ТРАНСПОРТНІ ТЕХНОЛОГІЇ (275)

УДК 656.6:629.067

ОРГАНІЗАЦІЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МОРСЬКОГО СУДНА

Кандидати техн. наук О. М. Мельник, А. О. Волошин, д-р техн. наук О. А. Онищенко, канд. техн. наук О. В. Щербина, канд. геогр. наук Н. В. Васалатій, старш. викл. П. В. Нікітюк

INFORMATION SECURITY ARRANGEMENTS OF SEAGOING SHIP

PhD (Tech.) O. Melnyk, A. Voloshyn, D. Sc. (Tech) O. Onishchenko, PhD (Tech.) O. Shcherbina, PhD (Geog.) N. Vasalatii, Senior Lecturers P. Nykytyuk

DOI: https://doi.org/10.18664/1994-7852.201.2022.267758

Анотація *Питання забезпечення безпеки сучасного транспортного флоту пов'язане насамперед із захистом інформації від несанкціонованого доступу та запобігання її витоку. Кожний судновласник, дбаючи про збереження конфіденційності даних, не тільки зменшує ризик і можливі збитки від їхнього витоку, але й підвищує рівень довіри в очах своїх клієнтів і партнерів. Якісні та кількісні зміни, а також впровадження інформаційних технологій, що відбувається на морських суднах останнім часом, значно підвищили безпеку їхньої експлуатації та покращили умови безперервної роботи, посприявши тому, що сучасне судноплавство стало великою мірою залежати від інформаційного забезпечення, яке є важливим елементом у процесах керування судном та експлуатацією його технічних систем. Застосування нових морських цифрових інформаційних систем на основі мережевої передачі навігаційних даних також стало суттєвим кроком на шляху до підвищення забезпечення безпеки мореплавства. Це дозволяє своєчасну обробку великих обсягів інформації для функціонування навігаційних систем судна. Такі системи дозволяють виключити прийняття рішення щодо керування судна, що ґрунтується на основі неповної або недостовірної інформації та зумовлює вжиття спеціальних заходів для забезпечення безпеки судна. У статті подано аналіз основних факторів, що становлять загрозу та вплив на забезпечення інформаційної безпеки судна. На основі концептуальної моделі виділено основні фактори впливу на стан кібербезпеки судна.*

Ключові слова: *захист інформації, безпека судна, суднові системи, витік даних.*

Abstract *Security of modern transport ships is primarily related to the protection of information from unauthorized access and prevention of leakage. Every shipowner, by protecting the confidentiality of data, not only reduces the risk and possible losses from its leakage, but also increases the level of trust in the eyes of its customers and partners. The quality and quantity changes, which have taken place in recent years on seagoing vessels, have significantly contributed to the safety of their operation and the smooth running of their operations. Modern ship navigation is heavily dependent on information support, which is an important element in ship handling processes. New marine digital information systems are being deployed based on digital data exchange, to ensure navigational safety. This allows immediate processing of summaries of information for the functioning of the ship's navigation systems. In addition, these systems provide the ability to exclude*

the decision-making process for ship management based on incomplete or unreliable information and require the maintenance of special measures to ensure its safety. Therefore, the task in the sphere of cyber security in maritime transport is the development of means of protection of information resources of the vessel, which is one of the first and urgent. Given these factors and the current situation, the international maritime organization has developed and adopted a number of maritime industry security documents that are designed to address a number of provisions and issues related to cybersecurity of ship and ship operations. The purpose of this article is to analyze main factors influencing ship's information security. And on the basis of the presented conceptual model of ship security the main factors influencing the information security of the ship are identified.

Keywords: *information security, ship security, data protection; ship systems.*

Вступ. Цифрова трансформація морської галузі – подія, що фактично відбулася. Сьогодні морські транспортні судна використовують комп'ютерні та кіберзалежні технології для навігації, керування судном, судновими технічними системами та системами зв'язку, вантажними операціями, здійсненням контролю за станом довкілля та для багатьох інших цілей. Системи спостереження судна, такі як моніторинг безпеки, виявлення пожеж і порушення герметичності корпусу, все більше залежать від кібертехнологій. Тому кібербезпека є однією з важливих складових у системі забезпечення безпеки судна та судноплавства в цілому, а кібератаки на морський транспорт – цілком актуальною проблемою, що потребує постійної уваги. До речі, з подальшим розвитком інформаційних технологій обумовлені ризики лише збільшуватимуться. На думку експертів, з часом потенційних каналів і можливостей для хакерських атак ставатиме все більше, їхні види варіюватимуться і видозмінюватимуться, що вчергове підкреслює роль кібербезпеки морського судна як невід'ємного елемента в системі забезпечення безпеки судноплавства.

