УДК 007:656.61
DOI 10.47049/2226-1893-2023-2-124-133

КІБЕРБЕЗПЕКА НА МОРСЬКОМУ ТРАНСПОРТІ

Ю.В. Даус
к.геогр.н, помічник ректора з інформаційної діяльності та кібербезпеки,
доцент кафедри «Технічна кібернетика й інформаційні технології
ім. проф. Р.В. Меркта»
ORCID: 0000-0001-9737-4663

М.Є. Даус
к.геогр.н., доцент кафедри «Безпека життєдіяльності, екології та хімії»
ORCID: *0000-0001-5298-795X*

О.І. Полікаровських
д.т.н, професор кафедри «Технічна кібернетика й інформаційні технології
ім. проф. Р.В. Меркта»
ORCID: 0000-0002-1893-7390

Д.Г. Ларін
к.т.н., доцент кафедри «Технічна кібернетика й інформаційні технології
ім. проф. Р.В. Меркта»
Scopus id: 6602177580

Одеський національний морський університет, Одеса, Україна

Анотація: *Сучасний світ все більше залежить від застосування комп'ютерних технологій.*

Застосування таких технологій допомагає знизити собівартість кінцевого продукту, збільшити продуктивність та зменшити вплив людських помилок на виробничі процеси і являється основою прогресу людства. Однак, при цьому зростає кількість кіберінцидентів на морському транспорті, що може призвести до великих втрат, і не тільки грошових, але й екологічних, технологічних та іміджевих.

Тому компаніям дуже важливо побудувати систему кіберзахисту на судні, використовуючи цілісну систему захисту, найновіші засоби ідентифікації користувачів та користуватися настановами ІМО.

Ключові слова: *морський транспорт, кібербезпека, суднові комп'ютерні системи, кіберінцидент, план кібербезпеки судна.*

UDC 007:656.61
DOI 10.47049/2226-1893-2023-2-124-133

CYBER SECURITY ON MARITIME TRANSPORT

Y.V. Daus
Ph.D. rector's assistant to the for information activities and cyber security,
docent of the Department «Technical Cybernetics and Information Technologies
named after prof. R.V. Merkt»
ORCID: 0000-0001-9737-4663

M.E. Daus
Ph.D., docent of the Department «Safety of Life, Ecology and Chemistry»
ORCID: *0000-0001-5298-795X*

O.I. Polikarovskykh
D.Sc., professor of the Department «Technical Cybernetics and Information Technologies
named after prof. R.V. Merkt»
ORCID: 0000-0002-1893-7390

D.G. Larin
Ph.D., docent of the Department «Technical Cybernetics and Information Technologies
named after prof. R.V. Merkt»
Scopus id: 6602177580

Odesa national maritime university, Odesa, Ukraine

Abstract: *The modern world is very much dependent on the use of computer technologies. The use of such technologies helps to reduce the cost of the final product, increase productivity and reduce the impact of human errors on production processes and is the basis of human progress. However, the number of cyber incidents in maritime transport is increasing that can lead to large losses, and not only money, but also environmental, technological and image. Therefore, it is very important for companies to build a cyber security system on board, use the latest user identification tools and use IMO guidelines.*

Keywords: *maritime transport, cybersecurity, ship computer systems, cyber incident, ship cybersecurity plan.*

Вступ. У сучасному світі великого значення набуває використання комп'ютерних технологій, які дозволяють значно економити на людських ресурсах, що в свою чергу знижує собівартість кінцевого продукту. Комп'ютерні технології все частіше і частіше стають невід'ємною частиною не тільки нашого повсякденного життя, але й невід'ємною частиною виробничого циклу та сервісних послуг. Віддалені сервіси та комунікаційні програми дозволяють отримати доступ до банківських рахунків, дистанційно навчатися, робити покупки та замовлення.

Але з більш широким застосуванням таких технологій, виникає необхідність захисту таких систем від зловмисного втручання в їх роботу. На сьогодні таке втручання вже перейшло від невдалого жарту до арсеналу збройних сил. Все частіше і частіше таке втручання приносить значні фінансові втрати не тільки для фізичних осіб, але і для компаній, великих корпорацій та державних органів. Тому вкрай необхідно проаналізувати всі загрози, та розробити комплекс заходів для мінімізації можливих втрат внаслідок кіберінцидентів.

