транспортування, що вважається вразливою і високоприбутковою ціллю, що було продемонстровано сучасною статистикою, згідно з якою на 400% збільшилися спроби кіберпіратів зчинити кібератаку в морській галузі в період з лютого по червень 2021 року. Зловмисники вимагачі, як повідомляється, заробили щонайменше 350 млн доларів США крипто валюти в 2022 році, показники різко зросли в порівнянні з 2018 роком. В свою чергу це змушує задуматися міжнародних судновласників про забезпечення надійного кіберзахисту.

Зловмисне програмне забезпечення кіберпіратів, яке як правило встановлено дистанційно спричиняє атаку на програмне забезпечення, щоб заблокувати доступ користувача до комп'ютерних систем або даних з метою вторгнення і блокування системі з подальшим вимаганням викупу в обмін на доступ, як правило, кібератаки відбуваються несподівано. Сегмент морського бізнесу замкнений з його IT-системами, з системами постачальників, системами судна, портовими системами, в процесі кібер-інциденту не може отримати дані, доступ до документів, що в сою чергу паралізує функціонування морської компанії. Хоча на борту судна IT-систем завжди знаходили шкідливе програмне забезпечення, більшість кібератак були здійснені на берегові системи морської галузі, такі як системи офісу морських компаній чи логістичних компаній. Атака на програмне забезпечення не тільки шифрує бізнес-систему, але й часто супроводжується загрозою опублікувати конфіденційну інформацію публічно. Наслідки цього подвійного здирництва можуть бути потенційно небезпечними, навіть катастрофічними. Сектор лілейних операцій, що володіє великими обсягами даних клієнтів, особливо вразливий. Фінансові ризики та їх наслідки для морського бізнесу можуть бути важкими. Крім втрат, пов'язаних з зривом морських операцій і перспективою виплати фрахту, існують супутні витрати на реагування на інцидент і затримки перевезення вантажу, що виникають в результаті кібератакі на галузь. Слід ще додати до цього витрати на вирішення потенційних скарг клієнтів/споживачів, витрати на залучення засобів реагування на інцидент, а також будь-які судові позови третіх осіб, чия особиста інформація була скомпрометована інцидентом, а також вартість будь-яких можливих штрафних санкцій, кількість матиме тенденцію до зростання. Репутаційні збитки також, ймовірно, виражені у втраті поточних і потенційних можливостей бізнесу, і можуть призвести до довгострокової втрати клієнтів, які прагнуть уникнути

ризиків в співпраці з морською галуззю, що розглядається як уразлива, особливо якщо порушення було прийнято як неминуче.

Після будь-якої кібератаки, першим намаганням морської компанії буде спроба терміново відновити свої системи і відновити операційний контроль. Компанія також буде прагнути запобігти будь-якій загрозі оприлюднення конфіденційних даних. Перше, що потрібно розглянути, чи є, потенційна альтернатива сплати викупу, чи є інший варіант протидії кібератаці. Якщо існує альтернативний варіант протидії кіберпіратству, то він повинен бути досліджений паралельно з своєчасним виявленням та відновленням безпеки системи для запобігання повторних атак.

Коли кіберпірати стверджують, що отримали доступ до конференційних даних для судноплавної компанії важливо перевірити цю інформацію. Чи справді хакери проникли в системи і отримали копію цих даних, чи роблять вони хибні твердження та/або покладаються на інформацію, зібрану ззовні з відкритих джерел.

У процесі залучення до дискусій і переговорів з кіберпіратами, слід спробувати створити профіль зловмисника. Ця інформація буде корисною для визначення намірів виконавців і визначення найбільш відповідних методів ведення переговорів. Деякі хакери розвинули репутацію «надійних» переговірників, в той час як інші можуть бути непередбачуваними та ненадійними.

В процесі розвитку та впровадження інноваційного прогресу, були розробленні кроки для перевірки ключів розшифровки, призначених для розблокування паралізованої системи. Що в свою чергу стосується кіберзагрози, чи аналізу інформації про її ідентичність. Критичні показники що подаються аналізу включають адреси електронної пошти, які використовуються для спілкування, надану адресу криптовалюти, будь-які унікальні ідентифікатори, і будь-яка інформаційні яка має відношення до інциденту, вся ця інформація перехресно перевіряється з визнаними санкційними списками.

Також першорядним є забезпечення можливого захисту IT-системам, які були скомпрометовані, по-перше слід запобігти подальшому розповсюдженню вірус-вимагача і запобігти подальшому нападу з боку кіберпіратства.