Аналіз останніх досліджень і публікацій. Забезпечення інформаційного захисту судна – це перш за все його захист від кібератак. Кібернетична атака - ніщо інше, як будь-яка несанкціонована дія, здійснена безпосередньо на суднове обладнання або, наприклад, опосередковано на електронний пристрій і через нього на суднову систему загалом. Будь-яка ланка в системі критично важливого суднового обладнання, включаючи бездротові канали зв'язку, може стати вразливою. У результаті відбувається активізація властивостей та інших інтегрованих в апаратуру функцій, що у свою чергу може призвести до різних спотворень і збоїв у роботі на численних етапах обробки, перетворення та подання інформації в різному судновому обладнанні [1, 2, 8, 9]. Важливо відзначити, що судно може бути схильним до хакерської атаки не тільки перебуваючи в порту, а й у відкритому морі. Кібератака може бути спрямована практично на все суднове обладнання, від навігаційних і радарних систем до електронних карт. Вона може проходити за класичним сценарієм, коли відбувається напад на систему INMARSAT (Міжнародна організація морського супутникового зв'язку) та аналогічне обладнання супутникового зв'язку. Зловмисникам досить вузької смуги пропускання каналу і короткого сеансу зв'язку, під час якого зазвичай судна роблять регулярний звіт, наприклад передають телеметричну інформацію про параметри руху судна, його обладнання, порти, стан вантажу і деталі маршруту [9]. Прогресуюча цифровізація морського транспорту несе нові загрози [3, 6, 7] і зумовлює ризики, виникаючі в системі морського транспорту [5, 12, 18]. Зокрема основи кібербезпеки критичної інфраструктури та морського сектору відіграють ключову роль [13-16].

Отже, все більш особливого значення набувають питання кібербезпеки на морі та

забезпечення цифрової безпеки морських маршрутів, а також майбутні правові проблеми, що очікуються в галузі. Особливий інтерес також становлять заходи протидії загрозам морських кібератак, рівень готовності до організації забезпечення кібербезпеки на морі в портах, а також порівняння практики різних країн.

Мета та завдання дослідження. Мета статті полягає в дослідженні існуючих засобів захисту інформаційних ресурсів судна, встановленні зв'язку між критичними системами судна та ідентифікованими ризиками в рамках забезпечення інформаційної безпеки судна. Для досягнення цієї мети необхідно провести аналіз основних загроз інформаційній безпеці судна, вивчити фактори, що спричиняють вплив на її забезпечення, і розробити концептуальну модель безпеки судна та ідентифікувати основні фактори впливу на стан цієї безпеки.

Основна частина дослідження. Вразливими об’єктами судна, з погляду кібербезпеки, є різні системи судна, що сьогодні керуються та контролюються відповідним програмним забезпеченням, інформаційними системами.

Слід відзначити, що в 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, управління сигналізацією, управління підрулюючими пристроями) (рис. 1).

