УДК 004.056.2 **DOI: 10.31653/2306-5761.34.2023.66-78**

ENSURING OPERATIONAL RESILIENCE OF SATELLITE NAVIGATION AT SEA

ЗАБЕЗПЕЧЕННЯ СТІЙКОЇ РОБОТИ СУПУТНИКОВОЇ НАВІГАЦІЇ НА МОРІ

V. Konovets, *senior researcher, PhD.,* **E. Pleshko,** *senior researcher, PhD.,*
O. Shyshkin, *associate professor, D.Sc.*

В.І. Коновец, *пров. наук. співроб., к.т.н.,* **Е.А. Плешко,** *пров. наук. співроб., к.ю.н.,*
О.В. Шишкін, *доцент, д.т.н.*

National University "Odessa Maritime Academy", Ukraine

Національний університет «Одеська морська академія», Україна

ABSTRACT

The article examines the challenges of global navigation satellite systems (GNSS) functioning at sea under unintentional and intentional interference. The article reviews the vulnerability of GNSS, the methods of protection against interference and the ways of mitigating their impact based on the marine concept of positioning, navigation and time synchronization (PNT). The main goal of this concept is the guaranteed obtaining of reliable data on coordinates, navigation and exact time due to the combined use and comparison of indication for disparate systems and sensors under the influence of natural or intentional interference (attacks) on ship's GNSS equipment.

The article analyzes various open sources of information to identify two methods of ensuring the integrity and accuracy of PNT data according to IMO documents and standards. The first method is the detection and direct countermeasures against attacks on shipboard GNSS equipment. The article determines that the most common and easy-to-implement type of attacks are jamming attacks of satellite signals, unlike the more complex and challenging spoofing attacks. The main approach to protection against jamming attacks is spatial signal processing using adaptive marine antenna arrays with a controlled pattern. Examples of modern practical developments of adaptive antenna arrays are given.

The second method to ensure reliable PNT data is the use of alternative navigation systems, redundant capabilities and non-traditional methods using the existing systems. Technical solutions in this method have limitations due to the requirements for the vessel's conventional navigation and radio communication installation. IMO has suggested structures of multisensor and multisystem receivers for obtaining reliable PNT data. These structures combine primary data from different systems based on different principles, such as satellite, terrestrial and augmented correction systems, vessel navigation data and reference systems. The processed PNT data must be accompanied by accuracy and integrity indicators.

Keywords: positioning, navigation, time synchronization, jamming, spoofing, spatial processing, antenna arrays, cyber risks, information protection.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У 2023 році виповнюється півсторіччя з того часу, коли на замовлення Міністерства оборони США було створено першу глобальну навігаційну супутникову систему (ГНСС) (англ. GNSS – Global Navigation Satellite System) під назвою NAVSTAR, відомою сьогодні як Global Positioning System (GPS) [23]. Сімейство ГНСС сьогодні крім GPS включає ГЛОНАСС, Galileo, Beidou, інші локальні системи, наприклад, японська квазізенітна супутникова система (Quasi-Zenith Satellite System, QZSS). GPS за час свого існування і вдосконалення подолала

шлях від надсекретної військової системи до технології, яка доступна кожній людині у будь-якому місці Землі. У теперішній час використання ГНСС – основний спосіб визначення місця розташування та часу у світі.

Проте всі ГНСС мають один істотний недолік: низький рівень завадостійкості, обумовлений наступними факторами:

- великою відстанню передачі сигналів (20000 км);
- обмеженою потужністю сигналу супутника (10...50 Вт);
- малим коефіцієнтом підсилення антени супутникового передавача (10...15 дБ).

За цих причин рівень їх сигналу на поверхні Землі становить від -155 дБВт до -160 дБВт (від -125 дБм до -130 дБм), а за наявності завад – ще менше [23].

Завади, як природні (іоносферні, тропосферні, багатопроменеве поширення сигналів тощо), так і штучні (навмисні та ненавмисні), істотно впливають на сукупність показників (точність, стійкість, цілісність) у процесах визначенні координат, навігаційної інформації та часової синхронізації (англ. PNT – Positioning, Navigation and Timing) [30].

В сучасних умовах та особливо в умовах війни, при застосуванні методів радіоелектронної боротьби (РЕБ), суднове навігаційне обладнання все частіше потрапляє під вплив штучних завад [3, 4, 7, 8, 26, 28, 31]. Питання подолання наслідків впливу завад на вже встановлене навігаційне обладнання ГНСС, діагностування фактів впливу на навігаційне обладнання штучних, навмисних завад, вибору напрямів модернізації суднового навігаційного обладнання з метою забезпечення його безперебійної роботи в умовах завад набуває ще більшої актуальності. Відповіді на всі ці питання досить неоднозначні, а простих та готових для впровадження рішень поки що не знайдено.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і виділення невирішених раніше частин загальної проблеми

Щоб скласти уявлення про ситуацію, що склалася на сьогоднішній день і отримати відповідь на запитання: що може зробити судноводій у разі дії навмисних завад, звернімося до сумісної публікації морських класифікаційних установ “Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)” INTERTANKO 2019 [21]. Тут, у розділі “Дії при виявленні глушіння та спуфінгу”, рекомендується виконати ряд дій, які задля простоти розуміння можна звести до таких:

- використовуйте іншу систему визначення позиції, якщо вона є на борту;
- у разі її відсутності, штурман повинен перейти на режим числення шляху (Dead Reckoning);
- слід враховувати, що суднова автоматична ідентифікаційна система (АІС), швидше за все, також підпаде під атаку з глушінням або спуфінгом, тому її слід використовувати з особливою обережністю;
- якщо неможливо визначити положення судна відносно навігаційних небезпек – необхідно зупинити судно.

