УДК 629.362
DOI 10.47049/2226-1893-2024-1-106-116

КІБЕРЗАГРОЗИ ЯК СУЧАСНИЙ ВИКЛИК МІЖНАРОДНОМУ МОРСЬКОМУ СУДНОПЛАВСТВУ

Булгаков Микола Петрович
к.т.н., доцент, доцент кафедри судноводіння і морської безпеки
ORCID ID: 0000-0002-7172-8678
та старші викладачі кафедри судноводіння і морської безпеки
Бурлаченко Дементій Анатольович – *ORCID ID:0000-0003-3749-4908*
Корякін Костянтин Сергійович – *ORCID ID: 0000-0003-2388-645X*
Никитюк Петро Володимирович – *ORCID ID: 0000-0002-5905-3807*
Чеча Олександр Павлович – *ORCID ID: 0000-0001-7155-6143*
Кучеренко Володимир Юрійович – *ORCID ID: 0009-0008-4906-9726*

Одеський національний морський університет, Одеса, Україна

Анотація. *Досягнення науки і техніки відіграють ключову роль у розвитку торговельного судноплавства. Поступове збільшення вантажопідйомності суден супроводжується скороченням чисельності екіпажу за рахунок автоматизації робочих процесів, у тому числі впровадження IT-технологій і сучасних систем управління судном. Це створює нові можливості для підвищення ефективності судноплавства, але також підвищує ризик кіберзагроз.*

Незважаючи на заклики міжнародних морських організацій посилити захист від кібератак на морі, проблеми в цій сфері залишаються невирішеними. Власники суден мовчать про спроби чи випадки кібератак, побоюючись комерційних втрат і можливих негативних наслідків.

Кіберзагрози можуть мати серйозні наслідки для безпеки судноплавства, включаючи: пошкодження або втрату керування судном; фізичні ушкодження судна або вантажу; заподіяння шкоди навколишньому середовищу; втрата конфіденційності інформації; фінансові втрати.

У статті аналізуються рекомендації щодо управління кіберризиками в морській галузі в рамках систем управління безпекою. Пропонуються заходи, спрямовані на підвищення рівня кібербезпеки суднових систем, керованих комп'ютером.

Ключові слова: *кіберзагрози, судноплавство, безпека судноплавства, морська аварія, кібербезпека судна, кібератака, безпека морського транспорту, вантажні перевезення, безпека порту, заходи безпеки, реагування на надзвичайні ситуації на морі.*

УДК 629.362
DOI 10.47049/2226-1893-2024-1-106-116

CYBER THREATS AS A MODERN CHALLENGE TO INTERNATIONAL SHIPPING

M. Bulgakov
PhD, (Eng.), Associate Professor, Associate Professor
of the Department of Navigation and Maritime Safety
ORCID ID: 0000-0002-7172-8678
and Senior Lecturers at the Department of Navigation and Maritime Safety
D. Burlachenko – *ORCID ID: 0000-0003-3749-4908*
K. Koryakin – *ORCID ID: 0000-0003-2388-645X*
P. Nykytiuk – *ORCID ID: 0000-0002-5905-3807*
O. Checha – *ORCID ID: 0000-0001-7155-6143*
V. Kucherenko – *ORCID ID: 0009-0008-4906-9726*

Odesa National Maritime University, Odesa, Ukraine

Abstract. *Advances in science and technology play a key role in the development of merchant shipping. The gradual increase in the carrying capacity of ships is accompanied by a reduction in the number of crew dueto the automation of work processes, including the introduction of IT technologies and modern ship management systems. This creates new opportunities to improve shipping efficiency, bu talso increases the risk of cyber threats. Despite calls from international maritime organisations to strengthen protection against cyber attacks at sea, problems in this area remain unresolved. Shipowners remain silent about at tempts or cases of cyber attacks for fear of commercial losses and possible negative consequences. Cyber threats can have serious consequences for safety of shipping, including: damage or loss of shipcontrol; physical damage to the ship or cargo; environmental damage; loss of information confidentiality; and financial losses. The article an alyses recommendations for managing cyber risks in the maritime industry with in the framework of security management systems. Measures aimed at improving the level of cyber security of computer-controlled ship systems are proposed.*

Keywords: *cyber threats, shipping, safety of shipping, maritime accident, ship cyber security, cyber attack, maritime transport security, freight transport, port security, security measures, maritime emergency response.*

Вступ. Судноплавство є важливою галуззю економіки, яка забезпечує перевезення вантажів та пасажирів по всьому світу. Однак у сучасних умовах судноплавство стикається з низкою нових загроз, зокрема кіберзагрозами.