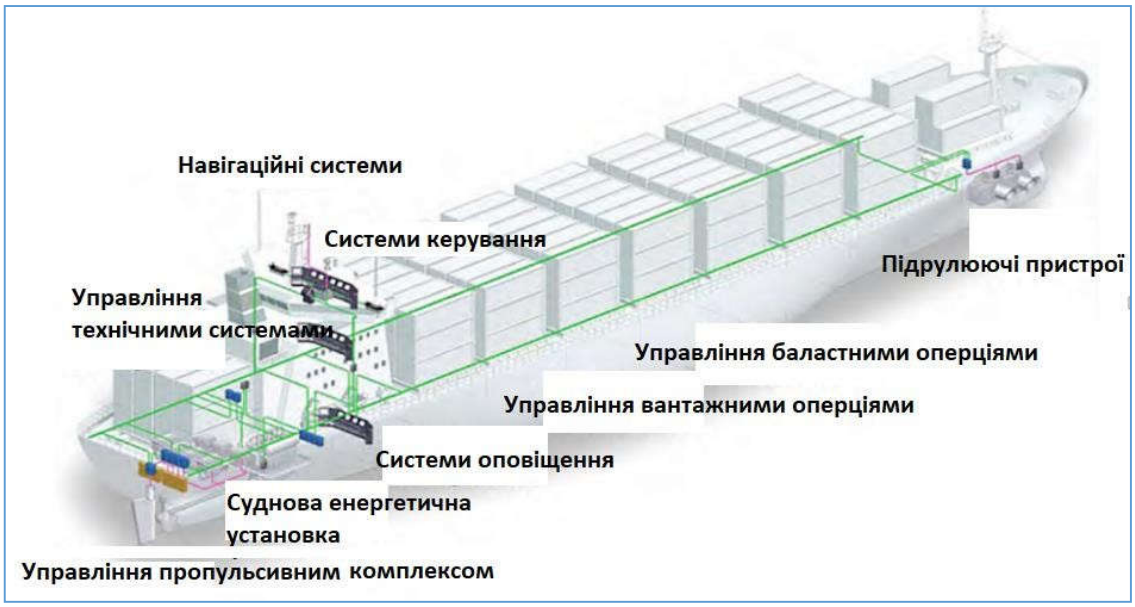

Рис. 1. Основні системи судна

Під засобами забезпечення інформаційної безпеки судна прийнято розуміти сукупність заходів, спрямованих на забезпечення цілісності, доступності і, якщо необхідно, конфіденційності інформації та ресурсів, що використовуються для її обробки.

Сучасні суднові інформаційні системи надають таку інформацію:

- дані про судно (поточне місце, кінематичні параметри, попередній шлях, запланований маршрут і ряд інших елементів);

- радіолокаційне зображення та кінематичні параметри цілей з засобів автоматичного радіолокаційного прокладання;

- дані з автоматичної ідентифікаційної системи про інші судна;

- відомості про навігаційні огорожі, 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 мати для критичних систем судна або обладнання, раптова відмова якого може створювати небезпечні ситуації на судні, тому вони є життєво важливими для функціонування судна (рис. 2).

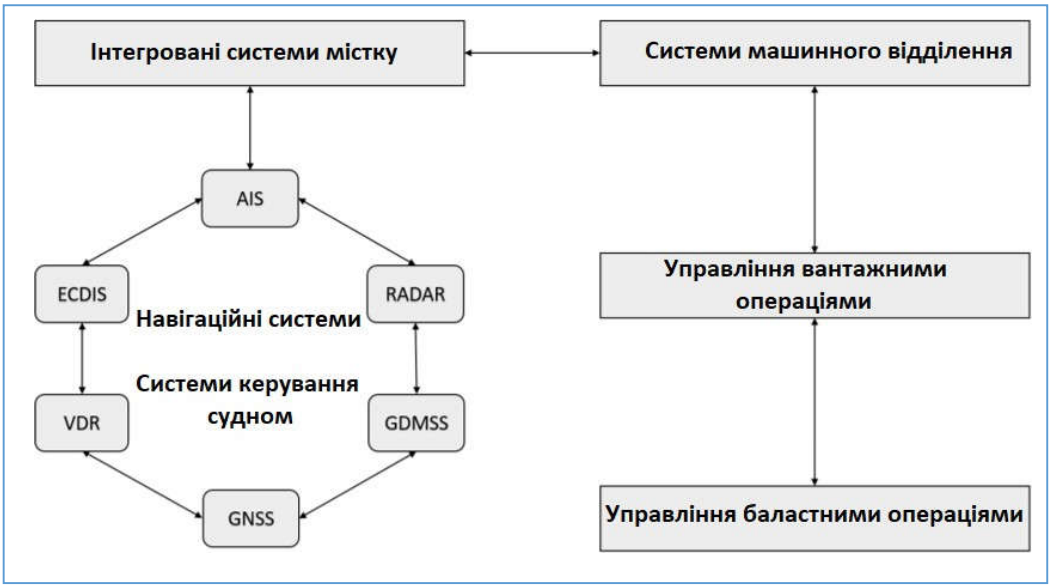

Рис. 2. Критичні системи судна

Так, основними системами вантажного судна, вразливими перед кібератаками, є:

- системи навігаційного містка (реєстрації даних рейсу - VDR);

- електронні системи відображення карт та інформації (ECDIS);

- системи автоматичної ідентифікації (AIC);

- системи супутникового позиціонування (GNSS);

- системи управління вантажами;

- системи радіолокаційного спостереження (RADAR);

- системи зв'язку в разі лиха та для забезпечення безпеки (GMDSS).