Постановка задачі. Комп'ютерні технології, розвиваючись шаленими темпами, все частіше і частіше змінюють підхід до управління та планування в морській галузі, як в області перевезень, так і області портово-складських послуг та сервісів. У разі виникнення кіберінциденту, затрати на ліквідування таких загроз можуть коштувати доволі значну суму. Пропонуємо структуру адміністративних заходів, які дозволять значно знизити ризики успішних атак зловмисників на комп'ютерні мережі, веб-сервіси та програмне забезпечення як суден, так і підприємств портової інфраструктури.

Огляд кіберінцидентів. Комп'ютерні системи України вже неодноразово були атаковані. Зловмисники намагалися вивести з ладу електромережу України, намагалися втручатись у роботу атомних електростанцій, та пробували дестабілізувати роботу деяких державних та приватних підприємств. Останній випадок масових атак був зафіксований 13-14 січня 2022 року та продовжується до сьогодні. Тому захист телекомунікаційних та інформаційних систем набуває дуже великого значення [1; 2].

Морський та річковий транспорт також стає об'єктом кіберінцидентів. Ізраїльська компанія Naval Dome [3], яка спеціалізується в області морської кібербезпеки, провела серію успішних демонстраційних кібератак на морські судна. В результаті атак «хакерами» були змінені відомості про місцезнаходження судна, введений в оману дисплей РЛС, включалось та виключалось суднове обладнання, були взяті під контроль рульове управління, баластна система, система управління паливом. Відеоролик про результати кібератаки доступний на сайті компанії (https://navaldome.com/) [3].

Компанія Naval Dome оцінює зростання кількості спроб злому з початку 2020 на 400%. Таке зростання в багатьох випадках пов'язано з переходом співробітників на дистанційний режим роботи та отримання співробітниками дозволу на віддалене підключення до суднової мережі. Окремі компанії, ігноруючи всі правила безпеки, дозволили використовувати неліцензовані програми дистанційного доступу (Any Desk, TeamViewer, Ammyy Admin).

Наведемо декілька фактів про вже проведені кібератаки. Так, 9 травня 2020 року кібератаку зазнав іранський порт Шахід Раджаі. Експерти погодилися з думкою, що кібератаку провів Ізраїль. У 2020 році двічі протягом трьох місяців піддалась кібератакам австралійська логістична група компаній Toll Group. У квітні 2021 року від кібератаки постраждала компанія Mediterranean Shipping Co. Через вимкнення мережі в одному з дата-центрів компанії в Женеві веб-сайт компанії msc.com був вимкнений протягом 10 годин, були недоступні її соціальні мережі, не працювали поштові служби. В середині травня 2021 року в результаті кібератаки

були зашифровані приблизно 370 (20%) робочих станцій та 20 (приблизно 10%) серверів компанії Anglo-Eastern.

Протягом 2022 року найбільших збитків було завдано портам. У грудні 2022 року порт Лісабона постраждав від атаки зловмисників через програму вимагача LockBit. Ця програма шифрує дані на сервері та вимагає кошти за надання паролю для розшифрування цих даних.

По даним РНБО України [4] в січні 2023 року приблизно 1000 суден постраждало внаслідок атаки програми вимагача на програмне забезпечення ShipManager компанії DNV. У результаті інциденту компанія DNV була змушена відключити свої сервери.

Основні принципи побудови кібербезпеки на морському судні. Підсумуємо, вже зараз потрібно зосереджувати найбільшу увагу на захисті від кібератак портові структури, а також самі судна та їх комп'ютерну мережу. Портова інфраструктура та судна мають дещо різні вразливі зони в плані доступу до комп'ютерних систем. З нашої точки зору портова інфраструктура має більшу кількість точок ураження, ніж судно, що перебуває в рейсі. Але, на жаль, перебування на великій відстані в морі зовсім не гарантує захищеність судна від кібератак.

Охопити всі аспекти в одній статті неможливо, тому, в першу чергу, пропонуємо розглянути принципи побудови кіберзахисту морського судна. Для цього розглянемо, комп'ютерні системи які існують на сучасному судні і мають потенціал бути задіяними в кіберінциденті.

