UDC 656.627.7 **DOI: 10.31653/2306-5761.39.2026.127-142**

USE OF AIS AIDS TO NAVIGATION TO IMPROVE SHIPPING SAFETY IN MODERN CONDITIONS

ВИКОРИСТАННЯ АІС ЗАСОБІВ НАВІГАЦІЙНОГО ОБЛАДНАННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ СУДНОПЛАВСТВА В СУЧАСНИХ УМОВАХ

A. Buha, *senior lecturer*, **V. Korniyuk**, *lecturer*, **V. Stepanenko**, *Ph.D., professor*

А.О. Буга, *ст. викладач кафедри Судноводіння,* **В.Я. Корніюк,** *викладач кафедри Судноводіння,* **В.В. Степаненко,** *Ph.D., професор*

Institute of Naval Forces of the National University "Odesa Maritime Academy", Ukraine

Інститут Військово-Морських Сил Національного університету «Одеська морська академія», Україна

ABSTRACT

The article examines modern approaches to ensuring maritime safety through the use of both traditional and innovative aids to navigation on seaways. A comparative analysis of the functioning of physical (visual) navigation aids and AIS-based aids to navigation (AIS AtoN) is presented.The main operational characteristics of traditional navigation aids are identified, along with their advantages and limitations under various hydro-meteorological conditions. Special attention is given to AIS-based aids to navigation, including physical, virtual, and synthetic AIS AtoN. Their operational principles, data transmission features, and representation on onboard navigation systems are analyzed. It is established that AIS AtoN provide high information availability regardless of weather conditions and enable rapid deployment for marking navigational hazards. At the same time, the study identifies key limitations associated with AIS AtoN, including positioning inaccuracies, potential technical failures and vulnerability to radio interference and signal manipulation. The feasibility of the integrated use of physical and AIS-based navigation equipment to enhance the level of maritime safety has been substantiated, and an upgrade option using controlled reception pattern antennas (CRPA) has been proposed to prevent the impact of false positioning signals.

Keywords: aids to navigation, AIS AtoN, e-Navigation, maritime safety, virtual navigation aids, CRPA.

Date received: 12-03-2026
Date accepted: 22-05-2026
Date published (online): 31-05-2026

Cite this article as: A. Buha, V. Korniyuk, V. Stepanenko, "Use of AIS aids to navigation to improve shipping safety in modern conditions," *Shipping & Navigation*, no. 39, pp. 127-142, 2026, doi: 10.31653/2306-5761.39.2026.127-142.

АНОТАЦІЯ

У статті розглянуто сучасні підходи до забезпечення безпеки мореплавання із застосуванням традиційних та інноваційних засобів навігаційного обладнання морських шляхів. Проведено порівняльний аналіз функціонування фізичних (візуальних) засобів навігації та засобів, що базуються на використанні автоматичної ідентифікаційної системи (AIS AtoN).Визначено основні експлуатаційні характеристики традиційних засобів навігаційного обладнання, таких як маяки, буї та навігаційні знаки, а також проаналізовано їх переваги та обмеження в різних гідрометеорологічних умовах. Особливу увагу приділено аналізу засобів навігаційного обладнання на базі AIS, зокрема фізичних, віртуальних та синтетичних AIS AtoN. Розглянуто принципи їх функціонування, особливості передачі інформації та відображення в суднових навігаційних системах. Встановлено, що AIS-засоби забезпечують високу інформативність та незалежність від погодних умов, а також дозволяють оперативно позначати навігаційні небезпеки. Разом з тим визначено основні ризики використання AIS AtoN, пов'язані з можливими похибками позиціонування, технічними несправностями та впливом радіоелектронних завад. Наголошено на необхідності належної підготовки судноводіїв для ефективного використання таких засобів. Обґрунтовано доцільність комплексного застосування фізичних та AIS-засобів навігаційного обладнання з метою підвищення рівня безпеки судноплавства та запропоновано варіант модернізації за допомогою приймальних антен з контрольованою діаграмою спрямованості (CRPA) для унеможливлення впливу хибних сигналів позиціонування.

Ключові слова: навігаційне обладнання, AIS AtoN, e-Navigation, безпека мореплавання, віртуальні засоби навігації, CRPA.

Постановка проблеми в загальному вигляді та її зв'язок з важливими науковими або практичними завданнями

У сучасних умовах інтенсивного розвитку морського транспорту, зростання обсягів перевезень та ускладнення умов судноплавства особливої актуальності набуває підвищення ефективності навігаційного забезпечення. Засоби навігаційного обладнання (ЗНО) є ключовим елементом системи безпеки мореплавання, забезпечуючи орієнтування суден, позначення навігаційних небезпек та підтримку безпечного руху на водних шляхах.

Традиційно ЗНО представлені фізичними (візуальними) засобами, такими як маяки, буї, навігаційні знаки та інші інженерні споруди. Водночас розвиток концепції електронної навігації (e-Navigation) [1] зумовив появу нових підходів до організації навігаційного забезпечення, зокрема із застосуванням технології автоматичної ідентифікаційної системи (AIS).

Використання AIS як засобу навігаційного обладнання (AIS AtoN) відкриває нові можливості щодо підвищення оперативності, гнучкості та інформативності навігаційного забезпечення, однак одночасно породжує низку технічних та експлуатаційних обмежень.

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

Сучасні дослідження AIS AtoN розглядають такі засоби не як самостійну заміну традиційного навігаційного обладнання, а як елемент комплексної системи ситуаційної обізнаності, що поєднує фізичні AtoN, ECDIS, РЛС, VTS та берегову цифрову інфраструктуру. У працях R. G. Wright і M. Baldauf [2] та M. Jurcovic [3] показано практичне значення віртуальних і синтетичних AIS AtoN для оперативного позначення небезпек, контролю положення плавучих знаків, а також для роботи на внутрішніх водних шляхах, де необхідно враховувати радіовидимість, енергоспоживання, навантаження на VHF-канали та точність позиціонування буїв.

Окремий блок джерел присвячений віртуальним AtoN, які дають змогу швидко попередити екіпаж про нову або тимчасову небезпеку до встановлення фізичного знака. Результати міжнародного опитування щодо

AIS AtoN [4], оглядові матеріали Канадської берегової охорони [5], документи CESNI/RIS щодо застосування AIS AtoN на внутрішніх водних шляхах [6] та матеріали European Boating Association [7] підтверджують доцільність такого підходу, але водночас наголошують, що віртуальний знак не повинен безумовно сприйматися як рівноцінний фізичному засобу навігаційного обладнання.

