УДК 656.61.052 doi.org/10.33298/2226-8553.2025.3.43.19

© Квасников П. К.

АВТОМАТИЧНА ІДЕНТИФІКАЦІЙНА СИСТЕМА ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУДНОПЛАВСТВА: СУЧАСНІ РЕАЛІЇ РОЗВИТКУ ТА ВИКЛИКИ КІБЕРБЕЗПЕКИ

Автоматична ідентифікаційна система (АІС) є критично важливою складовою сучасного морського судноплавства, забезпечуючи безпеку навігації та ефективне управління морським трафіком. Система, що спочатку створювалася як засіб запобігання зіткненням суден, трансформувалася у багатофункціональний глобальний інструмент моніторингу, який використовується службами руху суден, митними органами, портовими адміністраціями та правоохоронними органами по всьому світу. Відповідно до вимог Міжнародної конвенції СОЛАС, з 2004 року система АІС є обов'язковою для пасажирських суден, танкерів та суден вантажомісткістю понад 300 тонн. Станом на 2025 рік глобальна мережа моніторингу обробляє понад 300 мільйонів повідомлень АІС щоденно, відстежуючи більше 170 000 суден у реальному часі через наземні та супутникові системи. Стаття досліджує технічну архітектуру системи АІС, яка функціонує на основі УКВ-радіозв'язку у морських діапазонах частот (161,975 МГц та 162,025 МГц) з використанням методу самоорганізованого множинного доступу з розділенням часу (STDMA). Проаналізовано провідні міжнародні платформи відстеження суден: MarineTraffic (обслуговує понад 538 000 користувачів на добу), VesselFinder (близько 139 000 користувачів щоденно), Vesseltracker та ShippingExplorer, які забезпечують доступ до даних АІС у реальному часі. Особливу увагу приділено зростаючій проблемі кібербезпеки – явищу спуфінгу АІС, яке становить серйозну загрозу для міжнародного судноплавства. Дослідження 2020-2023 років виявили понад сто випадків підробки даних військових та комерційних суден з 14 країн світу. Систематизовано три основні типи обманних практик: AIS handshake (використання судна-приманки), судна-зомбі (використання ідентичності неіснуючих суден) та маніпулювання місцезнаходженням через GNSS. Розглянуто методи виявлення спуфінгу, включаючи застосування алгоритмів штучного інтелекту, перехресну перевірку з радіолокаційними та супутниковими даними. Проаналізовано використання даних АІС у протидії незаконній діяльності, включаючи виявлення порушень санкційних режимів, контрабанди та піратства. Підкреслено необхідність вдосконалення міжнародних протоколів безпеки системи АІС, розробки ефективних механізмів аутентифікації даних та координації зусиль урядів, міжнародних організацій та приватного сектору для забезпечення цілісності системи. Матеріал статті буде корисним для фахівців морської галузі, дослідників кібербезпеки, викладачів морських навчальних закладів та осіб, відповідальних за управління морським рухом та безпеку портових операцій.

Ключові слова: *автоматична ідентифікаційна система, АІС, безпека судноплавства, спуфінг, кібербезпека морського транспорту, моніторинг суден, GNSS, супутникове відстеження, морська навігація, управління морським рухом, СОЛАС, STDMA.*

Постановка проблеми. Сучасне морське судноплавство стоїть перед викликами, пов'язаними з необхідністю забезпечення безпеки навігації в умовах зростаючої інтенсивності морського трафіку та появи нових кіберзагроз. Автоматична ідентифікаційна система (АІС) є ключовим елементом інфраструктури безпеки мореплавства, що забезпечує ідентифікацію суден, моніторинг їх переміщення та координацію дій у складних навігаційних ситуаціях.

Відповідно до Міжнародної конвенції з охорони людського життя на морі (СОЛАС), з грудня 2004 року система АІС є обов'язковою на пасажирських суднах, танкерах та суднах вантажомісткістю понад 300 тонн. За даними Міжнародної морської організації (ІМО), станом на 2024 рік понад 100 000 суден у світі обладнані транспондерами АІС, що передають дані про своє місцезнаходження, курс, швидкість та інші навігаційні параметри [1].

