УДК 629.5:004.056 **DOI https://doi.org/10.33082/td.2023.3-18.10**

ВИКОНАННЯ АВТОМАТИЗОВАНИХ ШВАРТОВНИХ ОПЕРАЦІЙ МІЖ СУДНАМИ: ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ

І.П. Гончарук[1], А.І. Головань[2]
[1]к.т.н., доцент кафедри судноводіння і морської безпеки,
Одеський національний морський університет, Одеса, Україна,
ORCID ID: 0000-0002-5306-4206
[2]к.т.н., доцент кафедри судноводіння і морської безпеки,
Одеський національний морський університет, Одеса, Україна,
ORCID ID: 0000-0001-6589-4381

Анотація

Ця наукова стаття зосереджена на вивченні кібербезпеки в контексті автоматизованих швартовних операцій між суднами, які відомі як 'ship to ship docking' (STS). З розвитком технологій та автоматизації в морській галузі ці операції стають все більш поширеними і вразливими перед кібератаками та зловмисними діями. Кібербезпека є актуальним питанням у сучасному морському транспорті, зокрема при здійсненні автоматизованих швартовних операцій між суднами. Ці операції повинні виконуватися за допомогою спеціальних автоматизованих систем, які забезпечують точність та безпеку маневрування суден. Проте, разом з перевагами, ці системи також стають вразливими перед кібератаками та зловмисними діями. Операції STS вимагають великих обсягів обміну даними та комунікаційних протоколів між суднами. Під час цих операцій можуть виникнути потенційні ризики кібератак, таких як несанкціонований доступ, перехоплення даних, вплив на керування та навіть можливість виникнення аварійних ситуацій. Отже, основна ***мета*** *цієї наукової статті полягає в дослідженні кібербезпеки при виконанні автоматизованих швартовних операцій між суднами. Під час досягнення поставленої мети було проаналізовано загрози та ризики, пов'язані з цими операціями, а також розроблено та впроваджено заходи забезпечення кібербезпеки для зменшення ризиків кібератак, забезпечення надійності систем керування та безпеки під час виконання операцій STS. Дослідження, що викладені в даній статті, мають на меті покращити розуміння проблеми кібербезпеки в контексті автоматизованих швартовних операцій між суднами та сприяти розробці ефективних стратегій та політик забезпечення безпеки в цій галузі.* ***Результати.*** *У цій статті автори представили технологію децентралізованого управління як інструмент для зберігання значного обсягу інформації на борту суден для наукових цілей і заходів із запобігання аварій та інцидентів при виконанні швартовних операцій.* ***Висновки.*** *Обґрунтуванням використання технології децентралізованого управління є вирішення майбутніх труднощів, пов'язаних із впровадженням або прийняттям новітніх технології судноплавними компаніями. Ключовим викликом у цій галузі є заохочення судноплавних компаній до впровадження блокчейну (технологія розподіленого реєстру).*

Ключові слова: *кібербезпека, загрози, ризики, вразливості, швартовні операції, Ship to ship.*

AUTOMATED SHIP TO SHIP DOCKING: A CYBERSECURITY STUDY

I.P. Honcharuk[1], A.I. Golovan[2]
[1]Ph.D (Engineering), Associate Professor at the Department of Navigation and Maritime Safety,
Odesa National Maritime University, Odesa, Ukraine,
ORCID: 0000-0002-5306-4206
[2]Ph.D (Engineering), Associate Professor at the Department of Navigation and Maritime Safety,
Odesa National Maritime University, Odesa, Ukraine,
ORCID ID: 0000-0001-6589-4381

Summary

This research article focuses on the study of cybersecurity in the context of automated mooring operations between ships, known as ship to ship docking (STS). With the development of technology and automation in the maritime industry, these operations are becoming increasingly common and vulnerable to cyberattacks and malicious acts. Cybersecurity is an urgent issue in modern maritime transport, when performing automated ship to ship docking. These operations must be performed using special automated systems that ensure the accuracy and safety of ship maneuvering. However, along with their advantages, these systems also become vulnerable to cyberattacks and malicious acts. STS operations require large amounts of data exchange and communication protocols between ships. During these operations, potential risks of cyberattacks may arise, such as unauthorized access, data interception, impact on control, and even the possibility of accidents. Therefore, the main ***purpose*** *of this scientific paper is to study cybersecurity in automated mooring operations between ships. To achieve this goal, the threats and risks associated with these operations have been analyzed, and cybersecurity measures have been developed and implemented to reduce the risk of cyberattacks, ensure the reliability of control systems, and ensure safety during STS operations. The research presented in this article aims to improve the understanding of cybersecurity in the context of automated ship-to-shore mooring operations and to contribute to the development of effective security strategies and policies in this area.* ***Results****. In this article, the authors presented distributed control technology as a tool to store a significant amount of information on board ships for scientific purposes and to prevent accidents and incidents during mooring operations.* ***Conclusions****. The rationale for the use of decentralized management technology is to address future difficulties associated with the introduction or adoption of new technologies by shipping companies. The key challenge in this area is to encourage shipping companies to adopt blockchain (distributed ledger technology).*

Key words: *cybersecurity, threats, risks, vulnerabilities, mooring operations, Ship to ship.*

Вступ. Ефективне та стале судноплавство є важливим для безперервного зростання світової економіки, але рівною мірою має бути спрямоване на захист навколишнього середовища, економічну ефективність та забезпечення енергоефективного та безпечного транспортування товарів по всьому світу [1]. Незважаючи на значний прогрес в інноваційних рішеннях для діджиталізації суден, все ще існує

залежність від людських ресурсів з точки зору управління судном, контролю робочих процесів та відповідальності за перевірку роботи на борту судна. Крім того, важливо зазначити, що судноплавство і морський транспорт можуть спричинити велику кількість аварій і інцидентів під час виконання швартовних операцій [2].