Слід відзначити, що недоліком сучасних систем управління морськими транспортними суднами є висока частка участі людини у процедурі прийняття рішень і велика залежність процесу управління від психофізичного стану

штурмана-судноводія. Ключовим моментом при розгляді питань, що стосуються забезпечення безпеки інформаційних систем, є виняткова важливість і необхідність використання системного підходу до вирішення цієї проблеми. Це пояснюється тією обставиною, що безпека системи в цілому обумовлюється безпекою її найслабшої ланки. У зв'язку з цим набуває принципової важливості розгляд проблеми в комплексі, інакше вжиті заходи не принесуть очікуваного ефекту або виявляться надмірними та невиправдано дорогими.

Іншим важливим моментом під час вирішення питань безпеки інформаційних систем судна є принцип дотримання балансу. Слід чітко розуміти, що забезпечення абсолютної безпеки практично неможливе. Захистити від усього різноманіття загроз неможливо з цілої низки причин, серед яких досить назвати лише деякі:

- абсолютний захист зробить інформаційну систему практично недоступною та непридатною для використання;

- не всі можливі шляхи подолання загроз системі забезпечення безпеки можуть бути відомі і, отже, не всім загрозам може протистояти застосована система забезпечення безпеки;

- безпека комп'ютерних систем судна залежить від «людського фактора».

Отже, ще раз необхідно підкреслити, що будь-які заходи не можуть гарантувати абсолютної безпеки. З цієї причини слід досягати такого співвідношення складності системи забезпечення безпеки та реальних умов функціонування інформаційних систем, що не призводило б до перевищення вартості розроблення, впровадження, експлуатації та обслуговування системи забезпечення безпеки над масшабами можливої шкоди в разі її порушення. Концептуальна модель безпеки судна подана на рис. 3.

Рис. 3. Концептуальна модель безпеки судна

Втім існують два основних варіанти щодо забезпечення безпеки суднової інформації: самостійний та з залученням фахівців-консультантів. Перший підхід

виявив свою неспроможність у сучасних умовах через неможливість передбачити всі можливі ймовірні загрози та розмір евентуальної шкоди від їхнього прояву, що визначає жорсткі вимоги до питання захисту інформації, і другий підхід - експертний, що передбачає більш професійний рівень.

Приступаючи до вирішення завдання з забезпечення інформаційної безпеки судна, необхідна побудова її моделі і чітке визначення проблем. При цьому формальну модель на першому етапі бажано розглядати на концептуальному рівні, не зупиняючись на конкретних особливостях інформаційних систем. Далі після розгляду принципів стратегії розроблення системи забезпечення безпеки рекомендується перейти до реального змісту концептуальних положень, і здебільшого такий підхід є виправданим.

Найважливішим фактором при побудові формальної моделі безпеки є поняття «середовище безпеки». Необхідність введення цього терміна визначається тим, що безпека інформаційної системи судна не може забезпечуватися за будь-яких умов. Отже, поняття «середовище безпеки» служить для обмеження (визначення) сфер безпеки суднових системи. У багатьох дослідженнях проблеми безпеки інформаційних систем у складі середовища безпеки виділяють кілька самостійних компонентів, кожен з яких утворює певну сферу безпеки, що відповідає тому чи іншому аспекту забезпечення безпеки. Іншими словами, ці сфери дозволяють декомпозувати проблему забезпечення безпеки суднових систем і вирішувати її частинами.