У роботі [8] проаналізовано стійкість супутникової навігації на морі в умовах ненавмисних і навмисних завад, зокрема jamming і spoofing, а також обґрунтовано потребу в резервуванні PNT-даних та просторовій обробці сигналів. У статті [9] запропоновано підхід до автентифікації AIS-повідомлень на основі цифрового водяного знаку, а в роботі [10] розглянуто розвиток морського VHF-радіозв'язку як комунікаційної основи безпечної навігації. Ці праці дають підстави розглядати проблему AIS AtoN не лише як питання відображення навігаційних символів, а й як питання кіберстійкості каналу зв'язку та достовірності джерела даних.

Разом із тим у науковій літературі підкреслюється, що відкритий характер AIS-радіоканалу створює передумови для маніпуляції даними, підміни ідентифікації, формування хибних цілей та спотворення координат. Автори робіт [11] та [12] пов'язують маніпуляції AIS із прямими ризиками для безпеки судноплавства, тоді як інша низка робіт [13]–[15] присвячена аналізу технічних варіантів автентифікації AIS, зокрема із застосуванням криптографічних механізмів, відкритих ключів та сумісних із наявною інфраструктурою протоколів.

З огляду на розвиток VDES особливої актуальності набуває IALA Guideline G1192 [16], у якому розглядаються техніки автентифікації VDES-повідомлень, а також дослідження [17], присвячене практичному підходу до VDES Authentication. Ці джерела показують, що захист AIS/VDES-повідомлень має включати не лише перевірку цілісності повідомлення, а й підтвердження авторизованого джерела його формування.

З огляду на зазначений наявний науковий доробок, слід зазначити, що недостатньо розкритим залишається питання поєднання двох рівнів захисту AIS AtoN: захисту GNSS-приймача, від якого залежать координати та часові мітки, і захисту самого AIS/VDES-радіоканалу від підміни повідомлень. Саме тому в цій статті авторський підхід полягає у розгляді AIS AtoN як багатофакторної системи безпеки, де CRPA-антена використовується для підвищення стійкості GNSS-приймача, а автентифікація та цифровий підпис повідомлень — для підвищення довіри до даних, що передаються через AIS/VDES-канал.

Формулювання цілей статті (постановка завдання)

Метою статті є проведення порівняльного аналізу функціонування фізичних, віртуальних і синтетичних AIS-засобів навігаційного обладнання, визначення їх переваг, обмежень та умов ефективного застосування, а також обґрунтування технічних напрямів підвищення стійкості AIS AtoN до GNSS-спуфінгу, радіоелектронних завад і підміни повідомлень.

Наукова новизна роботи полягає у систематизації сучасних підходів до використання AIS AtoN у морській навігації та в обґрунтуванні багаторівневої моделі підвищення їх надійності, яка поєднує комплексне використання фізичних, синтетичних і віртуальних засобів навігаційного обладнання, захист GNSS-приймачів за допомогою CRPA-антен, а також автентифікацію і цифровий підпис AIS/VDES-повідомлень.

Виклад матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Зростання торговельного, промислового та військово-морського флотів, стале підвищення інтенсивності судноплавства, тоннажу та швидкості суден, зростання потенційної небезпеки аварій суден для життя людини та навколишнього середовища вимагають постійної уваги до навігаційно-гідрографічного та гідрометеорологічного забезпечення

безпеки мореплавства. Найважливішою складовою цього забезпечення є навігаційне обладнання морських театрів (океанів і морів), призначене для створення сприятливої в навігаційному відношенні обстановки для визначення місця корабля та вирішення поставлених завдань.

Навігаційне обладнання розглядається як сукупність технічних та організаційних рішень, що проводяться з метою підтримки або розгортання та введення в дію різних засобів навігаційного обладнання (ЗНО). До них належать: планування, техніко-економічне обґрунтування та проєктування розміщення ЗНО, розробка нових та модернізація діючих ЗНО, виконання будівельно-монтажних робіт зі спорудження нових та реконструкції діючих ЗНО, експлуатація, технічне обслуговування та ремонт ЗНО.

Ефективність навігаційного обладнання завжди розглядається у тісному зв'язку з умовами його використання. Головним критерієм ефективності навігаційного обладнання є можливість забезпечення вирішення завдання кораблів у даному районі із заданою точністю в певних умовах.

Забезпеченість ЗНО різних районів оцінюється з урахуванням тактико-технічних характеристик кораблів/суден (водотоннажності, осадки, швидкості, довжини, ширини), для забезпечення плавання яких воно призначене; навігаційно-гідрографічних та гідрометеорологічних умов у зонах дії ЗНО; вимог до точності визначення місця в районах, що випливають з умов плавання, поставлених перед кораблями завдань і рівня технічних засобів, що знаходяться на їх озброєнні.

Ефективність навігаційного обладнання залежить від наступних критеріїв: раціонального розміщення ЗНО на березі та на воді; забезпечення безперебійної дії в установленому режимі; складу технічних засобів, якості їх роботи та їх здібності у будь-який час доби, у певних гідрометеорологічних умовах забезпечити виконання завдання кораблем; методів навігаційно-гідрографічного забезпечення.

Підвищення ефективності навігаційного обладнання досягається постійним удосконаленням цих основних критеріїв.

Зорові ЗНО – спеціальні стаціонарні споруди та конструкції або плавучі пристрої характерної відмінної форми та фарбування, призначені для візуального визначення напрямків та відстаней до них, а також для огородження навігаційних небезпек; обладнуються, як правило, світлооптичними апаратами, що забезпечують відповідну дальність видимості вогню та створюють кругове, спрямоване або секторне освітлення, а також певний характер вогню.

Стаціонарні (берегові) ЗНО зберігають постійне місце розташування і служать надійним засобом для визначення місця або водіння кораблів фарватером, а також огородження навігаційних небезпек. Берегові ЗНО можуть бути побудовані капітально, з досить потужним та ефективним технічним обладнанням, що забезпечує велику дальність дії. До берегових ЗНО відносяться маяки, навігаційні знаки, вогні, звукосигнальні установки, радіомаяки, радіонавігаційні системи (РНС) і т.д.

Плавучі ЗНО використовуються, головним чином, як запобіжні засоби при огородженні навігаційних небезпек і відрізняються тією цінною властивістю, що вони безпосередньо огороджують навігаційну небезпеку.

Аналіз експлуатаційних характеристик фізичних засобів навігаційного обладнання свідчить, що вони забезпечують високу надійність функціонування та незалежність від суднових електронних систем. Завдяки безпосередньому візуальному сприйняттю такі засоби дозволяють судноводію оперативно оцінювати навігаційну обстановку.

Водночас їх ефективність істотно обмежується гідрометеорологічними умовами. Зокрема, в умовах туману, опадів або недостатньої освітленості спостерігається суттєве зниження дальності виявлення або повна втрата видимості. Крім того, утримання таких засобів потребує значних матеріальних витрат, пов’язаних із будівництвом та обслуговуванням.

