СУДНОВОДІННЯ ТА ЕНЕРГЕТИКА СУДЕН

УДК 629.5.052 doi.org/10.33298/2226-8553.2023.1.37.20

Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я.

ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ВПРОВАДЖЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ НА МОРСЬКОМУ ТРАНСПОРТІ

Метою роботи є дослідження можливих шляхів впровадження та поширення стандартів кібербезпеки на морському транспорті для реалізації вимог Міжнародної морської організації. Поставлена мета досягається шляхом аналізу змісту резолюції MSC.428(98) – Управління морськими кіберризиками в системах управління безпекою з метою поширення заходів кібербезпеки на морському транспорті. Визначена роль Міністерства інфраструктури України у нормативно-правовому регулюванні у сфері морської інформаційної безпеки. Доведена недостатня ефективність міністерства у формуванні конкретних кроків щодо інформаційної безпеки та захисту інформації, що торкаються особливостей організації цієї діяльності у сфері морських транспортних та вантажних перевезень, роботи портів та на окремих суднах. Проаналізовано зміст Закону України "Про основні засади забезпечення кібербезпеки України". Встановлено, що вимоги даного Закону потребують адаптації для компетентного використання на конкретному судні або портовому засобі. Окреслено коло основних загроз для суднових інформаційних ресурсів: несанкціонований доступ до каналів супутникового обміну інформацією між судном та його офісом керування; викривлення навігаційних GPS-даних, які отримуються судном; несанкціонований доступ до супутникового каналу оперативного керування судном. Відмічені заходи щодо запобігання кіберризикам проникнення зловмисників через інтерфейс судно/порт до навігаційно-інформаційної системи, системи оперативного морського зв'язку й системи планового технічного обслуговування обладнання Розкриті цілі, мотиви, можливі наслідки і ризики від впровадження промислових систем штучного інтелекту у роботу суден, портів, суднохідних компаній, визначена необхідність проведення ретельного аудиту морської компанії, що охоплюватиме окремі області функціонування системи штучного інтелекту. Найбільш суттєвими результатами є проведений ретельний аналіз організаційних ризиків і неупереджена оцінка вузьких місць у системі кіберзахисту судноплавної компанії та пропозиції щодо покращення стану роботи у захисті інтересів компанії від хакерських загроз. Значимість отриманих результатів полягає у дослідженні та виявленні можливих шляхів впровадження та поширення стандартів кібербезпеки на морському транспорті для реалізації вимог Міжнародної морської організації. Таким чином, проведені дослідження засвідчили необхідність активізації зусиль всіх зацікавлених сторін у прискоренні застосування всього запропонованого комплексу стандартів кібербезпеки на морському транспорті.

Ключові слова: *стандарти кібербезпеки, морський транспорт, кіберзахист, судно, загроза, інформаційна безпека*

Постановка проблеми. У будь-якій розвиненій країні світу транспорт відноситься до найважливіших сфер економіки. Стрімкий розвиток інформаційних технологій в останні десятиріччя вивів зв'язок, або як тепер кажуть, інформаційно-комунікаційну складову, на транспорті на перші ряди.

Зростання ролі інфо-комунікаційної складової пояснюється тим, що дане середовище галузі морського та річкового транспорту виконує важливі функції взаємодії з іншими

секторами економіки, а саме скорочення затримок при транспортуванні вантажів, обробці морських та річкових суден, контейнерів, залізничних вагонів і вантажів на основі використання електронних накладних, систем клієнт-банк, e-business, систем GSM-R, VSAT, взаємодії із клієнтурою й партнерами тощо.

Однак широке розповсюдження сучасних інформаційних технологій (ІТ), особливо в мобільному, розподіленому і бездротовому сегменті, значно підвищує ризик виникнення специфічних загроз для інформаційної безпеки. Про це наочно свідчить лавиноподібне зростання кількості виявлених уразливостей в інформаційних системах морської галузі та, відповідно, збільшення інцидентів, пов’язаних із захистом інформації на суднах, у портах, компаніях, організаціях та ін.

Для протидії кібер-злочинцям окреслимо проблеми, що стосуються захисту інформаційно-комунікаційного середовища морської галузі України.