Постановка проблеми. Судна, порти та морські об'єкти все більше залежать від сучасних інформаційних та операційних технологій. Кіберінциденти на суднах можуть спричинити збої в роботі критично важливих систем, що створюють проблеми для безпечної експлуатації судна. Тому судновласники повинні бути готові протистояти зростаючим кіберзагрозам. Для того, щоб запобігти кіберінцидентам на суднах і в компаніях, необхідно вжити заходів на рівні керівництва.

У автоматизованих швартовних операціях STS існують різноманітні ризики та загрози кібербезпеки, які можуть мати серйозні наслідки для безпеки та ефективності цих операцій. Ось деякі з них:

1. Кібератаки: зловмисники можуть спробувати зламати системи автоматизації, що керують швартовними операціями, з метою незаконного доступу, розкриття конфіденційної інформації або навіть зміни параметрів операцій.
2. Віруси та шкідливі програми: швартові системи можуть стати жертвами вірусів, шкідливих програм або програм-вимагачів, що можуть спричинити виток даних, перешкодити нормальному функціонуванню системи або навіть зупинити операції.
3. Несправності обладнання: автоматизовані системи можуть стикатися з технічними проблемами, помилками в програмному забезпеченні або апаратними несправностями, що можуть призвести до невірних дій під час швартовних операцій.
4. Втрати зв'язку: випадки втрати зв'язку між суднами або між судном і береговим оператором можуть створити ризик неконтрольованої або неправильної роботи систем керування швартуванням.

Для ефективного управління та пом'якшення наслідків цих ризиків і загроз кібербезпеки рекомендується вживати такі заходи:

1. Захист мережі та систем.
2. Аутентифікація та авторизація.
3. Захист від вірусів та шкідливих програм.
4. Резервне копіювання даних.
5. Технічна підтримка та навчання персоналу.
6. Аудит безпеки.
7. Встановлення протоколів реагування на інциденти.

Крім того, ведення документації відповідно до міжнародних стандартів, санкцій і змінних протоколів історично покладало значний тягар на екіпажі. Крім того, багато досвідчених співробітників не пройшли адекватного і послідовного навчання щодо найсучасніших і найновіших методів і несподіваних відхилень. Багато проблем виникло через обмін інформацією, координацію і комунікацію, прийняття рішень і управління часом, що збільшило навантаження на всі сторони, призвело до людських помилок і створило загальну плутанину, пов'язану із залученими сторонами та їхніми обов'язками.

Транспортна галузь потребує діджиталізації своїх операцій, зокрема, пов'язаних з обміном інформацією. Одним з рішень є використання нових технологій, в тому

числі технології розподіленого реєстру, часто званої технологією блокчейн, яка дозволяє обмінюватися даними для здійснення транзакцій, сприяючи переміщенню потоків даних безпосередньо між сторонами у високозахищений спосіб [3]. Використання блокчейну може підвищити прозорість, ефективність та моніторинг даних, що впливають на безпеку автоматизованих швартовних операцій.

Формулювання цілей статті. У цій статті автори ставлять на меті дослідження кібербезпеки при виконанні автоматизованих швартовних операцій між суднами, з використанням технології блокчейн, з метою підвищення безпеки автоматизованих швартовних операцій, як приклад зв'язку з реєстрацією даних Глобальної системи позиціонування (GPS), а отже, будь-які сумніви, щодо зон впливу будуть виключені. Однак важливо зазначити, що ця технологія може бути застосована в багатьох інших сферах судноплавства. Вона може поліпшити управління процесом і забезпечити потік даних в режимі реального часу, а отже, підвищити безпеку від маніпуляцій із записами.

Аналіз останніх досліджень і публікацій. Технологія розподіленого реєстру, також відома як технологія блокчейн [4], спочатку набула популярності як платформа для управління цифровою криптовалютою [5; 6]. У 2008 році Сатоші Накамото представив першу платіжну систему – біткоїн, засновану на технології блокчейн [7; 8; 9]. У цій роботі автори використовували технологію децентралізованого управління (ТДУ) як абревіатуру для технології блокчейн. ТДУ визначається як спільна технологія розподіленого реєстру (ТРР), яка полегшує процес запису [10]. ТДУ – це процес, який розділяє дані в режимі реального часу на вузли, які захищені за допомогою унікальних криптографічних алгоритмів для забезпечення конфіденційності та безпеки [11]. Як зазначено в [12], ТДУ є найпотужнішою розподіленою базою даних, яка складається з груп даних та інформаційних блоків, що робить конфіденційні дані високо захищеними та доступними для авторизованих користувачів за допомогою використання «ключів». Блокчейн – це технологія, яка підтримує розподіл записаних і незмінених даних у книзі між сторонами. Ці реєстри з інформацією передаються через сіткову топологію до більшої спільноти (також відомої як однорангова мережа або технологія) [13; 14]. ТДУ – це технологія децентралізованого управління [14; 15]. Залежно від технології, блокчейн може використовувати приватні або публічні реєстри та мережі [13; 16]. У публічному (відкритому або бездозвільному) ТДУ реєстри доступні, і будь-хто може записати транзакцію і відстежити історичну транзакцію в реєстрі (тобто повністю розподілені між великою кількістю публічних користувачів). Публічні ТДУ вимагають високого рівня безпеки та надійності через існування анонімних користувачів та відсутність довіри. Приватні мережі (закриті або дозволені) ТДУ означають, що сторони або вузли знають один одного або немає необхідності в анонімності, що є протилежністю публічним або відкритим ТДУ, де обмін даними та інформацією вимагає анонімних користувачів (криптографічний метод). У приватних ТДУ або дозволених доступ обмежений певними службами або сторонами. У цьому випадку з'являється нова специфічна роль (рекомендована національною або міжнародною організацією), яка забезпечує сертифікацію мережі та підтримує цю приватну мережу [13]. Структура ТДУ виглядає таким чином: визначення послуг/сторін; агент створює транзакцію для перевірки; вузли в ланцюжку схвалюють

кожну транзакцію; транзакція додається в новий блок; запис цієї транзакції зберігається в декількох розподілених вузлах для забезпечення безпеки.