Система АІС створювалася як засіб запобігання зіткненням між суднами, однак швидко еволюціонувала у багатофункціональний інструмент, який використовується для управління рухом суден, митного контролю, моніторингу екологічної безпеки, пошуково-рятувальних операцій та протидії незаконній діяльності на морі. Глобальна мережа наземних та супутникових приймачів АІС забезпечує майже повне покриття світового океану, обробляючи сотні мільйонів повідомлень щоденно [2].

Проте сучасні реалії демонструють серйозні вразливості системи до кіберзагроз. Явище спуфінгу АІС – навмисного спотворення даних про місцезнаходження та параметри суден – набуває системного характеру і створює ризики для міжнародної безпеки судноплавства. Дослідження неурядових організацій SkyTruth та Global Fishing Watch зафіксували з серпня 2020 року понад сто випадків підробки даних військових кораблів з 14 країн, включаючи судна НАТО, що може провокувати міжнародні конфлікти [3].

В умовах цифровізації морського транспорту та зростання залежності від автоматизованих систем навігації, питання захисту даних АІС від несанкціонованого втручання набуває критичного значення для забезпечення безпеки міжнародного судноплавства.

Аналіз останніх досліджень і публікацій. Проблематика функціонування та безпеки автоматичної ідентифікаційної системи активно досліджується міжнародною науковою спільнотою та спеціалізованими організаціями. Міжнародна асоціація морського обладнання та маяків (IALA) розробила рекомендації щодо технічних стандартів АІС та протоколів безпеки системи [4].

Технічні аспекти функціонування системи АІС висвітлено у документації Міжнародної морської організації (IMO), зокрема у Резолюції A.1106(29) щодо переглянутих керівних принципів експлуатації АІС [5]. Дослідження протоколу передачі даних NMEA (National Marine Electronics Association) та методу STDMA (Self-organizing Time Division Multiple Access) проводяться провідними науковими центрами морської галузі.

Питання кібербезпеки морського транспорту та захисту від спуфінгу АІС досліджували Б. Бергман (SkyTruth та Global Fishing Watch), який у 2020-2021 роках провів комплексне дослідження випадків підробки даних військових суден [3]. У своїх працях дослідник систематизував типи обманних практик та розробив методологію їх виявлення через аналіз невідповідностей між наземними та супутниковими даними.

Європейське агентство з морської безпеки (EMSA) у звіті за 2023 рік проаналізувало загрози кібербезпеці морського транспорту, включаючи вразливості системи АІС [6]. Агентство рекомендує впровадження багаторівневих систем аутентифікації та використання штучного інтелекту для виявлення аномалій у даних.

Комерційні платформи моніторингу суден накопичили значний досвід у обробці та візуалізації даних АІС. MarineTraffic (Греція, заснована у 2007 році) обслуговує понад 538 000 користувачів на добу та підтримує 34 мови інтерфейсу [7]. VesselFinder (Болгарія, 2011 рік) щоденно приймає близько 139 000 відвідувачів і надає безкоштовний доступ до відстеження суден у реальному часі [8]. Vesseltracker (Німеччина, 2006 рік) щоденно обробляє понад 500 мільйонів повідомлень АІС і відстежує більше 170 000 суден глобально [9].

Незважаючи на значний масив досліджень, недостатньо розробленими залишаються питання практичного впровадження ефективних механізмів протидії спуфінгу АІС на національному рівні, адаптації міжнародних стандартів безпеки до умов українського судноплавства та підготовки фахівців до роботи в умовах зростаючих кіберзагроз.

Мета дослідження полягає в комплексному аналізі сучасного стану та перспектив розвитку автоматичної ідентифікаційної системи, дослідження технічних аспектів її функціонування, систематизація основних загроз кібербезпеці в контексті використання АІС, аналіз міжнародного досвіду протидії спуфінгу та визначення шляхів підвищення захищеності системи для забезпечення безпеки морського судноплавства.