1. Не розроблені єдині підходи щодо створення захищеного інфо-комунікаційного середовища морської галузі, адаптованого до функціонування у жорстких умов експлуатації.
2. Недостатньо повно розроблені способи і методи до забезпечення схоронності інформації і резервування критичних даних галузі.
3. Не створена методологія оцінки якості функціонування системи захисту інформації (СЗІ) за причини не достатньо повного дослідження дій кібер-злочинців.
4. Неповно врахований вплив засобів і методів захисту інформації на характеристики інформаційних систем морського та річкового транспорту.
5. Не виконана формалізація задач щодо визначення складу і методів захисту інформації, що протистоятимуть сучасним викликам.
6. Недостатнє врахування в існуючих системах захисту інформації появи нових інформаційних загроз. Відповідно, запізнюється проведення необхідних досліджень, розробка раціональних способів протидії і нейтралізації наслідків,

Отже, забезпечення високих стандартів інформаційної безпеки на морському транспорті в умовах реалізації "Керівництва з кібербезпеки на борту суден" є актуальним дослідженням, спрямованим на вирішення проблем захисту інформації на об’єктах критичної інфраструктури держави.

Аналіз останніх досліджень і публікацій. Тема морської кібербезпеки не сходить з рубрик іноземних тематичних інформаційних ресурсів [1-3]. Частина з них присвячена випуску різних міжнародних і національних рекомендацій з кібербезпеки в найпотужніших морських державах світу – США, Великій Британії, Євросоюзі, Данії, Норвегії, Сінгапурі тощо. Так, у 2020 р. порти США створили некомерційний центр кібербезпеки, а у сенат США був внесений законопроект про посилення морської кібербезпеки. Міністерство внутрішньої безпеки США у 2015 р опубліковано "Посібник із впровадження системи кібербезпеки у транспортному секторі", Лондонський Інженерно-технологічного інституту за підтримки Мінтрансу Великої Британії та Міноборони Великої Британії у 2016 р. – посібник "Кібербезпека портів і портових систем" і у 2017 р. "Звід правил кібербезпеки для суден". Провідні судноплавні компаніями світу розробили, а Міжнародна морська організація у 2017 р. рекомендувала "Керівництво з кібербезпеки на борту суден". Характерною особливістю цих документів є їх масштабність, які містять загальні положення щодо організації кібербезпеки у портах, портових системах, на суднах або всіх членів ІМО, або окремих потужних морських держав. Їх рекомендації є не завжди доречними для таких невеликих з точки зору морської економіки держав як Україна.

У статті [4] розглянуто систему технічного обслуговування обладнання ММС (Machinery Maintenance Connect), фактори які впливають на ключову компетентність, у т. ч ризики загрози кібератаки на застосовувані інформаційні технології (ІТ), можливість впровадження сучасних технологій для кібер-безпеки і безпечного ведення бізнесу компанії, постійний захист критично важливих об’єктів інфраструктури, ІТ, взаємозалежність конкретної системи АІ безпеки при взаємодії ергатичної системи і системи машина-машина (Machine-to-Machine, M2M). Але розглянуті питання стосуються лише однієї сфери експлуатації морського

транспорту – технічного обслуговування.

У роботах [5-7] акцент зроблено на подальшому розвитку методів захисту інфокомунікаційних систем та забезпечення інформаційної безпеки у транспортній галузі в умовах створення державної єдиної інтегрованої інформаційної системи. У роботах не досліджено специфіку інформаційної безпеки на морських суднах як об’єктах критичної інфраструктури держави.

Мета дослідження. Дослідження можливих шляхів впровадження та поширення стандартів кібербезпеки на морському транспорті для реалізації вимог Міжнародної морської організації.

Основні результати дослідження. На теперішній час до складу Міжнародної морської організації (ІМО) входить 174 держави-члена і 3 асоційовані члени (Фарерські острови, Гонконг, Макао) [8]. Вищим органом організації є Асамблея держав-членів. У рамках ІМО функціонують секретаріат на чолі з Генеральним секретарем та 5 комітетів:

1. Комітет з безпеки на морі (Maritime Safety Committee, MSC – КБМ);
2. Комітет із захисту морського середовища (Marine Environment Protection Committee, MEPC – КЗМС);
3. Юридичний комітет (LEG – ЮРКОМ);
4. Комітет з технічного співробітництва (КТС);
5. Комітет з полегшення формальностей судноплавства (FAL).

Комітети з безпеки на морі і захисту морського середовища у своєму складі мають ще 9 підкомітетів.

Підкомітети готують для розгляду на сесіях комітетів документи, які ухвалюються, як правило, на чергових сесіях Асамблеї Організації. Але ІМО може організовувати Дипломатичні Конференції для ухвалення стратегічних рішень, що стосуються безпеки на морі, захисту довкілля та вирішення юридичних питань, пов'язаних із міжнародним судноплавством.

