УДК 627.7
DOI https://doi.org/10.32782/2663-5941/2023.6/41

Пліта Л.Л.
Дунайський інститут водного транспорту
Державного університету інфраструктури та технологій

Іваненко В.М.
Дунайський інститут водного транспорту
Державного університету інфраструктури та технологій

Федунов В.М.
Дунайський інститут водного транспорту
Державного університету інфраструктури та технологій

Трофименко І.В.
Дунайський інститут водного транспорту
Державного університету інфраструктури та технологій

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ВИЗНАЧЕННЯ ЦІЛІСНОСТІ СУЧАСНИХ ІНТЕГРОВАНИХ НАВІГАЦІЙНИХ СИСТЕМ

Метою статті є дослідження особливостей визначення цілісності сучасних інтегрованих навігаційних систем для підвищення безпеки забезпечення споживача інформацією про місцезнаходження судна та відображення її на електронних картах. Поставлена мета досягається шляхом аналізу джерел інформації щодо питань цілісності сучасних інтегрованих навігаційних систем в морській сфері, зокрема кібербезпеки морських систем. Встановлено, що сучасні суднові мостики і морські операції вже зазнали революції завдяки комп'ютеризованим системам. Ключовими компонентами є інтегровані навігаційні системи та системи відображення електронних карт та інформації, які забезпечують споживача інформацією про місцезнаходження судна та відображення її на електронних картах. Хоча цілісність цих систем має вирішальне значення для безпеки морських операцій, вона залишається недостатньо вивченою. Цілісність передбачає здатність системи швидко і точно попереджати користувачів про неможливість виконання вимог точності. Однак у новій літературі з морської кібербезпеки мало обговорюється це питання. Більшість загальних публікацій, які застосовують загальні принципи кібербезпеки до морських систем. Посилання на морські інциденти, атаки й уразливості не містять достатньої інформації і часто повторюються в різних джерелах. У даній статті розглянуто цілісність навігаційних систем, проаналізовано можливості інтегрованих навігаційних систем, а також випадки кібератак на навігаційні системи. Найбільш суттєвим результатом є запропонований загальний прототип інтегрованих навігаційних систем та визначені вимоги до можливих криптографічних контрзаходів щодо захисту цілісності навігаційних даних в інтегрованих навігаційних системах. При цьому визначено також два можливих варіанти втілення криптографічних контрзаходів: простіше рішення з відкритим ключем та рішення на основі ідентифікації, яке використовує апаратні модулі безпеки. Хоча повна безпека недосяжна, застосування криптографічних контрзаходів може потенційно поліпшити цілісність інтегрованих навігаційних систем.

Ключові слова: *інтегрована навігаційна система, цілісність, електронна карта, судно, прототип, кібербезпека, криптографічні контрзаходи.*

Постановка проблеми. Сучасні судна оснащені інтегрованими мостиковими системами (IBS) (рис. 1). IBS являє собою комбінацію систем, які взаємопов'язані для забезпечення централізованого доступу до сенсорної або командно-керуючої інформації з робочих станцій з метою підвищення безпеки та ефективності управління суднами відповідним кваліфікованим персоналом [1]. Іншими словами, IBS – це інтеграція систем, яка дозволяє контролювати і контролювати судно і його роботу з мостика.

До інтегрованих систем зазвичай входять навігаційні системи, системи зв'язку та системи управління двигуном, але й іноді також системи спостереження тощо. Ці комп'ютеризовані суднові мостики являють собою технологічну

Рис. 1. Приклад інтегрованої мостикової системи судна

революцію для морського судноплавства. Історично склалося так, що основним завданням для штурмана було знайти і зафіксувати положення судна, в той час як сучасний штурман стежить за положенням, застосовуючи дані, отримані навігаційними датчиками судна, та представлене навігаційне програмне забезпечення [2].