Інші важливі моменти:

- попередити правоохоронні органи про кримінальну подію і вимогу викупу;
- визначити і виконати різні звітні зобов'язання щодо санкцій, боротьби з відмиванням грошей, тероризмом та іншим закон порушенням;

- повідомити страхові компанії (якщо такі є) відповідно до полісу кіберстрахування;
- встановити законність і правомірність будь-якої перспективної виплати викупу.

Санкції також необхідно враховувати, щоб судноплавна компанія не порушила правила у застосованих санаційних обмежень. Санкції ЄС поширюються на громадян і компаній ЄС, а також на весь бізнес, що функціонує в ЄС, включаючи діяльність на судні, що знаходиться під юрисдикцією держави-члена ЄС. При цьому особам та суб'єктам ЄС заборонено, мати будь-які грошові операції з суб'єктами, що занесені до Європейського санкційного списку кіберзлочинців, який був створений в травні 2019 року і включає такі утворення і організації, як WannaCry, NotPetya та Operation Cloud Hopper. Виплата викупу вимагачам після кібератак підлягатимуть посиленому контролю і перевірці, власники суден, фрахтувальники або агенти, що сплатили викуп, повинні переконатися що не наражають себе на цивільну чи кримінальну відповідальність/

1 жовтня 2020 року OFAC опублікувала свої останні рекомендації у відповідь на зростання зловмисних кібератак пов'язаних з системи США під час пандемії. Консультативна рада попереджає компанії про потенційні ризики санкцій за надання викупу вимагачу, який може бути санкціонованим суб'єктом, а також встановлює фактори, що розглядаються при визначенні належного реагування на примусове виконання з явним порушенням. В останні роки, збільшилася кількість кібератак в морській галузі, саме тому FinCEN (The Financial Crimes Enforcement Network), урядове бюро США 1 жовтня 2020 року посилило відстеження фінансових операцій з метою боротьби з фінансовими злочинами.

Судноплавна компанія, зіткнувшись з кібератакою, може опинитися в незавидній ситуації або зіткнутися з наслідками порушення закону і/або санкцій, якщо компанія сплатить викуп або зіткнеться з наслідками кібератаки. Це може призвести до того, що системи компанії будуть паралізованими і недоступними для повноцінного функціонування, може спричинити руйнування системного забезпечення компанії чи оприлюднення конфіденційної інформацію, що включає приватну інформацію клієнтів, співробітників, комерційних партнерів, із забезпеченням ризику судових процесів від потерпілих сторін. Ризик високий. Понад 50 млн дол. криптовалюти, яку компанії виплатили на адреси кіберпіратів у 2020 році, була ідентифікована як фінансові оборудки які підпадають під санкції, Doppelpaymer і WastedLocker [27].

Кіберпіратство стає все більш витонченим. За оцінками експертів галузі напади, ймовірно, продовжать зростати у морському секторі завдяки зростанню вразливості систем в процесі впровадження інновацій, переходу до дистанційної праці в офісах компаній, в тому числі внаслідок пандемії. Законодавча та регуляторна база продовжить розвиватися разом з переліком міжнародних санкцій що можуть накладатися на компанії. Однак ті, компанії що задіяні у морському секторі повинні зберігати пильність. Не слід зневажати загрозою що несе кібератака яка включає вірусне програмне забезпечення, яке може бути використано паралельно з іншими кіберінцидентами, такими як хакерство систем портової логістики з метою крадіжки, як приклад, цінного вантажу. Хакери та кіберпірати навіть можуть здійснювати атаки в тандемі, щоб унеможливити здатність систем безпеки судна або портового обладнання протидіяти атаці, втім правопорушники можуть вдатися до фізичного пошкодження, тобто дистанційно відключення, скажімо, насосів або систем охолодження. З іншого боку інноваційний розвиток концепції автономних суден надає можливість віддаленого доступу до процесів керування судном, що в свою чергу може спричинити зіткнення з іншими суднами або перешкодами або навіть використовування самого судна як зброї.

Тому для морської галузі за необхідне буде розроблення інноваційних систем інформаційного захисту і їх постійного вдосконалення саме як засоби протидії кіберпіратству. До практичних організаційних заходів і методів забезпечення інформаційної безпеки судна відносять:

- Вибір надійного пароля. Надійний пароль не є пов’язаний з користувачем містить щонайменше 8 різних типів символів. Не зберігайте свої паролі у файлі чи в інтернет-браузері, особливо в випадку використання загальнодоступного чи спільного комп’ютера.
- Обережне користування електронною поштою. Не відкривайте вкладення та не натискайте на посилання в інтернеті.
- Не переміщення своїх професійних повідомлень електронної пошти в особисті повідомлення.
- Не використання особистих пристроїв зберігання таких як :USB-ключ, зовнішній жорсткий диск, хмара
- Слід обережно поводитися в соціальних мережах, форумах, тощо: остерігайтеся поширення вашої особистої інформації через інтернет.
- Контролюйте встановлене програмне забезпечення на ІТ-пристроях.
- Встановлюйте лише те програмне забезпечення, яке вам дійсно потрібно, і завжди за попередньою згодою адміністратора компанії.