Як бачимо, зазначені рекомендації не дають широкого вибору дій, оскільки вони у значній мірі пов’язані з конвенційними вимогами до переліку бортового оснащення суден на теперішній час.

У той же час слід розуміти, що настанова [21], та подібна [29], не є нормативними документами, але, такі документи, складені експертами робочих груп з підготовки майбутніх нормативних вимог ІМО та/або ІЕС, безумовно заслуговують на особливу увагу.

У документі [21] також наведено низку рекомендацій для судновласників щодо підвищення відмовостійкості обладнання та цілісності навігаційних даних при плануванні переоснащення суден.

Формулювання цілей статті (постановка завдання)

Цілями статті є аналіз:

- можливих типів навмисного шкідливого впливу (атакам) на суднову апаратуру користувачів ГНСС по супутниковим радіоканалам у військової та цивільної сферах;

− технічних рішень високого рівня для протидії зазначеним атакам за міжнародними стандартами та настановами.

Виклад матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Насамперед необхідно відзначити існуючі відмінності в рішеннях, орієнтованих на військовий та цивільний сектори. На початку XXI сторіччя технічні рішення в кожному з них розвивалися в різних напрямках, що обумовлено різницею в базових вимогах.

Апаратура ГНСС користувача для мобільної платформи військового призначення має забезпечити виконання платформою поставлених завдань в умовах дії навмисних завад. Тому пошук рішень йшов у напрямку підвищення завадо захищеності військової апаратури ГНСС. Найпоширенішим критерієм завадостійкості апаратури ГНСС є максимальне значення відношення потужності завади *J* до потужності корисного сигналу *S* на вході приймача, при якому приймач не втрачає працездатності, тобто виконує покладені нього функції.

Одним з кардинальних способів підвищення завадостійкості приймача ГНСС є просторова обробка сигналів. Вона базується на використанні просторових відмінностей справжніх навігаційних сигналів і завадових сигналів. Мета просторової обробки сигналів досягається за рахунок застосування антенної решітки з керованою діаграмою спрямованості (англ. Controlled Reception Pattern Antenna, CRPA). Зразків обладнання й прикладів використання навігаційної апаратури користувача ГНСС, з технологією CRPA, у військової сфері багато. Наприклад, завадостійка технологія (GPS Anti-Jam Technology, GAJT) від компанії NovAtel Inc. (Рис.1). забезпечує високоефективний захист приймача GPS в умовах завад, включаючи захист сигналів у різних піддіапазонах: GPS L1, L2, Galileo E1, QZSS L1, L2 та SBAS L1 [2]. Ця технологія також забезпечує захист широкосмугових сигналів М-коду.

GAJT є 7-елементною антеною з електронним керуванням діаграмою спрямованості, що формує нуль, у напрямку джерела навмисних та ненавмисних завад.

Для цивільного торгового флоту головною метою є забезпечення безпеки мореплавства. Координати та точний час, отримані за допомогою ГНСС, використовуються практично усіма системами навігації та радіозв’язку, зокрема, ECDIS (електронна картографічна навігаційна інформаційна система), AIS (автоматична ідентифікаційна система), ARPA (система автоматичного радіолокаційного прокладання), GMDSS (глобальна морська система зв'язку під час лиха та забезпечення безпеки мореплавства), SSAS (суднова система аварійного сповіщення, LRIT (система далекої ідентифікації і стеження), тощо.

Рис. 1. Завадостійка антена GAJT-710MS від компанії NovAtel Inc. [2]

Таким чином, ГНСС з огляду на її потенційну низьку стійкість до завад та вразливість до зовнішніх навмисно створених втручань (атак) обумовлюють критичність ГНСС для належного функціонування залежних від неї сервісів. Практичний досвід спостережень різними інституціями підтверджує критичний вплив ГНСС на інші суднові системи. Так, Інститутом зв'язку та навігації німецького аерокосмічного центру було проведено серію натурних досліджень завадової обстановки на найважливіших морських шляхах. Результати досліджень знайшли своє відображення у доповіді "Виявлення навмисних та ненавмисних завад для ГНСС в морському судноплавстві", яка була представлена на конференції Інституту навігації ION GNSS у Майамі, США у вересні 2018 р. [24]. В результаті річного експерименту в океані були виявлені різноманітні штучні завади ГНСС на всьому шляху судна. Більшість завад було виявлено у великих портових районах, трохи менше завад було зафіксовано під час руху корабля вздовж берегів. У відкритому океані також було виявлено завади, хоча й фіксувалися вони набагато рідше.

Небезпека штучних завад під час використання ГНСС для навігації у торговельному судноплавстві очевидна. ІМО відзначило потребу в подальшому підвищенні надійності, відмовостійкості та цілісності обладнання містка та навігаційної інформації як одну з найважливіших у своєму плані реалізації стратегії E-Navigation [13].

У цивільному секторі пошук рішень для згладжування наслідків збоїв у ГНСС просувався у напрямку покращення стійкості та цілісності рішень PNT. Така постановка припускає багатоваріантність рішень.

1. Характеристики навігаційних даних

Базові характеристики навігаційних даних: точність, цілісність, доступність і безперервність визначені в нормативних документах ІМО в контексті морської навігації: Revised Maritime Policy and Requirements for Future Global Navigation Satellite System (GNSS), IMO Resolution A.915(22), Jan. 2002 та Worldwide Radionavigation System, IMO Resolution A.1046(27), Dec. 2011 [15].

