УДК 629.5.056:004.732.056.5 doi.org/10.33298/2226-8553.2026.1.45.17

© Кучерук Г.Ю., Ганношина І.М.

МЕТОДИ ВИЯВЛЕННЯ СПУФІНГУ В СУДНОВИХ НАВІГАЦІЙНИХ СИСТЕМАХ

Стаття присвячена систематизації та порівняльному аналізу сучасних методів виявлення GPS/GNSS-спуфінгу у суднових навігаційних системах. Розглянуто фізичні принципи спуфінг-атак, їх класифікацію за складністю, цільовим об'єктом та наслідками для безпеки мореплавства. Детально проаналізовано методи виявлення на основі: моніторингу рівня сигналу та відношення несучої до шуму (C/N₀), перевірки узгодженості міжсупутникових доплерівських зсувів, кросперевірки з альтернативними позиційними системами (AIS, eLoran, IMO), гібридної інерційно-супутникової навігації з фільтром Калмана, а також методів машинного навчання – зокрема рекурентних нейронних мереж LSTM та ансамблевих класифікаторів. Запропоновано багаторівневу архітектуру захисту навігаційних систем, яка інтегрує сигнальний, навігаційний та мережевий рівні виявлення та визначені технічні передумови щодо її коректного функціонування.

Ключові слова: *GNSS-спуфінг, суднова навігація, GPS-безпека, виявлення аномалій, фільтр Калмана, машинне навчання, AIS, архітектура захисту навігаційних систем.*

Постановка проблеми. Глобальні навігаційні супутникові системи (GNSS), зокрема GPS, GLONASS, Galileo та BeiDou, стали невід'ємною основою сучасного судноплавства. Вони забезпечують позиціювання, навігацію та синхронізацію часу для більш ніж 90 % комерційних суден у світі. Однак зростаюча залежність від GNSS-сигналів створює серйозні вразливості перед навмисними атаками — зокрема GPS-спуфінгом.

Таким чином, виникає науково-технічна проблема побудови архітектури захисту навігаційних систем від спуфінгу, обумовлена необхідністю підвищення надійності навігаційного забезпечення суден в умовах зростання радіоелектронних та кібернетичних впливів. Традиційні підходи до навігації, що базуються виключно на GNSS, вже не забезпечують належного рівня стійкості, тому сучасні дослідження орієнтовані на розробку комплексних методів виявлення та протидії спуфінгу.

Аналіз останніх досліджень і публікацій. Проблема виявлення спуфінгу в суднових навігаційних системах зумовлена вразливістю GNSS-сигналів до навмисних атак, що спотворюють навігаційну інформацію [1]. У наукових дослідженнях сформовано кілька ключових підходів до її вирішення.

Методи аналізу радіосигналу базуються на контролі параметрів GNSS, зокрема рівня сигналу, співвідношення сигнал/шум та доплерівських зсувів, що дозволяє оперативно виявляти аномалії [1]. Їх розвитком є використання програмно-визначених радіосистем (SDR), які забезпечують гнучкий моніторинг сигналів у реальному часі. Зокрема, у дослідженні [2] запропоновано SDR-платформу для виявлення спуфінгу на борту суден, яка забезпечує високий рівень адаптивності до змін сигнального середовища. Водночас ефективність таких методів обмежена у випадку складних атак, що імітують характеристики справжнього сигналу.

Другий напрям досліджень пов’язаний із використанням інтегрованих навігаційних систем. В роботі [3] розглянуті інтегровані підходи, зокрема поєднання GNSS із інерційними системами (INS) та використання AIS, які дозволяють виявляти невідповідності між різними джерелами навігаційних даних. Застосування фільтру Калмана, за твердженням авторів [4], підвищує точність оцінювання стану судна в умовах нелінійної динаміки та морського хвилювання, однак такі методи залежать від доступності зовнішніх даних.

Суттєвий розвиток отримали методи машинного навчання. Зокрема, згорткові нейронні мережі (CNN) за даними дослідження [5], забезпечують точність понад 97 % при аутентифікації

сигналів, тоді як рекурентні мережі (зокрема LSTM) демонструють високу ефективність для аналізу часових залежностей GNSS-даних та перевершують класичні алгоритми машинного навчання у задачах виявлення спуфінгу [6]. В роботі [7] обґрунтовується застосування федеративного навчання, що дозволяє підвищити ефективність моделей без розкриття конфіденційних навігаційних даних, оскільки навчання відбувається локально, а передаються лише параметри моделей

Вагомий внесок у дослідження проблем виявлення спуфінгу здійснили українські науковці. Зокрема, у роботах [8-11] запропоновано моделі загроз GNSS-систем, гібридні методи виявлення атак із використанням алгоритмів машинного навчання, а також технічні рішення підвищення стійкості приймачів до спуфінгу. Окрему увагу приділено застосуванню антенних решіток, інтегрованих систем моніторингу та аналізу впливу радіоелектронних перешкод на навігаційні системи в умовах сучасних загроз.

У нормативних документах підкреслюється необхідність впровадження багаторівневих систем захисту та автоматизованого виявлення атак із мінімальною затримкою реакції [12, 13]. Загалом результати досліджень свідчать, що жоден окремий метод не забезпечує достатнього рівня надійності, що обґрунтовує доцільність комплексного підходу до виявлення спуфінгу [14, 15].