Виклад основного матеріалу та основні результати дослідження. В дослідженні проаналізовано технічну архітектуру та принципи функціонування автоматичної ідентифікаційної системи (АІС). Для аналізу роботи системи з урахуванням радіозв'язку, передачі даних та протоколів обміну інформацією використано структурно-функціональний підхід. Автоматична ідентифікаційна

система функціонує на основі УКВ-радіозв'язку у виділених морських діапазонах частот 161,975 МГц (канал AIS 1) та 162,025 МГц (канал AIS 2). Система використовує метод самоорганізованого множинного доступу з розділенням часу (STDMA – Self-organizing Time Division Multiple Access), при якому частотний діапазон розділяється на часові слоти тривалістю 26,6 мілісекунд [11].

Судова станція AIC класу A (для комерційних суден) включає наступні компоненти:

- УКВ передавач потужністю 12,5 Вт
- Два УКВ приймача для одночасного моніторингу обох каналів AIC
- Приймач супутникової навігації (GPS, ГЛОНАСС, Galileo, BeiDou)
- Процесорний блок з модулятором/демодулятором
- Інтерфейси введення-виведення даних (NMEA 0183/2000, USB, Ethernet)
- Антенна система

Станція AIC класу B (для невеликих комерційних суден та приватних яхт) має спрощену конфігурацію з меншою потужністю передавача (2 Вт) та знижену частоту передачі повідомлень.

Система передає три категорії даних, які представлено у таблиці 1.

Таблиця 1 Категорії даних, що передаються системою AIC

Категорія даних	**Параметри**	**Частота оновлення**
Статичні дані	-MMSI -Номер IMO -Позивний сигнал -Назва судна -Тип судна -Довжина та ширина -Розміщення антени GNSS	Кожні 6 хвилин та при запиті
Динамічні дані	-Координати (широта, довгота) -Мітка часу (UTC Time Stamp) -Курс відносно землі (COG) -Швидкість відносно землі (SOG) -Істинний курс (Heading) -Навігаційний статус -Швидкість зміни курсу (Rate of Turn, ROT)	Залежить від швидкості та маневрування (від 2 секунд до 3 хвилин)
Дані рейсу	-Осадка (Draught) -Тип та кількість небезпечного вантажу -Пункт призначення (Destination) -Розрахунковий час прибуття (ETA, MMDDhhmm) -Кількість осіб на борту (Persons on board)	Кожні 6 хвилин та при зміні даних

Частота передачі динамічних даних залежить від швидкості судна та його маневрування, що відображено у таблиці 2.

Таблиця 2 Частота оновлення динамічних даних AIC залежно від режиму руху судна

Режим руху судна	**Швидкість судна**	**Частота передачі**
На якорі	0 вузлів	3 хвилини
Прямолінійний рух	0-14 вузлів	12 секунд
Під час повороту	0-14 вузлів	4 секунди
Прямолінійний рух	14-23 вузли	6 секунд
Під час повороту	14-23 вузли	2 секунди
Прямолінійний рух	Понад 23 вузли	3 секунди
Під час повороту	Понад 23 вузли	2 секунди

Сучасна інфраструктура моніторингу АІС поєднує наземні станції приймання та супутникові системи, що забезпечує практично повне покриття світового океану. Станом на 2025 рік функціонує понад 5000 наземних станцій АІС у прибережних зонах та більше 100 супутників, обладнаних приймачами АІС [12].

Супутникова система АІС (S-AIS) забезпечує моніторинг суден у відкритих районах океану, де відсутнє покриття наземними станціями. Провідні оператори супутникових систем АІС включають exactEarth (Канада), ORBCOMM (США), Spire Global (США) та інші компанії, що надають послуги глобального відстеження суден.

Характеристики глобальної мережі моніторингу представлено у табл. 3.