Виклад основного матеріалу. Одними з основних особливостей представленої технології є використання смарт-контрактів та токенізація активів [11]. Основною перевагою цього є те, що вся інформація, яка зберігається в блоці, є незмінною і не може бути видалена або змінена без згоди мережі. Довіра, незмінність і прозорість, дезінтермедіація та суттєві покращення – це унікальні цінності блокчейн [17].

Замість того, щоб покладатися на центральний сервер для інтеграції, перевірки, зберігання даних вручну, а потім фізичного обміну, кожен вузол або учасники взаємопов'язаної мережі дублюють всю інформацію, яку можна контролювати і використовувати для різних розслідувань (морські аварії) або наукових цілей. Транзакція складається з даних, хешу і попереднього хешу, які представлені в окремому блоці (рис. 1). Кожен блок може складатися з однієї або декількох транзакцій. Кожен хеш є унікальним цифровим відбитком транзакції в блоці, і новий хеш надається всім новим блокам, які були створені в ланцюжку.

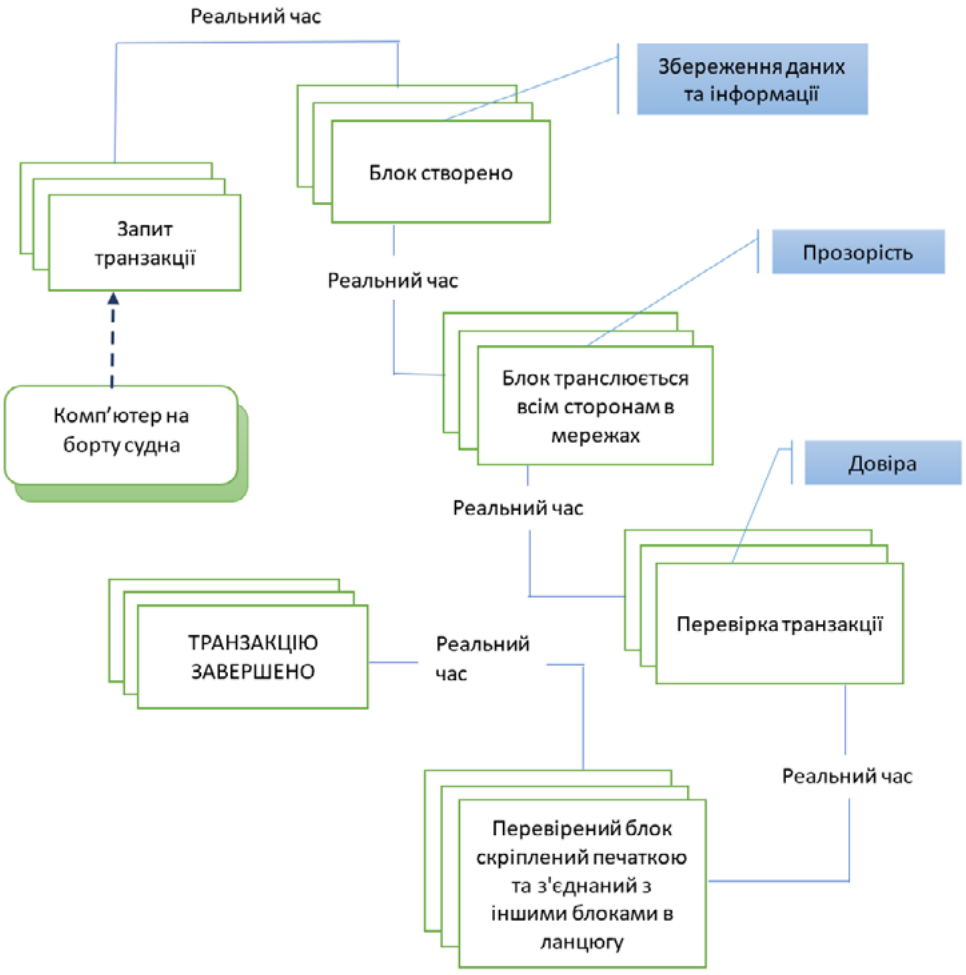

Рис. 1. Схема алгоритму виконання транзакцій по технології блокчейн

Набір інструментів, що забезпечують різні реалізації цієї технології, складається з наступного: однорангова мережа, база даних для запису транзакцій, набір функцій безпеки, доказ роботи (PoW) або доказ частки (PoS), механізм консенсусу, тощо [18]. Запропоновано публічний або бездозвільний ланцюжок блоків як інструмент для розподілу важливих даних між кількома сторонами, які не довіряють одна одній. Всі сторони в запропонованому блокчейні не мають публічної ідентичності. Блоки важко змінити, маніпулювати ними або зламати. Для успішної фальсифікації інформації необхідно переформатувати весь блокчейн [19]. Кожна транзакція в нашому випадку, наприклад, дані про місцезнаходження судна, час, відстань до іншого транспортного засобу, записується в цифрову книгу, а кілька транзакцій утворюють блок [20]. Однак певні сторони можуть обмежити публічний доступ до цих даних, щоб уникнути будь-яких публічних маніпуляцій з ними. Ці організації можуть виявляти особливий інтерес до діяльності, що відбувається на борту судна.