Так, Комітет з безпеки на морі ІМО у червні 2017 р. ухвалив резолюцію MSC.428(98) – Управління морськими кіберризиками в системах управління безпекою [9]. У зв’язку з масовим застосуванням засобів автоматизації на морському транспорті та зростаючими при цьому викликами ІМО звертає увагу на необхідність впровадження та поширення заходів кібербезпеки на морському транспорті. Після 1 січня 2021 р. Комітет закликає адміністрації забезпечити врахування кіберризиків у системах управління безпекою суден.

Рекомендації Міжнародної морської організації щодо регулювання морської кібербезпеки в іноземних державах зазвичай здійснюється шляхом її доповнення національними вимогами та рекомендаціями.

Водночас певні об’єднання та організації також не залишаються осторонь. З 2018 р. оцінка кібербезпеки є обов'язковою частиною комерційних контрактів у Міжнародному морському форумі нафтових компаній (OCIMF). А класифікаційне товариство DNV GL з 2017 р. надає послугу із затвердження типу кібербезпеки судна, а з 2018 р. – розробило позначення класу кібербезпеки, пов'язаного з рівнем охорони.

У теперішній час кожен моряк користується всесвітньою мобільним зв’язком, мережею інтернет та іншими інформаційними технологіями. Але разом з перевагами сучасного інформаційного життя все частіше приходиться стикатися з проблемами кібербезпеки. Тому у 2015 р. були та внесені певні зміни у Закон України «Про основи національної безпеки України».

Але проблема кібербезпеки на морському транспорті є дуже серйозною і викликана відсутністю спеціалістів у сфері кіберзахисту на борту судна. Тому це питання потребує ретельного дослідження та забезпечення належного рівня захисту від кібератак об’єктів морського транспорту.

Засоби масової інформації систематично описують про успішно проведені по всьому світові комп’ютерні напади на різні об’єкти морської транспортної інфраструктури: 2017 р. – зараження вірусом NotPetya 17 із 76 вантажних терміналів компанії Maersk; 2018 р. – кібератаки на порти Барселони і Сан-Дієго; 2020 р. кібератаки на термінал Шахід Раджаї

(Іран), на логістичну група компаній Toll Group (Австралія), на судноплавну контейнерну компанію Mediterranean Shipping, на робочі станції і сервери компанії Anglo-Eastern. Збитки від кібератак у морській галузі, як вважають фахівці Лондонського Ллойда, складають астрономічну суму у 200 млрд доларів. І порівняно невеликий відсоток компаній мають план забезпечення безперервності діяльності при виникненні кібернетичного нападу на них.

Останнім часом кібератаки є частиною загального злочину, а зловмисники намагаються взяти під контроль командні, контрольні та експлуатаційні мережі та системи суден. У такому разі захоплене у результаті кібервпливу судно як морський об’єкт саме по собі становить загрозу для портового об'єкта.

Морська інформаційна безпека в Україні лише починає розвиватися. Публікації з даної теми практично відсутні, обізнаність є дуже низькою, якихось дій Україна як адміністрація прапора, на жаль, не проводила. Спеціальне нормативне правове регулювання морської інформаційної безпеки державою не здійснюється, а у доктринальних документах ці питання відсутні.

Розроблена Національним інститутом стандартів і технологій США "Рамкова структура для поліпшення кібербезпеки критично важливої інфраструктури" рекомендована циркуляром ІМО. Низка інших важливих документів також розроблені в основному у США та декількох провідних морських країнах світу. І тому морська галузь України у питаннях морської кібербезпеки керуватиметься рекомендаціями державних структур США.

На жаль, Міністерство інфраструктури України не поспіває за стрімким життям, і нормативно-правове регулювання у сфері морської інформаційної безпеки проводить неефективно, спрямовуючи основні зусилля на організацію робіт з технічного регламенту інформаційної безпеки та захисту інформації.

До спеціального законодавства з протидії кіберзагрозам відноситься Закон України "Про основні засади забезпечення кібербезпеки України" (від 05.10.2017 №45) [10]. Однак цей Закон, визначаючи правові та організаційні основи забезпечення захисту національних інтересів України у кіберпросторі, напрями та принципи державної політики у сфері кібербезпеки, основні засади координації діяльності із забезпечення кібербезпеки, є універсальним і загальним для всіх галузей економіки та не враховує специфіку транспорту загалом і окремих видів транспорту, зокрема, морського.