Таблиця 3 Характеристики провідних платформ моніторингу АІС (станом на 2025 рік)

Платформа	**Рік заснування**	**Країна**	**Щоденні відвідувачі**	**Кількість відстежуваних суден**	**Оброблення повідомлень за добу**
MarineTraffic	2007	Греція	538 000+	130 000+ (наземна мережа)	Понад 300 млн
VesselFinder	2011	Болгарія	139 000+	100 000+	Понад 250 млн
Vesseltracker	2006	Німеччина	250 000+	170 000+ (наземна + супутникова)	Понад 500 млн
FleetMon	2005	Німеччина	20 000+	80 000+	Понад 150 млн
ShippingExplorer	2012	Данія	5 000+	60 000+	Понад 100 млн

Спуфінг АІС являє собою навмисне спотворення сигналів системи, що призводить до передачі неправдивої інформації про місцезнаходження, ідентифікаційні дані або параметри руху судна. За даними міжнародних досліджень, з 2020 року зафіксовано значне зростання випадків підробки даних АІС [3].

Систематизація обманних практик представлена у таблиці 4.

Таблиця 4 Основні типи спуфінгу АІС та їх характеристики

Тип спуфінгу	**Опис методу**	**Мета застосування**	**Складність виявлення**
AIS Handshake	Обмін ідентифікаційними даними між двома суднами під час зближення. "Чисте" судно передає свої дані "брудному", після чого прямує до порту під прикриттям	Приховування походження вантажу, обхід санкцій	Висока
Судно-зомбі	Використання ідентичності списаного, затонулого або неіснуючого судна для незаконних операцій	Уникнення юридичної відповідальності, контрабанда	Середня
GNSS-спуфінг	Маніпулювання супутниковими сигналами навігації для відображення хибних координат судна	Приховування справжнього маршруту, обхід морських кордонів	Висока
Спуфінг ідентичності	Одночасна передача однакового MMSI більш ніж одним судном	Створення плутанини, дезінформація	Низька

Дослідження Global Fishing Watch виявило наступну географічну концентрацію випадків спуфінгу:

- Чорне море – 28% зафіксованих випадків
- Балтійське море – 19%

- Перська затока – 15%
- Південно-Китайське море – 13%
- Східне Середземномор'я – 11%
- Інші регіони – 14% [13]

Характерними прикладами спуфінгу є інцидент з британським авіаносцем HMS Queen Elizabeth у 2020 році, коли підроблені дані показували рух флотилії з шести суден у напрямку Ірландського моря, тоді як супутникові знімки фіксували порожнє море. У листопаді 2020 року зафіксовано фальшиве вторгнення американського есмінця USS Roosevelt на 4 км у російські територіальні води біля Калінінграда, що могло спровокувати міжнародний конфлікт [3].

Виявлення підробки даних АІС здійснюється через комплексний аналіз множинних джерел інформації та застосування алгоритмів виявлення аномалій. Основні методи представлено у таблиці 5.

Таблиця 5 Методи виявлення спуфінгу АІС

Метод	**Технологія**	**Ефективність**	**Застосування**
Перехресна верифікація	Порівняння даних АІС з радіолокаційними даними та супутниковими зображеннями	85-90%	Центри управління рухом суден, морська охорона
Аналіз RF-сигналів	Оцінка характеристик радіочастотного сигналу (потужність, час проходження)	75-80%	Наземні станції АІС, спеціалізовані центри моніторингу
Алгоритми ШІ	Машинне навчання для виявлення аномальних патернів руху та передачі даних	90-95%	Комерційні платформи моніторингу, аналітичні центри
Часовий аналіз	Виявлення невідповідностей у часових мітках повідомлень	70-75%	Автоматизовані системи контролю
Геопросторовий аналіз	Оцінка фізичної можливості судна перебувати у заявленій точці з урахуванням швидкості та курсу	80-85%	Аналітичні системи, центри морської безпеки

Європейське агентство з морської безпеки (EMSA) розробило систему SeaTrackHub, яка інтегрує дані з різних джерел та використовує алгоритми машинного навчання для автоматичного виявлення аномалій у даних АІС [14]. Система аналізує понад 500 параметрів кожного повідомлення та порівнює їх з історичними даними і очікуваними патернами поведінки.