Невирішена частина проблеми. Аналіз наукової літератури дозволяє виявити такі систематичні прогалини, які й обумовлюють наукову новизну даної статті. Більшість досліджень розглядають окремі методи виявлення ізольовано, без оцінки їх взаємодоповнення у багаторівневій архітектурі, орієнтовані на авіаційний або наземний транспорт, відсутній єдиний публічний набір даних GNSS-атак у морському контексті. Це визначає спрямованість даного дослідження: запропонувати систематизований порівняльний аналіз методів виявлення та обґрунтовану архітектуру їх інтеграції, адаптовану до вимог морського судноплавства.

Метою статті є систематизація актуальних методів виявлення спуфінг-атак у суднових навігаційних системах, їх порівняльний аналіз за ефективністю, складністю реалізації та практичною застосовністю для морської галузі.

Виклад основного матеріалу. Сучасний розвиток морського транспорту супроводжується активною цифровізацією процесів судноводіння, що зумовлює широке використання глобальних навігаційних супутникових систем (GNSS) як основного джерела визначення координат, швидкості та курсу судна. Водночас зростає вразливість навігаційних систем до зовнішніх кіберзагроз, серед яких особливо небезпечним є спуфінг – навмисна підміна навігаційного сигналу з метою введення в оману систем позиціонування. Такі атаки можуть призводити до значних відхилень у визначенні місцеположення судна, створюючи передумови для аварійних ситуацій, зіткнень або посадок на мілину, що суперечить вимогам безпеки мореплавства, встановленим IMO. На відміну від глушіння (джамінгу), яке є очевидним через втрату сигналу, спуфінг значно небезпечніший: він формує хибну, але технічно достовірну картину навколишнього середовища, не активуючи стандартних сигналів тривоги.

За рівнем складності та технічними характеристиками спуфінг-атаки поділяються на три категорії. Спрощений (некогерентний) спуфінг – використовує заздалегідь записані GNSS-сигнали або генератор на основі програмно-визначеного радіо (SDR) без синхронізації з реальним сигналом. Такий тип легко реалізується, але залишає очевидні артефакти: різкий стрибок рівня сигналу, незбіг у часових мітках, миттєва зміна координат. Середньої складності (частково когерентний) спуфінг – атакуючий відстежує реальні сигнали GNSS та поступово вводить хибні з близькими параметрами. Перехід між легітимним і підробленим сигналом відбувається плавно, що ускладнює виявлення за порогом рівня сигналу. Складний (повністю когерентний) спуфінг – реалізується зі знанням точного положення цілі, дозволяє передавати сигнали з точними псевдодальностями та доплерівськими зсувами, що відповідають реальному сценарію. Для його реалізації необхідне спеціалізоване обладнання великої вартості.

За цільовою ознакою виділяють: атаки на позицію (підміна координат), атаки на час (спотворення PPS-імпульсу та UTC-часу), атаки на швидкість (маніпуляція вектором швидкості) та комплексні атаки (одночасна підміна PVT-рішення). За ефектом дії – атаки одиночного виведення (переміщення в конкретну хибну точку) та атаки захоплення і дрейфу (поступове відведення з реальної траєкторії).

У практиці судноводіння проблема ускладнюється тим, що сучасні інтегровані навігаційні комплекси поєднують дані з різних джерел, зокрема Automatic Identification System, радіолокаційних станцій та Electronic Chart Display and Information System, однак у більшості випадків саме GNSS залишається базовим джерелом координат. За умов спуфінгу ці системи можуть відображати узгоджену, але хибну інформацію, що значно ускладнює своєчасне виявлення загрози.

Для уникнення загрози спуфінгу потрібно використовувати інструменти протидії. Розглянемо сучасні методи виявлення спуфінгу в суднових навігаційних системах.

Одним із найбільш поширених підходів є методи аналізу радіосигналу. До них відноситься моніторинг AGC та C/N₀, метод аналізу міжсупутникових доплерівських зсувів та метод аналізу фазових вимірювань несучої (Carrier Phase).

Моніторинг AGC та C/N₀ - автоматичне регулювання підсилення (AGC) є першою лінією захисту приймача. У нормальних умовах AGC підтримує стабільний вихідний рівень, компенсуючи варіації вхідного сигналу. При спуфінгу потужний синтетичний сигнал викликає різке зменшення коефіцієнта підсилення AGC, що реєструється як цифровий показник AGC voltage (VAGC). Падіння VAGC більш ніж на 3 дБ за час менше 1 секунди є індикатором можливого спуфінгу.

Відношення потужності несучої до спектральної густини шуму (C/N₀, вимірюється у дБ-Гц) характеризує якість прийнятого сигналу. Норма для відкритого неба: 35-45 дБ-Гц. При спуфінгу синтетичний сигнал, як правило, має більшу потужність: значення C/N₀ перевищують 50–65 дБ-Гц, що фізично неможливо для природного GNSS-сигналу на відстані 20 200 км (орбіта GPS). Алгоритм виявлення: при $\Delta(C/N_0) > 10$ дБ-Гц протягом 2–3 послідовних епох = попередження. Однак аналіз лише рівня сигналу не завжди достатній — складніші атаки маскують потужність. Тому паралельно застосовується перевірка узгодженості доплерівських зсувів між супутниками.