Вимоги до експлуатаційних параметрів будь-якого морського обладнання, призначеного для отримання навігаційних PNT даних, формуються на базі цих 4 взаємозалежних характеристик.

Прийнята багато років тому Резолюція А.915(22), встановлює морські експлуатаційні вимоги до характеристик загальної навігації та ряду спеціалізованих морських додатків, враховує майбутні вимоги до GNSS, але не визначає часових рамок та способів виконання цих вимог.

Згодом, у Резолюції А.1046(27) [15], було змінено вимоги до характеристики "безперервність" (continuity), і додано вимогу наявності на суднах засобів прийому сигналів від відповідних радіонавігаційних систем протягом усього рейсу, що виконується, як для судноводіння у відкритому океані, так і на підходах до гаваней і в прибережних водах (Таблиця 1).

Таблиця 1. Вимоги до морських експлуатаційних параметрів згідно Резолюції ІМО А.1046.

(розроблені авторами за даними [15])

Фаза рейсу	Точність	Безперервність	Цілісність	Доступність	Інтервал оновлення
Відкритий океан	100 м (95%)	Немає даних	Коли попередження стане можливим	99,8%	2 с
Підходи до портів і прибережні води	10 м (95%)	≥99,97% (15 хвилин)	10 с	99,8%	2 с

Обидві резолюції А.915(22), 2002 р. та А.1046(27), 2011 р. на сьогодні мають статус чинних. Дані для характеристик: точність, цілісність, доступність та безперервність позиціонування, зазначені в них, є актуальними та відображають вимоги морського судноплавства.

2. Визначення

Міжнародна морська організація (IMO) дає наступні визначення термінам, пов'язаним з PNT:

Цілісність (integrity): *здатність системи своєчасно надавати попередження у випадках, коли її не можна використовувати для навігації*. Цілісність забезпечується за рахунок контролю і є безперервним процесом визначення того, чи дозволяють експлуатаційні якості системи (або окремі спостереження) використовувати її для цілей навігації.

Концепція цілісності на рівні користувача полягає у тому, що відповідальність за достовірність позиціонування поділяють між собою як навігаційний приймач користувача, так і система. Найбільший припустимий рівень помилки визначення місцезнаходження називається горизонтальним лімітом попередження (англ. Horizontal Alert Limit, HAL). У разі розпізнавання ситуації, коли визначення місцезнаходження проводиться з помилкою, що перевищує HAL, приймач повинен видати користувачеві відповідне попередження.

Точність (accuracy)**:** *міра відповідності між розрахованим та істинним місцезнаходженням споживача*. Характеристики точності зазвичай представлені як статистичні виміри системної помилки.

Безперервність (continuity)**:** *здатність системи здійснювати навігаційне обслуговування споживачів протягом заданого інтервалу часу без відмов та перерв*.

Доступність (availability)**:** *здатність системи (експлуатаційна готовність) забезпечувати проведення навігаційних визначень із заданими характеристиками точності.*

Примітка - Експлуатаційна готовність ГНСС виражається у відсотках часу на певному інтервалі часу, протягом якого забезпечуються задані умови.

Стійке позиціонування, навігація та синхронізація (Resilient PNT) - це об'єднання традиційних технологій позиціонування, навігації та синхронізації з нетрадиційними та новими технологіями для підвищення надійності, експлуатаційних характеристик та безпеки критично важливих застосувань. Стійкість гарантує надійну інформацію про час і місцезнаходження шляхом захисту, аутентифікації та запровадження альтернатив існуючим джерелам PNT, таким як ГНСС.

Стійкість (resilience) PNT визначається як: *"здатність системи готуватися до змінних умов, адаптуватися до них, а також протистояти їм і швидко відновлюватися після збоїв"*. Акцент на відновлення є важливим, тому що саме це відрізняє стійкість від надійності. У контексті морської навігації, дії щодо забезпечення стійкості включають:

1. Забезпечення "Цілісності на рівні користувача" - гарантує, що рішення щодо визначення позиції є стійким до будь-якої довільної несправності або збою, який може статися внаслідок різних причин, наприклад, кібератаки, несприятливої космічної погоди, навмисних завад.
2. Забезпечення підтримки від альтернативних систем і датчиків, щоб уникнути порушення безперервності при втраті даних ГНСС, наприклад, через попередження про порушення цілісності, виявлення глушіння (Jamming) або імітаційних завад (Spoofing).

При виявленні таких ефектів на рівні користувача, очікується, що навігаційна апаратура ГНСС проінформує користувача про проблему і, можливо, вдасться до будь-яких дій для видалення помилкових вимірювань з навігаційного рішення або забезпечити безперебійну навігацію шляхом перемикання на альтернативну навігаційну систему, наприклад, на одну з доступних наземних мереж забезпечення PNT [9].

3. *Архітектура мультисистемного суднового радіонавігаційного* приймача

Визнаючи нагальну потребу у стійкому способі отримання даних PNT в електронній навігації, IMO прийняла в 2015 році Резолюцію MSC.401(95) "Експлуатаційні вимоги до мультисистемних суднових радіонавігаційних приймачів" [16]. Документ фактично визначив генеральний напрям вирішення цієї проблеми: застосування мультисистемних радіонавігаційних приймачів (MSR), які підтримують використання одразу декількох ГНСС (наприклад, Galileo та GPS) та інших джерел. Простий приймач GPS використовує лише одну глобальну навігаційну супутникову систему, тоді як приймачі ГНСС з кількома сузір'ями отримують інформацію від багатьох таких систем одночасно, що дозволяє їм "бачити" набагато більше супутників у будь-який момент часу.

