УДК 007:656.61
DOI 10.47049/2226-1893-2024-2-234-247

ПРОТИДІЯ КІБЕРНЕТИЧНИМ АТАКАМ НА МОРСЬКОМУ ТРАНСПОРТІ

О.І. Полікаровських
д.т.н, професор кафедри «Технічна кібернетика
й інформаційні технології ім. проф. Р.В. Меркта»
ORCID: 0000-0002-1893-7390
М.О. Малаксіано
д.т.н, професор кафедри «Технічна кібернетика
й інформаційні технології ім. проф. Р.В. Меркта»
ORCID: 0000-0002-4075-5112
Ю.В. Даус
к.геогр.н, доцент кафедри «Технічна кібернетика
й інформаційні технології ім. проф. Р.В. Меркта»
ORCID: 0000-0001-9737-4663

Одеський національний морський університет, Одеса, Україна

Анотація. *Протягом багатьох років кількість кібератак стрімко зростає, що призводить до великих фінансових втрат підприємствам, а також побічних збитків ділової репутації підприємств.*

У цьому відношенні морський сектор, який досі вважався безпечним через відсутність стабільного підключення до Інтернету та ізольованість кораблів у морі, демонструє стрімке зростання кількості порушень кібербезпеки в цій сфері, коли вона вступає у цифрову еру.

Велика кількість загроз кібератак на морі лишаються не дослідженими глибоко. Отже, дана стаття містить детальне дослідження протидії кібернетичним атакам на морському транспорті з метою висвітлити проблеми та виклики безпеки.

У статті розглянуті суднові системи, якими оснащені морські судна, що можуть бути ціллю зловмисників. Їхні можливі вразливості, якими може скористатися зловмисник, наслідки доступу до системи та фактичні інциденти.

Також стаття описує та аналізує можливі заходи протидії, які можна використати заздалегідь, щоб запобігти таким нападам. Нарешті, обговорюються відкриті проблеми для майбутніх досліджень.

Ключові слова: *морський, кораблі, кібербезпека, вразливості, кіберзлочинці.*

UDC 007:656.61
DOI 10.47049/2226-1893-2024-2-234-247

COUNTERING CYBERNETIC ATTACKS ON MARINE TRANSPORT

O. Polikarovskykh
D.Sc., professor of the Department «Technical Cybernetics
and Information Technologies named after prof. R.V. Merkt»
ORCID: 0000-0002-1893-7390
M. Malaksiano
D.Sc., professor of the Department «Technical Cybernetics
and Information Technologies named after prof. R.V. Merkt»
ORCID: 0000-0002-4075-5112
Y. Daus
Ph.D., docent of the Department «Technical Cybernetics
and Information Technologies named after prof. R.V. Merkt»
ORCID: 0000-0001-9737-4663

Odesa National Maritime University, Odesa, Ukraine

Abstract: *Over the years, the number of cyber-attacks has been growing rapidly, resulting in large financial losses for businesses, as well as collateral damage to their business reputation. In this respect, the maritime sector, which has so far been considered safe due to the lack of stable internet connectivity and the isolation of ships at sea, is seeing a rapid increase in cybersecurity breaches in this area as it enters the digital age. A large number of cybersecurity issues at sea remain unexplored in depth. Therefore, our article provides a detailed study of countering cyber attacks on maritime transport in order to highlight security issues and challenges. The article discusses the systems equipped on ships that may be targeted by cybercriminals. Their possible vulnerabilities that can be exploited by an attacker, the consequences of accessing the system and actual incidents. The article also describes and analyses possible countermeasures that can be taken in advance to prevent such attacks. Finally, open issues for future research are discussed.*

Keywords: *maritime; ships; cybersecurity; vulnerabilities; cybercriminals*

Вступ. На морський транспорт припадає 90 % обсягу міжнародних перевезень [1]. У наш час прогресуюча цифровізація економіки стала світовим трендом, що повною мірою стосується і морського та річкового транспорту. Судна збільшуються, а екіпажі зменшуються через все більшу автоматизацію процесів на транспорті. Деякі бортові системи отримують оновлення під час рейсу, команди мають доступ до Інтернету. Окремі фахівці стверджують, що інформаційній безпеці морського та річкового транспорту приділяється дуже мало уваги [2]. Це легко перевірити на сайтах вітчизняних компаній, що надають послуги та виробляють продукти і рішення для морського і річкового транспорту. Як правило, в описі