Блокчейн був прийнятий у багатьох галузях, включаючи освіту, охорону здоров'я, адміністрування, транспортування товарів, кібербезпеку та фінансові послуги [8; 21]. В освіті він використовується для заміни паперових сертифікатів на цифрові сертифікати учня на блоках або в публічному реєстрі і має довіру між усіма сторонами (навчальним закладом, учнем і третьою стороною). Університет Нікосії був попередником цієї інновації і запровадив процес сертифікації через блокчейн [11]. Впровадження блокчейн в освіту принесло низку переваг, серед яких: обмін ідеями та навчанням, можливості взаємного навчання, інтегрована система відстеження документів, мульти-співпраця з транзакціями цифрових сертифікатів та зв'язок між усіма сторонами валідації, верифікації та видачі сертифікатів.

Впровадження технології блокчейн у судноплавну галузь та її застосування для оцифрування товаросупровідних документів детально розглянуто в роботі [22]. Автори дослідили процес впровадження технології блокчейн у сферу судноплавства. Вони виявили, що судноплавство – це інформаційна інфраструктура з соціально-технічним ядром, що розвивається з часом завдяки діяльності всіх зацікавлених сторін. Автори навели приклади застосування технології блокчейн у проекті підтвердження концепції Maersk Line та International Business Machines (IBM), а також у рішенні Marine Transport International під назвою Safety of Lives at Sea – Verified Gross Mass (SOLAS VGM), яке стосується передачі даних про вагу контейнера в системі електронного обміну даними (EDI) на вимогу IMO. Галузь тестує морські блокчейн-додатки з 2017 року. Деякі з найважливіших судноплавних компаній, такі як Maersk, Hyundai Merchant Marine і Maritime Silk Road Platform, об'єдналися з технологічними гігантами для створення блокчейн-судноплавних систем для оптимізації морської логістики [23].

Рішення та архітектура технології розподіленого реєстру у сфері морського захисту. Наведена нижче модель (рис. 2) має на меті надати спрощену версію перевіреної публічної мережі блокчейн-мережі між стейкхолдерами в рамках наскрізної моделі обміну інформацією про морські перевезення. Передумовою є те, що багато сторін (тобто судноплавна компанія, портові адміністрації, капітан порту або берегова охорона, IMO, національний законодавець) матимуть доступ до інформації, що міститься в ній, і зможуть підтвердити її достовірність, в той час як контент зберігатиметься і буде захищений в архітектурі публічної

хмари. Це дозволить місцевим службам руху суден, капітанам, відділам моніторингу головного офісу і державним органам мати колективний огляд маршрутів суден, записів про вантаж і пасажирів (за умови дотримання стандартного Загального регламенту про захист даних та інших глобальних вимог щодо конфіденційності). Механізм повернення цієї інформації також використовує передову технологію оптичного розпізнавання чартерів. Центральний базовий комп'ютер, який вже існує на борту судна, буде збирати дані, а всі дії, пов'язані з експлуатацією судна, будуть завантажуватися на платформу в режимі реального часу. Всі ці записи даних в тому числі і щодо виконання автоматизованих швартовних операції можна буде відслідковувати в блокчейні через платформу.

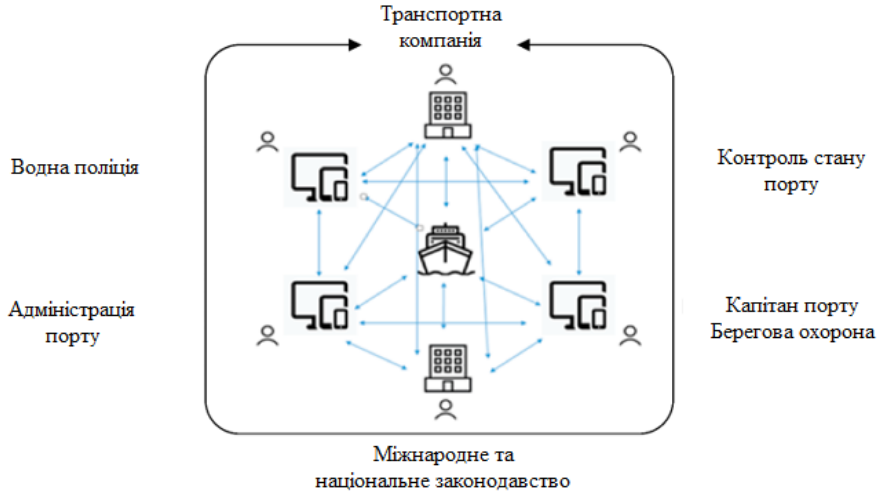

Рис. 2. Структура платформи обміну транспортною інформацією на основі блокчейну

Дані надходять і одночасно перевіряються всіма зацікавленими сторонами для досягнення консенсусу. Після розповсюдження в системі записи зберігаються та захищаються в централізованій книзі блокчейну. Згодом вони стають незмінними, а посередники/внутрішні відділи, які в минулому мали справу з паперовими записами, що передбачало ручні операції, тепер усуваються, що призводить до створення записів, захищених від несанкціонованого втручання. Процес міграції може бути ефективно керованим без втручання у встановлений протокол; проте для відповідних спеціалістів-моряків рекомендується і підтримується участь у спеціалізованих освітніх курсах. Завдяки індустріалізації даних для спільноти зацікавлених сторін і підвищенню рівня безпеки та співпраці результати сприятимуть прискоренню автоматизації перевірок, а в разі виникнення конфліктів – створенню єдиного джерела даних для вирішення запитів.

