International Science Journal of Engineering & Agriculture
2024; 3(4): 115-129
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20240304.12
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Розходження морських суден при кібернетичних атаках в рейсовому циклі

Дмитро Шумілов
Національний університет «Одеська морська академія», Навчально-науковий інститут навігації, Одеса, Україна
ORCID 0009-0009-6242-8620

Для цитування цієї статті:
Шумілов Дмитро. Розходження морських суден при кібернетичних атаках в рейсовому циклі. International Science Journal of Engineering & Agriculture. Vol. 3, No. 4, 2024, pp. 115-129. doi: 10.46299/j.isjea.20240304.12.
Надійшла до редакції: 19 червня 2024 р.; **Схвалено:** 23 липня 2024 р.;
Опубліковано: 31 серпня 2024 р.

Анотація: У процесі розвитку сучасного судноплавства, окрім навігаційних ризиків, додатково виникли й кібернетичні. Вони пов'язані з широким впровадженням комп'ютерних технологій та використанням безкабельних ліній зв'язку між приладами на суднах та при зовнішньому радіозв'язку. Крім того принцип роботи використовуваних приладів засновано на передачі і прийомі радіохвиль, що призводить до вразливості при кібернетичних атаках, яку не було враховано при проектуванні такого обладнання. Тому необхідно розробити рекомендації для судноводіїв по способам штурманської роботи при виникненні загроз кібернетичних атак для управління маневруванням судна при розходженні. Методи: використано сучасні способи рішення задачі розходження суден в звичайних умовах. Враховано закономірності маневру останнього моменту, методу каталогу і контролю небезпеки зіткнення за характером зміни відносного напрямку небезпечного судна. Результати: показано, що не існує способів рішення задачі розходження при відсутності приладів для вимірювання відстані до зустрічного судна в умовах кібернетичних атак. Тому запропоновано розділити стадію зближення на три етапи: надмірне; небезпечне; аварійне. Оцінку небезпеки зіткнення і вибір маневру для розходження пропонується виконувати за розташуванням цілі відносно діаметральної площини – справа/зліва, характером зміни лінії відносного напрямку за годинниковою чи проти годинникової стрілки і тенденцією наближення – віддаляється чи наближається. Обговорення: аналіз небезпеки зіткнення за розташуванням цілі – справа/зліва, за характером зміни відносного напрямку – постійний чи змінюється, за визначенням напрямку повороту лінії руху – від нас чи до нас, за каталогом – в табличній формі дозволяє вибрати ефективний маневр, який буде повертати лінію відносного руху від нас.

Ключові слова: кібератака; розходження суден; метод каталогу маневрів; кібернетичні ризики; ефективний маневр.

1. Вступ

Стрімке впровадження сучасних інформаційних технологій в суднові навігаційні системи викликало появу нових видів ризиків – кібернетичних. Причиною їх появи стало незахищене і застаріле програмне забезпечення, а також несанкціоноване підключення кіберзлочинцями до мережі суднових навігаційних систем, з метою виведення із ладу тих, які використовують прийом або передачу інформації за допомогою радіохвиль. Сучасні кіберзлочини здійснюються з метою впровадження шкідливих вірусів в програмне забезпечення суднового

інформаційно-навігаційного обладнання, викрадення критично важливих даних, створення суден-примар, проведення терористичних дій та ін. Тому суднові інформаційно-навігаційні системи стають вкрай вразливими перед спланованою кібератакою.

Серед морських операцій, якими управляє судноводій при переході морем, однією з найбільш поширених і небезпечних є маневрування при розходженні суден. Дії судноводія при цьому регламентуються правилами запобігання зіткненню суден у морі (МПЗЗС-72/2016). При роботі навігаційних приладів ходового містка в штатному режимі виконання рекомендацій МПЗЗС-72/2016 не представляє труднощів для судноводія. Отже, безпечне розходження буде визначатися тільки його відповідною кваліфікацією.

В рейсовому циклі судна завжди існують два види ризиків: навігаційні та кібернетичні. Для ідентифікації навігаційних ризиків необхідно заздалегідь виявляти аварійно-небезпечні ділянки переходу. Такий процес здійснюється під час планування рейсового циклу за навігаційними посібниками – картами, лоціями та іншими інформаційними джерелами.

Стрімка інтеграція в судноплавні процеси комп'ютерних технологій, поширення мереж 5G, впровадження складних технічних систем, використання безкабельних ліній зв'язку для передачі інформації між суднами обумовило виникнення кібернетичних ризиків.

В зв'язку з переходом суден всього світу з 2018 року на електронні навігаційні карти і широким використанням автоматизованих інформаційних систем (АІС), можливості для впливів зовнішнього середовища на роботу суднових систем значно розширились.

Принцип роботи використовуваних навігаційних приладів ходового містка і машино-котельного відділення засновано на передачі і прийомі інформації за допомогою радіохвиль, що призводить до їх вразливості при здійсненні кібернетичних атак. Зауважимо, що такі ризики не були враховані при проектуванні суднового обладнання. Тому міжнародні кіберзлочинці, а навіть і деякі держави можуть організовувати направлені перешкоди у вигляді кібернетичних атак, з метою виводу з ладу суднових навігаційних приладів. Це призводить до виникнення аварійних випадків і значних фінансових збитків для суден і судноплавних компаній. За цією причиною судноводій повинен ретельно планувати навігаційний план переходу в рейсовому циклі, включаючи пошук аварійно небезпечних відрізків шляху та ймовірність виникнення навігаційних і кібернетичних ризиків. На підставі такого аналізу необхідно визначити наявність резервних навігаційних приладів і використати способи безпечної штурманської навігаційної роботи, які дозволять забезпечити наступне: 1) нормативну точність визначення місця судна; 2) рішення задачі розходження; 3) контроль навігаційних параметрів зовнішнього середовища за шляхом переходу. Тому, для управління маневруванням судна при розходженні в складних умовах плавання, необхідні рекомендації щодо способів штурманської роботи для судноводіїв, які враховують навігаційні ризики та визначають вірогідність появи кібератак. Такі рекомендації є критично важливими для управління маневруванням судна при розходженні в складних умовах плавання.

2. Об'єкт і предмет дослідження

Проблема визначення кібернетичних ризиків є наразі дуже актуальною, оскільки відсутні систематизовані дані щодо кібернетично небезпечних районів плавання. Найбільш ймовірною загрозою у разі здійснення кібератак є акваторії, в яких існують навігаційні ризики, оскільки в них є багато передумов для виникнення аварії. За цією причиною необхідно ввести в процес підготовки до переходу окремо виділений етап, такий як «аналіз і оцінка навігаційних і кібернетичних ризиків», який необхідно виконувати після завершення планування координат переходу. Виконання такого етапу дозволить підготувати судно та екіпаж до плавання в аварійно небезпечних районах, для управління в складних навігаційних умовах при появі кібернетичних ризиків.