У даній статті розглядаються саме навігаційні системи. Морські навігаційні системи, пов'язані через бортові мережі, називаються інтегрованими навігаційними системами (INS) [3]. В INS датчики, що використовуються в навігації, такі як GPS, гіроскоп, датчики глибини і т. д., підключаються до робочих станцій, оснащених програмним забезпеченням для відображення електронних карт, відомим як Electronic Chart Display and Information Systems (ECDIS) [4]. Програмне забезпечення ECDIS показує положення судна на карті за допомогою даних навігаційних датчиків, а також положення суден, що знаходяться поруч, на основі даних, отриманих через систему автоматичної ідентифікації (AIS) [5]. Крім того, програмне забезпечення ECDIS має функціонал для планування маршрутів і моніторингу маршрутів.

Очевидно, що забезпечення цілісності INS відіграє важливу роль у забезпеченні безпечних і надійних морських операцій. Цілісність тут означає здатність системи швидко і точно попереджати користувачів про неможливість виконання вимог точності. Однак у новій літературі з морської кібербезпеки мало обговорюється це питання. Більшість загальних публікацій, які застосовують загальні принципи кібербезпеки до морських систем. Посилання на морські інциденти, атаки й уразливості не містять достатньої інформації і часто повторюються в різних джерелах.

Аналіз останніх досліджень і публікацій. Загальні питання цілісності INS в морській сфері розглядаються, наприклад, в роботах [2], [6], [7]. Так, у статті [2] визначено, що інформаційно-комунікаційні технології, а також операційні технології на борту суден все частіше об'єднуються в мережі і все більше підключаються до мережі Інтернет. Впровадження кіберсистем змінює робоче середовище для зниження навантаження на навігатор, але в той же час створює додаткові складності і вразливості, які, в свою чергу, можуть змінити компетенції, необхідні для безпечного й ефективного плавання. Сучасними прикладами цього є кібератаки, які можуть спотворити ситуаційну обізнаність і перешкодити визначеним морським операціям. У даній статті демонструються деякі з можливих векторів атаки, які кібератака може представляти для судна, а також обговорюється ймовірність і наслідки таких атак.

Питання кібербезпеки морських систем розглядаються, наприклад, в роботах [8–11]. Так, у роботі [11] визначено, що кібератаки швидко зростали протягом багатьох років, що призвело до великих фінансових втрат для бізнесу через відновлення, санкції з боку регуляторів та супутні збитки, такі як репутація та довіра. У зв'язку з цим морський сектор, який досі вважався безпечним через відсутність підключення до Інтернету та ізольований характер суден у морі, спостерігає 900-відсоткове збільшення порушень кібербезпеки в операційних технологіях, коли він вступає в цифрову епоху. Безпосередньо у даній статті проведено детальне дослідження кібербезпеки в морській галузі з метою виявлення проблем та викликів безпеці. По-перше, автор досліджує системи на суднах, які можуть стати мішенню зловмисників, їх можливі вразливості, якими може скористатися зловмисник, наслідки в разі доступу до системи і реальні інциденти. Потім автор описує та аналізує можливі дії щодо пом'якшення наслідків, які можуть бути заздалегідь використані для запобігання таким атакам. Нарешті, обговорюється кілька проблем і відкритих питань для майбутніх досліджень.

Метою статті є дослідження особливостей визначення цілісності сучасних інтегрованих навігаційних систем для підвищення безпеки забезпечення споживача інформацією про місцезнаходження судна та відображення її на електронних картах.

Викладення основного матеріалу. Дослідження особливостей визначення цілісності сучасної INS в даній статті здійснюється відповідно до таких етапів:

1) вивчення можливостей сучасних INS в рамках таких рішень:

– робочі станції (включаючи операційні системи);

– інтеграція датчиків;
– мережі передачі даних (включаючи протоколи зв'язку);
– радари;
– автопілот;
– підключення до мережі Інтернет;

2) дослідження кібербезпеки в рамках використання INS (включаючи атаки та інциденти);

3) визначення криптографічної цілісності та контрзаходів в INS.