Процес стратегічного розвитку електронної навігації (e-Navigation), ініційований Міжнародною Морською Організацією (IMO) [1], [18], [19] та підтриманий Міжнародною організацією морських засобів навігації (IALA), Міжнародною гідрографічною організацією (IHO), Міжнародним союзом електрозв'язку (ITU), Міжнародною електротехнічною комісією (IEC) та виробниками навігаційного обладнання, став вікном можливостей для вдосконалення існуючих та повноцінної розробки нових технологій для надання нових видів послуг морськими засобами навігаційного обладнання, які можна зробити гнучкими, недорогими та швидкими у розгортанні [20]–[23].

Впровадження AIS як засобу навігаційного обладнання дозволило суттєво розширити функціональні можливості систем навігаційного забезпечення. На відміну від традиційних засобів, AIS AtoN забезпечують передачу навігаційної інформації у цифровому вигляді з відображенням її на суднових інформаційних системах незалежно від умов видимості.

Система автоматичної ідентифікації (AIS) – система зв’язку, яка забезпечує автоматичний обмін відповідною (судновою та береговою) інформацією між станціями (пристроями) AIS [24]. Інформація може передаватися між суднами, пошуково-рятувальними літаками, береговими станціями тощо. Передавачі AIS також можуть бути закріплені на плавучому або стаціонарному засобі навігаційного обладнання, такому як буй, знак або вогонь, навіть на маяку.

Станції AIS ідентифікуються унікальним дев'ятизначним ідентифікатором морської рухомої служби (MMSI), який передається через радіочастотний спектр УКХ. Дві частоти спеціально виділені для обміну даними AIS (AIS1 – 161,975 МГц та AIS2 – 162,025 МГц). Кожен MMSI передається за допомогою відповідних повідомлень AIS. Для AIS AtoN це називається “Повідомленням 21” (“Message 21”).

MMSI складаються з серії з дев'яти цифр, які передаються по радіоканалу для унікальної ідентифікації суднових станцій, суднових наземних станцій, берегових станцій, берегових наземних станцій та інших несуднових станцій, що працюють у морській рухомій службі або морській рухомій супутниковій службі, а також групових викликів. Відповідно до Рекомендації ITU-R M.585 [23], усім AIS AtoN має бути присвоєно унікальний номер MMSI AMSA у такому форматі:

9 9 M I D X_1 X_2 X_3 X_4

де:

99 – ідентифікує станцію АІС ЗНО;

M I D – морська ідентифікаційна цифра, яка позначає адміністрацію, що має юрисдикцію над станцією AIS, ідентифікованою таким чином. MID України – 272.

X_1 – може використовуватися адміністрацією для розрізнення типу АІС ЗНО:

- X_1 = 1 для фізичних АІС ЗНО;
- X_1 = 6 для віртуальних АІС ЗНО;
- X_1 = 8 для мобільних ЗНО.

X_2 X_3 X_4 – це унікальний номер (від 000 до 999), призначений станції AIS.

АІС ЗНО (AIS AtoN) – цифровий засіб навігації, який транслюється уповноваженим постачальником послуг за допомогою АІС “Повідомлення 21” (звіт із засобу навігації) та відображається на навігаційному обладнанні, такому як ECDIS, РЛС або інтегрована навігаційна система (INS) (Циркуляр IMO MSC.1/Circ.1473 [25]).

Класифікація AIS AtoN включає фізичні, віртуальні та синтетичні засоби, кожен з яких має специфічні особливості застосування. Фізичні AIS AtoN забезпечують найбільш достовірну інформацію про стан об’єкта, тоді як віртуальні дозволяють оперативно позначати небезпеки без встановлення фізичної інфраструктури. Синтетичні засоби, у свою чергу, є компромісним рішенням між точністю та економічною доцільністю.

У циркулярі MSC.1/Circ.1473 IMO визначила два типи АІС ЗНО: фізичні (реальні) АІС ЗНО та віртуальні АІС ЗНО. Міжнародна асоціація морських засобів навігації та маяків (IALA), оцінивши можливості технології АІС

на думку постачальників послуг ЗНО (національних органів влади), у Рекомендації R0126 [22] запропонувала третій тип: синтетичні АІС ЗНО, які також поділяються на контрольовані та прогнозовані.

Фізичний АІС ЗНО – пристрій АІС встановлений безпосередньо на стаціонарному або плавучому ЗНО (рис. 1) і сам транслює власне АІС "Повідомлення 21", яке може містити таку інформацію: тип та назва ЗНО, координати в реальному часі, стан ЗНО – помилка роботи світлосигнального пристрою, помилка RACON, помилка «Не на місці» ("Off Position") тощо.

Рис. 1. Робота фізичного (реального) АІС ЗНО

У випадку плавучого засобу його позиція на електронних дисплеях може відрізнятися від позиції, нанесеної на карту. Також помилка «Не на місці» сигналізує про те, що засіб знаходиться поза межами призначеного йому радіуса положення.

Рис. 2. Приклад відображення фізичного АІС ЗНО на екрані ECDIS

Фізичний ЗНО АІС також може використовуватися для трансляції "Повідомлень 21" найближчих віртуальних та синтетичних АІС ЗНО. На рис. 2 наведено приклад відображення фізичного АІС ЗНО в електронній картографічній системі.

Рис. 3. Робота віртуального АІС ЗНО

Віртуальний АІС ЗНО – це засіб навігації, що сам по собі фізично не існує, на відміну від буїв та маяків, а являє собою АІС "Повідомлення 21", що транслюється в певне місце на водному шляху з берегової станції АІС або блоку АІС, встановленого на іншому, фізичному, пристрої (наприклад, стаціонарному або плавучому засобі) (рис. 3).

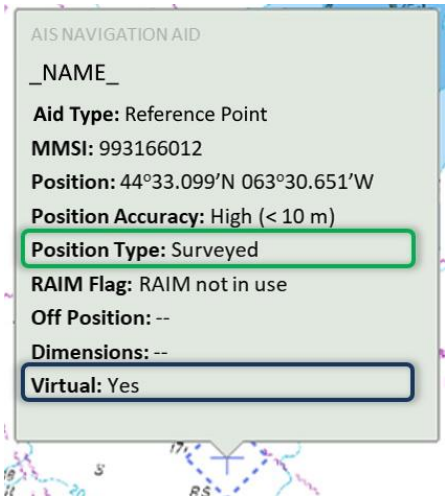

Рис. 4. Приклад відображення віртуального АІС ЗНО на екрані ECDIS

Ці засоби можна побачити лише на електронній картографічній інформаційній системі або іншому дисплеї з підтримкою АІС, такому як суднова РЛС. Приклад відображення інформації віртуального АІС ЗНО в електронній картографічній системі наведено на рис. 4.

1. Синтетичні АІС ЗНО

Синтетичні АІС ЗНО поділяються на дві категорії: контрольовані та прогнозовані.