Подібно до авіаційної галузі вимога щодо зниження витрат на передачу даних в морській галузі розвивалася повільніше. Однак створення функціональних можливостей у електронному форматі, які забезпечують інтероперабельність та кросплатформеність, а також інтеграцію операційних стандартів та загальноекономічну

ефективність, особливо в контексті ланцюга поставок, є потужним інструментом. Найбільшим викликом є залучення інвестицій та визначення піонерів, які зроблять ці технології стандартом в галузі. Дані є очевидним побічним продуктом цієї технології, який сам по собі може призвести до цілої низки інсайтів і, відповідно, до покращення сервісу. Опитування в режимі реального часу серії точок даних може бути використано для забезпечення предиктивної аналітики та обслуговування оповіщень, які, ймовірно, будуть розміщені у відкритій хмарі. Це також підвищить ефективність роботи капітана і старшого механіка, усунувши залежність від ручних стримувань і противаг з боку екіпажів з експлуатації та технічного обслуговування [23]. Проривні технології в контексті управління безпекою також мають великий потенціал. Насамперед, прості методи комунікації між членами екіпажу забезпечать інформування всіх членів екіпажу про ключові повідомлення у непомітний спосіб, без необхідності оголошень по радіо. Це пов'язано з дискретністю, вартістю і цільовою моделлю. На відміну від одночасного оповіщення всього екіпажу, важливу інформацію можна передавати конкретним особам, не відволікаючи весь екіпаж і використовуючи особисті пристрої на основі принципу «принеси свій власний пристрій», який поширений в інших галузях. Цифрові ролі в судноплавних і морських організаціях повинні бути розширені, в кінцевому рахунку, під керівництвом директора з цифрових технологій і даних. Ці особи повинні працювати як зі своїми організаціями, так і в консорціумах, очолюваних галузевими організаціями, для визначення пріоритетних напрямків і спільної розробки та структури інструментів, які можуть бути використані найкращим чином. Інноваційні хаби та акселераційні лабораторії можуть отримати найкращу підтримку від закладів вищої освіти, за умови, що вони знайомі з поточними розробками, для підтримки виробничих, технологічних та операційних пропозицій.

Технологія блокчейн може допомогти у вирішенні обох питань, скорочуючи адміністративні витрати і забезпечуючи безпеку судноплавства, одночасно захищаючи галузь від кіберзлочинності та піратства, а також забезпечуючи більш справедливі умови для всіх залучених сторін. Впроваджуючи блокчейн і заходи безпеки в критичних точках (тобто крок за кроком у часі), підвищення безпеки під час автоматизованих швартовних операцій можна було б запобігти заздалегідь. У цьому випадку блокчейн можна використовувати як інструмент для кращого прийняття рішень, що має бути спільним інтересом для всіх сторін у ланцюжку. Національні регулятори (законодавці) у співпраці з ІМО регулюватимуть морські операції. Поправки до нормативних актів, що стосуються застосування морського ТРР, будуть своєчасно і належним чином інтегровані в систему, що дозволить їй адаптуватися і залишатися актуальною. Наприклад, судноплавні компанії, згідно з правилами ІМО та прибережних держав, мають певні вимоги щодо оприлюднення різних даних, пов'язаних з безпекою суден, а також нових екологічних даних у відкритому доступі. Національні регулятори у співпраці з ІМО вирішуватимуть, хто буде сторонами і якими ключами вони володітимуть, щоб брати участь в обміні даними, а також які дані вони отримуватимуть. ІМО делегує спеціальну агенцію, яка відповідатиме за створення апаратного та програмного забезпечення, тобто морських додатків. Програмне забезпечення буде повністю налаштоване відповідно до вимог і правил ІМО. Іншими словами, буде

створено програмне забезпечення, яке покладатиметься на блокчейни для підвищення безпеки, захисту та плинності даних. Оскільки блокчейн – це архітектура, яка дозволяє розрізненим користувачам здійснювати транзакції, а потім створює незмінний, безпечний запис цих транзакцій, він спрощує управління даними, створюючи надійну цифрову книгу, з якою погоджуються всі сторони.

Традиційні письмові записи про судноплавні операції (спеціальні форми) повинні бути підписані і завірені печаткою капітана. Використання датчиків даних та інформаційних технологій разом з ТДУ могло б зменшити робоче навантаження, кількість порушень, упущень і помилок екіпажу, покращити моніторинг і підвищити рівень захисту навколишнього середовища. Завдяки використанню ТДУ капітан може бути поінформований про поточний стан конкретних пристроїв на судні за допомогою повідомлень, що надаються в режимі реального часу. Таким чином, виключається необхідність заповнення письмової форми, обмежується безпосередня відповідальність капітанів, а всі групи, які отримують інформацію, можуть своєчасно реагувати на неї в разі потреби. Помилки в комунікації зводяться до мінімуму, підвищується рівень знань та обізнаності, а також покращуються безпека швартовних операцій.

Обмеження технології TPP можуть виникати в дисковому просторі. Велика кількість транзакцій даних може сповільнити процес і знизити ефективність. Автори запропонували отримувати дані в режимі реального часу з певної відстані від узбережжя, щоб зменшити великі обсяги даних та інформації. Кількість користувачів у блокчейні може зробити систему стійкішою до будь-яких випадків атак (як кібернетичних, так і порушень шляхом зміни даних) або збоїв. Впровадження технології блокчейн в судноплавну галузь, особливо судноплавні компанії, повинні визнати цю технологію. Високоякісне апаратне і програмне забезпечення для ефективної роботи системи є основною проблемою, яка заважає великим установам впроваджувати блокчейн. Підтримка інформаційних систем також є важливим фактором і викликом.