Він, насамперед, націлений на захист значущих об'єктів критичної інформаційної інфраструктури: комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси або використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів і військових формувань; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб або у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу. Закон розглядає як об'єкти захисту саме мережі та системи, а не об'єкти, якими вони експлуатуються. Але міжнародний підхід націлений на захист саме судна або портового засобу, він відрізняється від вітчизняного підходу тим, що у нас підставою для захисту є значущість об'єктів критичної інформаційної інфраструктури, що захищаються. Незначущі об'єкти, на жаль, взагалі випадають із правового регулювання Закону. Міжнародні ж рекомендації поширюються на всі судна і портові засоби. Вимоги даного Закону не містять практичних керівництв і потребують адаптації для компетентного використання на конкретному судні або портовому засобі.

Як об'єкти кіберзахисту міжнародні документи виокремлюють ІТ-системи у взаємозв'язку і взаємодії. Вітчизняні підходи мають на меті захистити інформацію, що обробляється в АСУ, особливо в АСУ критично важливих об'єктів, потенційно небезпечних об'єктів, об'єктів, що становлять підвищену небезпеку. Будь-які галузеві особливості, що стосуються транспорту, зокрема, морського, відсутні.

Комп’ютеризація та всебічна автоматизація практично всіх сфер діяльності людей зачіпає і галузь торгівельного мореплавства, у тому числі і процес електронного документообігу, які застосовуються у міжнародній морській практиці. Торгівельне мореплавство характеризується

постійним обміном інформацією між вантажовідправником, вантажоотримувачем та адміністрацією судна з питань комерційної експлуатації судна, з одного боку; між судновласником або фрахтівником та адміністрацією судна з питань безпеки судноплавства, з другого; між адміністрацією судна та портовими, митними службами з питань контролю та оформлення вантажів та судна в порту прибуття, з третього; між моряком та його родиною, з четвертого.

Таке широко коло суб'єктів інформаційного процесу породжує багато загроз для суднових інформаційних ресурсів, а саме: несанкціонований доступ до каналів супутникового обміну інформацією між судном та офісом його керування; викривлення навігаційних GPS-даних, які отримуються судном; несанкціонований доступ до каналу оперативного керування судном.

Усі учасники інформаційного процесу обмінюються у тому числі конфіденційною інформацією, втручання в яку може стати причиною порушення роботи систем судна, що у подальшому може призвести до морської аварії; руху судна по хибній траєкторії; фінансових витрат через несанкціоноване розповсюдження комерційної або особистої інформації; неповноту, невірогідність або запізнення інформації щодо стану технічних параметрів обладнання, систем та механізмів судна. Насамперед, кіберзловмисники намагаються атакувати інформаційні ресурси навігаційно-інформаційних систем та систем оперативного морського зв'язку суден. Захист інформаційних ресурсів цих систем передбачає криптографічне кодування, різноманітні паролі, електронний цифровий підпис та ін. Так, Міжнародна гідрографічна організація (International Hydrographic Organization, IHO) для захисту офіційних векторних карт впровадила спеціальний стандарт S63 «IHO Data Protection Scheme».

У сучасному динамічному житті обробка паперових документів в основному породжує проблеми. Тому під час перевезення вантажів морем багато судноплавних компаній відповідно до Конвенції з полегшення міжнародного морського судноплавства широко застосовують системи електронного обміну інформацією: Electronic Date Exchange – EDI, Electronic Data Interchange for Administration, Commerce and Transport – EDIFACT та ін.).

Резолюція Асамблеї IMO про «Розвиток системи передачі повідомлень про лихо і безпеку на морі» (1979 р.) стала першим нормативним актом з організації обміну інформаційними повідомленнями на морі. Згідно з нею, для охорони людського життя на морі здійснювалося координоване використання різних елементів, включаючи радіозв'язок. Важливу роль для безпеки мореплавства і охорони людського життя на морі відіграють «Загальні принципи систем суднових повідомлень» (1983 р), які використовуються для збору інформації або обміну нею за допомогою радіоповідомлення. Ще у далекому 1990 р. Міжнародної морський комітет (ММК) схвалив Єдині правила для електронних коносаментів (Rules for Electronic Bills of Lading), які застосовуються тільки за згодою сторін, основу складає концепція «конфіденційного ключа», а не центрального реєстру. У 1996 р. був прийнятий Типовий закон ЮНСІТРАЛ про електронну торгівлю, а у 2001 р. – Типовий закон ЮНСІТРАЛ про електронні підписи. Відмічені акти стали основою не тільки міжнародних електронних проектів документообігу, а й профільного національного законодавства різних країн.