Робота контрольованого синтетичного АІС ЗНО нагадує роботу фізичного. Замість встановлення пристрою АІС на засобі, пристрій позиціонування підключається до системи моніторингу, яка передає інформацію про стан засобу на базову станцію АІС, а вже базова станція транслює АІС “Повідомлення 21” (рис. 5). Враховуючи, що місцезнаходження засобу відоме в режимі реального часу, контрольована синтетична АІС ЗНО може використовуватися як на плавучих, так і на стаціонарних засобах.

Рис. 5. Робота контрольованого синтетичного АІС ЗНО

Прогнозований синтетичний АІС ЗНО – це АІС “Повідомлення 21”, що транслюється з берегової станції АІС або блоку АІС, встановленого на іншому пристрої (наприклад, стаціонарному або плавучому засобі). ЗНО, за який транслюється АІС “Повідомлення 21”, фізично існує, але ні його місцезнаходження, ні його статус не контролюються (рис. 6).

Рис. 6. Робота прогнозованого синтетичного АІС ЗНО

Приклад відображення прогнозованої синтетичної АІС ЗНО в електронній картографічній системі наведено на рис. 7.

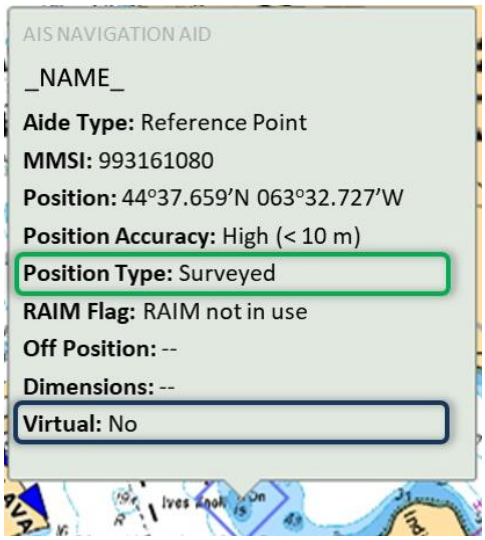

Рис. 7. Приклад відображення прогнозованого синтетичного АІС ЗНО на екрані ECDIS

Прогнозований синтетичний АІС ЗНО не може гарантувати цілісність АІС “Повідомлення 21”, оскільки місцезнаходження та статус не контролюються. Відповідно, не рекомендується використовувати його на плавучих ЗНО.

Використання прогнозованого синтетичного АІС ЗНО на стаціонарному засобі є прийнятним, оскільки місцезнаходження не змінюється, тільки статус ЗНО не може бути перевірений.

Для позначення АІС ЗНО у ECDIS та РЛС запропоновано використовувати символ у формі ромба (IEC 62288:2021+AMD1:2024 CSV) [26]. Фізичні та синтетичні АІС ЗНО використовують форму ромба із суцільною лінією, тоді як віртуальні АІС ЗНО використовують пунктирну лінію (рис. 8).

Інформація про АІС ЗНО відображається при наведенні на знак курсору або натисканням на знаку лівою кнопкою трекболу (миші).

Наразі немає конкретного визнаного символу для синтетичних АІС ЗНО, тому кожний тип визначається за номером MMSI, параметрами кодування АІС ЗНО (віртуальні: так/ні) та режимом позиціонування (див. рис. 2, 4, 7).

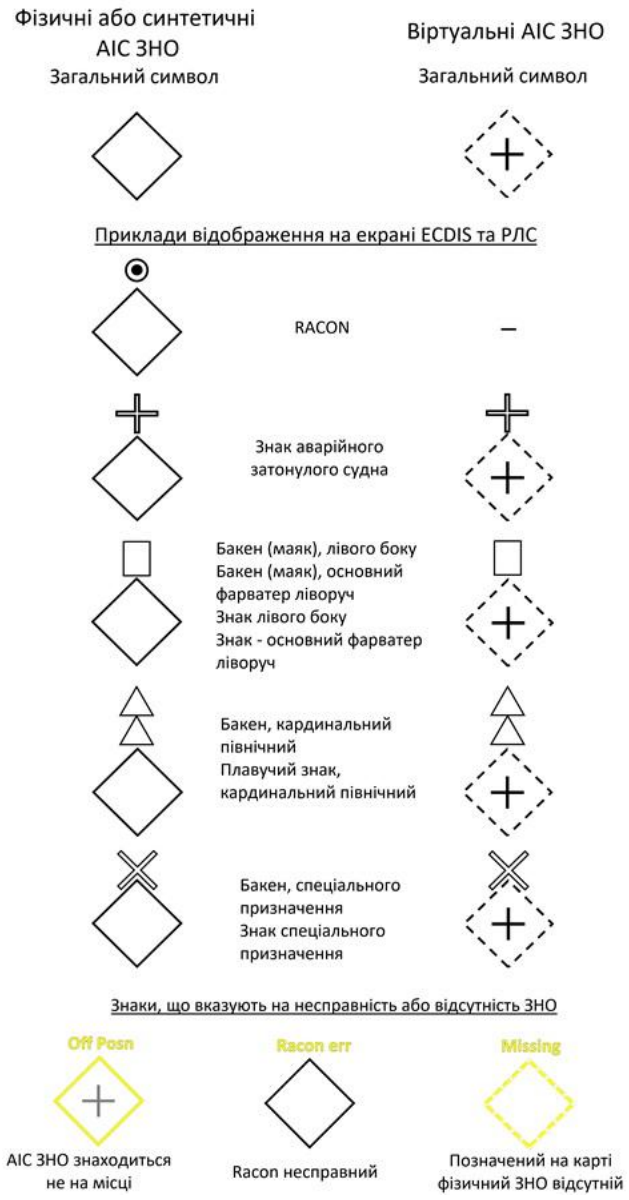

Рис. 8. Позначення АІС ЗНО на екрані ECDIS/РЛС

2. Переваги застосування АІС засобів навігаційного обладнання

Використання AIS AtoN є особливо ефективним у випадках, коли встановлення та обслуговування традиційних засобів є технічно складним або економічно недоцільним. До таких умов належать райони з суворими кліматичними умовами, інтенсивним льодоутворенням або значною динамікою водного середовища, де фізичні буї сезонно знімаються, можуть бути втрачені, зміщені зі свого місця або пошкоджені.

Додатковою перевагою є можливість оперативного розгортання віртуальних засобів для позначення аварійних ситуацій або тимчасових навігаційних небезпек. Це дозволяє значно підвищити рівень безпеки судноплавства за рахунок своєчасного інформування судноводіїв.

АІС ЗНО не залежать від погодних умов. На відміну від традиційних буїв, знаків або маяків, які можуть залишитись непоміченими в умовах поганої видимості, вони завжди відображаються на екранах ECDIS або РЛС, що дає судноводію можливість їх своєчасного виявлення.

Віртуальні засоби навігації можуть використовуватися для позначення якірних стоянок, обмежених або небезпечних зон, а також на екологічно чутливому та ізольованому узбережжі. Вони забезпечують хороше покриття, незважаючи на пересічений ландшафт.