INS – це інтеграція навігаційних датчиків з робочими станціями, оснащеними ECDIS. У теперішній час існує широкий спектр пропонованих рішень в цій області. Усі розробники проводять чітке розмежування між INS і IBS – можливо, тому, що навігація є невід'ємною частиною повсякденної роботи на містку. Для того щоб мати критерій включення або виключення системи будь-якого розробника, визначимо мінімальну вимогу, яка полягає в тому, що відповідний виріб повинен містити принаймні навігаційне обладнання (наприклад, робочі станції та датчики) та навігаційне програмне забезпечення (наприклад, ECDIS). Це можна розглядати як робоче визначення INS для даного дослідження, хоча воно відрізняється від визначень, даних Міжнародною морською організацією (IMO) [3].

Традиційно станції INS надають робочі місця для екіпажу на мостику. Це, в першу чергу, автономні комп'ютери, на яких працює локальне програмне забезпечення, тобто те, що називається «товстими клієнтами». У деяких рішеннях ці робочі станції є консолями ECDIS, призначеними тільки для відображення карт. У той час інші рішення пропонують багатофункціональні робочі станції (MFW)), які часто називають багатофункціональними дисплеями (MFD). Вони фактично є робочими станціями, які дозволяють оператору перемикатися між дисплеєм ECDIS і радарним дисплеєм. Деякі з рішень – це інфрачервоні системи на основі мостів, які інтегрують інші системи на додаток до навігаційних систем, але в більшості випадків MFW все ще є навігаційними робочими станціями, що забезпечують ECDIS, радари та дисплеї, тоді як інші функції, такі як управління двигуном, мають окремі робочі станції/консолі. Більшість рішень використовують операційну систему Microsoft Windows, а деякі рішення – операційну систему Linux.

Основною особливістю INS є інтеграція, інтерпретація та представлення сенсорного введення в навігаційне програмне забезпечення, таке як ECDIS. Під інтеграцією датчиків маються на увазі засоби, за допомогою яких дані з датчиків, таких як GPS, гіроскоп, ехолот або приймач AIS, передаються на робочі станції. Ці датчики мають послідовний вихід, який зазвичай відповідає стандарту IEC 61162-1/NMEA 0183 для морських навігаційних пристроїв. Переважна більшість існуючих рішень передбачає наявність своєрідного блоку інтеграції датчиків, які часто називаються по-різному: блок розподілу даних, блок збору даних, блок концентрації датчиків і т. д. Спільним для цих пристроїв є те, що вони отримують дані від навігаційних датчиків через послідовні інтерфейси і забезпечують єдине джерело даних датчиків для робочих станцій. Деякі рішення не мають блоків інтеграторів датчиків, і при цьому датчики мають прямі послідовні з'єднання з робочими станціями.

Одним з рішень є автономна робоча станція ECDIS з датчиками, підключеними до послідовних портів. Однак будь-яке рішення, більш складне, ніж це, вимагає різних компонентів, що взаємодіють певним чином. Тобто, інші рішення так чи інакше об'єднані в мережу. Їх мережі з'єднують блоки інтеграції датчиків з робочими станціями. Вони підключають робочі станції для обміну даними (наприклад, дані датчиків, маршрути та оновлення карт), і далі – підключають INS до інших бортових систем, наприклад, до системи зв'язку судна. Точна конфігурація варіюється, але в більшості рішень мережа є різновидом IP Ethernet LAN мережі. Крім того, в автономному рішенні робоча станція оснащена портами Ethernet, які забезпечують роботу в IP-мережі. Тобто Ethernet на базі IP є домінуючою мережевою технологією в навігаційних мережах. Іншими рішеннями є мережа CAN-шини, багатопрофільна система послідовної шини, яка була спочатку розроблена автомобільною промисловістю для використання в автомобілях. У багатьох рішеннях мережі, що з'єднують блоки інтеграції датчиків з робочими станціями, описуються як подвійні або резервні.

За протоколи зв'язку в навігаційних мережах використовуються протоколи TCP і UDP, які дотримуються стандарту IEC 61162-450 "Lightweight Ethernet (LWE)" для суднових мереж. LWE заснований на одній комутованій багатоадресній передачі Ethernet і UDP.