Наступною проблемою при підготовці до розходження в умовах кібернетичних атак являється підготовка резервних приладів для визначення напрямку на зустрічні судна,

включаючи наявність пеленгатора у головного магнітного компаса на верхньому навігаційному містку і таблиці девіації для нього.

Підготовка судна до переходу закладається у визначенні часу доби при проходженні аварійно небезпечних районів, наявності берегових орієнтирів для визначення місця судна, плавучих знаків навігаційного забезпечення та очікуваного стану видимості горизонту.

Після виконання вищезазначених процесів, планування появи аварійно-небезпечних районів навігаційних та кібернетичних ризиків, з метою технічної підготовки судна та його екіпажу до розходження в умовах кібернетичних атак, можна стверджувати, що судно буде підготовлено до плавання в умовах ризиків. Тому розглянуті проблеми є особливо актуальними і прийнятими для подальшого дослідження.

3. Мета і задачі дослідження

Метою дослідження є рішення задачі розходження суден під впливом кібернетичних атак, при обсерваційному зчисленні під час аварійного управління маневруванням судна в рейсовому циклі.

Для досягнення поставленої мети необхідно вирішити такі основні задачі:

- визначити перелік даних, які необхідні для рішення задачі розходження суден;
- резервні прилади для отримання даних;
- способи використання даних для вибору безпечного виду маневру для розходження.

При кібернетичних атаках навігаційні прилади ходового містка виходять із ладу, тому немає можливості для вимірювання напрямку і відстані до інших суден при будь-яких умовах видимості. Зрозуміло, що при обмеженій видимості окомірне спостереження використовувати неможливо, тому в такому випадку судноводій вимушений здійснити постановку судна на якір до покращання видимості або до приведення в робочий стан навігаційних приладів.

Для визначення напрямку з резервних приладів можна використовувати магнітний компас, але він повинен мати пеленгатор і таблицю девіації. Резервних приладів для визначення дистанції на судні немає. Використання секстанту для розрахунку дистанції можливо тільки при хорошій видимості і потребує наявності додаткових даних про судна, дистанцію до яких вимірюють.

4. Аналіз літературних джерел

Управління кібернетичними ризиками в судноплавстві базується на процесі виявлення, аналізу та оцінки впливу кіберзагроз, а також прийняття рішення щодо запобігання або пом'якшення їх до прийнятного рівня [1]. Пріоритетність питань кібербезпеки в морській галузі, яку розглянуто в джерелі [2] не враховує принципи роботи суднових інформаційно-навігаційних приладів під впливом кібератак. Проте, в статті вказано на найбільш вразливі об'єкти при здійсненні кібернетичної атаки, а саме навігаційні системи, портову інфраструктуру, бортові системи автоматизації руху судна та ін. Також зазначено про необхідність внесення змін з цього питання в Систему управління безпекою судна (СУБ). Згідно з опитуванням компанії NSSL Global [3], 84% членів екіпажів зовсім не проходили навчання з кібербезпеки та отримували лише поверхневі знання з цього питання. Також зазначено, що близько 64% опитуваних моряків беруть на себе відповідальність за безпеку інформаційно-навігаційних систем на борту судна.

Існуючі методи моделювання загроз та оцінки ризиків з питань кібербезпеки суден досліджено в роботі [4], в якій проаналізовано 25 наукових статей для розуміння мінливого ландшафту практик кібербезпеки для пілотованих і автономних суден. Підкреслено існування нагальної потреби в стандартизованому моделюванні загроз і системах оцінки ризиків. Але не розглянуто питання безпечного розходження суден під впливом кібератак, яке б могло значно підвищити стійкість морських систем до кіберзагроз.

В документі [5] проаналізовано 1181 джерело, яке висвітлює ризики, пов'язані з морським транспортом за двадцятирічний період (2000-2021 роки) та проведено спеціальний аналіз методів оцінки ризику, у відповідності до загального процесу оцінки ризику. Але в статті не розглянуто ефективні способи оцінки кіберзагроз для розходження морських суден при кібернетичних атаках в рейсовому циклі.

Контроль руху судна, який покладається на пристрій автоматичної системи ідентифікації (АІС) досліджено в джерелі [6]. Зазначено, що судна використовують розширені кібер-можливості, щоб фальсифікувати дані, які передає AIS та видавати себе за інше судно для здійснення незаконної діяльності. Значний аналіз для пошуку неправдивих звітів АІС полягає в пошуку звітів про місцезнаходження. Оскільки кожен пристрій АІС використовує трансивер на основі SOTDMA (Self-Organising Time Division Multiple Accsess, самоорганізований множинний доступ з тимчасовим поділом), він визначає свій розклад передачі (інтервал) на основі історії трафіку каналу передачі даних та інформації про можливі дії інших станцій. Протокол SOTDMA був розроблений наприкінці 1990-х років і не має вбудованих функцій безпеки. Це робить комунікаційні мережі судна вразливими до кіберзагроз. В такому випадку можливо прослуховування, підробка даних, несанкціонований доступ і здійснення кібератаки на інформаційно-навігаційні системи судна. Цей протокол широко використовується в системах бездротового зв'язку. Зауважимо, що жоден центральний орган не керує зв'язком між вузлами та динамічно пристосовується до змін у топології мережі, і вузли можуть з'являтися та зникати в будь-який час.

Проблеми кібербезпеки в протоколі АІС, який використовується на суднах, вказують на те, що більшість з цих викликів пов'язані з різними сферами використання протоколів SOTDMA, такими як бездротові датчики (WSN, Wireless sensor networks), мобільні пристрої (MANET, Mobile Ad hoc Network, бездротова та децентралізована мобільна IP-мережа), мережі надання допомоги при стихійних лихах, системи моніторингу охорони здоров'я, системи промислової автоматизації, мережі зв'язку між транспортними засобами (V2V, Vehicle 2 Vehicle), бездротові мережі тощо [6].

У документі [7] досліджується нова загроза, яка використовує АІС для встановлення прихованих каналів і передачі невеликих файлів для оновлення кібер-арсеналу без доступу до Інтернету. Крім того, встановлення та використання прихованих каналів виявилося можливим за допомогою існуючих різновидів кібератак і технологій, пов'язаних із широким спектром морських систем. Проте, розглянуті питання спрямовані лише на збільшення мотивування морського співтовариства щодо посилення зусиль для інтеграції методів кібербезпеки в інформаційно-навігаційні системи судна.