Кіберзагрози можуть спричинити значні наслідки для безпеки судноплавства, включаючи:

- пошкодження або втрату контролю над судном, фізичні ушкодження судна чи його вантажу;
- завдання шкоди навколишньому середовищу; порушення конфіденційності інформації;
- фінансові втрати.

Незважаючи на заклики міжнародних морських організацій посилити захист від кібератак на морі, проблеми в цій сфері залишаються невирішеними. Власники суден мовчать про спроби чи випадки кібератак, побоюючись комерційних втрат і можливих негативних наслідків.

Постановка проблеми. У розвитку водного транспорту та водних шляхів сучасності, безпека займає центральне місце. Забезпечення безпеки суден, портової інфраструктури та, передусім, людського життя на морі вимагає комплексу заходів та практик. Навігаційні інциденти становлять значну частину морських аварій, і згідно зі статистикою, дві третини таких подій пов'язані із неправильною, неточною або неповною навігаційною інформацією.

Сучасна морська індустрія стикається зі зростаючими викликами в області кібербезпеки, враховуючи залежність суднових систем від інтегрованих інформаційних технологій. Забезпечення безпеки та ефективності енергопостачання суден вимагає розробки інтегрованих систем кіберзахисту, які враховують унікальні особливості суднової інфраструктури.

За результатами опитування MaritimeBusinessSurvey, кібератаки розглядаються як значний ризик для 77 % учасників, але лише 64 % мають план забезпечення безперервності діяльності в разі кіберінциденту. Тільки 2 з 5 респондентів вживають заходів для захисту суден від кіберзагроз, пов'язаних із оперативними технологіями.

Класифікація небезпек на морі враховує стани судна, що становлять реальну загрозу. Шість основних типів небезпек включають пошкодження корпусу, перекидання судна, затоплення, втрату рушія, контакт із зовнішніми об'єктами та пожежі.

Міжнародна конвенція SOLAS-74, разом із Кодексом ISPS, встановлює мінімальні стандарти безпеки для міжнародних морських перевезень. Крім того, враховуються нові загрози, такі як тероризм, піратство, крадіжки та кіберзлочинність.

Міжнародний морський транспорт, який відіграє ключову роль у світовій торгівлі, також стає об'єктом терористичних загроз. Зростання кібератак вимагатиме від власників суден великих інвестицій, і очікується збільшення експлуатаційних витрат у найближчі роки. У 2020 році транспортний сектор посідав одинадцяте місце серед галузей, найбільш вразливих до кібершпигунства з 28 зареєстрованими інцидентами.

Потенційні витрати на підвищення безпеки на морі, включаючи захист від кіберзагроз, виявляються значно меншими, ніж економічні збитки від великого терористичного інциденту, як показують дослідження безпеки на морі. Заходи безпеки для суден можуть бути компенсовані підвищенням їх ефективності. Забезпечення виконання кодексу ISPS та добробуту екіпажів і портового персоналу потребує інвестицій у кваліфікований персонал, обладнання та технології.

Під час експлуатації судна існують фактори, що можуть впливати на його технічний стан і безпеку плавання. Математична модель системи мінімізації ризиків для безпеки судна використовує експертні оцінки ймовірностей загроз для розрахунку значущості кожної з них. Також враховується ефективність організа-

ційних заходів для відновлення працездатності судна у разі виникнення проблем. Загальний ризик несправності судна обчислюється як сума ризиків в різних напрямках. Вирішення цієї проблеми включає розподіл ресурсів екіпажу в зоні діяльності для мінімізації ризиків відмови чи погіршення працездатності судна з огляду на критерії безпеки.