Багато рішень реалізують радіолокаційну інтеграцію. Радар відрізняється від інших типів датчиків в INS тим, що його дані представляються у вигляді зображень, в той час як інші датчики передають числові та текстові дані. За цієї

причини дані від радарів обробляються інакше, ніж від інших датчиків. Тому радар дуже рідко підключається до блоку інтеграції датчиків. Деякі рішення мають радари, підключені до робочих станцій через окрему мережу або через мережу, що і блоки інтеграції датчиків, або радар підключається безпосередньо до робочих станцій якимось іншим способом.

Особливістю, описаною в декількох рішеннях, є інтеграція автопілоту з функціональністю планування маршруту програмного забезпечення ECDIS, тобто можливість автопілоту керувати судном за маршрутом, визначеним в ECDIS. Це, очевидно, означає, що блок автопілоту повинен отримувати команди від робочої станції, і надається опис, як команди передаються по мережі.

Навігаційні карти оновлюються регулярно. Тому навігаційні системи повинні отримувати регулярні оновлення карт. Крім того, стороннє програмне забезпечення, таке як операційна система Windows, також потребує регулярних оновлень і виправлень. Зазвичай оновлення інсталюються за допомогою фізичних носіїв. Однак зараз судна все частіше оснащуються супутниковим підключенням до Інтернету та / або широкосмуговим доступом 4G (для використання під час плавання поблизу берега). У той же час деякі рішення пропонують можливість надання підключення INS до Інтернету для онлайн-оновлень карт, в більшості випадків шляхом надання шлюзу від мережі INS до системи зв'язку судна.

Таким чином, хоча існують відмінності в конкретних конфігураціях різних INS, можна виділити ряд типових особливостей. Приклад узагальненого прототипу INS показаний на рис. 2. Типовою ситуацією є те, що один або кілька Ethernets використовуються для підключення різних компонентів INS: багатофункціональні робочі станції, блок інтеграції датчиків (іноді два для резервування), радар і автопілот тощо. Крім того, судно може мати шлюз для інших систем, які також можуть підключатися до інтернету.

Найбільшою проблемою щодо навігаційних систем досі була загроза підміни GPS, коли навігаційні системи обманюються шляхом передачі помилкових сигналів GPS. Хоча підміна GPS може становити загрозу цілісності положення GPS, розрахованого приймачем GPS судна, і, таким чином, загрозу цілісності положення, що відображається на електронних картах судна, вона не є загрозою цілісності самого INS.

Однак існують і приклади серйозних загроз цілісності навігаційних систем:

– при оновленні карт e-lectron за допомогою USB-накопичувачів консоль ECDIS на борту може бути заражена шкідливим програмним забезпеченням;

– INS все частіше підключаються до Інтернету для оновлення карт в Інтернеті, відомі реальні випадки атак на навігаційне програмне забезпечення.

У той же час, наприклад, в резервній програмі можна перехоплювати і маніпулювати GPS координатами, що передаються на робочу станцію з блоком інтеграції датчиків по мережі. Таким чином, шкідливе програмне забезпечення може змінити положення, яке з'явилося в програмному забезпеченні ECDIS. Відомі результати експери-