Безпека мореплавства і охорони людського життя на морі досягається застосуванням на суднах сучасних комп'ютерних засобів. Правило V/19 Міжнародної конвенції з безпеки життя на морі SOLAS-74 вимагає оснащення суден тоннажністю понад 300 тонн, які здійснюють міжнародні рейси, і всіх пасажирських суден незалежно від розміру Автоматичною Ідентифікаційною Системою (AIC). Резолюція IMO MSC.74(69), 1998 визначила основні функціональні вимоги щодо суднової AIC; технічні стандарти стосовно AIC розроблено в Рекомендації ITU-RM.1371,1998, а Керівництво з використання суднової AIC дається в Резолюції IMO 917(22), 2001.

Але й злочинний світ не стоїть на місці. Злодії активізували розробки програмно-технічних засобів для втручання у процеси обміну інформацією з(на) борту суден та шкідливого впливу на їх експлуатацію. Рівень загроз інформаційній безпеці торгівельного мореплавства з цього боку постійно зростає. Причому дані загрози мають транскордонний характер, що вимагає вироблення

і реалізації дієвих комплексних механізмів міжнародно-правової, організаційної та технічної протидії інформаційним загрозам.

Серйозною проблемою для комплексного підходу до морської кібербезпеки в Україні є створення єдиного понятійного апарату.

Прикладів, коли у нас відсутні однозначні синоніми до англомовних термінів, або вітчизняні терміни є подібними, але доволі неблизькими, є достатньо. Термінологічний дисбаланс веде до плутанини в юридичних і технічних документах, що зрештою не сприяє обізнаності морської галузі про кіберзагрози та відбивається на якості виконання рекомендацій щодо ефективного кіберзахисту на суднах і портових засобах.

Вже з 1 січня 2021 р. морські адміністрації деяких країн почали перевірки суден, що заходять в їхні порти, на предмет виконання рекомендацій IMO MSC.428(98) з кібербезпеки у системах управління безпекою суден. Однак далеко не всі судновласники й оператори українських суден знають, що і як робити. Невиконання рекомендації з кібербезпеки може стати причиною виникнення ризиків санкцій за невиконання рекомендацій IMO щодо кібербезпеки у суден під Державним прапором України в іноземних портах, відмови українському судну в комерційному контракті з боку фрахтувальника, зниження конкурентної спроможності українського флоту через високі тарифні ставки страхування морських вантажів у порівнянні з суднами, які виконують вказані рекомендації з кібербезпеки.

Рекомендації з кібербезпеки, що вже як 2 роки виконують свої функції у портах і на морі, стосуються не лише загроз з погляду кібербезпеки. На наш погляд, дивитися потрібно глибше та ширше. Ці рекомендації звісно даватимуть чіткий кібернетичний підхід до аналізу будь яких кіберінцидентів на інтерфейсі судно/порт. Ігнорування або не у повному обсязі або не з задовільною якістю виконані рекомендації можуть призвести до більш тяжких наслідків не тільки у конкретному українському порту або компанії. Наприклад, морські порти можуть визнаватися небезпечними з погляду кібербезпеки, що вплине на економічну привабливість портів і вартість перевезень з (в) них, та може стати приводом для санкцій щодо портів. Відповідно, суднам, які заходять у такі порти або побували в них, рекомендуватимуть підвищені заходи кібербезпеки.

У разі організації кібератак на суднові системи через інтерфейс судно/порт можливі серйозні фінансові претензії, які можуть багатократно перевищити вкладання у кіберзахист.

Морська кібербезпека не закінчується на тому, щоб вписати кілька рядків у наявну систему управління безпекою судна. Рекомендоване IMO "Керівництво з кібербезпеки на борту суден" визначає коло суб'єктів кібератак:

- активісти (включно з незадоволеними співробітниками);
- злочинці;
- опортуністи;
- держави;
- спонсоровані державою організації;
- терористи.

Система управління безпекою судна може дати ради проти першої категорії суб'єктів кібератак. Але захиститися від усіх інших категорій система у нинішньому вигляді не здатна. Система заходів має бути більш серйозною і комплексною. За кордоном вважається за необхідне рахувати оцінки кібербезпеки і план кібербезпеки окремими документами. А план кібербезпеки для судна пропонують зробити додатком до плану охорони судна. Крім того вважається, що посадова особа, яка відповідає за охорону, має охопити питання кібербезпеки.