Один з методів, який описується в джерелі [8], засновано на використанні інструменту оцінки ризиків для ідентифікації та визначення пріоритетів кіберзагроз. Недоліком більшості існуючих морських систем оцінки кіберризиків є нездатність динамічно оновлювати ризики в міру зміни зовнішнього середовища. Зрозуміло, що на морські операційні ризики можуть впливати як кібернетичні і кіберфізичні фактори, так і фізичні за своєю природою. У цій статті не розглянуто практичні проблеми при управлінні маневруванням судна під впливом факторів ризику, пов'язаних з кібернетичною діяльністю. Але в роботі проведено оцінку існуючих систем аналізу ризиків і запропоновано вдосконалення, які могли б тільки оцінити морські кіберризики. Більшість наукових досліджень мають узагальнений характер і не розглядають завдання розходження суден під впливом кібератак для виконання безпечного маневрування в рейсовому циклі і запобігання зіткненню у морі.

Розслідування загроз, інцидентів і ризиків у контексті автономного та стійкого судноплавства розглянуто в джерелі [9]. Але воно не охоплює розходження морських суден при кібернетичних атаках, а висвітлює лише спектр можливих дій для запобігання та пом'якшення небажаних подій та підвищення стійкості і гнучкості судноплавства.

Оцінка стійкості кіберфізичних систем живлення під час багатоетапних кібератак досліджена в роботі [10]. Вона заснована на реалістичних фізичних та кібер-моделях на основі

ймовірнісного правила відключення ліній GPS (Global Positioning System, система глобального позиціонування) та покращеного підходу до кіберпотоку для відновлення ефективності мережі після збою.

Результати аналізу вищевказаних сучасних наукових джерел показали, що найбільший ризик становить підробка AIC. Також перешкоди функціонуванню глобальної навігаційної системи супутникового зв'язку GPS є ще однією значною загрозою для навігаційних систем ходового містка під час впливу кібератак.

Всі ці дані наочно демонструють актуальність створення способів організації кібернетичного захисту в морському секторі. Тому проблема пошуку способів рішення задачі розходження суден під впливом сучасних кіберризиків є критично важливою і актуальною для міжнародного морського судноплавства.

5. Методи дослідження

Порядок рішення задачі розходження в штатному режимі системи управління маневруванням в рейсовому циклі розглянуто в роботі [11]. За момент початку виконання завдання розходження приймається судновий час зняття першого відліку пеленга і відстані зустрічного судна, які приймають за «нуль». Якщо використовується секундомір, то його запускають в цей момент. За момент закінчення процесу розходження приймається час, коли власне судно повернулося до первинних параметрів руху.

Для вибору маневру розходження використано метод закону маневру останнього моменту, маневрений планшет, ситуаційний планшет, закономірності відносного руху лінії зближення і каталог вибору маневрів для розходження.

В процесі рішення задачі вибрано ефективний маневр для розходження. Ефективним називається такий маневр, який призначений не тільки для вирішення задачі розходження, але й для того, щоб показати дії власного судна для суден, які спостерігають за навколишньою обстановкою (тільки з використанням радіолокатора в умовах нормальної та обмеженої видимості). У разі вибору маневру відвороту, ефективним слід вважати кут не менше 30-45º, а якщо вибрано маневр зменшення швидкості, то не менше, ніж наполовину. Отже, нижньою межею повинна бути швидкість втрати керованості. Крім того, необхідно зазначити, що під час маневрування і розходження параметри руху вибирають з запасом, використовуючи параметри кутів перекладки руля (до 15^0) та режими роботи головного двигуна (до середнього ходу).

6. Результати досліджень

В процесі наближення зустрічного небезпечного судна власне судно проходить три етапи наближення: надмірне; небезпечне; аварійне. Послідовність їх настання визначається відстанню до зустрічного судна, маневреними характеристиками власного судна та відносним курсом.

Надмірне наближення характерно тим, що в розпорядженні судноводія є три максимально можливих управляючих впливів на судно: «задній повний», «право на борт» та «ліво на борт». При небезпечному зближенні число альтернатив скорочується до двох, а при аварійному – залишається тільки одна можливість попередити зіткнення маневром, який визначається законом «маневру останнього моменту» [12].

Головна психологічна сутність і специфіка таких дій полягає в тому, що через відсутність достатнього часу, необхідного для вирішення завдання з вибору маневру для управління судном при аварійному зближенні судноводій, який діє в системі «людина-машина», приймає помилкове рішення [13].

Розглянемо приклад аварійної події при виконанні маневру для розходження двох суден в умовах обмеженої видимості, відстані та часу і при аварійному зближенні. Через бездіяльність

або втрату часу для оцінки обстановки капітан, щоб попередити аварію, зобов'язаний був давати команду на розворот в сторону судна, що рухається назустріч. Капітани т/х «Адмірал Нахімов» (1986 р.) і китайського балкера «Яо Хай» (2012 р.) здійснили розворот від судна, що призвело до зіткнення під кутом 90^0 [13] і загибелі українських суден «Адмірал Нахімов» і «Нафтогаз – 67».

Вищевказаний метод «маневру останнього моменту» може бути використаний при кібернетичних атаках на підставі окомірного визначення дистанції до зустрічного судна. Маневрений планшет дозволяє виконувати графічне вирішення задачі вибору виду маневру на підставі даних радіолокатора, які документують сам факт вибору виду маневру судноводієм [13, 14] у вигляді табл. 1.

Таблиця 1. Таблиця обробки радіолокаційної інформації

Судно А – Перетинає курс по носу ліворуч. Маневр: … 12-а хвилина: зміна курсу вправо 55º, $D_{зад}$ = 1,0 милі, ... 19-а хвилина: початковий режим руху								
Час, хв	*ІК*	$V_н$	$П^0$,	*D*, милі	$П^0$	*D*, милі	$П^0$	*D*, милі
0	355 °	15	45	9,1				
6	355 °	15	43	7,2				

На підставі таблиці 1 з центру планшету проводять вектор швидкості власного судна $V_н$ і круг радіуса $D_{зад}$ та наносять пеленг і відстань на 0’ та 6’ хвилинах судна А, як показано на рис. 1.