Як показано на рисунку 2, базова ідея побудови MSR полягає у використанні всіх доступних сигналів, а не тільки ГНСС [14].

Концептуально мультисистемний приймач (MSR) має два рівня: сенсорний (sensor) та рівень обробки (Position, Velocity, Timing Data Processing, PVT-DP), вихідні дані яких містять інформацію про швидкість, позицію та час, а також дані про цілісність та стан.

Архітектура MSR формує основу для інтеграції даних від суднових сенсорних систем (гірокомпас, лаг, тощо). Програмна обробка даних PNT (PNT-DP) може бути реалізована самим MSR (рис. 2) або інтегрована як програмний модуль в суднові навігаційні системи, такі як INS, ECDIS або RADAR, як показано на рисунку 3 [14].

Обробка даних PNT у Настанові MSC.1/Circ.1575, визначається як набір функцій, що забезпечуються:

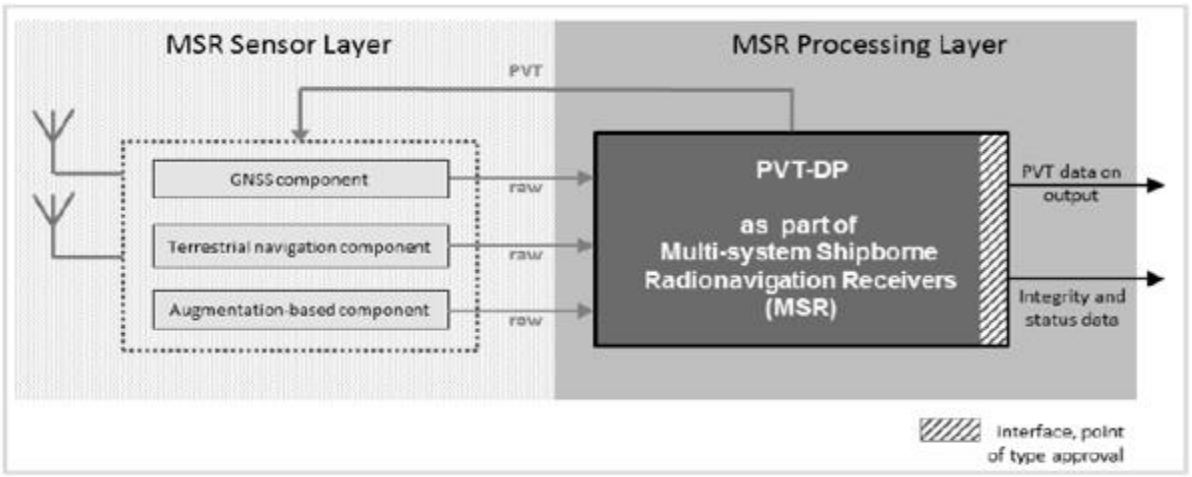

Рис. 2. Архітектура мультисистемного радіонавігаційного приймача [14].
MSR Sensor Layer – Рівень сенсорів мультисистемних приймачів; MSR Processing Layer – Рівень обробки (даних) мультисистемних приймачів; GNSS component – компонент ГНСС; Terrestrial navigation component – наземний навігаційний компонент; Augmentation-based component – компонент (системи), що доповнює; raw – первинна (інформація)

А. Чисельними джерелами даних, що надаються датчиками та службами, що відносяться до PNT (наприклад, приймач GNSS/DGNSS), та іншими бортовими датчиками та системами, що надають дані в реальному часі (наприклад, радіолокаційна станція, гірокомпас, обладнання для вимірювання швидкості та відстані (Speed and distance measurement equipment, SDME), ехолот) для створення та використання надмірності у вхідних даних, що відносяться до PNT;

Б. Мультисистемними та мультисенсорними методами для покращення надання PNT даних.

Таким чином, настанова [14] визначає модульну архітектуру як основу для подальшого вдосконалення надання суднових даних PNT, що досягається за рахунок:

1. узгодження та стандартизації вимог до надання суднових даних PNT з урахуванням різноманітності типів суден, морських завдань, морських додатків та складності ситуацій, що змінюються, аж до індивідуальних рівнів підтримки;

2. визначення залежності між джерелами даних, що відносяться до PNT (датчики та послуги), відповідними методами обробки PNT даних (методи і порогові значення) та досяжними рівнями експлуатаційних характеристик даних PNT (точність, цілісність, безперервність і доступність);

3. гармонізація та вдосконалення бортової обробки PNT даних на основі модульного підходу для поліпшення адаптації вимог до характеристик щодо морських завдань, різних типів суден, морських додатків та з урахуванням потреб користувачів (SN.1/Circ.274);

4. послідовного та скоординованого запровадження контролю цілісності даних та системи як інтелектуального засобу захисту даних PNT від порушень, помилок та збоїв у роботі (безпека), а також вторгнень зловмисників;

5. стандартизації вихідних даних PNT, включаючи виведення даних про цілісність та стан.