послуг, продуктів та рішень питання інформаційної безпеки не згадуються. У кращому випадку згадується можливість розмежування доступу за допомогою паролів і логінів або використання мережевих екранів. Робота з навігаційними системами, такими як автоматична ідентифікаційна система (AIS), глобальна навігаційна супутникова система (GNSS) і система радіолокаційного виявлення і визначення дальності (RADAR), дає можливість використовувати вразливості цих систем і знижує загальний рівень безпеки морської інфраструктури. Як правило, в описі послуг, продуктів та рішень питання інформаційної безпеки не згадуються Крім того, судна і порти піддаються дуже складним і невідомим системним кібератакам, які спрямовані на портові інформаційні системи та основне і додаткове обладнання суден. Підключення обладнання до мережі Інтернет, робота з комп'ютерами, які не підтримують належний рівень безпеки, а також відсутність підготовки команд до нових кібернетичних викликів ще більше підвищує ймовірність успішної атаки на морську транспортну інфраструктуру. Численні роботи доводять, що низький рівень підготовки співробітників і відсутність систематичного розгляду питань кібербезпеки є основною проблемою, з якою стикається галузь, в результаті чого зловмисники використовують стандартні методи: розсилають спам електронною поштою і месенджерами, організовують «відмову в обслуговуванні» (DoS) для досягнення своїх цілей [3]. Використання плану побудови системи безпеки на основі галузевих рекомендацій є життєво важливим завданням; такий план повинен бути узгоджений зі стратегіями міжнародних морських організацій [4]. Метод оновлення програмного забезпечення через USB-носії, обмін інформацією в режимі реального часу з пристроями Інтернету речей – підвищує ризик зламу системи за допомогою відомих методів з цивільної інфраструктури. Особливу роль тут відіграють незахищеність мережевих сервісів, відсутність ідентифікації та автентифікації. У нашій роботі представлено огляд систем кібербезпеки та запропонована систематизація кібератак на морський транспорт. Виконано класифікацію типів суднового обладнання. Ця класифікація дозволяє систематизувати загрози за типами атак. Зроблено висновки щодо можливих напрямків підвищення стійкості систем до комплексних атак на програмно-апаратні комплекси морської інфраструктури.

Постановка задачі. Відповідно до Європейської Директиви «EU 2016-679», кібербезпечні судна належать до найважливіші інфраструктури, які вже значною мірою залежать від цифрових послуг, а зловмисне порушення їх роботи може призвести до фінансової та екологічної шкоди або навіть загрожувати безпеці людини [3]. Хоча деякі дослідження з цього приводу проводяться області [2; 3; 6], проблеми морської кібербезпеки не були глибоко досліджені. У цій статті ми спочатку визначимо проблеми безпеки та загрози, з якими стикається сучасна індустрія судноплавства, особливо ті, що націлені на системи, присутні на суднах. Оглянемо можливі заходи пом’якшення, які можна використати заздалегідь, щоб запобігти таким атакам, і, нарешті, обговоримо кілька викликів і відкритих проблем для майбутніх досліджень.

Сучасні судна оснащені різними комплексами автоматизації та системами, які зробили море набагато безпечнішим місцем, ніж раніше [5]. Однак деякі з цих систем часто є незахищеними та вразливими до атак. Як показано на рис. 1, ці системи включають навігацію, системи радіовиявлення та визначення дальності (радіолокаційні системи), системи автоматичної ідентифікації суден (AIS), системи зв'язку, а також системи управління для широкого спектру електромеханічних систем на борту суден, такі як головний двигун, генератори, приводи конвертерів тощо [3-6].

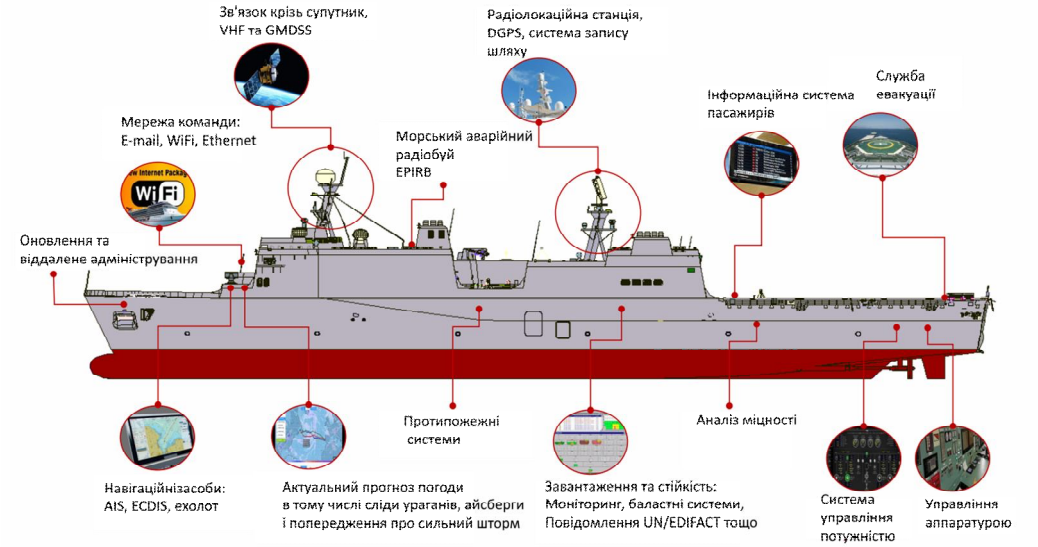

Рис. 1. Приклади важливих автоматичних систем сучасних суден, які можуть бути об'єктами кібератаки