ІМО визнала потенційну проблему і морський кіберризик. ІТ та операційні технології автоматизовані, і на борту суден та на березі необхідна висока компетентність. Технології можуть опинитися під загрозою через потенційні обставини або події, які можуть призвести до пов'язаних з судноплавством збоїв в експлуатації, безпеці або захищеності внаслідок пошкодження, втрати або компрометації інформації або систем. Керівництву судноплавства пропонується кілька керівних принципів ІМО. Всі сторони повинні пройти навчання з операційних технологій (ОТ) та інформаційних технологій (ІТ), навіть незважаючи на те, що блокчейн – це технологія з високим ступенем кіберзахисту. Всі сторони, що беруть участь у ТДУ, повинні бути добре підготовлені. Впровадження ТДУ під час автоматизованих швартовних операцій дозволить звести до мінімуму спілкування між членами екіпажу на борту судна з цього питання, таким чином мінімізуючи помилки через непорозуміння. Крім того, однією з переваг використання ТДУ в цьому випадку є мінімізація зовнішньої комунікації.

Ефективне управління кібербезпекою в процесі виконання автоматизованих швартовних операцій вимагає комплексного підходу, включаючи технічні, організаційні та освітні заходи. Систематичне оновлення заходів кібербезпеки та постійне

вдосконалення практик можуть допомогти позбавити швартові операції від багатьох потенційних ризиків і зберегти безпеку морського та річкового транспорту.

SWOT – аналіз (сильні та слабкі сторони, можливості, загрози) є корисним інструментом, який допомагає визначити та класифікувати аспекти внутрішнього та зовнішнього середовища. У цьому дослідженні середовище буде складатися з автоматизованих швартовних операціях Ship to ship, а шаблон SWOT-аналізу, показаний на рисунку 3, буде заповнений її внутрішніми сильними і слабкими сторонами, а також зовнішніми можливостями та загрозами.

СИЛЬНІ СТОРОНИ	СЛАБКІ СТОРОНИ
МОЖЛИВОСТІ	ЗАГРОЗИ

Рис. 3. Шаблон SWOT-аналізу

Огляд наявної літератури свідчить про те, що дуже мало відомо про кібербезпеку та її слабкі місця в галузі автоматизації швартовних операцій Ship to ship, зокрема на рисунку 4 показані результати дослідження згруповані за категоріями внутрішніх сильних та слабких сторін, а також можливостей та загроз.

СИЛЬНІ СТОРОНИ	**СЛАБКІ СТОРОНИ**
• Зростаюча увага до кібербезпеки у морському секторі, що створює сприятливе середовище для дослідження та розробки нових підходів до управління кіберризиками. • Використання автоматизованих систем у швартовних операціях Ship to ship, що забезпечує ефективність та точність операцій. • Наявність міжнародних стандартів та рекомендацій щодо кібербезпеки в морській галузі, що служить основою для розробки стратегій та політик.	• Недостатня усвідомленість ризиків кібербезпеки серед учасників морського сектору, зокрема операторів суден і берегового персоналу. • Відсутність обов'язкових нормативних актів, які б регулювали вимоги до кібербезпеки в швартовних операціях Ship to ship. • Складність координації між різними зацікавленими сторонами, включаючи судновласників, операторів терміналів, портові власті та органи регулювання.
МОЖЛИВОСТІ	**ЗАГРОЗИ**
• Постійний розвиток технологій та інновацій, що дозволяє впроваджувати нові рішення для підвищення кібербезпеки в швартовних операціях. • Міжнародне співробітництво та обмін досвідом між країнами щодо кібербезпеки в морському секторі. • Зростаюча свідомість про необхідність захисту від кіберзагроз у морській галузі, що сприяє підвищенню інвестицій у кібербезпеку.	• Динамічність природи кіберзлочинності та кібератак, що створює виклики для постійного оновлення стратегій та технологій кібербезпеки. • Висока складність виявлення та ідентифікації нових видів кіберзагроз та їхніх наслідків. • Недостатня координація та співпраця між судновласниками, операторами терміналів, портовими властями та органами регулювання щодо кібербезпеки.

Рис. 4. SWOT-аналіз процесу автоматизації швартовних операцій Ship to ship

Для ефективного управління та пом'якшення наслідків кіберризиків у швартовних операціях Ship to ship в морській галузі необхідно враховувати сильні сторони, здолати слабкі сторони, використовувати можливості та протидіяти загрозам. Це може бути досягнуто шляхом впровадження ефективних стратегій кібербезпеки, нормативного регулювання, посилення свідомості та освіти щодо кібербезпеки, співпраці між стейкхолдерами та постійного моніторингу та аналізу кіберзагроз.