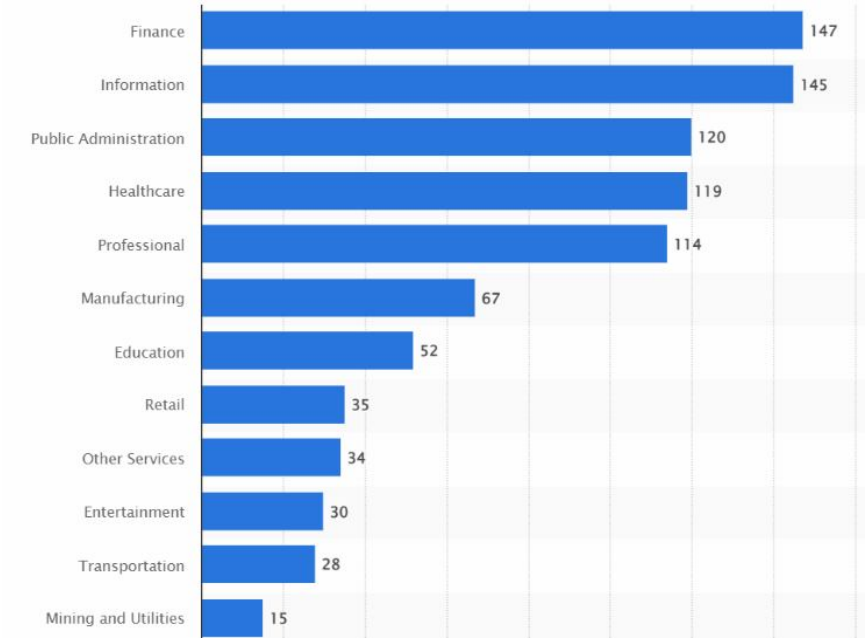

Рис. 1. Глобальні галузі, найбільш вразливі до кібершпигунства (www.statista.com)

Метою статті є дослідження сучасних загроз міжнародному судноплавству, аналіз причин морських аварій, виявлення потенційно небезпечних факторів і ризиків, що виникають під час експлуатації судна, порівняння та встановлення закономірностей їх виникнення, розробка заходів щодо забезпечення безпеки та захисту суден.

Результати досліджень. Глобальний тренд спрямований на цифровізацію в промисловості, включаючи морський транспорт. Зростання користування електронною навігацією, автоматизація управління судном, використання передових комунікаційних технологій і підвищення безпеки є активними тенденціями. Використання Інтернету під час морських рейсів для оновлення систем і програм безпеки є загальним явищем.

Міжнародна морська організація визначає певні суднові системи, такі як системи машинного відділення, контролю вантажоперевезень, керування насосами і енергопостачанням, контролю доступу та інші, як критичні для захисту від кіберзагроз. Сучасні судна, зокрема, стають уразливими до кібератак, і важливо забезпечити безпеку та своєчасне виявлення кіберзагроз.

Аналіз поточного стану морської безпеки і нормативної бази є обов'язковим, оскільки цифрові пірати виявляють зростаючий інтерес до контролю над інформаційними системами кораблів. Міжнародна морська організація вже розробила керівництво з управління кіберзагрозами в морській галузі та закликає до уваги до кіберризиків у системах управління безпекою.

Для того щоб розробити ефективні заходи щодо забезпечення безпеки та захисту суден проведемо деякі математичні розрахунки. Треба кількісно оцінити ризики, пов'язані з різними видами загроз, і визначити оптимальний розподіл ресурсів для їх мінімізації.

Позначимо через R_i ризик непрацездатності судна, а через C_i витрати, пов'язані з пом'якшенням цього ризику в і-му напрямку забезпечення безпеки (недостатні захисні заходи, відсутність пильності, системні збої, відмова систем судна) через недостатню кваліфікацію екіпажу). Тоді ми можемо встановити такі залежності:

$$R_i = f(C_i), \tag{1}$$

де i =1...i=1...n, а n – кількість заданих напрямків протидії небезпеці.

Щоб мінімізувати загальний ризик відмови системи

$$Min(\sum_{i=1}^{n} R_i) \cdot \tag{2}$$

З урахуванням обмежень загальні витрати на зниження ризику повинні бути меншими або дорівнювати максимально допустимим витратам

$$\sum_{i=1}^{n} Z_i \le Z \cdot \tag{3}$$

Витрати на пом'якшення кожного конкретного ризику повинні бути більшими або дорівнювати мінімальноприйнятним значенням

$$Z_{MIN_i} \le Z \le Z_{MAX_i}, \text{ for } i = 1,2,...,n. \tag{4}$$

Цю проблему можна вирішити за допомогою різних методів оптимізації, таких як лінійне програмування, градієнтні методи чи інші відповідні залежно від конкретних обставин і вимог проблеми.