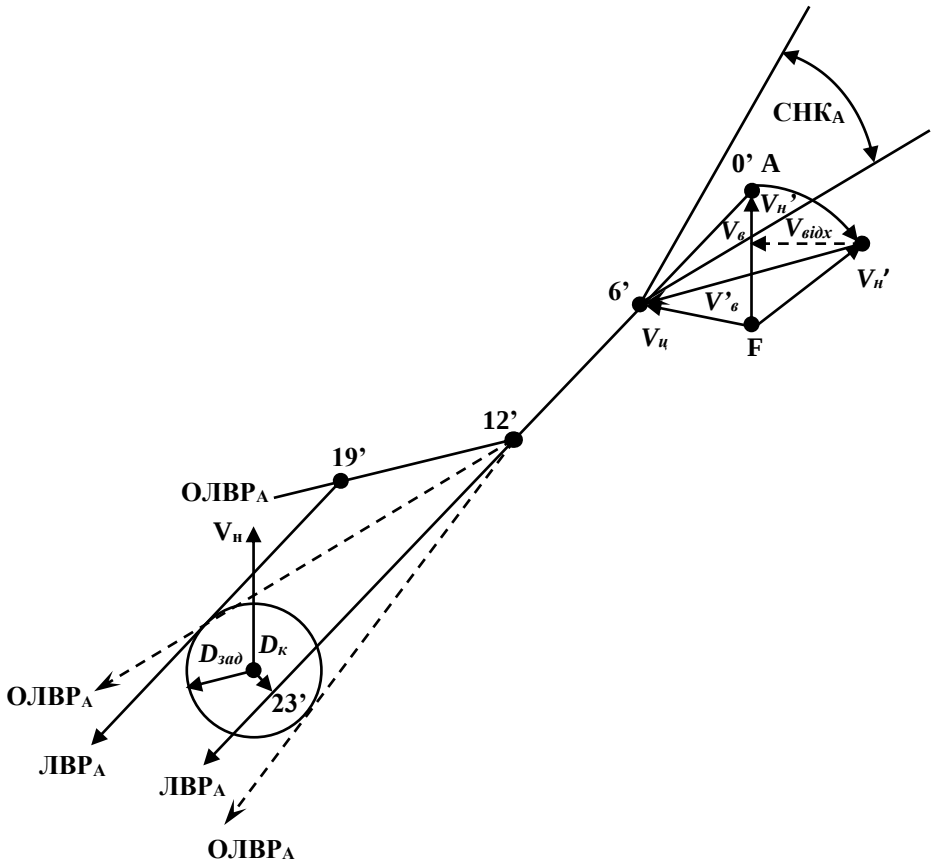

Рис. 1. Графічне рішення задачі розходження з одним судном.

Порядок дій при рішенні задачі розходження наступний:

1) з'єднують нульову і 6-ти хвилинну точки і отримують вектор відносного переміщення $V_{від}$, спрямований стрілкою в 6-у хвилину, продовжують його до центра планшета і отримують лінію відносного руху судна А (ЛВР$_А$); опускають перпендикуляр на ЛВР$_А$ і знімають значення $D_{кр}$ = 0,6 милі, а потім графічно вектором $V_{від}$, від нульової точки по ЛВР$_А$ і до основи перпендикуляра визначають час найкоротшого зближення $t_{кр}$ = 23 хв.

2) наносять випереджаючу точку на 12-ій хвилині і проводять з неї дотичні лінії до кола радіуса $D_{зад}$ і отримують очікувану лінію відносного руху (ОЛВР);

3) з 6-ї хвилини проводять лінії, паралельні ОЛВР$_{ам}$ – у протилежному напрямку і отримують сектор небезпечних курсів (СНК$_А$). Метою рішення задачі розходження є необхідність вивести кінець вектору $V_н$ за межі СНК. Якщо точка F знаходиться в межах СНК, то таке завдання вирішити шляхом зменшення швидкості не представляється можливим;

4) повертають вектор $V_н$ вправо на 30^0, отримують $V_н'$ та з його кінця проводять нове значення відносного вектору $V_{від}'$;

5) з випереджаючої точки проводять штриховану лінію, паралельну вектору $V_{від}$, у напрямку стрілки і отримують ОЛВР$_А$';

6) прикладають паралельну лінійку до ЛВР$_А$, проводять вектор, дотичний до кола $D_{зад}$ до перетину з ОЛВР$_А$' і отримують точку повернення до первинних параметрів руху власного судна:

7) графічно, за новим значенням вектору відносного переміщення $V_{від}$, від 12-ти хвилинної точки визначають 19-ти хвилинну точку. Проводять вектор з точки F за допомогою стрілки в 6-ти хвилинну точку і визначають курс та швидкість судна А, які заносять в таблицю.

На заключній стадії прийняття рішення з маневрування в умовах обмеженого простору, крім руху інших суден, доводиться враховувати стиснені акваторії і наявність засобів навігаційного огородження (ЗНО). Крім того, в умовах обмеженої видимості доводиться прискорено вирішувати задачу, без виконання значної частини допоміжних графічних побудов.

Після того, як сформована стійка навичка рішення задачі на маневреному планшеті, рекомендується використовувати планшет з нанесеною на ньому ситуацією розходження і ЗНО-ситуаційний планшет. В якості масштабу на такому планшеті служить довжина векторів переміщення за 6 хвилин власного судна і відносного руху інших об'єктів і суден. Переміщення знаків ЗНО легко виявляється візуально, оскільки вони зміщуються паралельно курсу власного судна в бік корми, а вектор їх відносного переміщення дорівнює мінус $V_н$.

При рішенні задачі з нанесенням навігаційної обстановки необхідно задати допустиму дистанцію найкоротшого зближення з ЗНО, яка може бути відмінною від тієї, що задана для розходження з суднами. З огляду на те, що мінімальне допустиме значення $D_{зад}$ для суден рекомендується не менше 0,5 милі – в обмежених умовах та 1,5-2 милі – у відкритому морі, то при обранні $D_{зад}$ із ЗНО його можна прийняти рівним 0,5 милі. Якщо дозволяють навігаційні умови, для розходження з суднами величину $D_{зад}$ рекомендується призначати приблизно в 2 рази більшою, ніж зі знаками ЗНО.

Однак використання маневреного і ситуаційного планшетів неможливо під час кібернетичних атак, оскільки навігаційні прилади ходового містка, які дозволяють отримати напрям і дистанцію до зустрічних суден, виходять із ладу.

Безпека плавання в стиснених водах, до яких відносять канали, фарватери, припортові води та акваторію порту забезпечується додатковим застосуванням [14, 16] спеціальних способів штурманської роботи. Для проходження акваторій стиснених вод, від прийому лоцмана до швартування біля причалу, а також при відході в процесі переходу до місця висадки лоцмана використовується лоцманське проведення.

Використання систем підтримки прийняття рішень, належне планування координат руху високоточним способом траєкторними точками, включаючи криволінійні ділянки шляху,

дозволяє забезпечити безаварійне управління процесом маневрування при будь-яких умовах видимості та складних навігаційних умовах.

Точність планування [17] забезпечується використанням таблиці шляхових точок, врахуванням маневрових характеристик для існуючого стану судна та геометрією руху, відповідно до параметрів маневрування, включаючи криволінійні ділянки шляху. Результати автоматичних розрахунків в комп'ютерній програмі «Path Planning IS» оформлено у вигляді матриці координат заходу/ виходу із порту в рейсовому циклі.

Верифікація аналізу ймовірності виникнення та впливу кібернетичних ризиків в рейсовому циклі судна виконується на підставі: 1) узагальненої таблиці аварійно-небезпечних районів навігаційних ризиків; 2) розробленого судноводієм реєстру стійкості до кібератак навігаційного обладнання; 3) визначення процедур кібернетичної безпеки на кожній аварійно-небезпечній ділянці шляху. Це дозволяє організувати кібернетичний захист суднових навігаційних приладів ходового містка в районах очікуваних кібератак та зменшити збитки від кіберзлочинів.