Доплерівський зсув частоти для кожного супутника залежить від відносної швидкості між супутником і приймачем і є строго детермінованим при заданих ефемеридах і відомому положенні приймача. Для n видимих супутників справжні доплерівські зсуви $\{f_{d,1}, f_{d,2}, ..., f_{d,n}\}$ взаємно узгоджені через спільний вектор швидкості приймача. Базова умова узгодженості визначається нерівнісю , де $\varepsilon \approx 0.5–1.0$ *Гц*.:

$$||\Delta f\_{d,measured} - \Delta f\_{d,predicted}|| < \varepsilon, \quad (1)$$

де, $\Delta f\_{d,predicted}$ - очікуване значення (predicted);
$\Delta f\_{d,measured}$ -виміряне значення (measured).

При спуфінгу зловмисник, який не знає точної швидкості руху судна, генерує доплерівські зсуви, що не відповідають кінематиці реального руху. Перевірка попарних різниць доплерівських зсувів між супутниками має розбіжність понад 2 Гц. Аналіз виконується з частотою 1–10 Гц і забезпечує виявлення більшості атак середньої складності.

Ще більш чутливим інструментом є аналіз фазових вимірювань несучої, який дозволяє виявляти навіть ретельно підготовлені атаки за субміліметровими аномаліями. Фазові вимірювання несучої мають похибку порядку 1–2 мм, тоді як кодові псевдодальності – порядку 1–3 м. При спуфінгу різниця між фазовими та кодовими псевдодальностями виходить за межі очікуваного шуму. Додатково, миттєве «захоплення» приймача хибним сигналом призводить до стрибка у накопиченому лічильнику цілих циклів фази (integer ambiguity), що є характерним індикатором атаки.

Описані методи аналізу радіосигналу спираються виключно на внутрішні параметри GNSS-приймача. Для підвищення надійності виявлення доцільно залучати незалежні зовнішні джерела позиційних даних, для чого використовуються методи кросперевірки з альтернативними джерелами. До них відноситься інтеграція з системою AIS і eLoran та наземні радіонавігаційні системи.

Інтеграція з системою AIS. Автоматична ідентифікаційна система (AIS) транслює позицію, курс і швидкість судна іншим учасникам руху незалежно від GNSS-прийому. При спуфінгу GNSS-позиція судна на власному екрані може не збігатися з AIS-позицією, яку спостерігають інші судна. Алгоритм виявлення порівнює власну GNSS-позицію з позицією, отриманою від сусідніх суден, та відстежує геометричну несумісність ситуаційної картини. Але є обмеження методу: AIS також може бути піддано

атаці (AIS-спуфінг), тому необхідна взаємна перевірка та ранжування джерел. Вирішення реалізується через Bayesian trust framework, де кожному джерелу позиції призначається вага довіри, що динамічно оновлюється.

Якщо AIS є мережевим джерелом і сам потенційно вразливий, то eLoran пропонує принципово інший фізичний принцип роботи, що робить його стійким навіть до координованих атак.

Система eLoran (Enhanced Long-Range Aid to Navigation) є вдосконаленою версією Loran-C і функціонує у НЧ-діапазоні (100 кГц). Її принцип роботи докорінно відрізняється від GNSS: наземні передавачі, розташовані за 1 000–2 000 км, є стійкими до перехоплення і глушіння через значно вищу потужність сигналу (250–1 000 кВт). Точність eLoran: 10–30 м при використанні диференціальних поправок (dLoran). Кросперевірка GNSS-позиції з eLoran-рішенням забезпечує незалежний контроль із затримкою менше 5 секунд.

Кросперевірка з зовнішніми системами ефективна, але залежить від їх доступності. Більш автономним підходом є інтеграція GNSS із бортовою інерційною системою навігації.

Гібридна інерційно-супутникова навігація (GNSS/INS) – це інерційна навігаційна система (INS) на базі гіроскопів і акселерометрів, яка забезпечує автономне визначення положення без зовнішніх радіосигналів. Якість сучасних тактичних IMU (Inertial Measurement Unit): дрейф гіроскопа – 0.001-0.01 °/год (клас навігаційної точності). Фундаментальна властивість: помилка INS накопичується у часі (інтеграція похибок), тоді як GNSS має незалежні та не пов'язані у часі похибки.

Класичний алгоритм інтеграції – розширений фільтр Калмана (EKF) або Unscented Kalman Filter (UKF) – об'єднує GNSS-вимірювання та INS-прогноз у оптимальній байєсівській оцінці стану (рівняння 2). Вектор стану включає: положення (3D), швидкість (3D), орієнтацію (quaternion), похибки акселерометра, похибки гіроскопа та GNSS-зміщення годинника.

$$\hat{x}_k = F_k\,\hat{x}_{k-1} + K_k(z_k - H_k\,F_k\,\hat{x}_{k-1}), \qquad (2)$$

де, $F_k\,\hat{x}_{k-1}$- прогноз інерціальної системи (INS)

$\hat{x}_k$ – нова оцінка стану

K_k – матриця підсилення Калмана,

z_k – вектор вимірювань GNSS,

H_k – матриця спостереження.