Лінійне програмування може бути використане для підвищення безпеки на морі, мінімізуючи загальний ризик відмов систем на судні. У цьому контексті термін «система» охоплює різні компоненти і процеси на судні, такі як машинне відділення, системи обробки вантажів, електропостачання та комунікаційні мережі. Мета полягає в тому, щоб розподілити ресурси так, щоб мінімізувати ризики, пов'язані з кожним із цих компонентів.

Цей підхід включає в себе кількісне визначення ризиків для різних сценаріїв відмови та розрахунок витрат, необхідних для пом'якшення цих ризиків.

Серед цих витрат можуть бути інвестиції в обладнання, навчання та технології. Шляхом формулювання проблеми як програми лінійної мінімізації, оператори суден можуть визначити оптимальний розподіл ресурсів для забезпечення безпеки та функціональності судна.

Обмеженнями в моделі лінійного програмування будуть максимально допустимі витрати на кожен захід із зменшення ризику, забезпечуючи, що загальні витрати не перевищуватимуть бюджету. Крім того, можна встановити обмеження, щоб гарантувати зниження рівня ризику, пов'язаного з кожним компонентом, до прийнятного рівня.

Крок 1. Визначте змінні – визначіть змінні R_i – ризик, пов'язаний з і-м напрямком забезпечення безпеки;

Z – максимальні загальні витрати на зниження ризику.

Крок 2. Визначте обмеження – визначте обмеження, яке гарантує, що загальний ризик з усіх боків не перевищує максимально допустимий ризик.

Крок 3. Визначте цільову функцію – визначте цільову функцію для мінімізації загального ризику відмови системи.

Крок 4. Визначте максимальні та мінімальні витрати для кожного напрямку – визначте максимальні та мінімальні витрати на зниження ризику для кожного напрямку Z_{MAXi} та Z_{MINi} відповідно. Наприклад: $Z_{MAX1} = 15$, $Z_{MIN1} = 3$; $Z_{MAX2} = 10$, $Z_{MIN2} = 4$; $Z_{MAX3} = 18$, $Z_{MIN3} = 2$.

Крок 5. Вирішіть проблему оптимізації: З визначеними змінними, обмеженнями та цільовою функцією використовуйте методи математичної оптимізації (наприклад, лінійне програмування), щоб знайти оптимальний розподіл ресурсів для мінімізації загального ризику відмови системи при дотриманні обмежень.

Крок 6. Інтерпретуйте результати – розподіл ресурсів по кожному напрямку забезпечить досягнення мінімального загального ризику відмови системи.

У результаті проведених розрахунків прийшли до висновку, що використання математичного підходу до оптимізації дозволило ефективно розподілити ресурси для мінімізації загального ризику відмов системи судин. Цей розподіл відповідає заданим обмеженням і забезпечує оптимальний розподіл ресурсів для мінімізації ризику.

Використання кругової діаграми (рис. 2) для візуалізації надає можливість наочно сприймати, як було розподілено бюджет на різні категорії ризику. Цей зручний інструмент полегшує розуміння розподілу ресурсів.

Отже, цей системний підхід дозволяє приймати обґрунтовані рішення щодо розподілу ресурсів, збалансовуючи зменшення ризиків із бюджетними обмеженнями. Такий підхід сприяє підвищенню безпеки судна завдяки раціональному та ефективному розподілу ресурсів.