На сучасному судні можемо розрізнити наступні комп'ютерно-інформаційні системи:

- AIS (automatic identification system) – система автоматичної ідентифікації;
- CTS (Container Tracking System) – система відстеження руху;
- ECDIS (Electronic Chart Display and Information System) – електронно-картографічна навігаційна система;
- EPIRB (Emergency Position Indicating Radio Beacon) – передавач, який при активації передає сигнал лиха в різноманітних діапазонах (УКХ, супутник, комбіновано). Деякі системи можуть передавати сигнали в синхронізації через AIS;
- ICN (internal computer network) – внутрішня комп'ютерна мережа вирішує локальні задачі, доступ членів екіпажу до глобальної мережі інтернет, отримання поштової кореспонденції;
- TOS (Terminal Operating System) – одна або кілька систем, що дозволяють автоматизувати процеси навантаження та розвантаження судна в порту, та інші супутні процеси. Іноді такі системи є власністю конкретної компанії;
- VDR (Voyage Data Recorder) регістратор даних рейсу;
- Центральний пункт управління машинною установкою.

Всі перераховані системи можуть потенційно стати об'єктом кібератаки. Збитки, які можуть завдати зловмисники в результаті кібератак, можуть стати занадто великими для морських компаній. Тут, напевно, необхідно вводити нове поняття: морське кіберпіратство MCP (Maritime Cyber Piracy) [5]. За деякими прогнозами, через 5-8 років збитки від морського кіберпіратства перевищать збитки

від звичайного піратства. Очікують появу на судні нового офіцера, який буде відповідати за кібербезпеку судна. Необхідність такої людини на судні ще не зовсім сприймається адміністрацією судновласників і частину роботи проводять офіцери судна. Але, не всі ці офіцери володіють тонкощами налаштування керованих комутаторів, маршрутизаторів, принципами побудови безпечних комп'ютерних мереж, встановленням сертифікатів безпеки. На нашу думку, такі люди повинні пройти спеціальне навчання, та оволодіти всіма необхідними навичками та компетенціями. Тому, вкрай необхідно розробити та запровадити оцінку кібербезпеки судна, а також план дії екіпажу при настанні кіберінциденту.

Розглянемо шляхи зараження програмного забезпечення на судні:

- автозапуск носіїв флеш-пам'яті;
- оновлення програмного забезпечення на підмінному сайті;
- завантаження шкідливого ПЗ (програмного забезпечення) із зараженого сервера компанії;
- отримання шкідливого ПЗ через поштову службу;
- зараження через недбалість співробітників компанії, застосування простих паролів, та їх зберігання в доступних місцях;
- ураження комп'ютерної мережі через мобільні пристрої співробітників;
- оновлення програмного забезпечення з великою затримкою.

Всі ці шляхи створюють потенціальну загрозу судну та мореплаванню в цілому. Для прикладу розглянемо можливість зупинки судна через доступ до пульта управління головним двигуном. Як правило, для цього використовують підмінні сайти для завантаження оновлення програмного забезпечення керування двигуном. Після «оновлення програмного забезпечення» зловмисники отримують доступ до елементів керування. Наприклад, вони можуть перекрити подачу палива та вимкнути головний двигун. Для експерименту британська компанія Cyber Mar [9] отримала такий доступ через завантаження програмного забезпечення на підмінному сайті та вимкнула головний двигун судна. Якщо це зробити під час входу в порт, або протягом проходу через протоки, то це може завдати шкоди на сотні мільйонів доларів, бо буде перекрито вхід та вихід до порту, а простій суден коштує доволі дорого. А репутаційні втрати навіть важко буде порахувати. Крім того, компанія Cyber Mar також повідомляє про реальні випадки такого вимкнення двигуна судна.

Також компанія Cyber Mar сповіщає про успішну атаку на портову інфраструктуру та перехоплення управління енергозабезпеченням, керування процесами завантаження та розвантаження судна. Процес зараження пройшов через механізм автозавантаження флеш-носія. Програма-шкідник змогла заволодіти паролем власника та передати його зловмисникам. У подальшому, було отримано доступ до серверів, що забезпечило практично повне захоплення порту. При такому експериментальному захопленні порту компанія-власник більш ніж добу відбудовувала свою комп'ютерну мережу.

На нашу думку, найбільш поширений та самий простий спосіб отримати зловмиснику доступ до комп'ютерної мережі суднових компаній – це недбалість та низька освіченість з кібербезпеки персоналу компанії.