На жаль, проблеми інформаційної безпеки судна найчастіше відносять до другорядних або взагалі змішують їх із загальними проблемами безпеки та автоматизації. При цьому передбачається, що в 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 з приводу того, що:

1) раптовість атаки може призвести до таких наслідків, що реакція на неї вже не матиме сенсу;

2) при описаному вище підході керівництво перебуває у стані очікування будь-яких порушень інформаційної системі як наслідку інформаційної атаки. Якщо говорити про витік інформації, то зазвичай подібні факти виявляються з великим запізненням. До моменту прояву і згодом можна буде лише констатувати про відсутність своєчасно вжитих заходів захисту;

3) вживання заходів захисту в терміновому порядку може призвести до неадекватної оцінки ситуації з боку екіпажу судна, що, безсумнівно, позначиться на якості його роботи. Крім того, якість будь-якого рішення в умовах дефіциту часу знижується, і швидше за все створити оптимальну систему захисту даних не вдасться.

Сучасний підхід до захисту інформації від несанкціонованого доступу полягає в комплексному застосуванні організаційних і технічних заходів. Заходи для забезпечення безпеки конфіденційної інформації проводяться, як правило, у трьох основних напрямах: захист від витоку інформації з технічних каналів, захист від несанкціонованого доступу до комп'ютерної інформації, обмеження вільного доступу сторонніх осіб до приміщень, де встановлено суднове критичне обладнання. Комплекс заходів, необхідних для забезпечення безпеки інформації, визначається виходячи з необхідного рівня захищеності конкретного об'єкта і допустимого рівня ризику, тому на попередньому етапі при розробленні плану захисту має проводитися визначення ймовірних загроз і розмірів можливих збитків від їхнього прояву. Крім того, необхідно враховувати гарантію безконфліктності функціонування встановлених засобів захисту для

забезпечення надійності загальної системи захисту. Зрештою неможливо побудувати систему інформаційної безпеки без урахування вимог нормативних документів, яких чимало, тому необхідне як глибоке знання змісту документів, так і певний досвід практичної діяльності з їх використання.

Щодо базових принципів забезпечення інформаційного захисту, то необхідно відділити такі:

- цілісність даних – захист від збоїв, що призводять до втрати інформації, захист від неавторизованого створювання і знищення даних;
- конфіденційність інформації та доступ до неї авторизованих користувачів.

Також можна виділити кілька основних етапів створення комплексної системи захисту фнформації, однак насамперед доцільно з'ясувати і визначити загрози інформаційній безпеці та можливі збитки, яких вони можуть завдати після прояву, тобто аналіз ризиків. Основні проблеми під час проведення такого аналізу виникають у зв'язку зі складністю визначення кількісного значення ймовірності прояву тих чи інших загроз і розміру можливих збитків від їхнього впливу. Тому захищеність інформації на судні описується якісними показниками, набір яких визначається спеціальними методиками.

З аналізу ризиків розробляється план захисту, що містить повний опис усіх рекомендованих заходів для захисту інформації:

- інструкція для керівництва компанії;
- модель потенційних загроз;
- економічне обґрунтування запропонованих рекомендацій;
- календарні план впровадження систем захисту;
- перелік відомостей, що становлять комерційну таємницю;
- перелік організаційних заходів і документів;
- рекомендації щодо виконання вимог керівних документів.

Склад технічних засобів визначається на основі чітких критеріїв, що виділяються як рекомендації щодо вибору засобів захисту. Наступним етапом після виявлення можливих загроз і визначення заходів щодо їхньої нейтралізації є створення спеціального підрозділу в компанії або відповідальної особи, яка відповідає за виконання плану захисту суден, і визначення завдань, чисельності, складу технічних засобів, характеру та режиму взаємодії його з іншими службами.

Регулювання взаємовідносин членів екіпажу щодо правил і режиму використання спеціальних технічних засобів при вирішенні завдань інформаційної безпеки є ще одним видом завдань для професійної організації системи захисту інформації на судні, тому регламентуючі документи, що стосуються організації систем захисту, мають розглядати всі можливі ситуації, пов'язані з експлуатацією суднових інформаційних систем.