Висновки. У цій статті автори представили технологію децентралізованого управління як інструмент для зберігання значного обсягу інформації на борту суден для наукових цілей і заходів із запобігання аварій та інцидентів при виконанні швартовних операцій. Обґрунтуванням використання ТДУ є вирішення майбутніх труднощів, пов'язаних із впровадженням або прийняттям технології судноплавними компаніями. Ключовим викликом у цій галузі є заохочення судноплавних компаній до впровадження блокчейну, які повинні бути першими, хто перейде на цю технологію, враховуючи, що судноплавні компанії є операторами або власниками суден. Виходячи з професійного досвіду авторів та розслідувань морських інцидентів з баз даних, зрозуміло, що на борту суден відбувається багато інцидентів, пов'язаних зі швартовними операціями. Якщо всі суднові технічні засоби будуть оцифровані, через додаткові застосування датчиків, інформація буде передаватися між відповідними сторонами, і управління більше не буде здійснюватися вручну. Зазначена важливість технології блокчейн і те, як вона може відігравати життєво важливу роль у морській індустрії, а також проаналізовані шляхи можливого застосування технології розподіленого реєстру як засобу контролю автоматизованих швартовних операцій. Застосування ТДУ може звести до мінімуму багато проблем, включаючи поліпшення обміну інформацією, посилення координації та комунікації, полегшення прийняття рішень, економію часу, зменшення робочого навантаження для всіх сторін, усунення помилок і недоліків, а також зниження відповідальності та підвищення рівня знань. Було рекомендовано, щоб усі дані, отримані з суден у режимі реального часу, були захищені кіберзахистом і постійно зберігалися в реєстрі, що могло б допомогти багатьом сторонам зменшити робоче навантаження, кількість перевірок і втрату часу. Стверджується, що для майбутнього розвитку морської індустрії існує широкий спектр можливостей для ТДУ. Традиційні паперові документи можуть бути оцифровані і прочитані за допомогою автоматизації, що забезпечує нову хвилю співпраці між безпекою судноплавства в усій судноплавній галузі. Таким чином, операційна ефективність може бути розподілена за допомогою нових технологій і безпечно впроваджена для стимулювання інновацій. Такі цифрові перетворення в судноплавній галузі повинні здійснюватися в кілька етапів. Згодом поетапний підхід до оптимізації обміну даними буде найкращим для подальших цифрових змін.

ЛІТЕРАТУРА

1. Li, X., Nosheen, S., Haq, N. U., & Gao, X. (2021). Value creation during fourth industrial revolution: Use of intellectual capital by most innovative companies of the world. Technological Forecasting and Social Change, 163, 120479. URL: https://doi.org/10.1016/j.techfore.2020.120479.

2. Khan, R. U., Yin, J., Mustafa, F. S., & Shi, W. (2023). Factor assessment of hazardous cargo ship berthing accidents using an ordered logit regression model. Ocean Engineering, 284, 115211. URL: https://doi.org/10.1016/j.oceaneng.2023.115211.
3. Loklindt, C., Moeller, M., & Kinra, A. (2018). How blockchain could be implemented for exchanging documentation in the shipping industry. In Lecture notes in logistics (pp. 194–198). Springer Nature. URL: https://doi.org/10.1007/978-3-319-74225-0_27.
4. Vujičić, S., Hasanspahić, N., Car, M., & Čampara, L. (2020). Distributed ledger technology as a tool for environmental sustainability in the shipping industry. *Journal of Marine Science and Engineering*, 8(5), 366. URL: https://doi.org/10.3390/jmse8050366.
5. Trump, B. F., Florin, M., Matthews, H. S., Sicker, D., & Linkov, I. (2018). Governing the use of blockchain and distributed ledger technologies: Not One-Size-Fits-All. *IEEE Engineering Management Review*, 46(3), 56–62. URL: https://doi.org/10.1109/emr.2018.2868305.
6. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135. URL: https://doi.org/10.1080/00207543.2018.1533261.
7. Open Sea. Pro: How Can the Shipping Industry Take Advantage of the Blockchain Technology? Open Sea: New York, NY, USA; Available online. URL: https://www.opensea.pro/blog/blockchain-for-shipping-industry.
8. Ayvaz, S., & Cetin, S. (2019). Witness of things. *International Journal of Intelligent Unmanned Systems*, 7(2), 72–87. URL: https://doi.org/10.1108/ijius-05-2018-0011
9. Ponte, E. B., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, 27(5), 725–740. URL: https://doi.org/10.1108/medar-11-2018-0406.
10. Gausdal, A. H., Czachorowski, K. V., & Solesvik, M. (2018). Applying Blockchain Technology: Evidence from Norwegian Companies. Sustainability, 10(6), 1985. URL: https://doi.org/10.3390/su10061985.
11. Harthy, K. A., Shuhaimi, F. A., & Ismaily, K. A. (2019). The upcoming Blockchain adoption in Higher-education: requirements and process. URL: https://doi.org/10.1109/icbdsc.2019.8645599.
12. Eaganathan, U., Indrian, V. V., & Nathan, Y. (2019). Ideation framework of block chain adoption in Malaysia higher education. Journal of Physics, 1228(1), 012072. URL: https://doi.org/10.1088/1742-6596/1228/1/012072.
13. Trump, B. F., Florin, M., Matthews, H. S., Sicker, D., & Linkov, I. (2018b). Governing the use of blockchain and distributed ledger technologies: Not One-Size-Fits-All. *IEEE Engineering Management Review*, 46(3), 56–62. URL: https://doi.org/10.1109/emr.2018.2868305.
14. Khatoon, A. (2020). A Blockchain-Based smart contract system for healthcare management. *Electronics*, 9(1), 94. URL: https://doi.org/10.3390/electronics9010094.