Зазвичай у компаніях або взагалі не проводиться або проводиться поверхнево інструктаж з кібербезпеки. Паролі не змінюються протягом довгого часу, а самі паролі не відповідають мінімальним вимогам з безпеки: довжина паролю, необхідність хоча б одної великої літери, числа та спеціального символу. Компанія може розглянути можливість доступу з використання ідентифікаційних карт та/або застосувати біометричні методи ідентифікації особи.

Відсутність посадових інструкцій з кібербезпеки та планів заходів при кіберінцидентах значно знижує стійкість комп'ютерних мереж судна до кібератак. Ця стійкість ще більше знижується при відсутності планів та вимог з періодичності проведення оновлення програмного забезпечення та зміни паролів.

Потрібно також підвищувати загальну комп'ютерну освіченість персоналу, особливо працівників, які мають доступ до об'єктів інформаційної діяльності судна. Зрозуміло, що така робота потребує додаткових фінансових зобов'язань, введення додаткових штатних одиниць, які повинні мати відповідні компетенції та досвід. Але фінансові втрати через кібератаки можуть бути на кілька порядків вищими за ці затрати, а ще більшими можуть бути репутаційні втрати, які відновити навіть важче ніж фінансові.

Тому, якщо керівники компаній, капітани суден будуть працювати в цьому напрямку з персоналом, то вони зможуть закрити більше ніж 50% можливостей ураження інформаційної структури підприємства або судна від кіберінцидентів. Це не викликає великих фінансових затрат, необхідно всього лише проведення аудиту об'єктів інформаційної діяльності та адміністрування поточних комп'ютерно-інформаційних систем.

Ще одним джерелом вразливості можуть бути мобільні пристрої. Кібератаки через мобільні пристрої членів екіпажу можуть приймати масштабні розміри. Кількість мобільних пристроїв в світі зростає шаленими темпами і наближається до 7 мільярдів пристроїв. Майже у кожного співробітника є мобільний пристрій, який під'єднаний через Wi-Fi до місцевої комп'ютерної мережі. Мобільні пристрої дозволяють комунікувати з близькими людьми, але можуть стати осередком кіберзагрози, особливо якщо на пристрої встановлені програми, які не сертифіковані навіть розробниками. Найбільш уразливі в цьому плані пристрої на операційній системі Android, яка дозволяє завантажити програми з невідомого джерела. Тому рекомендується будувати окрему мережу для мобільних пристроїв співробітників.

Наступним елементом ланцюжка несанкціонованого доступу до суднової комп'ютерної мережі є неякісне мережеве обладнання, програмне забезпечення якого містить програмні та апаратні вразливості. Бувають випадки, що виробники спеціально влаштовують шкідливе та шпигунське обладнання безпосередньо в свої пристрої. Всім відомий скандал у США з продукцією деяких іноземних компаній, у програмне забезпечення яких закладено можливість доступу через спеціальні функції до мобільних пристроїв, мережевого обладнання та отримання зашифрованого змісту цих пристроїв, шифрувальних ключів і персональної інформації.

З метою зниження джерел несанкціонованого доступу до комп'ютерних мереж судна необхідно виконувати існуючі методики зниження ризиків впливу несанкціонованого доступу до внутрішніх мереж судна. Звертаємо увагу на вже існуючі документи Державної служби «Держспецзв'язок» в яких детально прописано порядок та методи боротьби з загальними кіберзагрозами [10]. Ці документи дозволять вибудовати чітку систему захисту майже всіх типів комп'ютерних мереж.

Для підвищення стійкості судна від кібератак пропонується виконувати рекомендації, які наведені у документі «Збірка правил кіберпезпеки для суден», який розробив Лондонський інженерно-технологічний інститут (IET) при підтримці Міністерства оборони Великобританії [8]. Ці правила рекомендує міжнародна морська організація (IMO). Виконуючи рекомендації, які знаходяться в цих документах, можна значно підвищити стійкість судна до нападів кіберзлочинців.