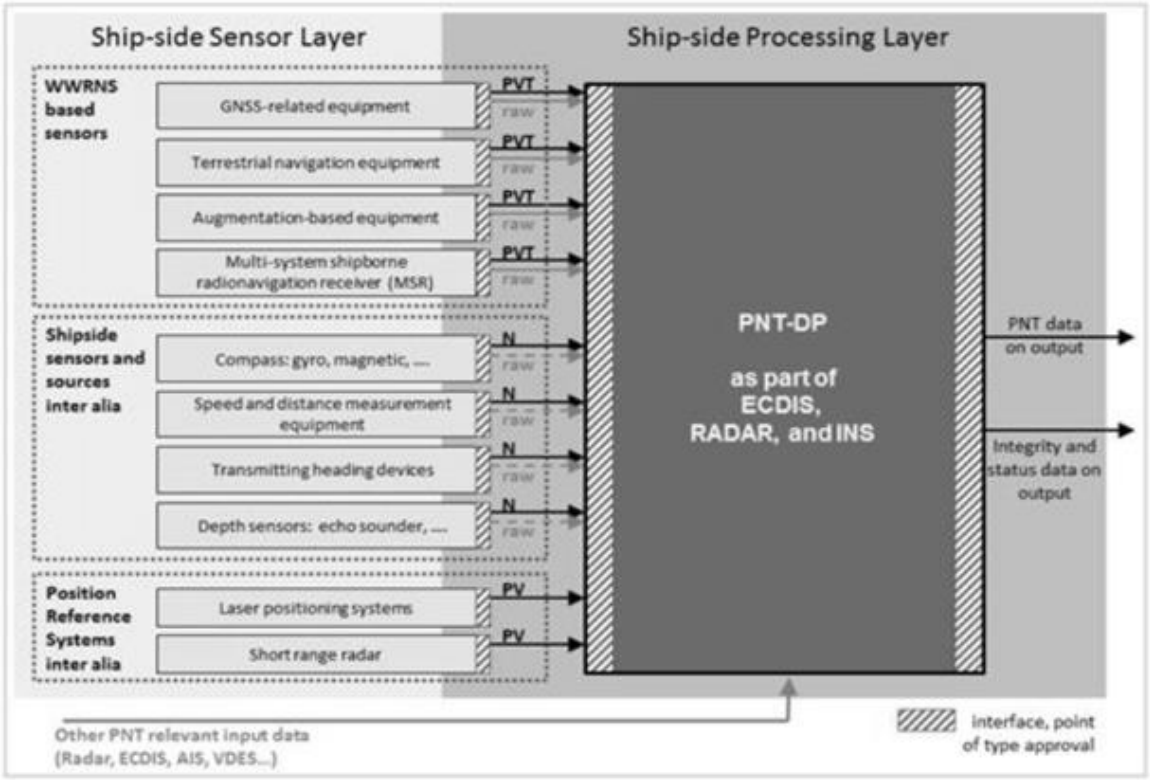

Рис. 3. Архітектура мультисенсорного модуля обробки PNT даних для використання в інтегрованих системах [14].

Worldwide Radionavigation Systems (WWRNS) based sensors – датчики всесвітньої радіонавігаційної системи; Shipside sensors and sources inter alia – суднові датчики та джерела, наприклад; Position Reference Systems inter alia – системи визначення координат по опорним точкам, наприклад; Position, velocity, time (PVT) – координати, швидкість, час; Navigation (N) – навігація; Position, velocity (PV) – координати, швидкість

Дані про цілісність можуть бути надані:

(a) як прапори, або

(b) як дані, що показують розрахункову точність.

Введенням в дію згаданих вище стандартів, ІМО фактично задала універсальний напрямок руху до підвищення точності, стійкості та цілісності навігаційних даних. Вони дозволяють використовувати різні комбінації визнаних ІМО Всесвітніх радіонавігаційних

систем (WWRNS) з наземними системами визначення місцезнаходження, а також іншими системами широкої дії.

Зростаюча кількість доступних сигналів для розрахунку відстані від різних джерел, сприяє підвищенню точності визначення місцезнаходження і пов'язаної з цим цілісності.

4. Дослідницькі проекти

Резервування для GNSS за рахунок використання різних наземних сервісів в даний час проходить стадію дослідження та апробації в рамках низки європейських проектів MarRINav - Maritime Resilience and Integrity in Navigation [25] та R-Mode Baltic - Baseline and Priorities [27], де аналізується використання в MSR таких наземних систем, як e-LORAN, e-Racons або майбутніх технологій, таких як R-Mode [6].

У той же час, не існує конкретного переліку "інших джерел даних для визначення розташування", що підключаються до MSR.

IMO заявила, що "було б передчасно виділяти будь-яку конкретну систему до доопрацювання вимог користувачів до електронної навігації" [20].

Також хотілося б звернути увагу на виконуваний в даний час під егідою Європейського агентства GNSS (EUSPA) проект ASGARD (Advanced Shipborne Galileo Receiver Double Frequency) [1].

Проект ASGARD - це дослідницький проект орієнтований на розробку суднового двочастотного приймача з кількома сузір'ями, який повинен використовувати європейські GNSS (European Geostationary Navigation Overlay Service (EGNOS) та Galileo), відповідати вимогам міжнародних стандартів: IEC 61108-1;3 [10, 11], IMO MSC 401 (95) [16], MSC 432 (98) [18] та використовувати механізм аутентифікації Galileo OS-NMA (Open Service Navigation Message Authentication) [5].

Мета ASGARD - підвищення популярності GNSS Galileo на морському транспорті та створення відносно дешевого та ефективного обладнання.

У резолюціях IMO MSC.401(95) і MSC.432(98) зазначено, що суднове обладнання повинне використовувати принаймні дві незалежні ГНСС та повинно мати можливість обробляти додаткові дані. Ця вимога може бути виконана, якщо приймач GNSS відстежує як Galileo так і GPS, а також використовує EGNOS для отримання диференціальної поправки та даних про цілісність. А поєднання з послугою аутентифікації для навігаційного повідомлення Galileo OS-NMA сприятиме реалізації концепції стійких навігаційних даних PNT в умовах дії навмисних завад.