Міжнародна морська організація (IMO) у Резолюції MSC.1/Circ.1659 (2021) надала рекомендації щодо захисту навігаційних систем від кібератак, включаючи заходи протидії спуфінгу GNSS та АІС [15].

Історичні дані АІС широко застосовуються правоохоронними та контрольними органами для виявлення незаконної діяльності на морі. Основні напрямки використання включають:

Дані АІС дозволяють відстежувати переміщення суден, що можуть порушувати міжнародні санкції. Дослідження 2023 року виявило системне використання спуфінгу танкерами для приховування маршрутів перевезення нафти у обхід санкцій [16].

Платформа Global Fishing Watch використовує дані АІС для моніторингу рибальських суден та виявлення незаконної діяльності у закритих морських зонах. За 2023 рік виявлено понад 15 000 випадків підозрілої поведінки рибальських суден [17].

Дані АІС критично важливі для швидкого виявлення суден у лихі та координації рятувальних операцій. Система дозволяє ідентифікувати найближчі судна до місця інциденту та оцінити їх спроможність надати допомогу.

Дані АІС використовуються для виявлення незаконних скидів, моніторингу викидів у зонах контролю емісій (ECA) та дотримання швидкісних обмежень у екологічно чутливих зонах.

Функціонування системи АІС регулюється комплексом міжнародних конвенцій та стандартів. Основні нормативні документи:

- Міжнародна конвенція СОЛАС (глава V, правило 19) – встановлює обов'язковість обладнання суден транспондерами АІС [1]
- Резолюція IMO A.1106(29) – керівні принципи експлуатації АІС [5]
- Резолюція IMO MSC.74(69) – технічні характеристики обладнання АІС
- Стандарт ITU-R M.1371 – технічні характеристики системи АІС [18]

В Україні регулювання функціонування системи АІС здійснюється відповідно до вимог Кодексу торговельного мореплавства України та нормативних актів Морської адміністрації України. Дунайська комісія встановлює додаткові вимоги щодо використання АІС на внутрішніх водних шляхах [19].

Висновок. Автоматична ідентифікаційна система є фундаментальною складовою сучасної інфраструктури морської безпеки, що забезпечує ідентифікацію та моніторинг більше 170 000 суден у реальному часі через глобальну мережу наземних та супутникових приймачів. Проведене дослідження дозволяє стверджувати, що система АІС, створена два десятиліття тому як засіб запобігання зіткненням суден, трансформувалася у багатофункціональний інструмент глобального значення, який використовується не лише для навігаційних цілей, а й для митного контролю, екологічного моніторингу, протидії незаконній діяльності та координації пошуково-рятувальних операцій.

Технічний аналіз архітектури системи АІС виявив її високу ефективність у передачі навігаційних даних через УКВ-радіозв'язок із використанням методу STDMA, що забезпечує обробку понад 300 мільйонів повідомлень щоденно провідними платформами моніторингу. Система демонструє надійність у передачі трьох категорій даних – статичних, динамічних та даних рейсу – з частотою оновлення від 2 секунд до 6 хвилин залежно від режиму руху судна. Інтеграція наземних станцій приймання (понад 5000 станцій у прибережних зонах) та супутникових систем (більше 100 супутників з приймачами АІС) забезпечує практично повне покриття світового океану.

Проте дослідження виявило критичні виклики кібербезпеки, що загрожують цілісності системи АІС у сучасних умовах. Явище спуфінгу АІС набуло системного характеру, з понад ста задокументованими випадками підробки даних військових та комерційних суден з 2020 року. Найбільш вразливими регіонами є Чорне море (28% випадків), Балтійське море (19%) та Перська затока (15%). Систематизація обманних практик дозволила виділити три основні типи спуфінгу: AIS handshake, судна-зомбі та GNSS-спуфінг, кожен з яких має різний рівень складності виявлення та різні цілі застосування.