Використовуючи та розвиваючи документи Лондонського інженерно-технологічного інституту [8], методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури затверджених наказом Адміністрації Держспецзв'язку [10], можемо значно знизити можливість кіберінцидентів на судні. З метою значного підвищення стійкості комп'ютерних мереж та можливості протистояти кіберзагрозам на судні чи в суднохідній компанії, для підвищення комп'ютерних мереж судна та стійкості до кіберінцидентів, пропонуємо провести наступні заходи:

- провести категоріювання приміщень по об'єктам інформаційної діяльності (ОІД);
- розробити план заходів з кібербезпеки;
- розробити загальні інструкції з кіберзахисту;
- розробити персональні посадові інструкції з кібербезпеки;
- розробити план перевірки об'єктів інформаційної діяльності вимогам кібербезпеки;
- розробити та впровадити комплексну систему захисту інформації (КСЗІ).

Загальний схематичний план кібербезпеки судна був розроблений та представлений на рисунку.

Звичайно запропонована схема може бути розписана більш детально, особливо в розділі «Політика компанії з кібербезпеки судна». Тут повинні бути прописані і нормативні документи [6,7], і внутрішні документи компанії. Зазвичай розробку такої документації проводять організації або фірми, що спеціалізуються в сфері кібербезпеки, виходячи з потреб та задач компанії-замовника. На жаль, таких компаній у нашій країні на цей момент ще дуже мало, але, враховуючи актуальність та крайню необхідність таких спеціалістів, сподіваємося, що їх підготовка зростатиме з року в рік. Сподіваємся, що вищі навчальні заклади в нашій країні будуть крокувати разом з часом, та підготують необхідну кількість спеціалістів у сфері кіберзахисту, або запропонують курси для підвищення кваліфікації.

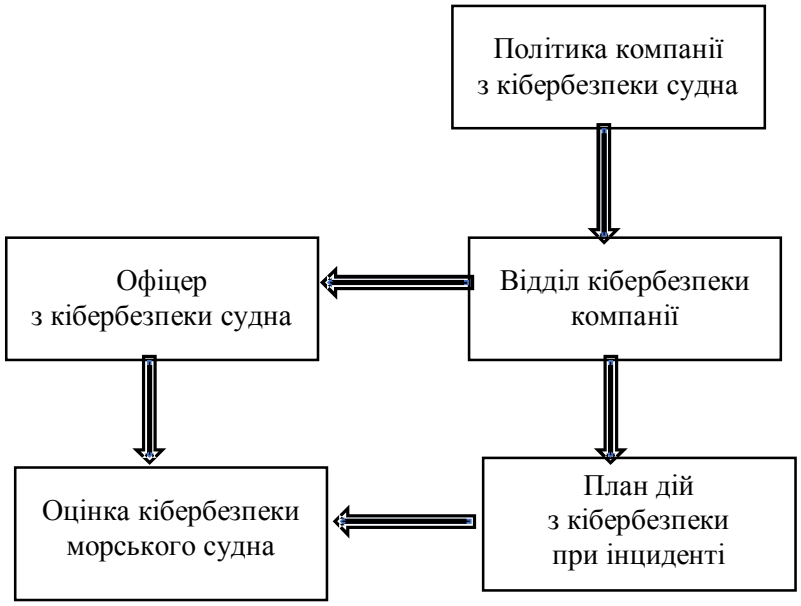

Рисунок. Схематичний план кібербезпеки судна

При відсутності офіцера з кібербезпеки на судні, ці обов'язки тимчасово можна покласти на помічника капітана, але зобов'язати його пройти відповідне навчання у сфері кібербезпеки. На нього можна також покласти наступні обов'язки та відповідальність:

- виконання плану дій при кіберінциденті;
- відповідальність за стале функціювання комп'ютерних мереж судна;
- проведення інструктажу по кібербезпеці;
- адміністрування локальних мереж судна;

Необхідність наявності такого офіцера на борту судна з часом напевно буде тільки посилюватися, тому пропонуємо керівництву суднохідних компаній подумати про це в найближчий час та створити умови для отримання таких людей.

Висновки. Для зменшення ризику виникнення кіберінциденту пропонується провести ряд заходів, які дозволять підвищити захищеність та стійкість систем судна до кібератак.

Провести додаткове навчання відповідного персоналу по безпечному адмініструванню комп'ютерних мереж, що дозволить значно підвищити рівень захисту таких мереж.

Підтримувати програмне забезпечення в актуальному стані.

Провести категоріювання приміщень та розробити план заходів з кібербезпеки.