Висновки. Для побудови ефективної системи захисту та інформаційної безпеки судна необхідне проведення ретельного аналізу законодавчої бази та сучасних існуючих засобів захисту інформації в інших галузях. У статті ідентифіковано основні фактори загрози інформаційній безпеці судна та досліджено їхній вплив на процес експлуатації судна, вивчено пропозиції щодо подолання загроз з урахуванням різних сценаріїв за допомогою розроблених і прийнятих документів з забезпечення кібербезпеки в морській галузі. Подано аналіз основних факторів, що становлять загрозу та впливають на забезпечення інформаційної безпеки судна. На базі запропонованої концептуальної моделі забезпечення безпеки судна акцентовано увагу на основних факторах впливу на стан інформаційної безпеки судна, що дозволяє здійснити правильний вибір методів і засобів захисту інформації та організувати оптимальну і гнучку систему

безпеки і необхідний рівень її надійності та захищеності.

Подальшими кроками є реалізація єдиних підходів щодо інтеграції систем зв'язку, навігації, гідрометеорологічного забезпечення з метою створення єдиного інформаційного простору на основі сучасних цифрових технологій. Також подальший розвиток сучасних інформаційних технологій і їх впровадження на сучасних суднах в елементах суднового навігаційного обладнання має бути узгоджено та скоординовано з береговими інформаційними системами і мати єдині стандарти для їхнього ефективного сумісного використання.

Список використаних джерел

1. Progoulakis I., Rohmeyer P., & Nikitakos N. 2021. Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering, 9(12):1384. URL: https://doi.org/10.3390/jmse9121384.

2. Lagouvardou S., 2018. Maritime Cyber Security: concepts, problems and models. Master thesis. Technical university of Denmark. 128 p.

3. Kardakova Maria & Shipunov Ilya & Nyrkov A. & Knysh Tatyana. (2020). Cyber Security on Sea Transport. 10.1007/978-3-030-19756-8_46.

4. Nyrkov A., Goloskokov K., Koroleva E., et al. Mathematical models for solving problems of reliability maritime system. Advances in Systems, Control and Automation. LNEE. Vol. 442 (2018). URL: https://doi.org/10.1007/978-981-10-4762-6_37.

5. Iris Malone and Anastasia Strouboulis (2021). Emerging Risks in the Marine Transportation System (MTS), 2001-2021 The National Counterterrorism Innovation, Technology, and Education (NCITE) Center. 70 p.

6. Kala N. and Mahesh Balakrishnan. Cyber Preparedness in Maritime Industry. International Journal of Scientific and Technical Advancements. Vol. 5, Is. 2. 2019. P. 19-28.

7. Melnyk O., Onyshchenko S., Koryakin K. (2021) Nature and origin of major security concerns and potential threats to the shipping industry. Scientific Journal of Silesian University of Technology. Series Transport. 113. P. 145-153. ISSN: 0209-3324. URL: https://doi.org/10.20858/sjsutst.2021.113.11.

8. Ships infected with ransomware, USB malware, worms. URL: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms].

9. Hyra Bartlomiej. Analyzing the Attack Surface of Ships In DTU Compute Department of Applied Mathematics and Computer Science. Kongens Lyngby: Technical University of Denmark, 2019.

10. Maritime cybersecurity project. (2018) Maritime Security Center. American Bureau of Shipping. URL: https://www.stevens.edu/sites/stevens_edu/files/files/MSC/ABS Maritime%20 CybersecurityFinalProject%20Report.pdf.

11. 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). P. 135-140. URL: https://doi.org/10.22937/IJCSNS.2022.22.3.18.

12. Melnyk O., Onyshchenko S., Onishchenko O., Lohinov O., Ocheretna V., Dovidenko Yu. Basic aspects of ensuring the shipping safety. Scientific Journal of Silesian University of Technology.

Series Transport. 2022. 115. P. 11-22. ISSN: 0209-3324. URL: https://doi.org/10.20858/sjsutst.2022.115.1.

13. Juan Ignacio Alcaide, Ruth Garcia Llave, Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia. 2020. Vol. 45. P. 547-554. URL: https://doi.org/10.1016/j.trpro.2020.03.058.

14. Коровин А. (2007). Обеспечение безопасной эксплуатации танкерного флота в районах разработки континентальных шельфов арктических морей. *Вестник камчатского государственного университета*. 2007. (6). С. 54-56.

15. Мельник О. М., Бичковський Ю. В. Сучасна методика оцінки рівня безпеки судна та шляхи його підвищення. *Розвиток транспорту*. 2021. № 2 (9). С. 37-46. URL: https://doi.org/:10.33082/td.2021.2-9.03.