За результатами проведених випробувань [2], [4] встановлено, що використання віртуальних засобів навігації є важливим фактором у підвищенні безпеки плавання. Але, незважаючи на значні переваги, застосування AIS AtoN пов’язане з рядом обмежень. Зокрема, достовірність переданої інформації залежить від справності та коректності роботи навігаційного обладнання, в тому числі на борту судна, відсутності радіоелектронних завад. Існує також ризик спотворення або навмисного втручання в передані дані (jamming, spoofing).

Крім того, ефективність використання таких засобів значною мірою залежить від рівня підготовки судноводіїв та їх здатності інтерпретувати інформацію, що відображається в електронних навігаційних системах.

3. Захист GNSS-приймачів AIS AtoN за допомогою CRPA-антен.

AIS є цифровою системою зв'язку, в якій використовується протокол SOTDMA. Згідно з цим протоколом кожному учаснику, який у даний момент знаходиться в мережі, періодично виділяються короткі часові проміжки (слоти) для прийому та передавання інформації [27]. Виділення та використання слотів

проводиться на базі Universal Coordinated Time (UTC), яке базові станції та транспондери AIS отримують у складі сигналів, що передаються супутниками GNSS. Звідси випливає, що необхідною умовою роботи системи AIS AtoN у будь-якій з розглянутих вище конфігурацій є надійне функціонування в даному районі хоча б однієї з мереж, що входять до складу GNSS: GPS, Galileo, BeiDou або інших доступних глобальних навігаційних супутникових систем.

В останні роки в деяких морських районах зафіксовано випадки зловмисного впливу на навігаційні сигнали систем GNSS, які виявилися недостатньо захищеними від таких атак. Єдиною системою, в якій застосовується захист сигналу у вигляді його автентифікації, є Galileo, однак цей захід також не забезпечує повного захисту. Зловмисний вплив на сигнали GNSS може бути одного з трьох видів:

- Jamming – придушення сигналу GNSS сигналами більшої потужності
- Spoofing – підміна навігаційних сигналів супутників хибними сигналами, які вводять судноводіїв в оману та створюють ризик навігаційної аварії.
- Meaconing - ретрансляція "правильних" сигналів навігаційних супутників після введення в них затримки в часі. Такий вплив також спотворює навігаційну інформацію, яку приймає судно.

Кожний із названих видів впливу може здійснюватися одним джерелом або групою джерел, які передають синхронізовані сигнали перешкод з різних напрямків. Другий випадок є більш складним для захисту та прийому неспотворених сигналів.

На сьогодні немає єдиного методу боротьби зі шкідливим впливом на сигнали GNSS. У складних випадках необхідно застосовувати комплекс заходів для отримання від GNSS надійної навігаційної інформації в умовах зловмисного впливу.

Пріоритет серед цих заходів має застосування антен з керованою діаграмою спрямованості (CRPA). Така антена являє собою комбінацію кількох антенних елементів, кожен з яких приймає сигнали незалежно. Прийняті сигнали обробляються процесором за спеціальними алгоритмами. В результаті цієї обробки антена визначає напрямок на передбачуване джерело перешкод і автоматично встановлює нульову чутливість у цьому напрямку. Ця властивість CRPA-антени називається формуванням діаграми спрямованості (beamforming) і показана на рис. 9 [8], [28], [29].

CRPA – це адаптивна антенна система, яка в режимі реального часу динамічно контролює свою діаграму спрямованості (форму та напрямок променя) та автоматично концентрується на слабких сигналах, одночасно активно пригнічуючи сильні перешкоди.

Реалізація CRPA-захисту має відрізнятися залежно від типу AIS AtoN. Для фізичних AIS AtoN CRPA-антену доцільно встановлювати безпосередньо на плавучому або стаціонарному засобі, де вона захищає GNSS-приймач, що формує фактичні координати, часову синхронізацію та ознаку положення «на місці / не на місці» (рис. 10).

Рис. 9. Формування нуля діаграми спрямованості на єдине джерело шкідливого впливу

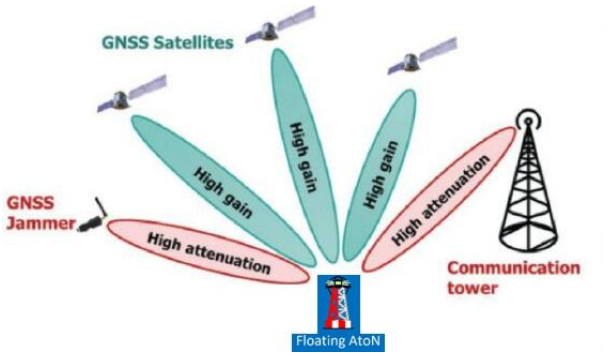

Рис. 10. Схема роботи CRPA-антени на плавучих AIS ЗНО

Для плавучих ЗНО це має особливе значення, оскільки зсув буя, помилка GNSS або навмисне спотворення координат можуть призвести до передавання суднам неправдивого Message 21.

Для контрольованих синтетичних AIS AtoN CRPA-захист доцільно застосовувати не на AIS-передавачі як такому, а на пристрої моніторингу або позиціонування, який контролює фактичне положення фізичного ЗНО та передає дані на берегову AIS-станцію. У прогнозованих синтетичних AIS AtoN ефективність CRPA є обмеженою, оскільки положення об'єкта не контролюється в реальному часі; у такому випадку CRPA може підвищити стійкість лише берегової інфраструктури, яка формує або транслює повідомлення.

Для віртуальних AIS AtoN, які не мають фізичного носія в точці позначення небезпеки, CRPA-антена не може бути встановлена «на знаку». Її доцільно використовувати у складі берегової GNSS/PNT-інфраструктури, що забезпечує точний час, координатну основу та формування AIS/VDES-повідомлень. Отже, CRPA не замінює автентифікацію AIS-повідомлень, а доповнює її, усуваючи або зменшуючи вплив хибних GNSS-сигналів на джерело позиційних і часових даних.

Зловмисний вплив на сигнали GNSS порушує також роботу транспондерів AIS AtoN, які не можуть стабільно працювати без сигналів точного часу. Ці сигнали надходять на транспондери AIS від внутрішніх або зовнішніх GNSS-приймачів. Окрім цього, сфальсифіковані повідомлення можуть бути введені в AIS безпосередньо на робочих частотах УКХ-діапазону, оскільки традиційна концепція AIS не передбачає повноцінного криптографічного захисту від такого втручання [9], [10], [16].

Аналіз наукових публікацій і рекомендаційних документів, присвячених захисту AIS/VDES-повідомлень, показує, що найбільш перспективними сьогодні є автентифікація джерела повідомлення, цифровий підпис, використання інфраструктури відкритих ключів (PKI), а також гібридні підходи, сумісні з наявною AIS/VDES-інфраструктурою [9], [13]–[17].