Вжиття заходів щодо запобігання перерахованим вище ризикам у кінцевому випадку є кращим, ніж очікування кібератак або санкцій.

Сучасні судна потерпають не лише від проникнення зловмисників через інтерфейс судно/порт до навігаційно-інформаційної системи та системи оперативного морського зв’язку. У теперішній час на порядку денному стоїть вже і кіберзахист системи планового технічного обслуговування обладнання MPMS (Machinery Planned Maintenance System). Мова йде про запропоноване міжнародним сертифікаційним і класифікаційним товариством DNV GL (Det

Norske Veritas & Germanischer Lloyd) дистанційне оцінювання, консалтинг і менеджмент ризику.

Система організації та проведення технічного обслуговування змінилася докорінно за рахунок впровадження MMC (Machinery Maintenance Connect). Тепер всі дані про стан та поведінку суднових систем і устаткування повно й оперативно у дистанційному режимі надходять до зацікавлених споживачів. Потужні алгоритми навчання разом з масивом отриманих даних з суден дозволяють віддалено проводити технічне обслуговування як окремого судна, так і всього флоту, і отримувати нові відомості про них [4].

Агрегування даних за рік експлуатації, що надходять від окремих бортів до DNV GL, дозволяє після доступу до додатку MMC, який дається тільки після отримання і перевірки інформації у MPMS, побачити загальну картину по всіх суднах. Перевірені актуальні дані стають доступними для керівництва компанії у режимі реального часу.

За допомогою системи MMC нарешті виконане завдання щодо визначення часу проведення будь-якого технічного обслуговування і термінів виконання робіт. Позитивними особливостями цього процесу є робота з даними у режимі реального часу, що дозволяє врахувати потреби окремих суден при створенні плану технічного обслуговування, а також надати рекомендації щодо проведення повного обслуговування суден у найближчих місцях від їх знаходження. Крім того, прозорість інформації дозволяє вести постійне відстеження технічного обслуговування будь-якого судна і всього флоту всіма зацікавленими сторонами, бачити відстрочки виконання завдань та планувати заходи щодо їх подолання.

Розробники вчинили традиційно, розділивши панель управління MMC на дві частини: одна стосується вичерпної інформації про увесь флот судновласника, інша – інформації конкретного судна. У MMC детально описані вже завершені завдання з ТО; плани проведення майбутніх робіт; перелік робіт, які залишаються ще не розпочатими або ще невиконаними за якихось причин; останні терміни, що залишилися до виконання робіт; виведена докладна карта AIS розташування всіх суден з актуальними погодними умовами у цих районах.

Обсяг та якість видаваної інформації на панелі MMC дозволяє судновласникам ефективно контролювати режими технічного обслуговування на своїх суднах, заздалегідь планувати часи простою і технічного обслуговування конкретного судна, пропонувати у зв’язку з цими обставинами своїм партнерам перевезення вантажу іншим судном тощо.

Використання MMC дозволяє проводити ТО судна або всього флоту за запитами, здійснювати повне технічне порівняння до і після обслуговування, проводити розширену аналітику з видачею вичерпної інформації про суднове устаткування.

Досвід позитивного застосування MMC має знайти своє місце у нових сервісах DNV GL, наприклад у нових правилах класифікації суден за класом DNV GL. Їх доробка здійснюється шляхом інтегрування у програмне забезпечення DNV GL сучасних новітних технологій, що дозволило ввести еквівалент Equivalent Design Waves (EDW) для розрахунку навантаження на навколишнє середовище і точніше структурувати судно, здійснювати СПГ-бункерування суден, реалізувати понад 2000 коментарів по верфях, виробниках, судновласниках, державах прапора та ін.

Штучним інтелектом (Artificial Intelligence, AI) називаються «системи, які демонструють інтелектуальну поведінку, аналізуючи своє середовище і роблячи дії – з деяким ступенем автономії – для досягнення конкретних цілей» [1]. Впровадження систем AI у морську справу створює певні цифрові ризики і відкриває суттєві небезпеки при впровадженні цих технологій. DNV GL виклала, як перевіряти і забезпечувати безпеку систем AI при їх повній інтеграції в існуючі цифрові системи.