Ідея детектора спуфінгу: якщо GNSS-інновація $\|z_k - H_k\,\hat{x}_k^-\|$ перевищує 3σ-поріг, визначений на основі коваріаційної матриці S_k, система фіксує аномалію та підвищує вагу INS-рішення. Фільтр Калмана є потужним математичним інструментом, однак залишається детерміністичним. Для розпізнавання складних нелінійних патернів атак перспективним доповненням є методи машинного навчання. До методів машинного навчання відноситься метод з використанням рекурентних нейронних мереж LSTM і ансамблеві методи та аномалій-детектори.

Рекурентні нейронні мережі LSTM - мережі Long Short-Term Memory (LSTM) здатні моделювати часові залежності у послідовностях навігаційних даних, що робить їх природним вибором для аналізу GNSS-трас. Вхідний вектор для кожного часового кроку включає: AGC, C/№ по кожному SV, доплерівські залишки, PDOP/HDOP, delta-position між послідовними епохами, температурні та кутові характеристики із IMU.

Архітектура класифікатора двошарова LSTM (256 + 128 нейронів) → GlobalAveragePooling → Dense(64, ReLU) → Dropout(0.3) → Dense(1, Sigmoid). Навчання виконується на синтетичних даних із відомими атаками різного типу та реальних лог-файлах GNSS-приймачів. Точність на тестовій вибірці: 94–97 % при хибнопозитивній тривозі менше 2 %. Завдяки батч-обробці LSTM дає відповідь з затримкою 1–3 секунди при частоті дискретизації 1-10 Гц.

LSTM є оптимальним вибором для потужних обчислювальних платформ. Для систем з обмеженими ресурсами або у разі відсутності розміченої навчальної вибірки доцільно застосовувати ансамблеві підходи та детектори аномалій.

Ансамблеві методи, зокрема Random Forest та Gradient Boosting (XGBoost, LightGBM), демонструють ефективність 88–93 % при значно меншій обчислювальній вартості порівняно з LSTM.

Вони особливо корисні на вбудованих системах із обмеженими ресурсами (ARM Cortex-M, FPGA-реалізації). Ізоляційний ліс (Isolation Forest) використовується як детектор аномалій без необхідності розміченої навчальної вибірки: ефективність для невідомих типів атак – 80-86 %.

Усі розглянуті методи є реактивними – вони виявляють атаку після її початку. Принципово інший, превентивний підхід пропонує криптографічна аутентифікація сигналу, яка унеможливлює підробку ще на рівні його формування.

Криптографічна аутентифікація навігаційного повідомлення (OSNMA – Open Service Navigation Message Authentication) є єдиним фундаментальним рішенням, що усуває загрозу спуфінгу на рівні формування сигналу. Система Galileo OSNMA використовує схему Tesla (Timed Efficient Stream Loss-tolerant Authentication) для підпису навігаційних повідомлень. Принцип TESLA: сервер генерує ланцюжок симетричних ключів K_0, K_1, ..., K_n та підписує кожне повідомлення ключем K_i, а сам ключ розкриває у наступному часовому кроці. Приймач зберігає MAC та перевіряє його після отримання ключа.

Отже, методи аналізу радіосигналу забезпечують швидке виявлення базових атак, але є недостатніми для складних сценаріїв. Інтеграція з зовнішніми системами та інерційною навігацією підвищує надійність, а методи машинного навчання дозволяють виявляти складні патерни атак. Використання криптографічної аутентифікації забезпечує запобігання спуфінгу на рівні сигналу.

Методи захисту суднових навігаційних систем від спуфінгу, принцип роботи, переваги і недоліки в узагальненому вигляді наведені у табл.1.

Таблиця 1 - Класифікація методів захисту суднових навігаційних систем від спуфінгу

Метод	Принцип роботи	Ключові параметри	Переваги	Недоліки
Методи аналізу радіосигналу				
AGC та C/N₀	Аналіз рівня сигналу	VAGC, C/N₀	Швидкість	Обмежена точність
Доплерівські зсуви	Узгодженість швидкостей	Δfd	Виявлення атак	Залежність від даних
Фазові вимірювання	Аналіз фазових аномалій	мм точність	Висока чутливість	Складність
Методи кросперевірки				
AIS	Порівняння позицій	Геометрія	Незалежність	Вразливість
eLoran	Наземна навігація	10–30 м	Стійкість	Обмеження
Інерційно-супутникові методи				
GNSS/INS	Фільтр Калмана	3σ критерій	Автономність	Дрейф
Методи машинного навчання				
LSTM	Часові ряди	94–97%	Висока точність	Ресурси
Random Forest/XGBoost	Класифікація	88–93%	Ефективність	Менша точність
Isolation Forest	Аномалії	80–86%	Без навчання	Нижча точність
Криптографічні методи				
OSNMA	Аутентифікація сигналу	~30 с	Надійність	Затримка

Джерело: систематизовано автором на основі [1- 7]

Наведені методи набувають практичного значення лише в контексті реальних загроз. Ефективний захист суднових навігаційних систем від спуфінгу потребує комплексного підходу. Тому, на основі аналізу переваг і недоліків кожного методу запропоновано трирівневу архітектуру виявлення і захисту суднових навігаційних систем від спуфінгу (рис.1).