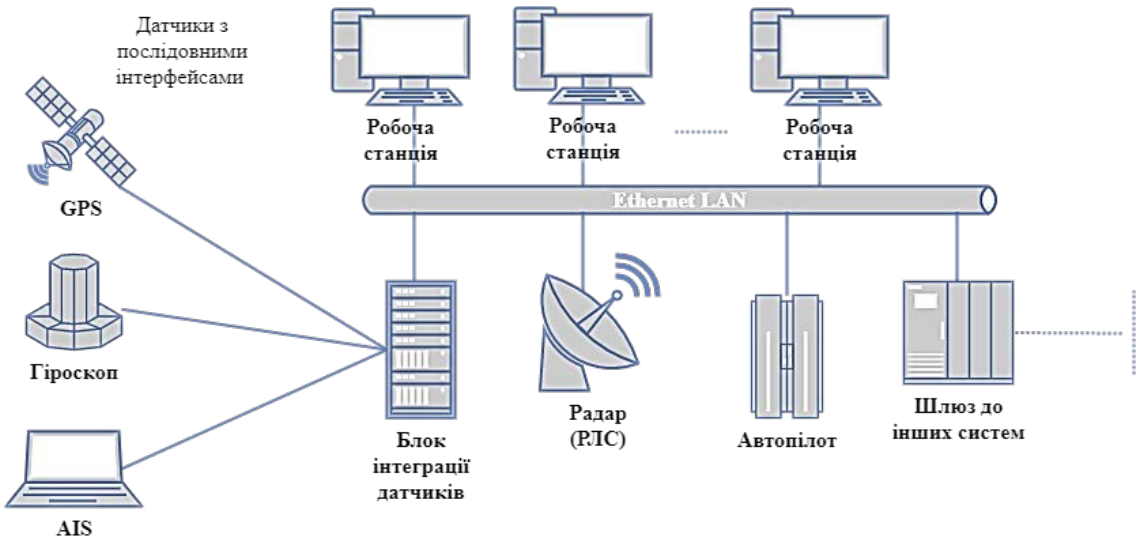

Рис. 2. Прототип інтегрованої навігаційної системи

ментів з підключенням комутатора до мережі INS. Моделювання з внесенням хибних GPS координат в мережі показує, що робочі станції не можуть відрізнити ці координати від GPS-координат, надісланих блоком інтеграції датчиків. Крім того, збільшивши частоту передачі, можна фактично перевизначити блок інтеграції датчиків.

Стандарти продуктивності INS IMO вимагають, щоб системи контролювали цілісність у формі порівняння інформації між надлишковими джерелами навігаційних даних. Хоча цього може бути достатньо для захисту від несправних пристроїв, цього недостатньо для захисту від кібератак. Якщо INS скомпрометовано, не можна маніпулювати даними з кількох джерел.

Розглянемо потенційні засоби захисту цілісності даних в INS. Обмеженням є використання даних *x*, що передаються від блоку інтеграції датчиків до робочих станцій, хоча подібні проблеми можуть стосуватися даних, що надсилаються з радара на робочі станції, між робочими станціями або з робочих станцій на автопілот. На основі прототипу INS, показаного на рис. 2, і потенційних кіберзагроз можна вивести певні вимоги до криптографічних контрзаходів (set of cryptographic countermeasures), які формально представимо у вигляді такого кортежу

$$SCC = CC_i, i = \overline{1,5}, \quad (1)$$

де CC_1 – вимога, яка обумовлена тим, що дані поширюються за допомогою мультиадресної передачі. Тому контрзаходи повинні бути придатними для мультиадресної передачі;

CC_2 – вимога, яка обумовлена тим, що контрзаходи повинні бути ефективними як для автономних, так і для підключених до Інтернету систем;

CC_3 – вимога, яка обумовлена тим, що контрзаходи повинні захищати від атак, пов'язаних з маніпулюванням або фабрикацією навігаційних даних;

CC_4 – вимога, яка обумовлена тим, що контрзаходи повинні захищати від повторних атак (навігаційні дані збираються і передаються пізніше);

CC_5 – вимога, яка обумовлена тим, що хоча блок інтеграції датчиків може вважатися апаратним пристроєм, робочі станції слід вважати звичайними комп'ютерами під управлінням (потенційно старих і невиправлених) операційних систем. Тому вкрай важливо, щоб контрзаходи забезпечували захист навіть у випадках, коли робочі станції скомпрометовані.