Аналіз методів протидії спуфінгу показав, що найвищу ефективність (90-95%) демонструють алгоритми штучного інтелекту, які здатні виявляти аномальні патерни руху та передачі даних. Перехресна верифікація з радіолокаційними даними та супутниковими зображеннями забезпечує ефективність 85-90%, тоді як традиційні методи часового та геопросторового аналізу показують нижчі результати (70-85%). Це підкреслює необхідність впровадження інтелектуальних систем моніторингу, здатних автоматично аналізувати великі обсяги даних та виявляти підозрілу активність.

Фундаментальною проблемою системи АІС є відкритий протокол передачі даних та відсутність вбудованих механізмів аутентифікації, що дозволяє зловмисникам відносно легко генерувати фальшиві повідомлення. Це створює серйозні ризики не лише для безпеки судноплавства, а й для міжнародної політичної стабільності, про що свідчать випадки фальшивого відображення військових кораблів у територіальних водах інших держав.

Перспективи розвитку системи АІС пов'язані з впровадженням технологій нового покоління: блокчейн для забезпечення незмінності даних, VDES для розширення каналів зв'язку, квантової криптографії для абсолютного захисту інформації та адаптації протоколів до потреб автономного судноплавства. Ці напрямки можуть суттєво підвищити захищеність системи від кібератак та розширити її функціональність, проте вимагають координованих зусиль міжнародного співтовариства та значних інвестицій у модернізацію інфраструктури.

Для України, як держави з розвиненою морською інфраструктурою та стратегічним розташуванням на узбережжі Чорного моря – регіону з найвищою концентрацією випадків спуфінгу АІС – питання забезпечення безпеки системи має особливе значення. Необхідно розробити та

імплементувати національну стратегію кібербезпеки морського транспорту, що включатиме конкретні практичні кроки:

1.Створення спеціалізованого національного центру моніторингу AIC при Морській адміністрації України з функціями виявлення спуфінгу, аналізу загроз та координації з міжнародними партнерами.

2.Модернізацію навчальних програм морських навчальних закладів, зокрема Національного університету "Одеська морська академія" та Дунайського інституту, з включенням обов'язкових курсів з кібербезпеки морського транспорту, методів виявлення спуфінгу та роботи з системами аутентифікації даних.

3.Гармонізацію національного законодавства з міжнародними стандартами безпеки AIC, включаючи імплементацію резолюцій IMO та рекомендацій IALA.

4.Участь у міжнародних проектах з розробки захищених протоколів передачі даних та обмін досвідом з провідними морськими державами.

5.Створення системи державного контролю за дотриманням вимог кібербезпеки на суднах під прапором України.

6.Розвиток науково-дослідної бази для проведення національних досліджень у сфері кібербезпеки морського транспорту.

Результати дослідження демонструють, що система AIC перебуває на критичному етапі свого розвитку, коли технологічні можливості моніторингу та обробки даних суттєво випереджають механізми захисту від кіберзагроз. Без термінової модернізації протоколів безпеки та впровадження надійних систем аутентифікації, система AIC ризикує втратити довіру користувачів та свою ефективність як інструменту забезпечення безпеки судноплавства.

Подальші дослідження повинні зосередитися на розробці практичних механізмів виявлення та нейтралізації спуфінгу в умовах української морської інфраструктури, адаптації міжнародного досвіду до національних потреб, створенні методології підготовки фахівців з кібербезпеки морського транспорту та оцінці економічних наслідків впровадження систем захисту для судновласників та портових операторів. Важливим напрямком є також дослідження правових аспектів відповідальності за спуфінг AIC та розробка механізмів міжнародного співробітництва у розслідуванні та попередженні таких інцидентів.