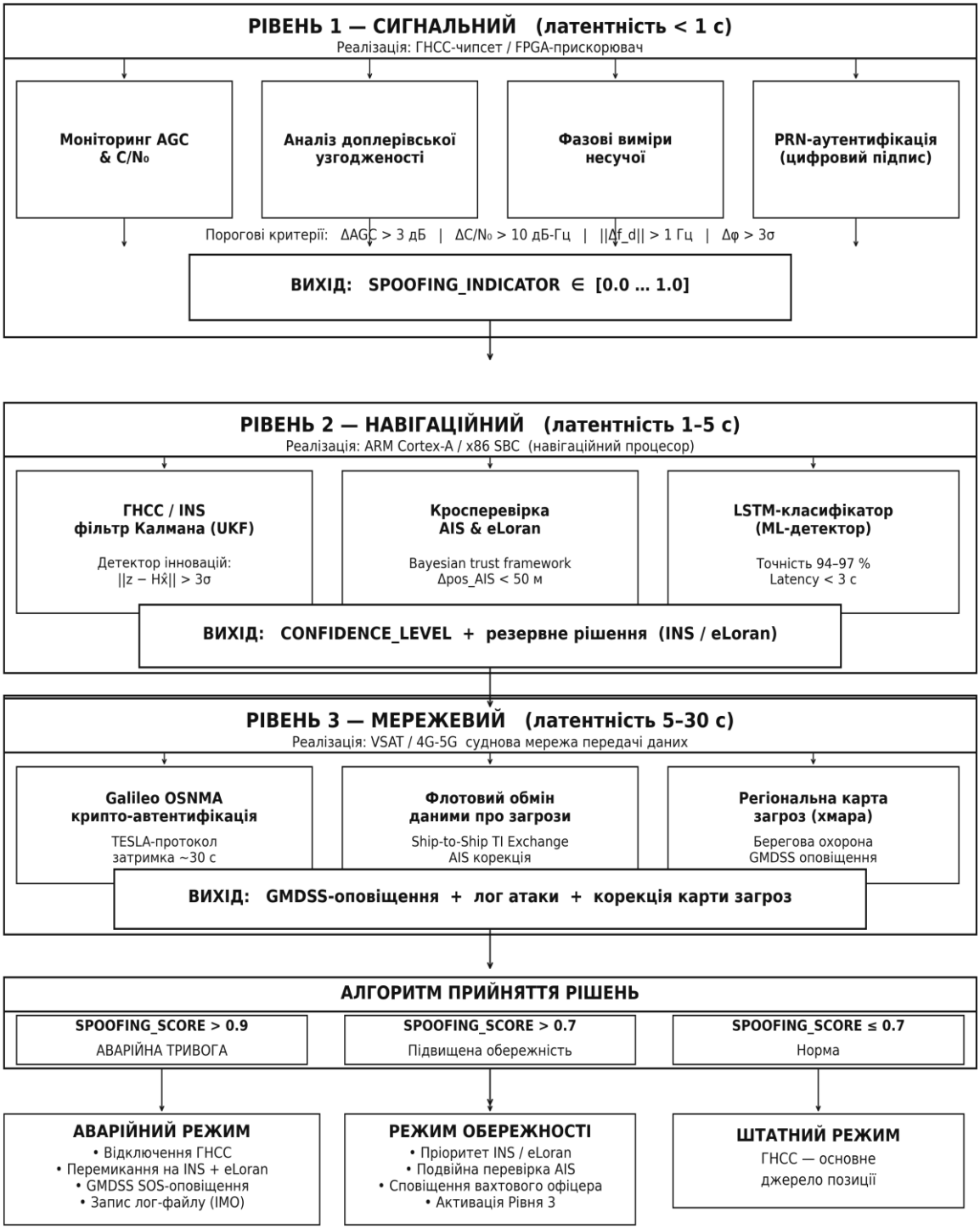

Рисунок 1 - Архітектура захисту суднових навігаційних систем від спуфінгу
Джерело: запропоновано авторами

Рівень 1 – Сигнальний рівень (латентність: < 1 с). Реалізується безпосередньо у GNSS-чипсеті або FPGA-прискорювачі. Включає: безперервний моніторинг AGC та C/N₀ з адаптивним порогом (3σ), аналіз доплерівської узгодженості між каналами, перевірку фазових вимірювань несучої. Формує: бінарний прапор підозрілого сигналу та метрику якості SPOOFING_INDICATOR (0.0–1.0).

Рівень 2 – Навігаційний рівень (латентність: 1–5 с). Реалізується у навігаційному процесорі (ARM Cortex-A або x86 SBC). Включає: GNSS/INS інтеграцію з UKF та детектором інновацій, кросперевірку

з AIS та eLoran, LSTM-класифікатор на агрегованих ознаках. Формує: рівень достовірності позиції CONFIDENCE_LEVEL та активацію резервного рішення.