Вимоги CC_1 і CC_3 вказують на рішення, яке використовує криптографію з відкритим ключем. Відправник (тобто блок інтеграції датчиків) криптографічно підписує повідомлення закритим ключем, тоді як кілька одержувачів (робочі станції) перевіряють підписи, використовуючи копію відповідного відкритого ключа. Вимогу CC_4 можна отримати, включивши порядковий номер або мітку часу в підписані повідомлення. Вимога CC_2 містить стандартне рішення інфраструктури відкритих ключів (PKI), засноване на онлайновому центрі сертифікації (CA). На основі інформації від бездротових сенсорних мереж (WSN) виділяють два основних варіанти:

− варіант 1 – спрощене рішення PKI з одним кореневим CA;

− варіант 2 – схема підпису на основі ідентифікації.

У варіанті 1 генерується ключ і встановлюється в блок інтеграції датчика – пара захищеного ключа (SK) і відкритого ключа (PK). PK підписується захищеним ключем SK автономного кореневого CA (наприклад, постачальника INS або судновласника) для отримання сертифіката C для блоку інтеграції датчиків. Сертифікат C встановлюється в блок інтеграції датчиків і розподіляється по мережі на робочі станції. Сертифікат CCA CA встановлюється на робочих станціях, які використовують CCA для перевірки C та перевірки повідомлень від блоку інтеграції датчиків.

Варіант 2 – це схема підпису на основі ідентичності. У цій схемі закритий ключ SK генерується автономним центром генератора ключів (знову ж таки, постачальником або судновласником INS), випадково відомим лише хабу, та ідентифікатором блоку інтеграції датчиків (наприклад, серійним номером або MAC-адресою). Як і у варіанті 1, PK встановлюється в блок інтеграції датчика, який використовує його для підписання повідомлень. На відміну від варіанту 1, другий тип ідентифікації сам по собі є відкритим ключем; сертифікат не потрібен, оскільки він може бути автентифікований шляхом перевірки. А ідентифікація блоку інтеграції датчиків встановлюється на робочі станції і використовується для перевірки повідомлень блоку інтеграції датчиків.

В обох випадках цілісність сканерів (CCA має місце у варіанті 1 та ідентифікація блоку інтеграції датчиків у варіанті 2) повинна бути забезпечена після установки на робочі станції, але вимога CC_5 не дозволяє покладатися на їх операційну систему для цього. Можливим рішенням може бути зберігання цих значень у захищених від несанкціонованого доступу апаратних модулях безпеки (HSM), з яких програмне забезпечення ECDIS може витягти їх (або, можливо, перевірити в безпечному середовищі). Використання знімних HSM також

може полегшити розповсюдження та встановлення сертифікатів безпеки або посвідчень.

Очевидно, що жоден із запропонованих варіантів не може гарантувати 100% цілісність навігаційних даних. Оскільки робочі станції можуть бути скомпрометовані, не може бути абсолютної гарантії безпеки. Якщо зловмисник може маніпулювати операційною системою робочих станцій, то він також потенційно може маніпулювати навігаційним програмним забезпеченням. Однак використання запропонованих криптографічних контрзаходів надасть додатковий рівень безпеки, тому що маніпулювати власницьким додатком ECDIS буде складніше, ніж маніпулювати недостатньо безпечною установкою операційної системи бортового комп'ютера. Таким чином, дані контрзаходи сприяють підвищенню безпеки системи, хоча і не можуть забезпечити стовідсоткову гарантію цілісності навігаційних даних.

Висновки. Оскільки сучасні морські судна замінюють традиційні паперові карти інтегрованими навігаційними та електронними системами відображення карт та інформації, цілісність цих систем стає ще більш важливою для забезпечення безпеки морських операцій. У даній статті було проведено дослідження цілісності наявних в даний час інтегрованих навігаційних систем. Це було засновано на аналізі можливостей, що надаються ринком, а також на аналізі можливих кіберінцидентів й атак, які могли вплинути на цілісність навігаційних систем. Ці дослідження показують, що в цілому цілісність інтегрованих навігаційних систем недостатньо захищена.