- Завантажуйте програмне забезпечення лише з перевірених веб-сайтів і регулярно оновлюйте його.

Також рекомендується розділяти особисте та професійне використання:

- не пересилайте професійні електронні листи на особисті поштові скриньки;
- не зберігайте професійні дані на особистих пристроях (USB-накопичувач, смартфон тощо) або в особистих онлайн-сховищах;
- не підключайте особисті знімні носії наприклад: USB-ключ, зовнішні жорсткі диски до суднових комп'ютерів або комп'ютерів компанії.

Також слід донести до відома офіцерський склад судна о необхідності наступних протидій кіберпіратству:

- створити резервну копію своїх даних, щоб відновити їх у разі втрати чи крадіжки пристрою;
- переконайтеся, що ваші паролі не зберігаються на вашому пристрої;
- тримайте свої пристрої та носії інформації при собі (не залишайте їх в офісі та, якщо вони містять конфіденційну інформацію, не користуйтеся готельним сейфом);
- вимкніть Wi-Fi і Bluetooth, коли ви не використовуєте свої пристрої;
- якщо ви змушені залишити телефон, вимкніть його та, якщо можливо, виміть SIM-карту та акумулятор;
- інформувати компанію судновласника у разі перевірки або конфіскації вашого пристрою іноземними органами;
- ніколи не підключайте свій пристрій до обладнання, якому не можна довіряти;
- Ніколи не використовуйте подаровані вам USB-ключі: пошкоджені USB-ключі зазвичай використовуються хакерами для зараження електронних пристроїв шкідливим програмним забезпеченням.

Обізнаність екіпажу та персоналу щодо передових практик безпеки є фундаментальною для ефективного зниження ризиків, пов'язаних із небезпечною поведінкою. Запобігання атакам на інформаційну систему можна здебільшого досягти за допомогою простих нормативів, таких як ті, що представлені в цих рекомендаціях. Тому важливо, щоб усі були залучені та обізнані за допомогою інструктажів, інструкцій та, в ідеалі, статуту користувача. Для забезпечення кібербезпеки інформації на борту судна рекомендується робити регулярні резервні копії. В ідеалі захищена мережа сервера зберігання даних - або NAS (Network Attached Storage) - може бути встановлена в судновій мережі. Такий сервер складається з кількох резервних дисків, що забезпечує

високий захист даних. Слід регулярно проводити перевірку NAS, щоб якомога раніше виявити можливі несправності диска.

Тому потрібно прийняти кілька контрзаходів і глибинних стратегій оборони з метою побудови стійкості до зовнішніх і внутрішніх загроз кібербезпеці [26]. Перший — створення безперервної системи моніторингу, яка може надавати аналітичну інформацію в режимі реального часу про стан систем судна. У цьому контексті, технологія блокчейну була запропонована для поліпшення безпеки управління кібербезпекою судна [27]. Головна перевага технології блокчейну, включає трекездатність, прозорість, можливість повної перевірки доступу до даних, непорушність і децентралізація, технологія надає можливість забезпечити безпечний зв'язок і безпечне зберігання даних, що обмінюються між суднами і центром контролю берега. Використання цієї технології дозволить усунути деякі критичні загрози кібербезпеки для мереж зв'язку судна, а саме втрата даних, зміна даних зловмисниками або викрадення даних [27]. Згідно з новітніми інноваційними дослідженнями саме блокадна технологія буде відігравати головну роль в ідентифікації і забезпеченні кіберзахисту, забезпечуючи цілісність даних і інформаційну безпеку в майбутньому в морській промисловості.