ЛІТЕРАТУРА

1. International Maritime Organization. SOLAS Convention Chapter V – Safety of Navigation, Regulation 19. IMO, 2004.

2. Maritime Safety Committee. Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS). Resolution MSC.1/Circ.1659. IMO, 2021.

3. Bergman B., Jackson T. Spoofed at Sea: Global Fisheries Analysis of AIS Data Falsification. SkyTruth and Global Fishing Watch Report. 2021.

4. International Association of Marine Aids to Navigation and Lighthouse Authorities. IALA Guideline G1082 – An Overview of AIS. Edition 2.0. IALA, 2019.

5. International Maritime Organization. Revised Guidelines for the Operational Use of Shipborne Automatic Identification Systems (AIS). Resolution A.1106(29). IMO, 2015.

6. European Maritime Safety Agency. Annual Overview of Marine Casualties and Incidents 2023. EMSA, 2024.

7. MarineTraffic. About Us – Global Ship Tracking Intelligence. 2025.

8. VesselFinder. Real-time AIS Vessel Tracking Platform Statistics. 2025.

9. Vesseltracker. Global Maritime Intelligence Platform Overview. 2025.

10. International Telecommunication Union. Technical Characteristics for an Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Frequency Band. Recommendation ITU-R M.1371-5. ITU, 2014.

11. exactEarth. Global Maritime Monitoring and Vessel Tracking. Company Report 2024.

12. Global Fishing Watch. Tracking Dataset: AIS Anomaly Detection 2020-2023. GFW Data Portal, 2024.

13. European Maritime Safety Agency. Integrated Maritime Services – SafeSeaNet and SeaTrackHub. EMSA Technical Documentation, 2023.

14. International Maritime Organization. Guidelines on Maritime Cyber Risk Management. Resolution MSC-FAL.1/Circ.3/Rev.1. IMO, 2021.

15. Centre for Research on Energy and Clean Air. Shadow Fleet: Tracking Oil Tankers Evading Sanctions Using AIS Manipulation. CREA Report, 2023.
16. Global Fishing Watch. Illegal, Unreported, and Unregulated Fishing Detection Through AIS Analysis. Annual Report 2023. GFW, 2024.
17. International Telecommunication Union. Technical Characteristics for an Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Frequency Band. Recommendation ITU-R M.1371-5. ITU, 2014.
18. Danube Commission. Recommendations on Technical Requirements for Inland AIS. DC/SES 93/17. Budapest, 2019.
19. Gao M., Liu J., Shen Z. Blockchain-based Data Integrity Verification for Maritime Automatic Identification System. IEEE Access, vol. 8, 2020, pp. 53300-53309.
20. International Association of Marine Aids to Navigation and Lighthouse Authorities. VDES Overview. IALA Guideline G1139. Edition 2.0. IALA, 2021.