В дослідженнях [14, 15, 16, 18] вже розроблено маршрути заходу та виходу від кожного причалу порту Чорноморськ, у вигляді суднового плану лоцманської проводки для навігаційних цілей. На основі отриманої інформації здійснено комп'ютерне планування рекомендованих маршрутів лоцманського проведення всіх типів суден, які заходять в порт Чорноморськ. Також в роботі [15] виконано верифікацію запропонованої моделі автоматичного планування шляху за координатами траєкторних точок і використано системи підтримки прийняття рішень з автоматичного контролю параметрів маневрування технічними засобами порту, для забезпечення радіолокаційного спостереження заходу/виходу суден. Проведений порівняльний аналіз точності суднових і берегових радіолокаційних систем дозволив розробити методику натурних спостережень портовими радіолокаційними станціями. В дослідженні виконано радіолокаційне спостереження 300 випадків заходу і 200 випадків виходу суден із порту Чорноморськ за розробленими планами для кожного причалу порту [15].

На основі отриманої інформації здійснено планування рекомендованих маршрутів матрицями траєкторних точок для навігаційних цілей до всіх причалів та лоцманського проведення всіх типів суден, які заходять в порт Чорноморськ. Інтегрування розроблених маршрутів в комп'ютерну програму «Path Planning IS» дозволило скласти для кожного причалу таблицю координат шляхових точок та розрахувати матриці траєкторних точок. Аналіз комп'ютерного моделювання та практичного проходження суден рекомендованою ділянкою акваторії порту підтвердив доцільність запропонованої моделі результатами натурних спостережень. На підставі їх аналізу зроблено висновки, що розроблена модель забезпечує кібернетичну безпеку процесів маневрування в стиснених водах, тому може бути рекомендована для впровадження в морські порти України, для виконання вимоги Міжнародної морської організації (ММО) до планування шляху рейсового циклу, від причалу порту відходу до причалу порту приходу.

При виникненні кібернетичних атак необхідно систему управління маневруванням переключати із штатної роботи навігаційних приладів ходового містка, які вийшли із ладу, на резервні та використовувати ручні способи виконання штурманської роботи.

Для цього було розроблено автоматичний перемикач роботи системи управління навігаційними приладами ходового містка зі штатного режиму в режим обсерваційного зчислення. Блок-схема фрагменту системи перемикання із штатного режиму в режим обсерваційного зчислення і навпаки приведена на рис. 2.

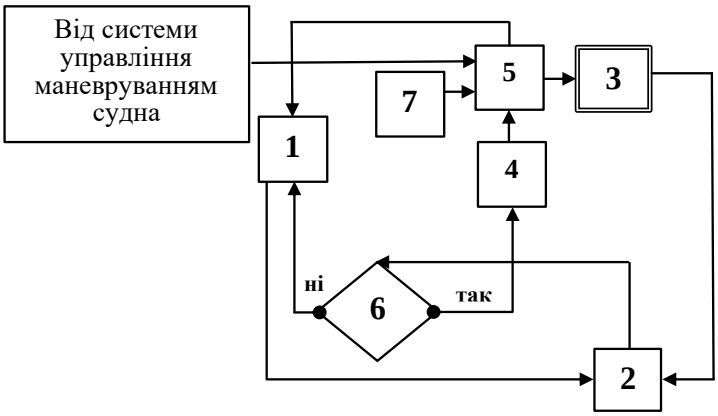

Рис. 2. Фрагмент блок схеми алгоритму автоматичного перемикання системи управління маневруванням із штатного режиму в режим обсерваційного зчислення і навпаки при кібернетичних атаках:
1 – система виконання обсерваційного числення і контролю стану навігаційних приладів; 2 – аналізатор відмов приладів навігаційного кластера ходового містка і вибору способу управління маневруванням; 3 – система штатного функціонування приладів ходового містка; 4 – накопичувальний аналізатор кількості навігаційних приладів ходового містка в робочому стані; 5 – перемикач режиму роботи системи в штатний режим або для обсерваційного зчислення; 6 – селектор відбору приладів в робочому стані, який направляє в блок 4 через вихід «так», а в неробочому стані повертає в блок 1 через вихід «ні» для приведення їх до ладу; 7 – електронна обчислювальна машина.

Основними блоками системи являються: 5 – перемикач режиму роботи; 3 – система штатного функціонування приладів ходового містка; 1 – система обсерваційного зчислення; 2 – аналізатор відмов приладів навігаційного кластера ходового містка, вибору резервних навігаційних приладів або способу управління маневруванням.

Працює система наступним чином: від навігаційної системи управління маневруванням судна на перемикач режиму роботи системи поступають необхідні дані. При робочому стані приладів ходового містка перемикач запускає в роботу систему штатного функціонування приладів ходового містка. При роботі системи, в аналізаторі відмов приладів навігаційного кластера, постійно контролюється стан навігаційних приладів. При появі кібератаки навігаційні прилади ходового містка проходять перевірку в аналізаторі відмов, потім інформація надходить в селектор відбору приладів. Якщо вони знаходяться в неробочому стані, то через вихід «ні» ця інформація передається в систему виконання обсерваційного зчислення, для приведення їх до ладу. У випадку належного робочого стану приладів селектор відбору обладнання направляє відповідну інформацію в накопичувальний блок через вихід «так».

При відсутності інформації щодо робочого стану всіх навігаційних приладів ходового містка в накопичувальному блоці, перемикач режиму роботи системи здійснює її перехід в обсерваційне зчислення. В результаті всі штатні навігаційні прилади відмикаються і включаються резервне обладнання. Далі, починається рукописне документування процесу маневрування, виконання графічного зчислення на навігаційній карті і визначення місця судна візуальними чи астрономічними способами.

Після отримання даних аналізатора про всі навігаційні прилади, які знаходяться в робочому стані, він автоматично перемикає роботу системи управління маневруванням в штатний режим.

В процесі обсерваційного зчислення виконується вимога ММО щодо точності визначення місця судна, оскільки використовуються апробовані методи візуальних і астрономічних способів. Але виникає проблема з вирішенням задачі розходження суден в умовах появи

кібератак, при відмовах інформаційно-навігаційного обладнання, які впливають на можливість візуального спостереження навігаційної обстановки та місцезнаходження інших суден. Оскільки резервних приладів для визначення наявності інших суден в умовах відсутності видимості немає, то рекомендується вибирати мінімальну швидкість, близьку до швидкості втрати керованості. Також, у випадку відмови всіх систем радіолокаційного спостереження, альтернативою може бути постановка на якір для очікування покращення видимості.