Таблиця 2 - Засоби і способи ефективної протидії кіберзагрозам та кіберпиратству на морі

Засоби протидії	**Методи протидії кібератаки і пом'якшення наслідків**
Автоматизована ідентифікаційна система (AIC)	- Вся інформація про AIC повинна бути перевірена; - Шифрування сигналів УКХ; - Контроль цілісності інформації про трансляцію повинен бути забезпечено, щоб позиція та ідентичність були подані правильними; - Обладнання, яке транслює сигнали AIC, повинно бути забезпечене захистом, а несанкціонований доступ не повинен бути можливим; - Попередження навігації слід розглядати, якщо транслюються хибні сигнали AIS.
Система (ECDIS) Electronic Chart Display Information System	- Розробники ECDIS повинні постійно удосконалювати безпеку; - Регулярна документація, моніторинг, і виправлення ECDIS структури; - Оновлення схеми ECDIS має відслідковуватися та реєструватися, особливо вручну через CD або USB-диск; - Всі файли оновлення повинні бути відскановані антивірусним програмним забезпеченням;

Засоби протидії	**Методи протидії кібератаки і пом'якшення наслідків**
	- Внутрішня мережа, з якою пов'язаний ECDIS, повинна бути обстеженою, щоб діагностувати, чи система ECDIS може бути повністю ізольованою або за брандмауером; - Тільки затверджені співробітники повинні мати фізичний доступ до ECDIS і його основних компонентів.
GNSS and GPS	- Ідентифікація та автентифікація пристрою; - Криптографічний захист; - Захист інформації у стані спокою.
Радар	- Ідентифікація та автентифікація пристрою; - Криптографічний захист; - Резервне копіювання інформаційної системи.
Global Maritime Distress and Safety System (GMDSS)	- Криптографічний захист; - Ідентифікація та автентифікація пристрою; - Захист інформації у стані покою; - Фізичний контроль доступу; - План дії у непередбачених обставинах.
Industrial Control Systems (ICSs)	- Використовувати криптографію або інші захищені методи для захисту паролів від несанкціонованого перехоплення; - Для збереження систем управління безпечними, реалізації управління конфігурацією і управління патчними засобами; - Наскільки це можливо, зв'язок між зонами безпеки повинен охоронятися; - Забезпечити захист всіх підключених до Інтернету пристроїв ІПС і регулярну оновлення паролів; - Адміністратори мережі ICS повинні використовувати правила сегментації мережі та брандмауера, які блокують доступ до файлообмінних портів; - Убезпечити файли складнішими хешованими паролями; - Системні адміністратори повинні забезпечити виконання залучення складних паролів; - Використання конкретної політики віддаленого доступу; - Аудиторський віддалений доступ і пов'язані з ним зміни; - Заблокувати непотрібні USB-порти; - Забезпечити навчання з обізнаності про кібербезпеку для всіх користувачів.
Силова установка і механізм управління і системи контролю	- Резервне копіювання інформаційної системи; - Моніторинг фізичного доступу.

Засоби протидії	**Методи протидії кібератаки і пом'якшення наслідків**
Very Small Aperture Terminal (VSAT)	- Треба розглядати зашифровані системи зв'язку; - Механізми кіберзахисту постачальника послуг повинні бути ретельно розглянуті, але вони не повинні покладатися виключно на захист кожного пристрою і даних на судні; - Автентифікація та управління доступом повинні бути суворо дотримані; - Захист інформації у стані покою.
Мережа IT систем	- Резервне копіювання інформаційної системи; - Автентифікація та контроль доступу; - Сегментація функцій екіпажу та бізнесу; - Забезпечити механізми захисту від загроз; -Управління системою керування конфігурацією/патч/оновленням; - Забезпечити правила BYOD; - Забезпечити навчання з обізнаності про кібербезпеку для всіх користувачів.
Людський фактор	- Сприяння культурі кібербезпеки всередині організації; - Забезпечити навчання з кіберобізнаності; - Оцінити ефективність навчання за допомогою модулювання кіберінцидентів; - Сприяти кібергігієні в середині екіпажу.

Висновки

Морська кібербезпека це проблема сьогодення, яка, привертає все більшу увагу та викликає занепокоєння. З погляду на те що сучасні суднові системи добре інтегровані, втім вони залишаються погано захищені що створює величезні потенційні ризики. Оскільки судна все більше покладаються на автоматизацію та дистанційний моніторинг, такі ключові системи, включаючи навігаційне обладнання, можуть бути скомпрометовані в разі атаки або якщо мимоволі завантажується вірус. Важливо оцінити кожен із факторів кіберзагрози, щоб зменшити ймовірність уразливості інформаційної безпеки судна, які могли б дозволити зловмиснику отримати доступ до системи судна. Одним з перших кроків у протидії потенційним кібератакам є усвідомлення вразливостей, які по суті є нішею в мережі. Однак, інтеграція комплексного плану безпеки в мережеві системи судна забезпечує найефективніший спосіб підготуватися до кібератаки і ефективно протидіяти їй. Для досягнення цього необхідно провести комплексну оцінку ризиків, і це сприятиме розробці надійних способів ефективної протидії кіберзагрозам та кіберпіратству на морі.