Рівень 3 — Мережевий рівень (латентність: 5–30 с). Реалізується через суднову мережу передачі даних (VSAT, 4G/5G). Включає: обмін даними про GNSS-якість із береговою охороною та іншими суднами, агрегацію флотових спостережень у хмарній платформі, криптографічну аутентифікацію через Galileo OSNMA. Формує: регіональну карту загроз та оповіщення для берегових служб.

Алгоритм прийняття рішень використовує зважену суму індикаторів усіх рівнів: якщо SPOOFING_SCORE > 0.7, система переходить у режим «підвищеної обережності» та починає пріоритизувати INS та eLoran над GNSS. При SPOOFING_SCORE > 0.9 активується аварійна сигналізація, записується лог-файл для подальшого розслідування та надсилається сповіщення GMDSS.

Запропонована архітектура є масштабованою та може застосовуватися у різних конфігураціях залежно від типу судна, операційного середовища та наявного обладнання.

Повна трирівнева архітектура (рівні 1 + 2 + 3) повинна бути обов'язковою для суден, що відповідають хоча б одному з таких критеріїв: валова місткість понад 500 GT відповідно до вимог IMO та SOLAS Convention, що передбачає обов’язкове встановлення систем AIS і ECDIS, оскільки саме такі судна є першочерговими цілями спуфінг-атак через високу цінність вантажу або пасажирів; плавання у зонах підвищеного ризику, зокрема в акваторії Балтійського моря, Перській затоці, Ормузькій та Малаккській протоках, а також уздовж узбережжя Північної Кореї, де систематично фіксуються випадки GNSS-спуфінгу; перевезення небезпечних вантажів класів IMO 1–9, де відхилення від затвердженого маршруту є кримінальним правопорушенням і може мати катастрофічні наслідки; експлуатація пасажирських суден і поромних ліній через високий рівень публічного інтересу та значний масштаб потенційних збитків у разі аварії; а також участь суден у морських операціях під егідою NATO або ЄС, де GNSS-спуфінг розглядається як один з інструментів гібридної війни.

Конфігурація рівнів 1 + 2 без мережевого компонента є достатньою для суден каботажного плавання (до 200 морських миль від берега) зі стабільним покриттям мобільних мереж, де мережевий рівень може бути реалізований через LTE замість супутникового зв’язку VSAT із суттєво нижчою вартістю; суден із застарілою інфраструктурою зв’язку, де впровадження третього рівня потребує повної модернізації суднової мережі та є економічно недоцільним у короткостроковій перспективі; а також промислових і рибопромислових суден, що працюють у районах із відсутністю покриття супутникового зв’язку, де перші два рівні можуть ефективно функціонувати автономно без зовнішніх мережевих з’єднань.

Мінімальна конфігурація, що включає лише сигнальний рівень, є прийнятною як тимчасовий захід для малих суден (GT < 500) та яхт, на які не поширюються обов’язкові вимоги SOLAS Convention, але власники яких прагнуть забезпечити базовий захист від некогерентних атак; портів, де впровадження повної архітектури здійснюється поетапно, і така конфігурація застосовується першою, дозволяючи самостійно виявляти до 75 % атак; а також навчальних суден і тренажерних центрів, у яких архітектура використовується з демонстраційною та освітньою метою.

Для коректного функціонування архітектури захисту суднових навігаційних систем від спуфінгу необхідне виконання таких технічних передумов:

1. Використання GNSS-приймача, що підтримує виведення «сирих» вимірювань (raw measurements): AGC-значення, C/№ по кожному каналу, фазові псевдодальності несучої. Більшість сучасних морських приймачів (u-blox M9, NovAtel OEM7, Septentrio mosaic-X5) надають ці дані через стандартний інтерфейс NMEA 0183 / NMEA 2000 або власні бінарні протоколи.

2. Наявність IHC (або IMU) з класом точності не нижче «тактичного» (дрейф гіроскопа ≤ 0.01 °/год). Використання MEMS-IMU навігаційного класу є мінімально прийнятним; стратегічний клас (≤ 0.001 °/год) забезпечує кращу якість детектора інновацій на Рівні 2.

3. Для Рівня 3 необхідна пропускна здатність каналу зв'язку не менше 64 кбіт/с для передачі GNSS-метаданих у режимі реального часу. VSAT-термінали класу VSAT-mini (Intellian v100, Cobham SAILOR 900) задовольняють цю вимогу за будь-яких умов плавання.

Запропонована структура захисту суднових навігаційних систем від спуфінгу може бути практично реалізованою та відповідає чинним вимогам IMO і BIMCO.

Висновок. Проведений аналіз методів виявлення GPS/GNSS-спуфінгу в суднових навігаційних системах дозволяє сформулювати такі висновки.

Жоден одиночний метод не забезпечує прийнятного захисту для всього діапазону загроз від спрощених до повністю когерентних атак. Тільки комплексний підхід, що поєднує сигнальний аналіз, навігаційну кросперевірку та методи машинного навчання дають достатню ефективність. Найбільш практично реалізованим методом є гібридна GNSS/INS інтеграція на базі фільтра Калмана середньої ефективності, доступна як оновлення програмного забезпечення для більшості сучасних суднових навігаційних комплексів. Криптографічна аутентифікація Galileo OSNMA є єдиним методом, що забезпечує теоретично незламний захист, проте потребує сумісного обладнання і поширена лише серед нових суден та суден із модернізованими GNSS-приймачами. Методи машинного навчання, зокрема LSTM-класифікатори, показують найвищу ефективність для складних атак, проте вимагають якісних навчальних наборів даних, які наразі є обмеженими у публічному доступі через конфіденційність інцидентів.