Навігаційні системи включають систему відображення електронних карт та інформації (ECDIS), глобальної системи позиціонування (GPS) і системи глобального позиціонування (GNSS).

GPS і GNSS є ключовими факторами для сучасного та автономного судноплавства у всьому світі [8]. Супутникове позиціонування можна використовувати в поєднанні з іншими ситуаційними системами обізнаності, які надають інформацію щодо просторового положення транспортних систем для прийняття рішень [11].

Система автоматичної ідентифікації (AIS) – це система радіомовлення, яка діє як на судах, так і на березі. Використовується для моніторингу руху суден і допомоги, а також для повідомлень портової та морської влади про місцезнаходження судна. Ця система також є дуже корисною при нещасних випадках, пошуково-рятувальних роботах та для отримання прогнозу погоди. Фактично, здатність покладатися на передані дані має вирішальне значення для підтримки ситуаційної обізнаності та уникнення зіткнення на морі.

ECDIS – це інтегрована електронна навігаційна система, яка об'єднує дані отримані від ряду електронних навігаційних датчиків, таких як GPS, радіолокаційна станція і AIS, і відображає його у вигляді графічного зображення [10]. Міжнародна морська організація (IMO) вимагає, щоб усі комерційні судна мали ECDIS, яка зазвичай встановлюється на містку [12]. Радіолокація та визначення дальності (РЛС) також є важливою системою для сучасних кораблів оскільки він надає цінну інформацію про оточення судна, а також виявляє фізичні об'єкти за допомогою радіохвиль, наприклад мікрохвиль в електромагнітному спектрі.

Щоб забезпечити високу швидкість передачі даних більшість сучасних кораблів і суден обладнані терміналами (VSAT), які діють як наземна станція для передачі та прийому даних з супутникових антен. Трансивер встановлено над палубою, щоб забезпечити огляд супутників, а блок керування розташований під палубою та виконує роль комп'ютерного інтерфейсу [11]. VSAT пропонує різноманітні послуги зв'язку та безпеки, такі як ECDIS, AIS, телефонія, Інтернет-зв'язок, обробка вантажів, бездротова інтеграція до систем керування, розваги екіпажу та прогноз погоди. У сучасній галузі судноплавства також зростає попит на автоматизовані інтелектуальні системи відеоспостереження для моніторингу транспортних операцій, зокрема у великих складських приміщеннях, генераторах і великих суднах, що перевозять цінні вантажі [14]. Крім того, судноплавство та морська промисловість значною мірою залежать від індустріальної контролюючої системи (ICS) та мереж IT систем на борту судна [11-14]. ICS допомагають швидко збирати та накопичувати дані безпеки та оперативні дані усього управління судном і системи автоматизації. Вона контролює температуру, тиск, рівень, в'язкість, контроль потоку, швидкість, крутний момент, напруга, струм, а також стан машин і обладнання на борту для підтримки безпеки та експлуатаційної надійності, а також дозволяє йти в ногу з мінливим ландшафтом загроз.

Глобальна морська система зв'язку під час лиха та безпеки на морі (GMDSS-Global Maritime Distress and Safety System) [15], система управління силовою установкою, Інтегровані системи містка (IBS), керування механізмами та системи контролю живлення є іншими ключовими характеристиками систем автоматизації на борту судна, які відіграють дедалі важливішу роль у забезпеченні безперебійної, безпечної та ефективної роботи суден. Як складні, цифровізовані та автоматизовані системи – сучасні кораблі та судна стикаються з дедалі більшою кількістю нових проблеми, пов'язані з безпекою та захистом даних IT-систем на борту суден [7; 13; 16].

Реєструються масові випадки кіберзлочинності в морській галузі, хоча багато випадків залишаються невідомими, оскільки судновласники не бажають повідомляти про них через втрату репутації.

Розглянемо потенційні загрози безпеці та конфіденційності суднових IT-систем, а також фактичні випадки кібератак на ці системи.