REFERENCES

1. International Maritime Organization. SOLAS Convention Chapter V – Safety of Navigation, Regulation 19. IMO, 2004.
2. Maritime Safety Committee. Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS). Resolution MSC.1/Circ.1659. IMO, 2021.
3. Bergman B., Jackson T. Spoofed at Sea: Global Fisheries Analysis of AIS Data Falsification. SkyTruth and Global Fishing Watch Report. 2021.
4. International Association of Marine Aids to Navigation and Lighthouse Authorities. IALA Guideline G1082 – An Overview of AIS. Edition 2.0. IALA, 2019.
5. International Maritime Organization. Revised Guidelines for the Operational Use of Shipborne Automatic Identification Systems (AIS). Resolution A.1106(29). IMO, 2015.
6. European Maritime Safety Agency. Annual Overview of Marine Casualties and Incidents 2023. EMSA, 2024.
7. MarineTraffic. About Us – Global Ship Tracking Intelligence. 2025.
8. VesselFinder. Real-time AIS Vessel Tracking Platform Statistics. 2025.
9. Vesseltracker. Global Maritime Intelligence Platform Overview. 2025.
10. International Telecommunication Union. Technical Characteristics for an Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Frequency Band. Recommendation ITU-R M.1371-5. ITU, 2014.
11. exactEarth. Global Maritime Monitoring and Vessel Tracking. Company Report 2024.
12. Global Fishing Watch. Tracking Dataset: AIS Anomaly Detection 2020-2023. GFW Data Portal, 2024.
13. European Maritime Safety Agency. Integrated Maritime Services – SafeSeaNet and SeaTrackHub. EMSA Technical Documentation, 2023.
14. International Maritime Organization. Guidelines on Maritime Cyber Risk Management. Resolution MSC-FAL.1/Circ.3/Rev.1. IMO, 2021.
15. Centre for Research on Energy and Clean Air. Shadow Fleet: Tracking Oil Tankers Evading Sanctions Using AIS Manipulation. CREA Report, 2023.
16. Global Fishing Watch. Illegal, Unreported, and Unregulated Fishing Detection Through AIS Analysis. Annual Report 2023. GFW, 2024.
17. International Telecommunication Union. Technical Characteristics for an Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Frequency Band. Recommendation ITU-R M.1371-5. ITU, 2014.
18. Danube Commission. Recommendations on Technical Requirements for Inland AIS. DC/SES 93/17. Budapest, 2019.
19. Gao M., Liu J., Shen Z. Blockchain-based Data Integrity Verification for Maritime Automatic Identification System. IEEE Access, vol. 8, 2020, pp. 53300-53309.
20. International Association of Marine Aids to Navigation and Lighthouse Authorities. VDES Overview. IALA Guideline G1139. Edition 2.0. IALA, 2021.

Kvasnikov P.K

AUTOMATIC IDENTIFICATION SYSTEM FOR MARITIME SAFETY: CURRENT DEVELOPMENT REALITIES AND CYBERSECURITY CHALLENGES

The Automatic Identification System (AIS) is a critically important component of modern maritime shipping, ensuring navigation safety and effective maritime traffic management. The system, originally created as a means of preventing vessel collisions, has transformed into a multifunctional global monitoring tool used by vessel traffic services, customs authorities, port administrations, and law enforcement agencies worldwide. According to SOLAS Convention requirements, since 2004, the AIS has been mandatory for passenger vessels, tankers, and vessels with gross tonnage exceeding 300 tons. As of 2025, the global monitoring network processes over 300 million AIS messages daily, tracking more than 170,000 vessels in real-time through terrestrial and satellite systems. The article examines the technical architecture of the AIS, which operates based on VHF radio communication in maritime frequency bands (161.975 MHz and 162.025 MHz) using Self-organizing Time Division Multiple Access (STDMA) method. Leading international vessel tracking platforms are analyzed: MarineTraffic (serving over 538,000 users daily), VesselFinder (approximately 139,000 daily users), Vesseltracker, and ShippingExplorer, providing access to real-time AIS data. Particular attention is paid to the growing cybersecurity problem – the phenomenon of AIS spoofing, which poses a serious threat to international shipping. Research from 2020-2023 revealed over one hundred cases of data falsification involving military and commercial vessels from 14 countries worldwide. Three main types of deceptive practices are systematized: AIS handshake (using decoy vessels), ghost ships (using identities of non-existent vessels), and location manipulation through GNSS. Methods for detecting spoofing are examined, including the application of artificial intelligence algorithms and cross-verification with radar and satellite data. The use of AIS data in combating illegal activities is analyzed, including detection of sanctions violations, smuggling, and piracy. The need to improve international AIS security protocols, develop effective data authentication mechanisms, and coordinate efforts among governments, international organizations, and the private sector to ensure system integrity is emphasized. The article material will be useful for maritime industry professionals, cybersecurity researchers, maritime educational institutions instructors, and those responsible for maritime traffic management and port operations security.

Keywords: *automatic identification system, AIS, maritime safety, spoofing, maritime transport cybersecurity, vessel monitoring, GNSS, satellite tracking, marine navigation, maritime traffic management, SOLAS, STDMA*

Стаття прийнята 20.09.2025