Galileo OS-NMA забезпечує цифрові підписи навігаційних повідомлень Galileo Open Service. Це дає приймачам з підтримкою Galileo OS-MNA засіб для перевірки того, що отримані навігаційні дані Galileo надходять від супутника Galileo і не були сфальсифіковані.

На завершення відзначимо, що на сьогоднішній день, незважаючи на відмінності у підходах і, відповідно, у технічних рішеннях, спостерігається зростання взаємопроникнення рішень між цивільним і військовим секторами. При цьому спроби пошуку, виділення та обґрунтування якогось одного – найкращого з точки зору завадозахищеності навігаційної апаратури користувача ГНСС технічного рішення, позбавлені сенсу. Різні технічні рішення апаратури користувача ГНСС, з різним ступенем забезпечення завадозахищеності, мають право на використання. Вибір багато в чому визначається особливостями та призначенням мобільної платформи, де встановлено навігаційне обладнання PNT.

Висновки і перспектива подальшої роботи по даному напрямку

1. Навігаційна апаратура користувачів ГНСС зберігає провідну роль у забезпеченні морської навігації даними PNT.

2. Рішення щодо забезпечення стійких даних PNT на військових кораблях і цивільних суднах (мобільних морських платформах) активно розвиваються, взаємно впливають і при цьому часто доповнюють один одного.

3. Універсальний напрямок підвищення стійкості та цілісності даних PNT для цивільних суден вже задано IMO - це мультисистемний судновий радіонавігаційний приймач (MSR), який має одночасно використовувати кілька джерел інформації для визначення позиції, серед яких GNSS є основними, але не єдиними.

4. Формування нормативної бази для MSR поки що не завершено. Стандарт IEC, в якому регламентуються питання випробувань обладнання MSR, знаходиться у розробці. Однак у Настанові MSC.1/circ.1575 вже стандартизовано виведення даних PNT, а також даних про цілісність та стан у формі генерації обов'язкового набору інформаційних повідомлень згідно з IEC 61162-1 [12]. Це дозволить легко інтегрувати різні рішення MSR від різних виробників до навігаційної системи корабля при модернізації обладнання містка.

5. На сьогоднішній день на ринку відсутні MSR, що серійно випускаються та сертифіковані на відповідність стандартам IMO MSC 401 (95) та MSC.1/circ.1575. Як рішення, що сприяє забезпеченню стійкості даних PNT, можна відзначити ГНСС приймачі з адаптивними антенними решітками (технологія CRPA), а також багаточастотні та мультисистемні приймачі ГНСС.

Рекомендації для подальших досліджень:

1. Вбачається доцільним подовжити дослідження у напрямку вдосконалення дистанційної діагностики завадової обстановки ГНСС у зоні відповідальності берегових служб.

На підходах до портів, у прибережних водах і узкостях, безпека мореплавання забезпечується не тільки судноводіями, а й операторами берегових служб: СРРС (служба регулювання руху суден), МПРС (Морська пошуково-рятувальна служба) та інших. Для операторів берегових систем також важливо отримувати інформацію щодо цілісності рішень PNT на суднах. Вирішення завдання дистанційної діагностики завадової обстановки на суднах у зоні відповідальності берегових служб є актуальним і є важливим інформаційним компонентом системи морської ситуаційної обізнаності.

2. З огляду на впровадження на морських суднах процедури управління кіберризиками [17, 19] продовжити дослідження в напрямку розвитку національного правового і науково-навчального забезпечення у сфері морської кібербезпеки.

ЛІТЕРАТУРА

1. *Advanced Shipborne Galileo Receiver Double Frequency (Project ASGARD).* [Online]. Available: https://asgard.gmv.com/wp-content/uploads/2022/06/ASGARD-Technical-Brochure.pdf. (дата звернення: 15.03.2023).

2. *Anti-Jam Antenna for Marine*. [Online]. Available: https://www.unmannedsystems technology.com/company/novatel/gajt-710ms-anti-jam-antenna-for-marine/ (дата звернення: 15.03.2023).

3. Buesnel G., "Thousands of GNSS Jamming and Spoofing Incidents Reported in 2020," December 2, 2020. [Online]. Available: https://rntfnd.org/2020/12/24/thousands-of-gnss-jamming-and-spoofing-incidents-reported-in-2020-guy-buesnel/. (дата звернення: 15.03.2023).

4. Burgess M., "GPS Signals Are Being Disrupted in Russian Cities," December 15, 2022. [Online]. Available: https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story /gps-jamming-interference-russia-ukraine/amp. (дата звернення: 15.03.2023).

5. Chen X., Luo R., Liu T., Yuan H., Wu H., "Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS," *Remote Sensing, vol.* 15(5):1462, doi: https://doi.org/10.3390/rs15051462, 2023.

6. Gewies S., Grundhöfer L., Hehenkamp N., "Availability of Maritime Radio Beacon Signals for R-Mode in the Southern Baltic Sea," *TransNav, The International Journal on Marine*

Navigation and Safety of Sea Transportation, vol. 14(1), DOI: 10.12716/1001.14.01.21, pp. 173-178, March, 2020.