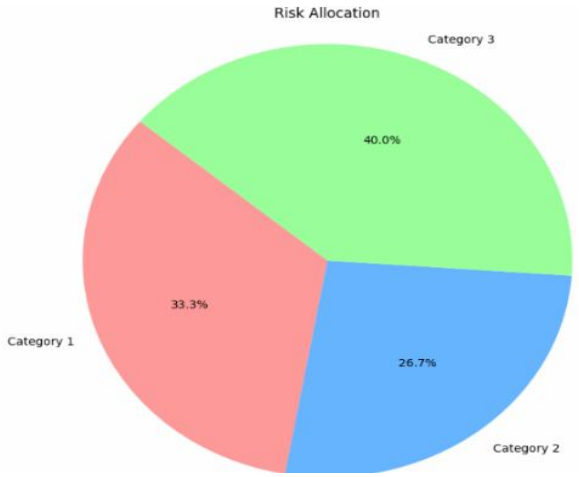

Рис. 2. Розподіл бюджету суднової компанії за різними категоріями ризику

У підсумку можна стверджувати, що розглянуті компоненти можна представити у вигляді концептуальної моделі безпеки судна, аналогічно до моделі інформаційної безпеки, яка зображена на наступній діаграмі (рис. 3).

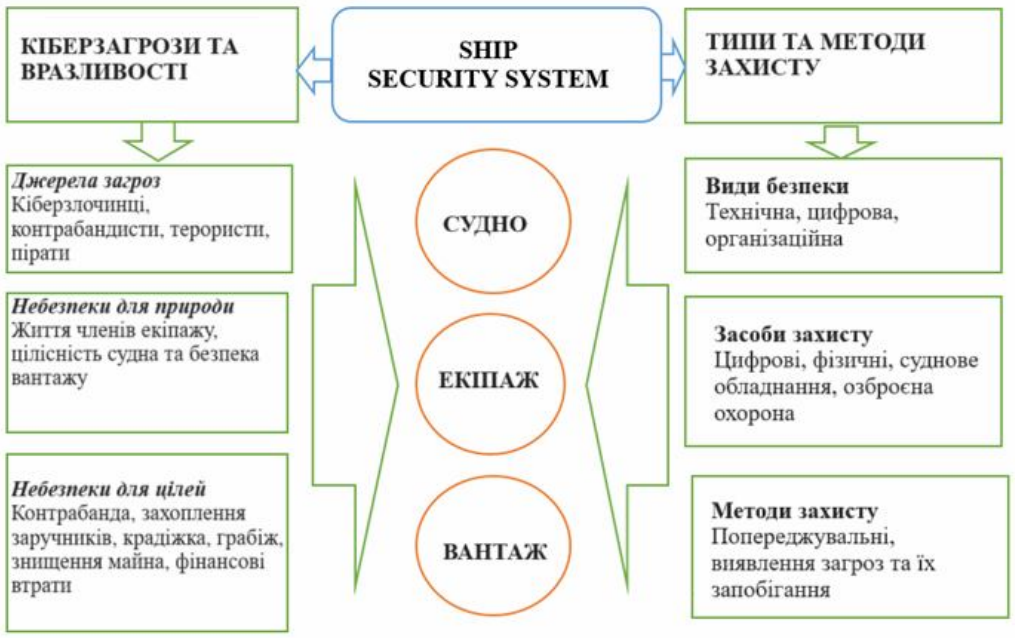

Рис. 3. Концептуальна модель кіберохорони судна

Концептуальна модель кіберохорони судна є комплексним підходом до забезпечення кібербезпеки морських транспортних засобів у світлі зростаючого ризику кіберзагроз. Основна мета цієї моделі полягає в розробці ефективних стратегій та технологічних рішень для запобігання кібератак, виявлення інцидентів та реагування на них. У рамках моделі ідентифікуються основні етапи забезпечення кібербезпеки, такі як аналіз потенційних загроз, розробка систем виявлення та моніторингу, визначення стратегій реагування на інциденти та впровадження заходів з попередження кібератак.

Інтегрована система кіберзахисту включає в себе сучасні технічні рішення, такі як системи шифрування, мережеві брандмауери, системи виявлення вторгнень та суперконденсатори для забезпечення надійного енергозабезпечення в умовах кібератак. Важливою складовою концепції є постійне оновлення систем та навчання персоналу, щоб вони були в готовності реагувати на нові типи загроз та вдосконалювати заходи безпеки відповідно до змінюючогося кіберландшафту. Крім того, враховується роль енергетичної стійкості судна та його систем в умовах кібератак, забезпечуючи надійне живлення електричних систем та функціонал силової установки.