Для прийняття рішення з розходження при кібернетичних атаках в умовах доброї видимості відмовимося від чисельного розв'язання задачі, а розходитися будемо шляхом використання ефективного маневру з урахуванням закономірностей відносного руху.

Для оцінки ситуації, визначення небезпеки зіткнення і прийняття рішення з використання виду ефективного маневру, необхідно чітко знати закономірності переміщення суден в режимі відносного руху та вихідні дані, які необхідні для цього. Для їх розуміння немає необхідності проводити будь-які обчислення при кібернетичних атаках, а потрібно чітко вести безперервне спостереження за пеленгатором магнітного компасу на верхньому ходовому містку та знати чинники, від яких залежить зміна обстановки при маневруванні власного та інших суден.

Характер зміни відносного руху залежить від трьох чинників (рис. 3):

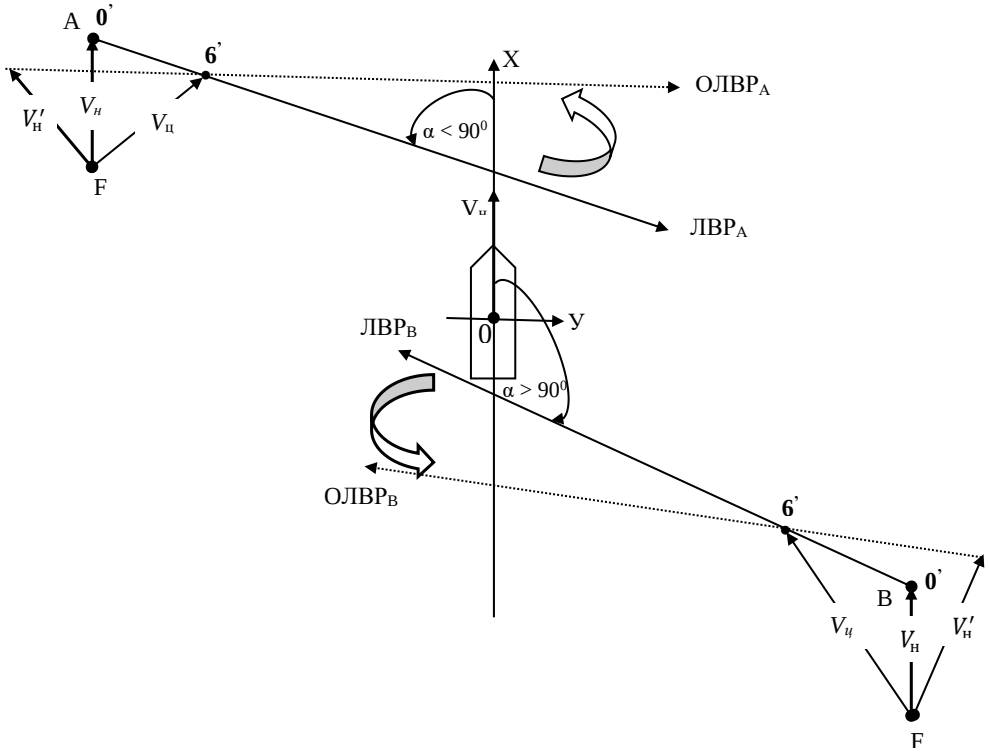

Рис. 3. Закономірності відносного руху.

- відносного розташування інших суден щодо курсу власного судна – справа або зліва;
- величини курсового кута між лінією відносного руху і діаметральною площиною свого судна, курсового кута лінії відносного руху (ЛВР): ЛВР – $\alpha < 90^0$, $\alpha = 90°$, $\alpha > 90°$;
- розташуванням ЛВР щодо власного судна: перетинає курс по носі; проходить через наше судно або перетинає лінію курсу по кормі.

На підставі цих принципів було розроблено таблицю у вигляді каталогу ситуацій наближення і видів маневру для розходження [16]. Вона складається з 18 блоків вибору маневру і займає 288 позицій. Для розходження ефективним маневром достатньо знайти декілька позицій, але існують принципи, яких потрібно дотримуватися оптимального вибору. У залежності від часу виконання маневру на першому місці стоїть маневр повороту. Маневр зменшення швидкості і комбінований поворот зі зменшенням швидкості не рекомендується

використовувати як ефективний, оскільки він надмірно інерційний, тому його рекомендується використовувати тільки в крайньому випадку, коли інших альтернатив немає. Маневр збільшення швидкості і виконання повороту відноситься до розряду ефективних, оскільки при його виконанні керованість покращується.

Для прикладу використання каталогу [16] розглянемо два рішення задачі (рис. 3).

Судно А. Якщо воно розташоване зліва відносно діаметральної площини (ДП) власного (нашого) судна, то курсовий кут ЛВР $\alpha < 90°$, ЛВР перетинає курс по носі.

При розташуванні судна В справа відносно ДП власного судна, курсовий кут ЛВР $\alpha > 90°$, ЛВР перетинає лінію курсу по кормі.

Зміну відносного руху характеризують двома параметрами:

1) за напрямком розвороту очікуваної лінії відносного переміщення судна щодо первісної ЛВР , яке здійснюється за годинниковою стрілкою або проти годинникової стрілки;

2) зміною розташування очікуваної лінії відносного руху (ОЛВР), за відношенням до власного (нашого) судна, яка визначає віддалення або наближення до нього.

Рішення 1. Ціллю рішення задачі розходження є необхідність вибору маневру, при виконані якого очікувана ЛВР (ОЛВР) віддаляється від нас.

Приклад (див. рис. 3). Для розходження з судном А, як вибрано із каталогу [16] за пунктом 2, власне судно повинно виконати ефективний маневр повороту ліворуч і мати вектор переміщення $V_н'$. В результаті $ЛВР_А$ розвертається за годинниковою стрілкою і віддаляється від нас. Зауважимо, що для розходження суден в каталозі [16], за пунктами 3, 8, 9, 11 існують також інші варіанти вирішення задачі, але при їх використанні, через інерційність зміни швидкості, маневр займає більше часу, тому вибраний варіант являється оптимальним.

Судно В. Для розходження з судном В власне (наше) судно повинно виконати розворот вправо, збільшити швидкість згідно пункту 278 каталогу [16] і мати вектор переміщення $V_н'$. В результаті ЛВРВ розвертається за годинниковою стрілкою і віддаляється від нашого судна.

Рішення 2. Використання збільшення швидкості в зазначеному випадку є оправданим, оскільки цей маневр менш інерційний. Зрозуміло, що інші види маневрів потребують зменшення швидкості, яке не може бути рекомендовано для даного випадку.

У статті виконано аналіз впливу кібернетичних атак на морські судна і встановлено, що це може завдати значні економічні втрати для морського транспорту. Науковою новизною статті є вирішення задачі розходження суден при кібернетичних атаках.