Огляд кіберінцидентів. Широке використання систем автоматизації та IT на сучасних суднах забезпечує нові можливості для хакерів і зловмисників здійснювати різні кібератаки, що може призвести до катастрофічних інцидентів і спричинити серйозні втрати безпеки [2; 5]. Мета атак полягає у дистанційному контролі суден, викраденні важливої і конфіденційної інформації, яка може бути використана для здійснення подальших атак або для зриву роботи судна шляхом пошкодження важливих компонентів і недоступності автоматизованих систем. Насправді більшість інформаційних систем на сучасних суднах незахищені та вразливі до атаки, оскільки вони вважаються менш критичними для безпеки та продуктивності [6]. Розглянемо кібератаки на сучасні судна на основі вже зламаних систем та реальних інцидентів.

Транспондери AIS взаємодіють в радіоефірі без будь-якої автентифікації чи перевірки цілісності, що дозволяє хакерам використовувати їх для поширення фальшивих повідомлень. Як зазначено в [11] програмно визначене радіо SDR (Software Defined Radio) [17] використовується зловмисниками для створення підроблених сигналів, що робить судно непомітним, а також може передавати підроблені прогнози погоди. Довіра до неточних даних може призвести до неправильного вибору та катастрофічних результатів. Дані AIS також вільно доступні для громадськості через такі веб-сайти, як Vessel Finder LimitedNetwork (https://www.vesselfinder.com/) і Marine Traffic. У цьому контексті IMO розкритикувала розкриття інформації про судна та їхні маршрути, оскільки ця інформація може зашкодити судну та екіпажу у разі цілеспрямованої атаки.

GPS і навігаційні технології, які активно використовуються в морській сфері, є конкретними цілями різних кібератак, спрямованих на використання недоліків конструкції для дестабілізації послуги, що залежать від цих технологій [15]. Такі атаки становлять середній або високий ризик оскільки, окрім порушень даних і протоколу обслуговування, існує ймовірність фізичного пошкодження судна. На приклад, підроблені сигнали GPS дозволили зловмисникам змінити маршрут судна без попередження від системи. У подібному випадку, глушіння сигналу GPS у Південній Кореї вплинуло на прийом сигналу понад 1000 літаків і 700 суден більше тижня [14]. Відповідно до [15], супутникові системи зв'язку (SATCOMs), у т.ч. зв'язок суден через Інтернет між собою та з материком, містять велику кількість вразливостей і критичних дірок у безпеці, як-от пристрої, що використовують незахищені або навіть не документовані протоколи, облікові записи заводських налаштувань, можливість використовувати паролі за замовчуванням, певні функції скидання налаштувань обладнання та бекдори.

Однією з найбільш розповсюджених систем є Глобальна навігаційна супутникова система (GNSS). Як наслідок, автономні судна, які покладаються на вдосконалений супутниковий зв'язок для передавання оперативних команд та даних датчиків можуть бути під загрозою кібератак [8], наприклад такі атаки як атака на відмову в обслуговуванні, підміна пакетів і атаки «людина посередині». Крім того, супутникові сигнали малої потужності мають істотний технічний недолік через просте перевантаження. Як наслідок, підробка та глушіння є значними проблемами, які можуть спричинити високі втрати при атаці з низькими зусиллями [15; 16]. Крім

того, оскільки багато суднових систем сильно покладаються на розташування супутника, збій GNSS може призвести до поломки інших суднових систем (наприклад – AIS).

Питання безпеки, пов'язані з системою ECDIS, були глибоко досліджені в багатьох роботах [7; 10]. Фактично існує довгий список недоліків у реалізації програмного забезпечення ECDIS. Система часто запускаються на старих комп'ютерах, на яких немає оновлень безпеки. Карти завантажені з Інтернету або вручну через USB у систему, що може призвести до зламу системи під час спроби оновити карти. Цей носій оновлення може відкрити великий простір для атаки. Автори в [14] досліджували програмне забезпечення ECDIS та виявили кілька недоліків безпеки, які могли дозволити зловмиснику видалити або перевстановити систему файли, а також впроваджувати шкідливий вміст. У результаті підміни даних вони можуть надсилатися ECDIS, що впливає на навігаційні оцінки, тим самим викликаючи зіткнення.