Довіра до AI має координуватися з довірою до цифрових систем взагалі та відповідати таким вимогам:

1) легітимність системи AI, яка визначається досконалістю застосовуваних алгоритмів AI й моделей управління, законністю і повнотою отриманих даних, можливістю, доцільністю і придатністю обраного алгоритму для вирішення певного завдання. Крім того, при застосуванні системних методів та інструментів AI необхідно встановити залишковий ризик системи AI,

прийнятний для всіх зацікавлених сторін, та способи управління тими ризиками;

2) чітко визначена і поставлена ціль до її виконання;

3) здатність виконувати і перевіряти поставлені делеговані завдання, дотримуючись встановлених принципів. Це досягається встановленням системи AI з певним рівнем компетентності, якості та надійності. Багато алгоритмів AI піддані хакерським атакам, що вимагає впровадження системи кібер-захисту, яка має довести свою ефективність шляхом постійної перевірки достовірності та законності рішень, вироблених AI;

4) взаємозалежність елементів систем ергатичної і M2M;

5) прозорість, доступність і її вплив на відповідні зацікавлені сторони.

Для забезпечення надійності при впровадженні промислової системи AI повинні бути повністю розкриті цілі, мотиви, можливі наслідки і ризики від такої діяльності. Для цього необхідно проведення ретельного аудиту морської компанії, що охоплюватиме окремі області функціонування системи AI, які вимагають незалежної експертизи з метою виявлення, яких збитків буде завдано компанії, якщо порушиться одна із вказаних вимог щодо інформаційних ресурсів самої компанії.

Основні цілі проведення аудиту у судноплавній компанії з AI безпеки:

– аналіз ризиків, пов'язаних з безпекою ресурсів інформаційної мережі IT (Information Technology);
– оцінка поточного рівня захищеності всіх інформаційних ресурсів;
– виявлення та локалізація потенційно небезпечних місць у системі захисту компанії;
– оцінка відповідності системи AI до існуючих стандартів безпеки;
– вироблення рекомендацій щодо підвищення рівня ефективності існуючих механізмів кіберзахисту.

Розвиток інтелектуальних IT вимагає прискорених темпів впровадження заходів кібербезпеки. Відставання у впровадженні своєчасних змін у кіберзахисті роблять буді-які організації вразливішими для кіберзлочинців. Тому, ретельний аналіз організаційних ризиків і неупереджена оцінка вузьких місць у системі кіберзахисту судноплавної компанії допоможуть захистити її від хакерських загроз.

Висновки.

1. Необхідно чітко визначити зміст та класифікацію загроз інформаційній безпеці мореплавства. Таке дослідження дозволить на законодавчому рівні розмежувати різні види загроз інформаційної безпеці мореплавства та вдосконалити механізм державної протидії цим викликам.

2. Комплексне вирішення проблем кібербезпеки на морському транспорті значною мірою залежить від наявності підготовлених, а не паперових спеціалістів у сфері кіберзахисту на борту судна.

3. Невиконання рекомендації з кібербезпеки може значно знизити конкурентоспроможність портів та суден нашої держави порівняно з суднами та портами, які виконують вказані рекомендовані заходи.

4. Можливе проведення кібератак на суднові системи через інтерфейс потребують проведення ретельного аудиту сфери кіберзахисту у судноплавній компанії та портах щодо забезпечення безпеки. Тому потрібно кропітка робота про створення адаптованих до морських реалій заходів з кібербезпеки.

ЛІТЕРАТУРА

1. Analysis of cyber security aspects in the maritime sector. *ENISA* (10.2011). P. 31.

2. AIS Exposed: Understanding Vulnerabilities & Attacks 2.0 (4. video), Dr. M. Balduzzi, Black Hat Asia. (2014).

3. Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, Yevgen Dyryavyy, NCC Group. (03.03.2014).

4. Слюсаренко А. Впровадження та вплив кібер-безпеки на сучасне технічне обслуговування обладнання суден і судноплавних компаній. *ЛОГОΣ. ОНЛАЙН*. 2020. № 10.

DOI: 10.36074/2663-4139.10.09.

5. Лахно В.А. Інформаційна безпека інтелектуальних транспортних систем. *Захист інформації.* 2015. Том 17. No 4. С. 298-305.

6. Лахно В.А. Кібербезпека комп'ютерних систем транспорту. *Електротехнічні та комп'ютерні системи.* 2016. No 21 (97). С. 76-80.

7. Лахно В.А. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту. *Безпека інформації.* 2016. Том 22. No 1. С. 44-50.