Запропонована трирівнева архітектура захисту відповідає вимогам IMO ISM Code та рекомендаціям BIMCO/IACS для суднових кіберсистем і може бути інтегрована у наявні ECDIS та IBNS без заміни базового обладнання.

ЛІТЕРАТУРА

1. Singh S., Singh J., Singh S., Goyal S. B., Raboaca M. S., Verma C., Suciu G. Detection and Mitigation of GNSS Spoofing Attacks in Maritime Environments Using a Genetic Algorithm // *Mathematics*. 2022. Vol. 10, No. 21. Article 4097. URL: https://www.mdpi.com/2227-7390/10/21/4097
2. IACS**.** UR E26/E27: Cyber resilience of ships. – 2022. – URL: https://iacs.org.uk
3. Zhang H., Wang J., Wang J., Liu X. GNSS spoofing detection based on multi-feature fusion and machine learning // *Computers & Fluids*. 2021. Vol. 231. Article 105141. URL: https://www.sciencedirect.com
4. Cole B., Schamberg G. Unscented Kalman Filter for Long-Distance Vessel Tracking in Geodetic Coordinates // *Applied Ocean Research*. 2022. Vol. 124. Article 103205. URL: https://www.sciencedirect.com/science/article/pii/S0141118722001468
5. BIMCO**.** Guidelines on Cyber Security Onboard Ships. Version 4. – London: BIMCO, 2020. – 61 p. – URL: https://www.bimco.org/media/oq0ft0gr/guidelines-on-cyber-security-onboard-ships-v4-1.pdf
6. Semanjski S., Semanjski I., De Wilde W., Gautama **S.** GNSS spoofing detection by supervised machine learning with validation on real-world meaconing and spoofing data — Part II // *Sensors*. 2020. Vol. 20, No. 7. Article 1806. URL: https://www.mdpi.com/1424-8220/20/7/1806
7. Liu W., Papadimitratos P. Self-Supervised Federated GNSS Spoofing Detection with Opportunistic Data // *Proceedings of the ION GNSS+ Conference*. 2025. URL: https://arxiv.org/abs/2505.06171
8. Снєосіков О. А. Методи виявлення та протидії кібератакам типу gps spoofing і gps jamming з використання аі для систем диференційної корекції та глобальної навігаційної супутникової системи // *Вісник Хмельницького національного університету. Технічні науки*. 2025. Т. 355, № 4. С. 584–592. DOI: https://doi.org/10.31891/2307-5732-2025-355-82
9. Снєосіков О. А., Нарєжній О. П. Моделі загроз та порушника автономної системи диференціальної корекції глобальних навігаційних супутникових систем // *Вісник Херсонського національного технічного університету*. 2025. № 3. DOI: https://doi.org/10.35546/kntu2078-4481.2025.3.2.54
10. Наритник Т., Присяжний В., Капштик С. та ін. Improvement of the GPS signal receiving resistance against electromagnetic interference, jamming, and spoofing // *Information and Telecommunication Sciences*. 2022. Vol. 13, No. 2. P. 4–14. DOI: https://doi.org/10.20535/2411-2976.22022.4-14
11. Авілов А. І. Боротьба зі спуфінгом на безпілотних літальних апаратах // *Збірник наукових праць ХНУПС*. 2024. № 2(80). DOI: https://doi.org/10.30748/zhups.2024.80.06
12. BIMCO. Guidelines on Cyber Security Onboard Ships. Version 4. – London: BIMCO, 2020. – URL: https://www.bimco.org/media/oq0ft0gr/guidelines-on-cyber-security-onboard-ships-v4-1.pdf.
13. IACS. UR E26/E27: Cyber resilience of ships. – 2022. – URL: https://iacs.org.uk.

14. Androjna A., et al. Cybersecurity in maritime navigation systems: threats and mitigation // 2021. https://www.researchgate.net/publication

15. Strohmeier M., Schäfer M., Lenders V., Martinovic I. On perception and reality in wireless air traffic communication security // *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22, No. 1. P. 249–291. DOI: 10.1109/COMST.2019.2949178 https://dl.acm.org/doi/10.1109/COMST.2019.294917

REFERENCES

1. Singh S., Singh J., Singh S., Goyal S. B., Raboaca M. S., Verma C., Suciu G. Detection and Mitigation of GNSS Spoofing Attacks in Maritime Environments Using a Genetic Algorithm // Mathematics. 2022. Vol. 10, No. 21. Article 4097. URL: https://www.mdpi.com/2227-7390/10/21/4097

2. IACS. UR E26/E27: Cyber resilience of ships. – 2022. – URL: https://iacs.org.uk

3. Zhang H., Wang J., Wang J., Liu X. GNSS spoofing detection based on multi-feature fusion and machine learning // Computers & Fluids. 2021. Vol. 231. Article 105141. URL: https://www.sciencedirect.com/science/article/abs/pii/S0045790621001592