З широким використанням систем VSAT в сучасній морській галузі деякі аспекти мережі VSAT, як-от прозора передача та відкритість становлять проблему і виникає потреба удосконалити систему для протидії загрозам безпеки, особливо неавторизованому доступу та перехопленню даних. У 2014 році IOActive [11] протестували кілька VSAT від різних постачальників і дійшли висновку, що оскільки вони використовували передачу звичайного тексту без автентифікації, шифрування, безпеки або перевірки особистої інформації, всі протестовані пристрої були вразливі на рівні реалізації. Через слабкий захист зловмисники можуть надсилати помилкові чи спотворені сигнали GPS або шкідливий код на пристрій, щоб вимкнути його або скомпрометувати систему, знижуючи безпеку судноплавства. Агрегатори AIS зазвичай надають дані про місцезнаходження судна. Реальний ризик полягає в тому, що мережеві інтерфейси VSAT можна знайти у Інтернет за допомогою таких інструментів, як Shodan Ship Tracker. Тут можна виявити цінну та чутливу інформацію, як назви брендів, коди продуктів та інші дані, які можна використовувати при плануванні кібератаки. Стандартна інформація зазвичай доступна на веб-сайтах постачальників, і багато їх терміналів продовжують використовувати ті самі заводські налаштування, включаючи ім'я користувача та пароль. Зловмисник може змінити координати та налаштування GPS, а також завантажити зловмисне програмне забезпечення, якщо він знаходить відкритий інтерфейс VSAT, і це дозволяє здійснити подальший злам та забезпечує доступ до критичних систем управління [16].

Хоча радіолокаційні сигнали важче перервати, ніж сигнали супутників, вони все ж чутливі до завад і DDoS-атак. У разі кібератаки, радар може надавати неправдиву інформацію про сусідні об'єкти через помилкові відлуння, викликані зовнішніми хвилями від радарів. Ця неправильна інформація може стати причиною зіткнення суден, або зіткнення судна з фізичним об'єктом.

Системи відеоспостереження (VSS) відіграють вирішальну роль у безпеці судна, вантажу і екіпажу на всіх типах сучасних суден. Ці системи в основному використовуються для моніторингу і відстеження критичних операцій судна та для захисту від атак терористів та піратів. Однак нещодавно було виявлено, що VSS

є вразливими до кількох кібератак, і виникла низка проблем безпеки. Наприклад, дослідники з Bitdefender виявили, що є моделі камер відеоспостереження, які використовуються на сучасних суднах, вразливі до недоліків переповнення буфера. Використовуючи цю вразливість, дослідники були здатні відстежувати дії зламаної камери та перезаписувати паролі. Крім того, ця вразливість може спричинити збій системи VSS або, що ще гірше, створити точку входу для інших кібератак.

Більшість промислових систем керування (ICS) розроблені та запрограмовані таким чином, що не відповідають вимогам безпеки, а дані передаються у вигляді відкритого тексту [3; 4; 12]. Безпека компонентів повинна забезпечуватися постачальниками, які підтримують безпечні структури розробки, і операторами, які налаштовують компоненти відповідно до галузевих стандартів та найкращих практик захисту інформаційних систем. Розробники та оператори ICS повинні розуміти обмеження системи, а також слабкі місця її компонентів і протоколів, оскільки вони мають вирішальне значення для безпеки судна. Ця мережа дозволяє інформаційним системам керувати та взаємодіяти одна з одною. Безперервний зв’язок між IT-мережею та веб-сайтом забезпечує віддалений моніторинг, усунення несправностей і налагодження, одночасно знижуючи витрати на відрядження та спрощуючи збір і оцінку даних. Однією з головних проблем є оператори та інженери, які часто нехтують безпекою заради зручності та ефективності, що може мати далекосяжні наслідки для всієї галузі судноплавства [13]. Ця поведінка викликана комерційним тиском з метою економії часу та обходу політики безпеки.

У морській промисловості для передачі використовується декілька типів мереж передачі даних, що збираються та обробляються мережевими інформаційними системами. Прикладом таких технологій є SHIPNET, SAFENET, система C3I, RICE 10, система SHIP 2000, Smart Ship та TSCE [14]. Ці технології мають багато вразливостей у безпеці, оскільки проектуванню та конфігурації каналів зв'язку між IT-мережами приділяють мало уваги. Також мало уваги приділяється до методів автентифікації, авторизації\ та шифрування, що призводить до потенційно вразливої та застарілої системи доступу в мережу Інтернет. Власне, суднові інформаційні системи часто пов’язані з наземними об’єктами, що збільшує ризик систематичних і постійних загроз. Фінансовий тиск, законодавчі вимоги та віддалений моніторинг збільшують потребу в IT-системах і підключенні до мережі у сучасному судноплавстві; однак ці системи збільшують спектр атак, від яких повинні захищати групи безпеки. Тому вразливості в цих автоматизованих системах слід ретельно досліджувати. Сьогодні критичні мережі керування повинні бути ізольовані від суднових IT та Інтернет-мереж у безпечній зоні. Крім того, людський фактор стає ще більш складним через складну взаємопов’язану екосистему в морському секторі. Отже, відсутність культури кібербезпеки не судні, може значно спростити рівень задачі для будь-якого зловмисника, який хоче отримати доступ до судна та його систем, викрасти фактичну інформацію або порушити роботу судна.