Оновити посадові інструкції з врахуванням актуальних загроз з кібербезпеки. Особливо звернути увагу на підмінні сайти при оновленні програмного

забезпечення та загрози від фішингових листів та повідомлень. Ознайомити персонал з вимогами до формування паролів, пін-кодів та періодичності їх зміни.

Розглянути можливість введення біологічної ідентифікація особи. Це є ще одним із способів зменшення можливості викрадення паролів та несанкціонованого доступу до комп'ютерних мереж. У наш час такі методи набули популярності та стали більш доступними. Це сканери відбитків пальців, та FaceID – ідентифікація по обличчю користувача.

Розробити або актуалізувати комплексну систему захисту інформації на судні. Відокремити закриту та публічну комп'ютерні мережі.

ЛІТЕРАТУРА

1. *Закон України № 2163-VIII від 05.10.2017 Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.*
2. *Про основні засади забезпечення кібербезпеки України: Закон України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (23.11.2020)*
3. *https://navaldome.com/ [Електронний ресурс]*
4. *РНБО України. [Електроний ресурс] Режим доступу: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf*
5. *Даус Ю.В., Даус М.Є. Матеріали IV Міжнародної науково-практичної морської конференції кафедри СЕУ і ТЕ Одеського національного морського університету, квітень 2022. – Х.: Видавництво Іванченка І., 2022. – С. 273-276.*
6. *ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України. м. Київ, 5 жовтня 2017 року № 2163-VIII*
7. *УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»*
8. *Міжнародна морська організація. [Електронний ресурс]. Режим доступу: pttps://wwwcdn.imo.org/localresources/en/OurWork/Security/ Documents/Resolution %20MSC.428(98).pdf*
9. *[Електронний ресурс] https://www.eventbrite.co.uk/e/lesson-learned-from-cyber-mar-pilots-scada-system-in-port-container-term-tickets-515714454817?utm_source=eventbrite&utm_medium=email&utm_campaign=reminder_attendees_48hour_email&utm_term=eventname&ref=eemaileventremind*
10. *Державна служба спеціального зв'язку та захисту інформації. [Електронний ресурс] https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601*

REFERENCES

1. *Law of Ukraine No. 2163-VIII dated 05.10.2017 Information of the Verkhovna Rada (VVR). 2017. No. 45. Art. 403.*
2. *On the main principles of ensuring cyber security of Ukraine: Law of Ukraine [Electronic resource]. Access mode: https:// zakon. rada. gov. ua/ laws/show/ 2163-19 (November 23, 2020)*
3. *https://navaldome.com/ [Electronic resource]*
4. *NSDC of Ukraine. [Electronic resource] Access mode: https://www. rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf*
5. *Daus Y.V.. Daus M.E. Materials of the IV International Scientific and Practical Maritime Conference of the SEU and TE Department of Odessa National Maritime University, April 2022. – Kh.: Ivanchenko I. S. Publishing House, 2022. – P. 273-276.*
6. *THE LAW OF UKRAINE On the basic principles of ensuring cyber security of Ukraine. Kyiv, October 5, 2017 No. 2163-VIII*
7. *DECREE OF THE PRESIDENT OF UKRAINE No. 447/2021 On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine»*
8. *International Maritime Organization. [Electronic resource]. Access mode: http://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution %20MSC.428(98).pdf*
9. *[Electronic resource] https://www.eventbrite.co.uk/e/lesson-learned-from-cyber-mar-pilots-scada-system-in-port-container-term-tickets-515714454817?utm_source= eventbrite&utm_medium=email&utm_campaign=reminder_attendees_48hour_email&utm_term=eventname&ref=eemaileventremind*
10. *State Service for Special Communications and Information Protection. [Electronic resource] https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601*

Стаття надійшла до редакції 10.04.2023

Посилання на статтю: Даус Ю.В., Даус М.Є., Полікаровських О.І., Ларін Д.Г. Кібербезпека на морському транспорті // Вісник Одеського національного морського університету: Зб. наук. праць, 2023. № 2 (69). С.124-133. DOI 10.47049/2226-1893-2023-2-124-133.

. Article received 10.04.2023

Reference a journalartic: Daus Y.V., Daus M.E., Polikarovskykh O.I., Larin D.G. Cyber security on maritime transport // Herald of the Odessa national maritime university. Coll. scient. works, 2023. № 2 (69). P. 124-133. DOI 10.47049/2226-1893-2023- 2-124-133.