Використання автентифікації транспондера забезпечує підтвердження джерела повідомлення, дає змогу перевірити цілісність прийнятих даних та зменшує ризик підробки або несанкціонованої трансляції AIS AtoN.

Використання цифрового підпису на основі асиметричної криптографії сьогодні вважається одним із перспективних методів захисту AIS/VDES-повідомлень. Сутність цього методу полягає в тому, що після формування повідомлення воно підписується приватним ключем (Private Key), а після прийому іншим судном або береговою станцією електронний підпис автоматично перевіряється за допомогою відкритого ключа (Public Key). Такий підхід дозволяє переконатися, що повідомлення було сформоване конкретним авторизованим пристроєм і не було змінене під час передавання.

Для реалізації автентифікації повідомлень необхідно створити інфраструктуру відкритих ключів (Public Key Infrastructure, PKI), яка має забезпечити генерацію ключів, видачу цифрових сертифікатів та перевірку їх легітимності. Скомпрометовані сертифікати повинні автоматично відкликатися.

Інфраструктура PKI забезпечує централізоване керування довірою між AIS AtoN, береговими системами, VTS та іншими авторизованими учасниками обміну навігаційними даними.

При цьому переваги впровадження автентифікації AIS AtoN супроводжуються низкою технічних складностей, серед яких додаткове навантаження на канал, збільшення розміру

повідомлень, потреба у керуванні сертифікатами та необхідність модернізації обладнання відповідно до міжнародних стандартів.

Висновки і перспектива подальшої роботи по даному напрямку

Проведений аналіз показав, що традиційні фізичні засоби навігаційного обладнання залишаються необхідним елементом системи безпеки мореплавства завдяки їх надійності, наочності та незалежності від суднових електронних систем. Водночас їх ефективність обмежується умовами видимості, гідрометеорологічними факторами та витратами на утримання.

AIS-засоби навігаційного обладнання, зокрема віртуальні та синтетичні, забезпечують вищу оперативність навігаційного інформування, можуть застосовуватися для тимчасового позначення небезпек і є особливо корисними там, де встановлення фізичного знака є складним, небезпечним або економічно недоцільним. Разом з тим AIS AtoN не повинні розглядатися як повноцінна заміна фізичних AtoN у всіх випадках, оскільки їх надійність залежить від GNSS/PNT-даних, VHF-радіоканалу, коректності налаштувань і кіберстійкості інфраструктури.

Власний науковий внесок авторів полягає в обґрунтуванні багаторівневої моделі підвищення стійкості AIS AtoN, яка поєднує три взаємопов'язані напрями: комплексне використання фізичних, синтетичних і віртуальних AtoN; захист GNSS-приймачів AIS AtoN за допомогою CRPA-антен; автентифікацію та цифровий підпис AIS/VDES-повідомлень для підтвердження джерела і цілісності даних.

Практичне впровадження AIS AtoN має здійснюватися відповідно до SOLAS V/13 та рекомендацій IMO/IALA таким чином, щоб не знижувати основну функцію AIS як засобу запобігання зіткненням. При цьому необхідно враховувати можливу плутанину між картографічним положенням фізичного ЗНО і динамічно відображеним символом AIS AtoN, а також уникати необґрунтованого використання віртуальних AIS AtoN для постійного позначення об'єктів, які можуть бути позначені фізичними засобами.

Застосування CRPA є найбільш доцільним для фізичних і контрольованих синтетичних AIS AtoN, де існує GNSS-приймач або пристрій моніторингу фактичного положення об'єкта. Для прогнозованих синтетичних і віртуальних AIS AtoN CRPA має допоміжне значення і повинна застосовуватися переважно на рівні берегової GNSS/PNT-інфраструктури. Тому CRPA, автентифікація транспондерів і цифровий підпис повідомлень мають розглядатися не як альтернативні, а як взаємодоповнювані засоби підвищення довіри до AIS AtoN.

Подальші дослідження доцільно спрямувати на оцінювання навантаження AIS/VDES-каналів під час упровадження автентифікації, формування практичних сценаріїв використання CRPA для різних типів AtoN, а також на розроблення процедур перевірки достовірності AIS AtoN шляхом зіставлення даних AIS, ECDIS, РЛС, VTS та інших незалежних джерел навігаційної інформації.

ЛІТЕРАТУРА

[1] International Maritime Organization, "E-Navigation Strategy Implementation Plan – Update 1," Maritime Safety Committee, MSC.1/Circ.1595, May 25, 2018. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC.1-Circ.1595%20-%20E-Navigation%20Strategy%20Implementation%20Plan%20-%20Update%201%20%28Secretariat%29%20%282%29.pdf. [Accessed: March 10, 2026].

[2] Wright R. G. and Baldauf M., "Correlation of Virtual Aids to Navigation to the Physical Environment," TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation, vol. 10, no. 2, pp. 311–316, Jun. 2016, doi: 10.12716/1001.10.02.11

[3] Jurkovič M., Molnárová Baracková A., Kadnár R., Melnyk O., Gorzelanczyk P., and Prabowo A. R., "Operational Research of AIS AtoNs in Inland Waterways: A Case Study of a Selected Stretch on the Danube," Transactions on Maritime Science, vol. 14, no. 1, 2025, doi: 10.7225/toms.v14.n01.w02

[4] Canadian Coast Guard, "Results of the AIS AtoN International Survey Conducted by the Canadian Coast Guard," Nov. 2016. [Online]. Available: https://e-navigation.canada.ca/docs/studies/Canada_AIS_AtoN_International_Survey_Results-2016.pdf. [Accessed: March 10, 2026].

[5] Canadian Coast Guard, "Section 2. What is an AIS Aid to Navigation (AIS AtoN)?" [Online]. Available: https://e-navigation.canada.ca/topics/aids/docs/ais-aton/what-is. [Accessed: March 10, 2026].

[6] CESNI/RIS Expert Group, "Information Paper on AIS AtoN," May 9, 2017. [Online]. Available: https://ris.cesni.eu/docs/File/620/Information_paper_on_AIS_AtoN_edition_1_1.pdf. [Accessed: March 10, 2026].

[7] European Boating Association, "AIS Virtual Aids to Navigation." [Online]. Available: https://eba.eu.com/technical/ais-virtual-aids-to-navigation/. [Accessed: May 10, 2026].

[8] Коновець В. І., Плешко Е. А. і Шишкін О. В., "Забезпечення стійкої роботи супутникової навігації на морі," Судноводіння, вип. 34, с. 66–78, 2023, doi: 10.31653/2306-5761.34.2023.66-78.