Протидія кібернетичним атакам на морському транспорті. У політиці морської безпеки людський фактор відіграє значну роль, оскільки це може бути найслабшою ланкою. Людський фактор стає ще більш складним зі складною взаємопов'язаною екосистемою, такою як та, яка існує в морському секторі. Судна, порти та треті сторони часто працюють зі змінними екіпажами які мають різні рівні розуміння кібербезпеки та кібергігієни. Іноді це призводить до повного не розуміння наслідків що можуть настати при успішних кібератаках. Відсутність культури кібербезпеки може бути вигідним для будь-якого зловмисника, який хоче отримати доступ до судна та його систем, викрасти фактичну інформацію або порушити роботу судна. Отже, існує критична потреба в морській галузі підвищення рівня обізнаності та розуміння кіберризиків які пов'язані з безпекою судноплавства. Найефективніший спосіб досягти цього – просування культури кібербезпеки, яка, серед іншого, включає навчання з питань кібербезпеки, належну освіту та сертифікацію для відповідних частин експлуатації судна (екіпаж, треті сторони, порти, оператори). Нарешті, необхідним є створення системи спільної оборони, яка залучає багато зацікавлених сторін. Ці системи захисту можуть брати участь у ідентифікації та пом'якшенні потенційних кібератак на кількох рівнях

У таблиці 1 представлені можливі контрзаходи та заходи пом'якшення наслідків кібератаки, які можуть допомогти побудувати стійку інфраструктуру судна до зовнішніх і внутрішніх загроз безпеки.

Таблиця 1

Можливі варіанти протидії кібератакам

Система	Можливі варіанти протидії кібератакам
AIS	- Уся інформація AIS повинна бути перевірена. - Необхідне шифрування УКХ сигналів. - Потрібно контролювати цілісність трансльованої інформації, щоб переконатися, що позиція та ідентифікація є правильними. - Обладнання, яке транслює сигнали AIS, повинно бути захищене, і несанкціонований доступ повинен бути унеможливлений.
ECDIS	- Розробники ECDIS повинні прагнути прийняти життєві цикли розробки безпеки. - Регулярне документування, моніторинг і оновлення структури ECDIS. - Необхідно відстежувати та реєструвати оновлення карт ECDIS, особливо оновлення вручну через компакт-диск або USB-диск. - Усі файли оновлення слід сканувати антивірусним програмним забезпеченням. - Слід перевірити внутрішню мережу, до якої підключено ECDIS, чи може система ECDIS бути повністю ізольована або закрита Брандмауером. - Лише схвалений персонал повинен мати фізичний доступ до ECDIS та її основних компонентів.

Продовження табл. 1

GMDSS	- Криптографічний захист. - Ідентифікація та автентифікація пристрою. - Захист інформації в неактивному режимі роботи. - Контроль фізичного доступу. - Резервний план.
GNSS (GPS)	- Ідентифікація та автентифікація пристрою. - Криптографічний захист. - Захист інформації в неактивному режимі роботи.
Radar	- Ідентифікація та автентифікація пристрою. - Криптографічний захист. - Резервне копіювання інформаційної системи.
ICS	- Використання криптографії для захисту паролів від несанкціонованого перехоплення. - Щоб забезпечити безпеку систем керування, запроваджувати керування конфігурацією та керування оновленнями. – Наскільки це можливо, комунікації між охоронними зонами мають бути обмежені. - Переконайтеся, що всі підключені до Інтернету пристрої ICS захищені та що паролі регулярно оновлюються. - Адміністратори мережі ICS повинні використовувати сегментацію мережі та правила брандмауера, які блокують доступ до портів обміну файлами. - Належним чином захищати файли паролів, ускладнюючи отримання хешованих паролів. - Системним адміністраторам слід застосовувати надійні паролі. - Використовуйте конкретну політику віддаленого доступу. - Аудит віддаленого доступу та пов'язаних змін. - Блокування непотрібних портів USB. - Для всіх користувачів проводити навчання з питань кібербезпеки.
Система керування двигуном	- Резервне копіювання інформаційної системи. - Захист від відмови в обслуговуванні. - Контроль фізичного доступу.
VSAT	- Слід використовувати зашифровані системи зв'язку. - Слід ретельно розглянути механізми кіберзахисту постачальника послуг. - Автентифікація та управління контролем доступу повинні суворо дотримуватись. - Захист інформації в неактивному режимі роботи.