Оскільки кібернетичні ризики виникають через навігаційну складову рейсового циклу та призводять до виходу із ладу приладів суднового ходового містка та технологічних приладів забезпечення руху, пошук рішення задачі розходження і управління судном під впливом кібернетичних атак є критично важливим.

Виконаний аналіз рішення навігаційних задач на ходовому містку показав, що найбільші труднощі виникають при рішенні саме задачі розходження. Через вихід із ладу навігаційних приладів ходового містка неможливо отримати необхідні дані для чисельного рішення задачі розходження, за причиною відсутності резервних приладів. Тому, замість чисельного рішення, було запропоновано прийняття принципового рішення з маневрування, для якого необхідно наступне:

- використання ефективного маневру;
- визначення характеру зміни напрямку на небезпечне судно, за допомогою пеленгатора магнітного компасу верхнього ходового містка;
- визначення виду маневру за характером зміни лінії відносного руху – від нас;
- визначення видів маневру розходження та ситуацій наближення за каталогом [16].

Отже, такий спосіб прийняття принципового рішення з ефективним маневром, замість чисельного рішення, як прийнято при роботі системи в штатному випадку (коли працюють всі навігаційні прилади ходового містка), дозволяє попередити зіткнення. Тому, розроблений спосіб є зрозумілим, не потребує багато часу і являється єдиною можливістю вирішити

навігаційну задачу розходження при кібернетичних атаках для безаварійного виконання переходу.

7. Перспективи подальшого розвитку досліджень

У зв’язку з посиленням інтеграції інформаційних технологій у морські операції та згідно з вимогами Резолюції ММО, в СУБ судноплавної компанії та судна повинно враховуватися управління кіберризиками, відповідно до цілей та функціональних вимог Міжнародного кодексу з управління безпекою (МКУБ). Рекомендації ММО спрямовані на реалізацію положень резолюції ММО MSC.428(98), а саме «Управління кіберризиками в морській галузі в рамках систем управління безпекою». Для виконання цих вимог кожна судноплавна компанія може вносити зміни до існуючої СУБ щодо реалізації стратегії кібербезпеки судна [18, 19, 20] та визначати ці питання самостійно.

Тому, для безпечного розходження суден при кібернетичних атаках важливо дотримуватись наступних процесів [21, 22, 23]:

- своєчасно проводити моніторинг процедур оцінки ризиків, які встановлено у СУБ компанії та судна:
- враховувати ризики, пов'язані з кібератаками або кібер-інцидентами;
- приймати кадрові рішення для управління кібербезпекою судна;
- ідентифікувати збої у роботі інформаційно-навігаційних систем, при яких виникають кіберризики, які пов'язані з маневруванням судна та виконанням суднових операцій;
- розробляти захисні заходи для суднових комп'ютеризованих систем, які забезпечать безперервність виконання судноплавних операцій;
- своєчасно оновлювати застаріле суднове програмне забезпечення;
- реалізовувати заходи для своєчасного виявлення ймовірності появи кібератак та збоїв у роботі інформаційно-навігаційного обладнання.

Додатково необхідно зобов’язати країни, в зоні яких сталася кібернетична атака, передавати детальну інформацію в міжнародну організацію ММО, для розміщення її на картах, в лоціях та інших інформаційних джерелах з безпеки судноплавства, оскільки така система лише частково налагоджена.

В статті запропоновано змістовну модель системи перемикання зі штатного режиму в режим обсерваційного зчислення, для вирішення критично важливої задачі безпечного розходження суден під час кібернетичних атак та впровадження в практику роботи судноводіїв маневреного буклету [24].

Перспективою подальшого дослідження з питань кібербезпеки судноплавства може стати інтеграція нових способів боротьби проти кібератак з методами штучного інтелекту. Вона дозволить ідентифікувати нові види кібератак на суднове обладнання, оцінити ймовірні впливи кіберризиків, визначити необхідні фінансові ресурси і підвищити кваліфікацію суднового та берегового персоналу. Це забезпечить розробку сучасних методів щодо запобігання впливу кіберризиків для своєчасного реагування на кібератаки в міжнародному морському секторі.

8. Висновки

Інформаційна безпека водних шляхів, визначає необхідність наукової розробки нового сегменту для кібербезпеки судноплавства. На підставі існуючих методів рішення задачі розходження показано, що способів рішення задачі розходження при відсутності приладів для вимірювання відстані до зустрічного судна, в умовах кібернетичних атак, не існує. Тому, запропоновано розділити стадію зближення на три етапи: надмірне, небезпечне та аварійне. Етап зближення пропонується виконувати на підставі закону маневру останнього моменту.

Оцінку небезпеки зіткнення і вибір маневру для розходження пропонується виконувати за наступними параметрами:

- розташуванням цілі відносно діаметральної площини судна – справа/зліва;
- характером зміни лінії відносного напрямку – до нас чи від нас;
- тенденцією наближення – віддаляється чи приближається.

Правий чи лівий борт та тенденція наближення визначаються окомірно, а характер зміни відносного напрямку – при допомозі магнітного компасу, який повинен бути розташований на верхньому ходовому містку і мати пеленгатор.

Проведений в статті аналіз небезпеки зіткнення за розташуванням цілі – справа/зліва, характером зміни відносного напрямку – постійний чи змінюється, визначенням напрямку повороту лінії руху – від нас чи до нас та за каталогом [16] – в табличній формі, дозволяє вибрати маневр, який буде повертати лінію відносного руху від нас.

Список літератури:

1. Guidelines on maritime cyber risk management. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf (дата звернення: 26.05.2024).

2. Shumilova K., Onishchenko O. Action planning in comprehensive shipping risk identification. The scientific heritage | International independent scientific journal. No 49 (2020), P.1. – P. 40-46. ISSN 9215 – 0365.

3. Embrace the future of maritime. URL: https://www.nsslglobal.com/markets/maritime/ (дата звернення: 25.05.2024).

4. Muhammed Erbas, Shaymaa Mamdouh Khalil, Leonidas Tsiopoulos. Systematic literature review of threat modeling and risk assessment in ship cybersecurity. Ocean Engineering, Volume 306, 2024, 118059, ISSN 0029-8018. https://doi.org/10.1016/j.oceaneng.2024.118059

5. Huang X., Wen Y., Zhang F., Han H., Huang Y., Sui Z. A review on risk assessment methods for maritime transport. Ocean Eng., 279 (2023), Article 114577, https://doi.org/10.1016/j.oceaneng.2023.114577

6. Levy, S., Gudes, E., Hendler, D. (2023). A Survey of Security Challenges in Automatic Identification System (AIS) Protocol. In: Dolev, S., Gudes, E., Paillier, P. (eds) Cyber Security, Cryptology, and Machine Learning. CSCML 2023. Lecture Notes in Computer Science, vol 13914. Springer, Cham. https://doi.org/10.1007/978-3-031-34671-2_29