[9] Шишкін О. В. і Коновець В. І., "Автентифікація повідомлень автоматичної ідентифікаційної системи на основі використання технології цифрових водяних знаків," Судноводіння, вип. 37, с. 109–122, 2025, doi: 10.31653/2306-5761.37.2025.109-122

[10] Шишкін О. В., Пашенко О. Л. і Купровський В. І., "Розвиток морського УКХ радіозв'язку для ефективного та безпечного судноводіння," Судноводіння, вип. 37, с. 47–62, 2025, doi: 10.31653/2306-5761.37.2025.47-62

[11] Melnyk O., Kuznichenko S., and Onishchenko O., "Impact of AIS Manipulation on Shipping Safety and Strategic Countermeasures," Lex Portus, vol. 10, no. 4, pp. 31–39, 2024, doi: 10.62821/lp10403

[12] Androjna A., Perkovič M., Pavić I., and Mišković J., "AIS Data Vulnerability Indicated by a Spoofing Case-Study," Applied Sciences, vol. 11, no. 11, art. 5015, 2021, doi: 10.3390/app11115015

[13] Wimpenny G., Šafář J., Grant A., and Bransby M., "Securing the Automatic Identification System (AIS): Using Public Key Cryptography to Prevent Spoofing Whilst Retaining Backwards Compatibility," The Journal of Navigation, vol. 75, no. 2, pp. 333–345, 2022, doi: 10.1017/S0373463321000837

[14] Sciancalepore S., Tedeschi P., Aziz A., and Di Pietro R., "Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2709–2726, 2022, doi: 10.1109/TDSC.2021.3069428

[15] Goudosis A. and Katsikas S., "Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation," Journal of Marine Science and Engineering, vol. 10, no. 6, art. 805, 2022, doi: 10.3390/jmse10060805

[16] IALA, "VDES Authentication," Guideline G1192, ed. 1.0, Jun. 13, 2025. [Online]. Available: https://www.iala.int/product/g1192/. [Accessed: May 10, 2026].

[17] Wimpenny G., Lazaro F., Šafář J., and Raulefs R., "A Pragmatic Approach to VDES Authentication," NAVIGATION: Journal of the Institute of Navigation, vol. 72, no. 1, 2025, doi: 10.33012/navi.681

[18] International Maritime Organization, “Strategy for the Development and Implementation of e-Navigation,” Maritime Safety Committee, MSC 85/26/Add.1, Annex 20, 2008. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC%2085%20-%20annex%2020%20-%20Strategy%20for%20the%20development%20and%20implementation%20of%20e-nav.pdf. [Accessed: March 10, 2026].

[19] International Maritime Organization, “Framework for the Implementation Process for the e-Navigation Strategy,” Maritime Safety Committee, MSC 85/26/Add.1, Annex 21, 2008. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC%2085%20-%20annex%2021%20-%20Framework%20for%20the%20implementation%20process%20for%20the%20e-nav%20strategy.pdf. [Accessed: March 10, 2026].

[20] IALA, “Provision of Virtual Aids to Navigation,” Guideline G1081, ed. 2.1, Jun. 10, 2021. [Online]. Available: https://www.iala.int/product/g1081/. [Accessed: March 10, 2026].

[21] IALA, “Provision of Virtual Aids to Navigation,” Recommendation R0143, ed. 2.0, Jun. 10, 2021. [Online]. Available: https://www.iala.int/product/r0143/. [Accessed: March 10, 2026].

[22] IALA, “The Use of the Automatic Identification System (AIS) in Marine Aids to Navigation Service,” Recommendation R0126, ed. 2.0, Dec. 17, 2021. [Online]. Available: https://www.iala.int/product/r0126/. [Accessed: March 10, 2026].

[23] ITU, “Assignment and use of identities in the maritime mobile service,” Recommendation ITU-R M.585-9, May 2022. [Online] Available: https://www.itu.int/rec/R-REC-M.585-9-202205-I/en. [Accessed: March 10, 2026].

[24] IALA, “An Overview of AIS,” Guideline G1082, ed. 2.1, Jun. 24, 2016. [Online]. Available: https://www.iala.int/product/g1082/. [Accessed: March 10, 2026].

[25] International Maritime Organization, “Policy on Use of AIS Aids to Navigation,” Maritime Safety Committee, MSC.1/Circ.1473, May 23, 2014. [Online]. Available: https://www.e-navigation.nl/sites/default/files/IMO_SN_Circ1473.pdf. [Accessed: March 10, 2026].

[26] International Maritime Organization, “Guidelines for the Presentation of Navigation-Related Symbols, Terms and Abbreviations,” Maritime Safety Committee, SN.1/Circ.243/Rev.2 + Corr.1, Jun. 14, 2019. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/IMO%20Documents%20related%20to/SN.1-Circ.243-Rev.2%20%2B%20Corr.1.pdf. [Accessed: March 10, 2026].

[27] ITU, “Technical characteristics for VHF automatic identification system using time division multiple access in the maritime mobile service,” Recommendation ITU-R M.1371-6, Feb. 2026. [Online]. Available: https://www.itu.int/rec/R-REC-M.1371-6-202602-I/en. [Accessed: March 10, 2026].

[28] SAFEGNSS, “Що таке технологія CRPA (антена з контрольованою діаграмою випромінювання)?,” 21 верес. 2025. [Електронний ресурс]. Доступно: https://www.safegnss.com/ua/what-is-crpa-controlled-radiation-pattern-antenna-technology/. [Дата звернення: 10 березня 2026].

[29] Inside GNSS, “CRPA for GNSS: Benefits, Challenges and Testing,” Mar. 10, 2022. [Online]. Available: https://insidegnss.com/crpa-for-gnss-benefits-challenges-and-testing/. [Accessed: March 10, 2026].

REFERENCES

[1] International Maritime Organization, "E-Navigation Strategy Implementation Plan – Update 1," Maritime Safety Committee, MSC.1/Circ.1595, May 25, 2018. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC.1-Circ.1595%20-%20E-Navigation%20Strategy%20Implementation%20Plan%20-%20Update%201%20%28Secretariat%29%20%282%29.pdf. [Accessed: March 10, 2026].

[2] Wright R. G. and Baldauf M., "Correlation of Virtual Aids to Navigation to the Physical Environment," TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation, vol. 10, no. 2, pp. 311–316, Jun. 2016, doi: 10.12716/1001.10.02.11

[3] Jurkovič M., Molnárová Baracková A., Kadnár R., Melnyk O., Gorzelanczyk P., and Prabowo A. R., "Operational Research of AIS AtoNs in Inland Waterways: A Case Study of a Selected Stretch on the Danube," Transactions on Maritime Science, vol. 14, no. 1, 2025, doi: 10.7225/toms.v14.n01.w02

[4] Canadian Coast Guard, "Results of the AIS AtoN International Survey Conducted by the Canadian Coast Guard," Nov. 2016. [Online]. Available: https://e-navigation.canada.ca/docs/studies/Canada_AIS_AtoN_International_Survey_Results-2016.pdf. [Accessed: March 10, 2026].