16. Обеспечение безопасности плавания судов и предотвращение загрязнения окружающей среды / В. И. Дмитриев, В. Е. Леонов, Б. Г. Химич и др.; под ред. В. И. Дмитриева, В. Е. Леонова. Херсон: ХГМА, 2012. 397 с.

17. 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). P. 135-140. URL: https://doi.org/10.22937/IJCSNS.2022.22.3.18.

18. Melnyk O., Bychkovsky Yu., Shumylo O., Onyshchenko S., Onishchenko O., Voloshyn A., Cheredarchuk N. Study of the risk assessment quality dependence on the ships accidents analysis. Scientific Bulletin of Naval Academy. 2022. Vol. XXV. P. 136-146. URL: https://doi.org/:10.21279/1454-864X-22-I1-015.

Мельник Олексій Миколайович, кандидат технічних наук, доцент кафедри судноводіння і морської безпеки, Одеський національний морський університет. Тел.: (048) 732-06-38. E-mail: m.onmu@ukr.net. ORCID: 0000-0001-9228-8459.

Волошин Андрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри судноводіння і морської безпеки, Одеський національний морський університет. Тел.: (048) 732-06-38. E-mail: aavoloshin61@gmail.com. ORCID: 0000-0003-3993-5826.

Онищенко Олег Анатолійович, доктор технічних наук, професор, професор кафедри технічної експлуатації флоту, Національний університет «Одеська морська академія». Тел.: (048) 728-55-12. E-mail: oleganaton@gmail.com. ORCID: 0000-0002-3766-3188.

Щербина Ольга Василівна, кандидат технічних наук, доцент, доцент кафедри експлуатації флоту і технологій морських перевезень, Одеський національний морський університет. Тел.: (048) 732-06-38. E-mail: olshcherbina@i.ua. ORCID: 0000-0002-9247-5972.

Васалатій Надія Василівна, кандидат географічних наук, доцент кафедри навігації і керування судном, Одеський національний морський університет. Тел.: (048) 732-06-38. E-mail: vnv0920@gmail.com. ORCID: 0000-0002-7188-9922.

Никитюк Петро Володимирович, старший викладач кафедри судноводіння і морської безпеки, Одеський національний морський університет. Тел.: (048) 732-06-38. E-mail: gelaevnyk@gmail.com. ORCID:0000-0002-5905-3807.

Melnyk Oleksiy Mykolayovych, PhD (Tech.), Associate Professor, Department of Navigation and Maritime Safety, Odesa National Maritime University. Tel.: (048) 732-06-38. E-mail: m.onmu@ukr.net. ORCID: 0000-0001-9228-8459.

Voloshin Andriy Oleksandrovych, PhD (Tech.), Professor, Head of Department, Department of Navigation and Maritime Safety, Odesa National Maritime University. Tel.: (048) 732-06-38. E-mail: aavoloshin61@gmail.com. ORCID: 0000-0003-3993-5826.

Onishchenko Oleg Anatoliyovych, D. Sc. (Tech.), Professor, Department of Fleet Technical Operation, National University «Odesa Maritime Academy». Tel.: (048) 728-55-12. E-mail: oleganaton@gmail.com. ORCID: 0000-0002-3766-3188.

Shcherbina Olha Vasilivna, PhD (Tech.), Associate Professor, Department of Fleet Operation and Shipping Technology, Odesa National Maritime University. Tel.: (048) 732-06-38. E-mail: olshcherbina@i.ua. ORCID: 0000-0002-9247-5972.
Vasalatii Nadiia Vasilivna, PhD (Geog.), Associate Professor, Department of Navigation and Ship Control, Odesa National Maritime University. Tel.: (048) 732-06-38. E-mail: vnv0920@gmail.com. ORCID: 0000-0002-7188-9922.
Nykytyuk Petro Volodymyrovych, Senior Lecturer, Department of Navigation and Maritime Safety, Odesa National Maritime University. Tel.: (048) 732-06-38. E-mail: gelaevnyk@gmail.com. ORCID:0000-0002-5905-3807.

Статтю прийнято 05.09.2022 р.