8. Міжнародний кодекс з охорони суден і портових засобів. URL: https://ips.ligazakon.net/document/MU02257 (дата звернення 18.04.2023).

9. Resolution MSC.428 (98) (adopted on 16 June 2017) Maritime Cyber Risk Management in Safety Management Systems.

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov. ua /laws/show/2163-19#Text (дата звернення: 02.05.2023).

REFERENCES

1. (2011). Analysis of cyber security aspects in the maritime sector. *ENISA* P. 31.

2. (2014). AIS Exposed: Understanding Vulnerabilities & Attacks 2.0 (4. video), Dr. M. Balduzzi, Black Hat Asia.

3. Yevgen, Dyryavyy (2014). Preparing for Cyber Battleships – Electronic Chart Display and Information System Security. *NCC Group.*

4. Sliusarenko, A. (2020). Vprovadzhennia ta vplyv kiber-bezpeky na suchasne tekhnichne obsluhovuvannia obladnannia suden i sudnoplavnykh kompanii[Implementation and impact of cyber security on modern maintenance of equipment of ships and shipping companies]. *ΛΟΗΟΣ. ONLAIN.* № 10.

5. Lakhno, V.A. (2015). Informatsiina bezpeka intelektualnykh transportnykh system[Information security of intelligent transport systems]. *Zakhyst informatsii*, 17(4), P. 298-305.

6. Lakhno, V.A. (2016). Kiberbezpeka kompiuternykh system transportu[Cyber security of transport computer systems]. *Elektrotekhnichni ta kompiuterni systemy,* 21 (97), P. 76-80.

7. Lakhno, V.A. (2016) Pidvyshchennia kiberbezpeky informatsiino-komunikatsiinykh system transportu[Increasing the cyber security of information and communication systems of transport]. *Bezpeka informatsii*, 22(1), P. 44-50.

8. Mizhnarodnyi kodeks z okhorony suden i portovykh zasobiv[International Code for the Protection of Ships and Port Facilities]. Retrieved from https://ips.ligazakon.net/document/MU02257.

9. Resolution MSC.428 (98) (adopted on 16 June 2017) Maritime Cyber Risk Management in Safety Management Systems.

10. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the main principles of ensuring cyber security of Ukraine]: Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII : stanom na 17 serp. 2022. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Trofymenko A.O., Maidanevych S.B., Voichenko T.O., Dorofieieva Z.Ia.

SOME PROBLEMATIC ISSUES OF IMPLEMENTING CYBERSECURITY STANDARDS IN MARITIME TRANSPORT

The purpose of the study is to investigate possible ways to implement and disseminate cybersecurity standards in maritime transport to meet the requirements of the International Maritime Organization. This goal is achieved by analysing the content of Resolution MSC.428(98) - Maritime Cyber Risk Management in Security Management Systems with a view to disseminating cybersecurity

measures in maritime transport. The role of the Ministry of Infrastructure of Ukraine in regulatory and legal regulation in the field of maritime information security is determined. The insufficient effectiveness of the Ministry in formulating specific steps for information security and information protection, which relate to the specifics of organizing these activities in the field of maritime transport and cargo transportation, port operations, and on individual ships is proven. The content of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" was analysed. It is established that the requirements of this Law need to be adapted for competent use on a particular ship or port facility. The main threats to shipboard information resources: unauthorized access to satellite information exchange channels between the ship and its control office; distortion of GPS navigation data received by the ship; unauthorized access to the satellite channel for operational control of the ship are outlined. Measures to prevent cyber risks of intruders penetrating the ship/port interface into the navigation information system, maritime operational communication system, and scheduled equipment maintenance system were identified The goals, motives, possible consequences, and risks of introducing industrial artificial intelligence systems into the operation of ships, ports, and shipping companies were revealed, and the need for a thorough audit of a shipping company covering certain areas of the artificial intelligence system was identified. The most significant results are a thorough analysis of organizational risks and an unbiased assessment of bottlenecks in the shipping company's cybersecurity system and proposals for improving the state of work in protecting the company's interests from hacker threats. The significance of the results obtained lies in the study and identification of possible ways to implement and disseminate cybersecurity standards in maritime transport to meet the requirements of the International Maritime Organization. Thus, the studies conducted have shown the need to intensify the efforts of all stakeholders to accelerate the application of the entire proposed set of cybersecurity standards in maritime transport.

***Keywords**: cybersecurity standards, maritime transport, cyber defense, ship, threat, information security*