[5] Canadian Coast Guard, "Section 2. What is an AIS Aid to Navigation (AIS AtoN)?" [Online]. Available: https://e-navigation.canada.ca/topics/aids/docs/ais-aton/what-is. [Accessed: May 10, 2026].

[6] CESNI/RIS Expert Group, "Information Paper on AIS AtoN," May 9, 2017. [Online]. Available: https://ris.cesni.eu/docs/File/620/Information_paper_on_AIS_AtoN_edition_1_1.pdf. [Accessed: March 10, 2026].

[7] European Boating Association, "AIS Virtual Aids to Navigation." [Online]. Available: https://eba.eu.com/technical/ais-virtual-aids-to-navigation/. [Accessed: May 10, 2026].

[8] Konovets V. I., Pleshko E. A., and Shyshkin O. V., "Zabezpechennia stiikoi roboty suputnykovoi navihatsii na mori," Sudnovodinnia, no. 34, pp. 66–78, 2023, doi: 10.31653/2306-5761.34.2023.66-78. [in Ukrainian].

[9] Shyshkin O. V. and Konovets V. I., "Avtentyfikatsiia povidomlen avtomatychnoi identyfikatsiinoi systemy na osnovi vykorystannia tekhnolohii tsyfrovykh vodianykh znakiv," Sudnovodinnia, no. 37, pp. 109–122, 2025, doi: 10.31653/2306-5761.37.2025.109-122. [in Ukrainian].

[10] Shyshkin O. V., Pashenko O. L., and Kuprovskyi V. I., "Rozvytok morskoho UKKh radiozviazku dlia efektyvnoho ta bezpechnoho sudnovodinnia," Sudnovodinnia, no. 37, pp. 47–62, 2025, doi: 10.31653/2306-5761.37.2025.47-62. [in Ukrainian].

[11] Melnyk O., Kuznichenko S., and Onishchenko O., "Impact of AIS Manipulation on Shipping Safety and Strategic Countermeasures," Lex Portus, vol. 10, no. 4, pp. 31–39, 2024, doi: 10.62821/lp10403

[12] Androjna A., Perkovič M., Pavić I., and Mišković J., "AIS Data Vulnerability Indicated by a Spoofing Case-Study," Applied Sciences, vol. 11, no. 11, art. 5015, 2021, doi: 10.3390/app11115015

[13] Wimpenny G., Šafář J., Grant A., and Bransby M., "Securing the Automatic Identification System (AIS): Using Public Key Cryptography to Prevent Spoofing Whilst Retaining Backwards Compatibility," The Journal of Navigation, vol. 75, no. 2, pp. 333–345, 2022, doi: 10.1017/S0373463321000837

[14] Sciancalepore S., Tedeschi P., Aziz A., and Di Pietro R., "Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2709–2726, 2022, doi: 10.1109/TDSC.2021.3069428

[15] Goudosis A. and Katsikas S., "Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation," Journal of Marine Science and Engineering, vol. 10, no. 6, art. 805, 2022, doi: 10.3390/jmse10060805

[16] IALA, "VDES Authentication," Guideline G1192, ed. 1.0, Jun. 13, 2025. [Online]. Available: https://www.iala.int/product/g1192/. [Accessed: March 10, 2026].

[17] Wimpenny G., Lazaro F., Šafář J., and Raulefs R., "A Pragmatic Approach to VDES Authentication," NAVIGATION: Journal of the Institute of Navigation, vol. 72, no. 1, 2025, doi: 10.33012/navi.681

[18] International Maritime Organization, "Strategy for the Development and Implementation of e-Navigation," Maritime Safety Committee, MSC 85/26/Add.1, Annex 20, 2008. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC%2085%20-%20annex%2020%20-%20Strategy%20for%20the%20development%20and%20implementation%20of%20e-nav.pdf. [Accessed: March 10, 2026].

[19] International Maritime Organization, "Framework for the Implementation Process for the e-Navigation Strategy," Maritime Safety Committee, MSC 85/26/Add.1, Annex 21, 2008. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC%2085%20-%20annex%2021%20-%20Framework%20for%20the%20implementation%20process%20for%20the%20e-nav%20strategy.pdf. [Accessed: March 10, 2026].

[20] IALA, "Provision of Virtual Aids to Navigation," Guideline G1081, ed. 2.1, Jun. 10, 2021. [Online]. Available: https://www.iala.int/product/g1081/. [Accessed: March 10, 2026].

[21] IALA, "Provision of Virtual Aids to Navigation," Recommendation R0143, ed. 2.0, Jun. 10, 2021. [Online]. Available: https://www.iala.int/product/r0143/. [Accessed: March 10, 2026].

[22] IALA, "The Use of the Automatic Identification System (AIS) in Marine Aids to Navigation Service," Recommendation R0126, ed. 2.0, Dec. 17, 2021. [Online]. Available: https://www.iala.int/product/r0126/. [Accessed: March 10, 2026].

[23] ITU, "Assignment and use of identities in the maritime mobile service," Recommendation ITU-R M.585-9, May 2022. [Online]. Available: https://www.itu.int/rec/R-REC-M.585-9-202205-I/en. [Accessed: March 10, 2026].

[24] IALA, "An Overview of AIS," Guideline G1082, ed. 2.1, Jun. 24, 2016. [Online]. Available: https://www.iala.int/product/g1082/. [Accessed: March 10, 2026].

[25] International Maritime Organization, "Policy on Use of AIS Aids to Navigation," Maritime Safety Committee, MSC.1/Circ.1473, May 23, 2014. [Online]. Available: https://www.e-navigation.nl/sites/default/files/IMO_SN_Circ1473.pdf. [Accessed: March 10, 2026].

[26] International Maritime Organization, "Guidelines for the Presentation of Navigation-Related Symbols, Terms and Abbreviations," Maritime Safety Committee, SN.1/Circ.243/Rev.2 + Corr.1, Jun. 14, 2019. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/IMO%20Documents%20related%20to/SN.1-Circ.243-Rev.2%20%2B%20Corr.1.pdf. [Accessed: March 10, 2026].

[27] ITU, “Technical characteristics for VHF automatic identification system using time division multiple access in the maritime mobile service,” Recommendation ITU-R M.1371-6, Feb. 2026. [Online]. Available: https://www.itu.int/rec/R-REC-M.1371-6-202602-I/en. [Accessed: March 10, 2026].

[28] SAFEGNSS, “What is CRPA (Controlled Radiation Pattern Antenna) technology?,” Sep. 21, 2025. [Online]. Available: https://www.safegnss.com/ua/what-is-crpa-controlled-radiation-pattern-antenna-technology/. [Accessed: March 10, 2026].

[29] Inside GNSS, “CRPA for GNSS: Benefits, Challenges and Testing,” Mar. 10, 2022. [Online]. Available: https://insidegnss.com/crpa-for-gnss-benefits-challenges-and-testing/. [Accessed: March 10, 2026].