Продовження табл. 1

IT мережа судна	- Резервне копіювання інформаційної системи. - Автентифікація та контроль доступу. - Сегментація екіпажу на основі їх бізнес-функцій. - Забезпечити обов'язкові механізми захисту від зовнішніх кібер-загроз. - Просування системи управління конфігураціями, виправленнями/оновленнями. - Для всіх користувачів проводити навчання з питань кібербезпеки.
Людський фактор	- Сприяти розвитку культури кібербезпеки в організації. - Створювати стосунки з учасниками операційного ланцюга. - Проводити навчання з кіберобізнаності. - Оцінювати ефективність навчання за допомогою вправ та тестів з кібербезпеки. - Сприяти кібергігієні в рамках робочих процесів

Висновки. Хоча морська галузь загалом стикається з тими ж проблемами кібербезпеки, що й інші сектори економіки, проте стає все більш очевидним, що галузь відповідає профілю критичної інфраструктури, на яку спрямовані кіберзлочинці, і вона також стикається з ризиками, які можна розглянути як унікальні для природи цієї галузі. Наприклад, успішна кібератака може завершитися знищенням судна, розкрити цінну інформацію, відключити AIS судна та/або створити помилкові чи оманливі звіти AIS, які сприяють кіберпіратству та злочинцям, терористам. У нашій роботі розглянуто поточні загрози безпеці та вразливі місця в сучасній галузі судноплавства. З численних повідомлень про кіберінциденти та їхні наслідки є чіткі докази того, що кожне судно чи навіть порт знаходиться в ризикові потрапити під кібератаку, якщо ключові інформаційні системи не захищені належним чином. Тому IT-системи на сучасних суднах повинні бути підготовлені з посиленими заходами безпеки, через їх велику вразливість до кіберзагроз. У цій статті ми обговорили деякі можливі контрзаходи, які можуть пом'якшити потенційні кібератаки та зробити галузь судноплавства більш безпечною. Однак багато проблем безпеки залишаються невирішеними, особливо із збільшенням використання автономних і напівавтономних суден.

СПИСОК ЛІТЕРАТУРИ

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

3. *Alcaide J.I., Llave R.G. Critical infrastructures cybersecurity and the maritime sector. Transp. Res. Procedia 2020, 45, P. 547-554.*
4. *Kavallieratos G., Katsikas S., Gkioulos V. Cyberattacks against the autonomous ship. In Computer Security; Springer: Berlin/Heidelberg, Germany, 2018. P. 20-36.*
5. *Mednikarov B., Tsonev Y. and Lazarov A. Analysis of Cybersecurity Issues in the Maritime Industry. Inf. Secur. 2020, 47, P. 2743.*
6. *Tam K., Moara-Nkwe K., Jones K. The Use of Cyber Ranges in the Maritime Context. 2020.Available online: https://pearl.plymouth.ac.uk/handle/10026.1/16067 (accessed on 11 November 2021).*
7. *Bou-Harb E., Kaisar E.I., Austin M. On the impact of empirical attack models targeting marine transportation. In Proceedings of the 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Naples, Italy, 26-28 June 2017. P. 200-205.*
8. *Yastrebova A., Hoyhty A.M., Boumard S. Ometov, A. Comparative study on GNSS positioning systems for autonomous vessels ¨ in the arctic region. In Proceedings of the WiP Proceedings of the International Conference on Localization and GNSS (ICL-GNSS 2020), Tampere, Finland, 1-3 June 2020*
9. *Lagouvardou S. Maritime Cyber Security: Concepts, Problems and Models; Kongens Lyngby: Copenhagen, Denmark, 2018.*
10. *Tam K., Jones K. Cyber-risk assessment for autonomous ships. In Proceedings of the 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity), Scotland, UK, 11-12 June 2018. P. 1-8.*
11. *Balduzzi M., Pasta A., Wilhoit K. A security evaluation of AIS automated identification system. In Proceedin Annual Computer Security Applications Conference, New Orleans, LA, USA, 8-12 December 2014. P. 436-445.*
12. *LR. Cyber Enabled Systems. Available online: https:// unece.org/ fileadmin/ DAM/trans/doc/2018/sc3wp3/07. LR.pdf (accessed on 31 January 2022).*
13. *Siddiqi, Murtaza Ahmed, Wooguil Pak, and Moquddam A. Siddiqi. 2022. «A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures» Applied Sciences 12, no. 12: 6042. https://doi.org/10.3390/app12126042.*
14. *Kessler G.C.. Craiger J.P., Haass J.C. A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. Int. J. Mar. Navig. Saf. Sea Transp. 2018, 12, 429 p. [CrossRef].*
15. *Ilcev M. New Aspects for Modernization Global Maritime Distress and Safety System (GMDSS). Int. J. Mar. Navig. Saf. Sea Transp. 2020, 14, P. 519-530. [CrossRef].*
16. *Chang C., Wenming S., Wei Z., Changki P., Kontovas C. Evaluating cybersecurity risks in the maritime industry: A literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference, Tokyo, Japan, 30 October-1 November 2019.*