15. McGhin, T., Choo, K. R., Liu, C. Y., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135, 62–75. URL: https://doi.org/10.1016/j.jnca.2019.02.027.
16. Kouhizadeh, M., & Sarkis, J. (2018). Blockchain Practices, Potentials, and Perspectives in greening supply Chains. *Sustainability*, 10(10), 3652. URL: https://doi.org/10.3390/su10103652.
17. Makridakis, S., & Christodoulou, K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. *Future Internet*, 11(12), 258. URL: https://doi.org/10.3390/fi11120258.
18. Hofmann, E., Strewe, U. M., & Bosia, N. (2017). Background III—What is blockchain technology? In SpringerBriefs in finance. *Springer International Publishing*. URL: https://doi.org/10.1007/978-3-319-62371-9_4.
19. White, G. R. (2017). Future applications of blockchain in business and management: A Delphi study. Strategic Change, 26(5), 439–451. URL: https://doi.org/10.1002/jsc.2144.
20. Swan, M. (2015). Blockchain: blueprint for a new economy. URL: http://cds.cern.ch/record/2000805.
21. Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: a literature review. *International Journal of Physical Distribution & Logistics Management*, 49(9), 881–900. URL: https://doi.org/10.1108/ijpdlm-11-2018-0371.
22. Jabbar, K., & Bjørn, P. (2018). Infrastructural grind. URL: https://doi.org/10.1145/3148330.3148345.
23. Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and Manufacturing Industry: Real-Time transparency and cost savings. *Sustainability*, 10(11), 4274. URL: https://doi.org/10.3390/su10114274.

REFERENCES

1. Li, X., Nosheen, S., Haq, N. U., & Gao, X. (2021). Value creation during fourth industrial revolution: Use of intellectual capital by most innovative companies of the world. Technological Forecasting and Social Change, 163, 120479. https://doi.org/10.1016/j.techfore.2020.120479
2. Khan, R. U., Yin, J., Mustafa, F. S., & Shi, W. (2023). Factor assessment of hazardous cargo ship berthing accidents using an ordered logit regression model. Ocean Engineering, 284, 115211. https://doi.org/10.1016/j.oceaneng.2023.115211
3. Loklindt, C., Moeller, M., & Kinra, A. (2018). How blockchain could be implemented for exchanging documentation in the shipping industry. In Lecture notes in logistics (pp. 194–198). Springer Nature. https://doi.org/10.1007/978-3-319-74225-0_27
4. Vujičić, S., Hasanspahić, N., Car, M., & Čampara, L. (2020). Distributed ledger technology as a tool for environmental sustainability in the shipping industry. Journal of Marine Science and Engineering, 8(5), 366. https://doi.org/10.3390/jmse8050366

5. Trump, B. F., Florin, M., Matthews, H. S., Sicker, D., & Linkov, I. (2018). Governing the use of blockchain and distributed ledger technologies: Not One-Size-Fits-All. IEEE Engineering Management Review, 46(3), 56–62. https://doi.org/10.1109/emr.2018.2868305
6. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261
7. Open Sea. Pro: How Can the Shipping Industry Take Advantage of the Blockchain Technology? Open Sea: New York, NY, USA; Available online: https://www.opensea.pro/blog/blockchain-for-shipping-industry
8. Ayvaz, S., & Cetin, S. (2019). Witness of things. International Journal of Intelligent Unmanned Systems, 7(2), 72–87. https://doi.org/10.1108/ijius-05-2018-0011
9. Ponte, E. B., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. Meditari Accountancy Research, 27(5), 725–740. https://doi.org/10.1108/medar-11-2018-0406
10. Gausdal, A. H., Czachorowski, K. V., & Solesvik, M. (2018). Applying Blockchain Technology: Evidence from Norwegian Companies. Sustainability, 10(6), 1985. https://doi.org/10.3390/su10061985
11. Harthy, K. A., Shuhaimi, F. A., & Ismaily, K. A. (2019). The upcoming Blockchain adoption in Higher-education: requirements and process. https://doi.org/10.1109/icbdsc.2019.8645599
12. Eaganathan, U., Indrian, V. V., & Nathan, Y. (2019). Ideation framework of block chain adoption in Malaysia higher education. Journal of Physics, 1228(1), 012072. https://doi.org/10.1088/1742-6596/1228/1/012072
13. Trump, B. F., Florin, M., Matthews, H. S., Sicker, D., & Linkov, I. (2018b). Governing the use of blockchain and distributed ledger technologies: Not One-Size-Fits-All. IEEE Engineering Management Review, 46(3), 56–62. https://doi.org/10.1109/emr.2018.2868305
14. Khatoon, A. (2020). A Blockchain-Based smart contract system for healthcare management. Electronics, 9(1), 94. https://doi.org/10.3390/electronics9010094
15. McGhin, T., Choo, K. R., Liu, C. Y., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027
16. Kouhizadeh, M., & Sarkis, J. (2018). Blockchain Practices, Potentials, and Perspectives in greening supply Chains. Sus-tainability, 10(10), 3652. https://doi.org/10.3390/su10103652
17. Makridakis, S., & Christodoulou, K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. Future Internet, 11(12), 258. https://doi.org/10.3390/fi11120258
18. Hofmann, E., Strewe, U. M., & Bosia, N. (2017). Background III—What is blockchain technology? In SpringerBriefs in finance. Springer International Publishing. https://doi.org/10.1007/978-3-319-62371-9_4

19. White, G. R. (2017). Future applications of blockchain in business and management: A Delphi study. Strategic Change, 26(5), 439–451. https://doi.org/10.1002/jsc.2144
20. Swan, M. (2015). Blockchain: blueprint for a new economy. Retrieved from http://cds.cern.ch/record/2000805
21. Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: a literature review. International Journal of Physical Distribution & Logistics Management, 49(9), 881–900. https://doi.org/10.1108/ijpdlm-11-2018-0371
22. Jabbar, K., & Bjørn, P. (2018). Infrastructural grind. https://doi.org/10.1145/3148330.3148345
23. Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and Manufacturing Industry: Real-Time transparency and cost savings. Sustainability, 10(11), 4274. https://doi.org/10.3390/su10114274