Загалом, концептуальна модель кіберохорони судна спрямована на створення високоефективного, надійного та інтегрованого підходу до забезпечення кібербезпеки сучасних морських транспортних засобів.

Висновки. З розвитком водного транспорту та водних шляхів забезпечення безпеки суден, портової інфраструктури та, що найважливіше, життя людей на морі, стає першочерговою проблемою. Комплексна система безпеки включає низку заходів, методів і технологій, спрямованих на запобігання або зменшення ризику аварій, загибелі людей та шкоди навколишньому середовищу. Ці заходи включають: технічні вимоги до суден (такі як правила щодо конструкції); обладнання та експлуатації; правила та процедури для екіпажів суден, спрямовані на забезпечення їхньої кваліфікації та компетентності; системи управління безпекою, що допомагають судноплавним організаціям і портам координувати свої зусилля з забезпечення безпеки.

Міжнародні конвенції відіграють вирішальну роль у встановленні та уніфікації мінімальних стандартів безпеки. Ці конвенції, такі як Міжнародна конвенція з охорони людського життя на морі (SOLAS) та Міжнародна конвенція з попередження забруднень з суден (MARPOL), є значним кроком до створення глобальної системи безпеки на морі.

Однак сучасний морський сектор стикається з новими викликами, такими як зростаюча проблема кіберзагроз. Оскільки кораблі стають цифровими, вони стають більш вразливими до кібератак. Це вимагає значних інвестицій у заходи кібербезпеки, що відображає фундаментальний зсув у проблемі морської безпеки.

Для захисту морської галузі та життів, які від неї залежать, необхідні надійні протоколи безпеки, міжнародна співпраця та технологічні досягнення.

СПИСОК ЛІТЕРАТУРИ

1. *Melnyk, O., Onyshchenko S., Pavlova N., Kravchenko O., Borovyk S. (2022) Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. International Journal of Computer Science and Network Security, vol.22 (03), 135-140. 10.22937/IJCSNS.2022.22.3.18.*
2. *Yoo, Yunja& Park, Han-Seon. (2021). Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. Journal of Marine Science and Engineering. 9. 565. 10.3390/jmse9060565.*
3. *Soner, Omer &Kayişoğlu, Gizem& Yilmaz Bolat, Pelin& Tam, Kimberly. (2023). Cybersecurity risk assessment of VDR. Journal of Navigation. 1-18. 10.1017/S0373463322000595.*
4. *Guo, Jian &Guo, Hua. (2023). Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. Symmetry. 15. 988. 10.3390/sym15050988.*
5. *Pöyhönen, Jouni. (2022). Cybersecurity risk assessment subjects in information flows. European Conference on Cyber Warfare and Security. 21. 222-230. 10.34190/eccws.21.1.263.*
6. *Longo, Giacomo &Orlich, Alessandro &Musante, Stefano & Merlo, Alessio&Russo, Enrico. (2023). MaCySTe: A Virtual Testbed for Maritime Cybersecurity. 10.2139/ssrn.4374685.*
7. *Boudehenn, C., Cexus, J.-C., Abdelkader, R. Lannuzel, M., Jacq, O., Brosset, D., Boudraa, A.-O. (2023). Holistic Approach of Integrated Navigation Equipment for Cybersecurity at Sea. 10.1007/978-981-19-6414-5_5.*
8. *Karaca, I., Soner, O. (2023). An evaluation of students' cybersecurity awareness in the maritime industry. International Journal of 3D Printing Technologies and Digital Industry. 7. 10.46519/ij3dptdi.1236264.*
9. *Al Ali, N., Chebotareva, A., Chebotarev, V. (2021). Cyber security in marine transport: opportunities and legal challenges. Pomorstvo. 35. 248-255. 10.31217/p.35.2.7.*
10. *Golubkova, I. (2023). Impact of globalization of the world market and internationalization of the cargo transportation process on the maritime transport system. Ukrainian Journal of Applied Economics and Technology. 8. 22-30. 10.36887/2415-8453-2023-2-3.*
11. *Melnyk O., Onyshchenko S., Onishchenko O., Shumylo O., Voloshyn A., Koskina Y., Volianska Y. (2022). Review of Ship Information Security Risks and Safety of Maritime Transportation Issues. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 16, No. 4, pp. 717-722doi:10.12716/1001.16.04.13.*
12. *Melnyk, O., Onyshchenko, S..,Onishchenko, O., Lohinov, O. and Ocheretna, V. (2023) Integral Approach to Vulnerability Assessment of Ship's Critical Equipment and Systems, Transactions on Maritime Science. Split, Croatia, 12(1). doi: 10.7225/toms.v12.n01.002.*