17. *Boiko J., Polıkarovskykh O., Tkachuk V., Yehoshyna H., Karpova L. (2023). Design Concepts for Mobile Computing Direction Finding Systems. In: Shakya S., Papakostas G., Kamel K.A. (eds) Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-99-0835-6_7.*

REFERENCES

1. *DiRenzo J., Goward D.A., Roberts F.S. The little-known challenge of maritime cybersecurity. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 6-8 July 2015. – P. 1-5.*
2. *Jensen L. Challenges in maritime cyber-resilience. Technol. Innov. Manag. Rev. 2015, 5, 35.*
3. *Alcaide J.I., Llave R.G. Critical infrastructures cybersecurity and the maritime sector. Transp. Res. Procedia 2020, 45, P. 547-554.*
4. *Kavallieratos G., Katsikas S., Gkioulos V. Cyberattacks against the autonomous ship. In Computer Security; Springer: Berlin/Heidelberg, Germany, 2018. – P. 20-36.*
5. *Mednikarov B., Tsonev Y. and Lazarov A. Analysis of Cybersecurity Issues in the Maritime Industry. Inf. Secur. 2020. – 47, P. 27-43.*
6. *Tam K., Moara-Nkwe K., Jones K. The Use of Cyber Ranges in the Maritime Context. 2020.Available online: https://pearl.plymouth.ac.uk/handle/10026.1/ 16067 (accessed on 11 November 2021).*
7. *Bou-Harb E., Kaisar E.I., Austin M. On the impact of empirical attack models targeting marine transportation. In Proceedings ofthe 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Naples,Italy, 26-28 June 2017. P. 200-205.*
8. *Yastrebova A., Hoyhty A.M., Boumard S., Ometov A. Comparative study on GNSS positioning systems for autonomous vessels in the arctic region. In Proceedings of the WiP Proceedings of the International Conference on Localization and GNSS (ICL-GNSS 2020), Tampere, Finland, 1-3 June 2020*
9. *Lagouvardou S. Maritime Cyber Security: Concepts, Problems and Models; Kongens Lyngby: Copenhagen, Denmark, 2018.*
10. *Tam K., Jones K. Cyber-risk assessment for autonomous ships. In Proceedings of the 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity), Scotland, UK, 11-12 June 2018. – P. 1-8.*
11. *Balduzzi M., Pasta A., Wilhoit K. A security evaluation of AIS automated identification system. In Proceedin Annual Computer Security Applications Conference, New Orleans, LA, USA, 8-12 December 2014. P. 436-445.*
12. *LR. Cyber Enabled Systems. Available online: https://unece.org/fileadmin/DAM/trans/ doc/2018/sc3wp3/07. LR.pdf (accessed on 31 January 2022).*

13. *Siddiqi, Murtaza Ahmed, Wooguil Pak, and Moquddam A. Siddiqi. 2022. «A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures» Applied Sciences 12, no. 12: 6042. https:// doi.org/ 10.3390/app12126042.*
14. *Kessler G.C., Craiger J.P., Haass J.C. A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. Int. J. Mar. Navig. Saf. Sea Transp. 2018, 12, 429 p. [CrossRef].*
15. *Ilcev M. New Aspects for Modernization Global Maritime Distress and Safety System (GMDSS). Int. J. Mar. Navig. Saf. Sea Transp. 2020. 14, P. 519-530. [CrossRef].*
16. *Chang C., Wenming S., Wei Z., Changki P., Kontovas C. Evaluating cyber-security risks in the maritime industry: A literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference, Tokyo, Japan, 30 October-1 November 2019.*
17. *Boiko J., Polıkarovskykh O., Tkachuk V., Yehoshyna H., Karpova L. (2023). Design Concepts for Mobile Computing Direction Finding Systems. In: Shakya S., Papakostas G., Kamel K.A. (eds) Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-99-0835-6_7.*

Стаття надійшла до редакції 15.05.2024

Посилання на статтю: Полікаровських О.І., Малаксіано М.О., Даус Ю.В. Протидія кібернетичним атакам на морському транспорті // *Вісник Одеського національного морського університету:* Зб. наук. праць, 2024. № 2 (73). С. 234-247. DOI 10.47049/2226-1893-2024-2-234-247.

Article received 15.05.2024

Reference a journal artic: Polikarovskykh O., Malaksiano M., Daus Y. Countering cybernetic attacks on marine transport // *Herald of the Odesa national maritime university:* Coll. scient. works, 2024. № 2 (73). P. 234-247. DOI 10.47049/2226-1893-2024-2-234-247.