7. Goudossis A., Katsikas S.K., "Towards a Secure Automatic Identification System (AIS)," *Journal of Marine Science and Technology*, vol. 24(2), pp. 410-423, DOI: 10.1007/s00773-018-0561-3, June, 2019.
8. Goward D.A., "Why Isn't Russia jamming GPS harder in Ukraine?" July 22, 2022. [Online]. Available: https://www.c4isrnet.com/opinion/2022/07/22/why-isnt-russia-jamming-gps-harder-in-ukraine/.
9. Hansen A., Mackey S., Wassaf H., et al, "Complementary PNT and GPS Backup Technologies Demonstration Report," Cambridge (MA): U.S. Department of Transportation, John A Volpe National Transportation Systems Center, Report DOT-VNTSC-20-07. 2021, January. [Online]. Available: https://www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20CongressCombinedv2_January%202021.pdf.
10. IEC 61108-1:2003, *Maritime navigation and radio communication equipment and systems - Global navigation satellite systems (GNSS) - Part 1: Global positioning system (GPS) - Receiver equipment - Performance standards, methods of testing and required test results*. 2003.
11. IEC 61108-3:2010, *Maritime navigation and radiocommunication equipment and systems - Global navigation satellite systems (GNSS) - Part 3: Galileo receiver equipment - Performance requirements, methods of testing and required test results.* 2010.
12. IEC 61162-1:2016, *Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 1: Single talker and multiple listeners*. 2016.
13. IMO MSC.1/Circ.1595, *E-NAVIGATION STRATEGY IMPLEMENTATION PLAN – UPDATE 1. 25 May 2018*. [Online]. Available: https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx.
14. IMO MSC.1/Circular.1575, *Guidelines for Shipborne Position, Navigation And Timing (PNT) Data Processing*. 2017. [Online]. Available: https://www.imorules.com/MSCCIRC_1575.html.
15. IMO Resolution A.1046(27), *Worldwide Radionavigation System*. Dec, 2011.
16. IMO Resolution MSC.401(95), *Performance Standards For Multi-System Shipborne Radionavigation Receivers. Adopted 8 June 2015*. [Online]. Available: https://www.imorules.com /MSCRES_401.95.html.
17. IMO Resolution MSC.428(98), *Maritime Cyber Risk Management in Safety Management Systems*. 2017.
18. IMO Resolution MSC.432(98), *Amendments to performance standards for multi-system shipborne radionavigation receivers*. 2017.
19. IMO Resolution MSC-FAL.1/Circ.3, *Guidelines on Maritime Cyber Risk Management*. 2021.
20. IMO SUB-COMMITTEE ON SAFETY OF NAVIGATION NAV 53/22, *Report of the E-Navigation Working Group. i.13.24: session paper. 14 August 2007*. [Online]. Available: https://www.safety4sea.com/wp-content/uploads/2014/09/pdf/nav53-22.pdf.
21. *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)*. INTERTANKO, 2019. [Online]. Available: https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

22. López M., Antón V., "SBAS/EGNOS Enabled Devices in Maritime," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 12(1), pp. 23-27. DOI: 10.12716/1001.12.01.01, March, 2018.

23. Major F.G., *Quo Vadis: Evolution of Modern Navigation. The Rise of Quantum Techniques*. Springer, 2013.

24. Marcos E. Pérez, Konovaltsev A., Caizzone, S., et al, "Interference and Spoofing Detection for GNSS Maritime Applications using Direction of Arrival and Conformal Antenna Array," *31st International Technical Meeting of the Satellite Division of The Institute of Navigation:* conference paper. ION GNSS+, pp. 2907-2922. https://doi.org/10.33012/2018.15901, 2018.

25. MarRINav, *Maritime Resilience and Integrity in Navigation*. [Online]. Available: https://marrinav.com. (дата звернення: 15.03.2023).

26. Oruç A., Gkioulos V., Katsikas S., "Towards a Cyber-Physical Range for the Integrated Navigation System (INS)," *Journal of Marine Science and Engineering*, vol. 10, 107, DOI: 10.3390/jmse10010107, 2022.

27. R-Mode Baltic, *Baseline and Priorities*. [Online]. Available: https://interreg-baltic.eu/project/r-mode-baltic/. (дата звернення: 15.03.2023).

28. Świerczyński S., Zwolan P., Rutkowska I., "Jamming as a Threat to Navigation," *ANNUAL OF NAVIGATION*, vol. 23/2016, pp. 219-233, DOI: 10.1515/aon-2016-0016, 2016. [Online]. Available: https://www.researchgate.net/publication/316358430_Jamming_as_a_Threat_to_Navigation.

29. *The Guidelines on Cyber Security Onboard Ships, version 4*. BIMCO et al, 2020. [Online]. Available: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

30. Weintrit A., "The Concept of Time in Navigation," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 11(2), DOI: 10.12716/1001.11.02.01, pp. 209-219, June, 2017.

31. Westbrook T., "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," *Journal of Strategic Security*, vol. 12(2), pp. 1-16. DOI: 10.5038/1944-0472.12.2.1720, 2019.

REFERENCES

1. *Advanced Shipborne Galileo Receiver Double Frequency (Project ASGARD)*. [Online]. Available: https://asgard.gmv.com/wp-content/uploads/2022/06/ASGARD-Technical-Brochure.pdf. [Accessed: 15.03.2023].

2. *Anti-Jam Antenna for Marine*. [Online]. Available: https://www.unmannedsystemstechnology.com/company/novatel/gajt-710ms-anti-jam-antenna-for-marine/ [Accessed: 15.03.2023].

3. Buesnel G., "Thousands of GNSS Jamming and Spoofing Incidents Reported in 2020," December 2, 2020. [Online]. Available: https://rntfnd.org/2020/12/24/thousands-of-gnss-jamming-and-spoofing-incidents-reported-in-2020-guy-buesnel/. [Accessed: 15.03.2023].

4. Burgess M., "GPS Signals Are Being Disrupted in Russian Cities," December 15, 2022. [Online]. Available: https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/gps-jamming-interference-russia-ukraine/amp. [Accessed: 15.03.2023].