Після аналізу інтегрованих навігаційних систем був запропонований узагальнений їх прототип. Цей прототип складає основу для виявлення криптографічних заходів, здатних підвищити цілісність захисту навігаційних даних в INS. У результаті представлений набір вимог і два можливих варіанти їх реалізації: спрощене рішення з відкритим ключем і рішення на основі ідентифікації, об'єднане з використанням апаратних модулів безпеки. Хоча гарантована безпека є недосяжною, передбачається, що використання криптографічних контрзаходів потенційно може поліпшити цілісність INS.

Список літератури:

1. Resolution MSC.64(67): Adaption of new and amended performance standars, International Maritime Organization (IMO), 1996.

2. Hareide O. S., Jøsok Ø., Lund M. S., Helkala K., Ostnes R. Enhancing navigator competence by demonstrating maritime cyber security. *Journal of Navigation*. 2018. No 71(5). P. 1-15.

3. Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems (INS), International Maritime Organization (IMO), 2007.

4. Resolution MSC.232(82): Adoption of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS), International Maritime Organization (IMO), 2006.

5. Norris A. Integrated Bridge Systems Vol 1: Radar and AIS. The Nautical Institute, 2008.

6. Demchak C., Patton K., Tangredi S. J. Why are our ships crashing? Competence, overload, and cyber considerations. *Center for International Maritime Security*, URL: https://cimsec.org/ships-crashing-competence-overload-cyber-considerations/ (дата звернення: 23.04.23).

7. Jones K. D., Tam K., Papadaki M. Threats and impacts in maritime cyber security. *Engineering & Technology Reference.* 2016. DOI: 10.1049/etr.2015.0123

8. *The Coast Guard Journal of Safety & Security at Sea* : Proceedings of the Marine Safety & Security Council, Special Issue on Cybersecurity. Vol. 71. No. 4. U. S. Coast Guard, Winter 2014–2015.

9. Issues in Maritime Cyber Security / ed. by J. III Direnzo, N. K. Drumiller, F. S. Roberts. Westphalia Press, 2017. 602 p.

10. Lund M. S., Hareide O. S., Jøsok Ø. An attack on an Integrated Navigation System. *Necesse*. 2018. P. 149-163.

11. Frank Akpan, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis, Michalis Michaloliakos. Cybersecurity Challenges in the Maritime Sector. *Network.* 2022. No *2*(1). P. 123-138.

Plita L.L., Ivanenko V.M., Fedunov V.M., Trofymenko I.V. STUDYING THE PECULIARITIES OF DETERMINING THE INTEGRITY OF MODERN INTEGRATED NAVIGATION SYSTEMS

The purpose of the article is to study the peculiarities of determining the integrity of modern integrated navigation systems to improve the security of providing consumers with information about the location of a vessel and displaying it on electronic charts. This aim is achieved by analyzing the sources of information on the integrity of modern integrated navigation systems in the maritime sphere, particularly the cybersecurity of maritime systems. It has been established that modern ship bridges and maritime operations have already

undergone a revolution due to computerized systems. The key components are integrated navigation systems and electronic chart and information display systems that provide the consumer with information about the vessel's location and display it on electronic charts. Although the integrity of these systems is critical to the safety of maritime operations, it remains poorly understood. The integrity of the transmission of the building of the system is fast and exactly ahead of the users about the impossibility of implementation could not be accurate. However, in the new literature on maritime cyber security, there is little discussion of food. More global publications, like stating global principles of cyber security to maritime systems. Forced on maritime incidents, attacks and frivolity do not retaliate for sufficient information and are often repeated in different seas.

This article discusses the integrity of navigation systems, analyses the capabilities of integrated navigation systems, and examines cases of cyber-attacks on navigation systems. The most significant result is the proposed general prototype of integrated navigation systems and the requirements for possible cryptographic countermeasures to protect the integrity of navigation data in integrated navigation systems. Two possible cryptographic countermeasures are identified: a simple public key solution and an identity-based solution using hardware security modules. Although complete security is not achievable, the use of cryptographic countermeasures can potentially improve the integrity of integrated navigation systems.

Key words: *integrated navigation system, integrity, electronic chart, ship, prototype, cybersecurity, cryptographic countermeasures.*