REFERENCES

1. *Melnyk, O., Onyshchenko S., Pavlova N., Kravchenko O., Borovyk S. (2022) Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. International Journal of Computer Science and Network-Security, vol.22 (03), 135-140. 10.22937/IJCSNS.2022.22.3.18.*
2. *Yoo, Yunja & Park, Han-Seon. (2021). Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plansin Consideration of Digitalized Ship. Journal of Marine Science and Engineering. 9. 565. 10.3390/jmse9060565.*
3. *Soner, Omer & Kayişoğlu, Gizem & Yilmaz Bolat, Pelin & Tam, Kimberly. (2023). Cybersecurity risk assessment of VDR. Journal of Navigation. 1-18. 10.1017/S0373463322000595.*
4. *Guo, Jian & Guo, Hua. (2023). Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. Symmetry. 15. 988. 10.3390/sym15050988.*
5. *Pöyhönen, Jouni. (2022). Cybersecurity risk assessment subjects in information flows. European Conferenceon Cyber Warfare and Security. 21. 222-230. 10.34190/eccws.21.1.263.*
6. *Longo, Giacomo & Orlich, Alessandro & Musante, Stefano & Merlo, Alessio & Russo, Enrico. (2023). MaCySTe: A Virtual Testbed for Maritime Cybersecurity. 10.2139/ssrn.4374685.*
7. *Boudehenn, C., Cexus, J.-C., Abdelkader, R. Lannuzel, M., Jacq, O., Brosset, D., Boudraa, A.-O. (2023). Holistic Approach of Integrated Navigation Equipment for Cybersecurity at Sea. 10.1007/978-981-19-6414-5_5.*
8. *Karaca, I., Soner, O. (2023). Anevaluation of students' cybersecurity awareness in the maritime in dustry. International Journal of 3D Printing Technologies and Digital Industry. 7. 10.46519/ij3dptdi.1236264.*
9. *AlAli, N., Chebotareva, A., Chebotarev, V. (2021). Cybersecurity in marine transport: opportunities and legal challenges. Pomorstvo. 35. 248-255. 10.31217/p.35.2.7.*
10. *Golubkova, I. (2023). Impact of globalization of the world market and internation alization of the cargo transportation process on the maritime transport system. Ukrainian Journal of Applied Economics and Technology. 8. 22-30. 10.36887/2415-8453-2023-2-3.*
11. *Melnyk O., Onyshchenko S., Onishchenko O., Shumylo O., Voloshyn A., Koskina Y., Volianska Y. (2022). Review of Ship Information Security Risks and Safety of Maritime Transportation Issues. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 16, No. 4, pp. 717-722doi:10.12716/1001.16.04.13.*

12. Melnyk O., Onyshchenko S.., Onishchenko O., Lohinov O. and Ocheretna V. (2023) Integral Approach to Vulnerability Assessment of Ship's Critical Equipment and Systems, Transactions on Maritime Science. Split, Croatia, 12(1). doi: 10.7225/toms.v12.n01.002.

Стаття надійшла до редакції 15.11.2023

Посилання на статтю: Булгаков М.П., Бурлаченко Д.А., Корякін К.С., Никитюк П.В., Чеча О.П., Кучеренко В.Ю. Кіберзагрози як сучасний виклик міжнародному морському судноплавству: *Вісник Одеського національного морського університету:* Зб. наук. праць, 2024. № 1 (72). С. 106-116. DOI 10.47049/2226-1893-2024-1-106-116.

Article received 15.11.2023

Reference a journalartic: Bulgakov M., Burlachenko D., Koryakin K., Nykytiuk P., Checha O., Kucherenko V. Cyber threats as a modern challenge to international shipping: *Herald of the Odesa national maritime university:* Coll. scient. works, 2024. № 1 (72). 106-116. DOI 10.47049/ 2226-1893-2024-1-106-116.