5. Chen X., Luo R., Liu T., Yuan H., Wu H., "Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS," *Remote Sensing, vol.* 15(5):1462, doi: https://doi.org/10.3390/rs15051462, 2023.

6. Gewies S., Grundhöfer L., Hehenkamp N., “Availability of Maritime Radio Beacon Signals for R-Mode in the Southern Baltic Sea,” *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 14(1), DOI: 10.12716/1001.14.01.21, pp. 173-178, March, 2020.

7. Goudossis A., Katsikas S.K., “Towards a Secure Automatic Identification System (AIS),” *Journal of Marine Science and Technology*, vol. 24(2), pp. 410-423, DOI: 10.1007/s00773-018-0561-3, June, 2019.

8. Goward D.A., “Why Isn't Russia jamming GPS harder in Ukraine?” July 22, 2022. [Online]. Available: https://www.c4isrnet.com/opinion/2022/07/22/why-isnt-russia-jamming-gps-harder-in-ukraine/.

9. Hansen A., Mackey S., Wassaf H., et al, “Complementary PNT and GPS Backup Technologies Demonstration Report,” Cambridge (MA): U.S. Department of Transportation, John A Volpe National Transportation Systems Center, Report DOT-VNTSC-20-07. 2021, January. [Online]. Available: https://www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20CongressCombinedv2_January%202021.pdf.

10. IEC 61108-1:2003, *Maritime navigation and radio communication equipment and systems - Global navigation satellite systems (GNSS) - Part 1: Global positioning system (GPS) - Receiver equipment - Performance standards, methods of testing and required test results*. 2003.

11. IEC 61108-3:2010, *Maritime navigation and radiocommunication equipment and systems - Global navigation satellite systems (GNSS) - Part 3: Galileo receiver equipment - Performance requirements, methods of testing and required test results.* 2010.

12. IEC 61162-1:2016, *Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 1: Single talker and multiple listeners*. 2016.

13. IMO MSC.1/Circ.1595, *E-NAVIGATION STRATEGY IMPLEMENTATION PLAN – UPDATE 1. 25 May 2018*. [Online]. Available: https://www.imo.org/en/OurWork/Safety/Pages/eNavigation.aspx.

14. IMO MSC.1/Circular.1575, *Guidelines for Shipborne Position, Navigation And Timing (PNT) Data Processing*. 2017. [Online]. Available: https://www.imorules.com/MSCCIRC_1575.html.

15. IMO Resolution A.1046(27), *Worldwide Radionavigation System*. Dec, 2011.

16. IMO Resolution MSC.401(95), *Performance Standards For Multi-System Shipborne Radionavigation Receivers. Adopted 8 June 2015*. [Online]. Available: https://www.imorules.com /MSCRES_401.95.html.

17. IMO Resolution MSC.428(98), *Maritime Cyber Risk Management in Safety Management Systems*. 2017.

18. IMO Resolution MSC.432(98), *Amendments to performance standards for multi-system shipborne radionavigation receivers*. 2017.

19. IMO Resolution MSC-FAL.1/Circ.3, *Guidelines on Maritime Cyber Risk Management*. 2021.

20. IMO SUB-COMMITTEE ON SAFETY OF NAVIGATION NAV 53/22, *Report of the E-Navigation Working Group. i.13.24: session paper. 14 August 2007*. [Online]. Available: https://www.safety4sea.com/wp-content/uploads/2014/09/pdf/nav53-22.pdf.

21. *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)*. INTERTANKO, 2019. [Online]. Available: https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

22. López M., Antón V., "SBAS/EGNOS Enabled Devices in Maritime," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 12(1), pp. 23-27. DOI: 10.12716/1001.12.01.01, March, 2018.

23. Major F.G., *Quo Vadis: Evolution of Modern Navigation. The Rise of Quantum Techniques*. Springer, 2013.

24. Marcos E. Pérez, Konovaltsev A., Caizzone, S., et al, "Interference and Spoofing Detection for GNSS Maritime Applications using Direction of Arrival and Conformal Antenna Array," *31st International Technical Meeting of the Satellite Division of The Institute of Navigation:* conference paper. ION GNSS+, pp. 2907-2922. https://doi.org/10.33012/2018.15901, 2018.

25. MarRINav, *Maritime Resilience and Integrity in Navigation*. [Online]. Available: https://marrinav.com. [Accessed: 15.03.2023].

26. Oruç A., Gkioulos V., Katsikas S., "Towards a Cyber-Physical Range for the Integrated Navigation System (INS)," *Journal of Marine Science and Engineering*, vol. 10, 107, DOI: 10.3390/jmse10010107, 2022.

27. R-Mode Baltic, *Baseline and Priorities*. [Online]. Available: https://interreg-baltic.eu/project/r-mode-baltic/. [Accessed: 15.03.2023].

28. Świerczyński S., Zwolan P., Rutkowska I., "Jamming as a Threat to Navigation," *ANNUAL OF NAVIGATION*, vol. 23/2016, pp. 219-233, DOI: 10.1515/aon-2016-0016, 2016. [Online]. Available: https://www.researchgate.net/publication/316358430_Jamming_as_a_Threat_to_Navigation.

29. *The Guidelines on Cyber Security Onboard Ships, version 4*. BIMCO et al, 2020. [Online]. Available: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

30. Weintrit A., "The Concept of Time in Navigation," *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 11(2), DOI: 10.12716/1001.11.02.01, pp. 209-219, June, 2017.

31. Westbrook T., "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," *Journal of Strategic Security*, vol. 12(2), pp. 1-16. DOI: 10.5038/1944-0472.12.2.1720, 2019.