7. Esma Uflaz, Sukru Ilke Sezer, Ahmet Lutfi Tunçel, Muhammet Aydin, Emre Akyuz, Ozcan Arslan. Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. Reliability Engineering & System Safety, Volume 243, 2024,109825, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2023.109825

8. Tam, K., Jones, K.: Factors affecting cyber risk in maritime. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, pp. 1–8 (2019). https://doi.org/10.1109/CyberSA.2019.8899382

9. Fjørtoft, K., Parvasi, S. P., Nesheim, D. A., Wennerberg, L. A. L., Mørkrid O. E., Psaraftis, H. N. Assessing the resilience of sustainable autonomous shipping: New methodology, challenges, opportunities. Cleaner Logistics and Supply Chain. 2023, Volume 9, 100126, ISSN 2772-3909. https://doi.org/10.1016/j.clscn.2023.100126

10. Chen, L., Wang, B. Robustness assessment of weakly coupled cyber-physical power systems under multi-stage attacks. Electric Power Systems Research. 2024, Volume 231, 110325, ISSN 0378-7796. https://doi.org/10.1016/j.epsr.2024.110325

11. Мальцев А. С. Маневрування суден під час розходження: навчальний посібник./ А. С. Мальцев, С. С. Тюпіков, І. І. Ворохобін, І. Л. Сурінов. – Одеса, НУ «ОМА», 2021. – 178 с.

12. Мальцев А.С. Методологические основы маневрирования судов при сближении. Монография. / А.С. Мальцев, В.В. Голиков, И.В. Сафин, В.В. Мамонтов.// – Одесса.: ОНМА, 2013. – 218 с.

13. Мальцев А.С. Психологические аспекты маневра последнего момента. /А.С. Мальцев, И.М. Стариков // Судовождение: Сб. науч. трудов/ ОГМА. – Одесса: Латстар, 2002. – Вып. 4. – С. 36 – 45.

14. Surinov I., Shumilov D.: Cybersecurity of the processes of manoeuvring in confined waters. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 17, No. 3, pp. 723-732, 2023. – Available at: https://doi.org/10.12716/1001.17.03.25

15. Сурінов І. Л. Удосконалення методики навігаційного планування шляху судна під час лоцманського проведення: дисертація д-ра філософії: 29.01.2024. Одеса, 2024. 409 с.

16. Мальцев А. С. Системы принятия решений по управлению движением судна, монография/ А. С. Мальцев, А. П. Бень. – Херсон.: ХГМА, 2019. – 240 с.

17. Мальцев, А. С. Побудова криволінійних траєкторій маневрування методом відрізків. In The 9 th International scientific and practical conference «Science, innovations and education: problems and prospects» (April 6-8, 2022) CPN Publishing Group, Tokyo, Japan, 2022. 580 p. (p. 152).

18. Шумілова К. В. Реалізація стратегії кібербезпеки в системі управління безпекою судна. Науково-технічний збірник «Судноводіння» / «Shipping & Navigation». – Одеса: НУ «ОМА», 2022, Випуск 31. – С. 99-107. ISSN 2306-5761 | 2618-0073. https://doi.org/10.31653/2306-5761.31.2021.99-107

19. Shumilova, K., Shumilov, D., & Maltsev, A. (2024). Classification of Cyber Risks for Sea Vessel's Voyage Cycle. Transactions on Maritime Science, 13(1). https://doi.org/10.7225/toms.v13.n01.w20

20. Onishchenko O., Shumilova K., Volyanskyy S., Volyanskaya Y., Volianskyi Y.: Ensuring Cyber Resilience of Ship Information Systems. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 16, No. 1, http://dx.doi.org/10.12716/1001.16.01.04, pp. 43-50, 2022.

21. Шумілова, К. Систематизований підхід до класифікації навігаційних ризиків рейсового циклу морського судна. Scientific Collection «InterConf+», 2022, (24(121), 337-358. https://doi.org/10.51582/interconf.19-20.08.2022.032

22. Шумілова К. В., Мальцев А. С. Управління індивідуальними навігаційними ризиками рейсового циклу морського судна. Науково-технічний збірник «Судноводіння» / «Shipping & Navigation». – Одеса: НУ «ОМА», 2022, Випуск 33. – С. 128-142. ISSN 2306-5761 | 2618-0073. DOI: 10.31653/2306-5761.33.2022.128-142.

23. Патент на винахід МПК G08G 3/02 (2006.01). Система управління кібербезпекою маневрування морського судна при рейсовому циклі. / Мальцев А. С., Шумілова К. В., Шумілов Д. І., Муравйов Г. М. Заявник Національний університет «Одеська морська академія». – № a202300014; заявлено 03.01.2023; опубліковано 09.08.2023, Бюл. № 32, стор. 139-140.

24. Maltsev A.S. Navigation support for the process of managing the maneuvering of a sea vessel. (Maneuvering booklet)/ – Eliva Press, 2023, – 218 p. URL: https://www.elivabooks.com/en/book/book-8240761357

Collision avoidance of the sea vessels during cyber attacks in the voyage cycle

Dmytro Shumilov
National University «Odessa Maritime Academy», Educational and Scientific Institute of Navigation, Odessa, Ukraine
ORCID 0009-0009-6242-8620

Abstract: In the course of the development of modern shipping, in addition to navigational risks, cyber risks have also arisen. They are associated with the wide implementation of computer technologies and the use of wireless communication lines between devices on ships and in external radio communication. In addition, the principle of operation of the devices used is based on the transmission and reception of radio waves, which leads to vulnerability to cyber-attacks, which was not taken into account when designing such equipment. Therefore, it is necessary to develop recommendations for navigators on the methods of work in the event of threats of cyber-attacks to control the maneuvering of the ship during collision avoidance. Methods: modern methods of solving the problem of vessel collision avoidance under normal conditions were used. The patterns of the maneuver of the last moment, the catalog method and the control of the risk of collision by the nature of the change in the relative direction of the dangerous vessel are taken into account. Results: it is shown that there are no ways to solve the collision avoidance problem in the absence of devices for measuring the distance to the oncoming ship in the conditions of cyber-attacks. Therefore, it is proposed to divide the stage of approach into three stages: excessive; dangerous; emergency. It is suggested to assess the risk of collision and choose a maneuver for collision avoidance based on the location of the target relative to the diametrical plane – right/left, the nature of the change in the relative direction line clockwise or counterclockwise and the tendency of approach – moving away or approaching. Discussion: analysis of the risk of collision according to the location of the target – right/left, according to the nature of the change in the relative direction – constant or changing, and according to the direction of the turn of the line of movement – from us or towards us – according to the catalog in tabular form, which allows to choose an effective maneuver that will turn the line of relative motion away from us.

Keywords: Cyber-attack; Collision avoidance of ships; Maneuver catalog method; Cyber risks; Effective maneuver.