4. Cole B., Schamberg G. Unscented Kalman Filter for Long-Distance Vessel Tracking in Geodetic Coordinates // Applied Ocean Research. 2022. Vol. 124. Article 103205. URL: https://www.sciencedirect.com/science/article/pii/S0141118722001468

5. BIMCO. Guidelines on Cyber Security Onboard Ships. Version 4. – London: BIMCO, 2020. – 61 p. – URL: https://www.bimco.org/media/oq0ft0gr/guidelines-on-cyber-security-onboard-ships-v4-1.pdf

6. Semanjski S., Semanjski I., De Wilde W., Gautama S. GNSS spoofing detection by supervised machine learning with validation on real-world meaconing and spoofing data — Part II // Sensors. 2020. Vol. 20, No. 7. Article 1806. URL: https://www.mdpi.com/1424-8220/20/7/1806

7. Liu W., Papadimitratos P. Self-Supervised Federated GNSS Spoofing Detection with Opportunistic Data // Proceedings of the ION GNSS+ Conference. 2025. URL: https://arxiv.org/abs/2505.06171

8. Snieosikov O. A. Metody vyiavlennia ta protydii kiberatakam typu gps spoofing i gps jamming z vykorystannia ai dlia system dyferentsiinoi korektsii ta hlobalnoi navihatsiinoi suputnykovoi systemy // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. 2025. T. 355, № 4. P. 584–592. DOI: https://doi.org/10.31891/2307-5732-2025-355-82

9. Snieosikov O. A., Nariezhnii O. P. Modeli zahroz ta porushnyka avtonomnoi systemy dyferentsialnoi korektsii hlobalnykh navihatsiinykh suputnykovykh system // Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu. 2025. № 3. DOI: https://doi.org/10.35546/kntu2078-4481.2025.3.2.54

10. Narytnyk T., Prysiazhnyi V., Kapshtyk S. ta in. Improvement of the GPS signal receiving resistance against electromagnetic interference, jamming, and spoofing // Information and Telecommunication Sciences. 2022. Vol. 13, No. 2. P. 4–14. DOI: https://doi.org/10.20535/2411-2976.22022.4-14

11. Avilov A. I. Borotba zi spufinhom na bezpilotnykh litalnykh aparatakh // Zbirnyk naukovykh prats KhNUPS. 2024. № 2(80). DOI: https://doi.org/10.30748/zhups.2024.80.06

12. BIMCO. Guidelines on Cyber Security Onboard Ships. Version 4. – London: BIMCO, 2020. – URL: https://www.bimco.org/media/oq0ft0gr/guidelines-on-cyber-security-onboard-ships-v4-1.pdf.

13. IACS. UR E26/E27: Cyber resilience of ships. – 2022. – URL: https://iacs.org.uk.

14. Androjna A., et al. Cybersecurity in maritime navigation systems: threats and mitigation // 2021. https://www.researchgate.net/publication/358676229_CYBER_SECURITY_CHALLENGES_FOR_SAFE_NAVIGATION_AT_SE

15. Strohmeier M., Schäfer M., Lenders V., Martinovic I. On perception and reality in wireless air traffic communication security // IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 1. P. 249–291. DOI: 10.1109/COMST.2019.2949178 https://dl.acm.org/doi/10.1109/COMST.2019.294917

Kucheruk G.Yu., Hannoshyna I.M.

METHODS FOR DETECTING SPOOFING IN MARITIME NAVIGATION SYSTEMS

The article is devoted to the systematization and comprehensive comparative analysis of modern methods for detecting GPS/GNSS spoofing in maritime navigation systems. Particular attention is paid to the growing relevance of this issue in the context of increasing dependence on satellite navigation and the associated risks to the safety and reliability of maritime operations. The physical principles underlying spoofing attacks are examined in detail, including signal generation, synchronization, and manipulation mechanisms, as well as their classification according to the level of technical sophistication, target objects (shipborne receivers, navigation subsystems), and potential consequences for maritime safety, such as route distortion, collision risks, and loss of situational awareness.

The study provides an in-depth analysis of detection methods based on several complementary approaches. These include monitoring of signal parameters, in particular signal strength and carrier-to-noise density ratio (C/N_0), which allows identification of abnormal signal behavior; consistency checks of inter-satellite Doppler shifts to detect inconsistencies in satellite motion patterns; and cross-verification with alternative positioning, navigation, and timing (PNT) sources, such as AIS, eLoran, and other independent systems, ensuring redundancy and reliability. Special emphasis is placed on hybrid inertial-satellite navigation systems that employ Kalman filtering to integrate data from multiple sensors and enhance robustness against spoofing.

In addition, the article explores advanced data-driven techniques, including machine learning methods for anomaly detection. Specifically, the application of recurrent neural networks (LSTM) for temporal pattern recognition and ensemble classifiers for improving detection accuracy and reducing false positives is discussed. The advantages and limitations of each method are critically evaluated in terms of implementation complexity, computational requirements, and effectiveness under real-world conditions.

Based on the conducted analysis, a multi-layered architecture for protecting maritime navigation systems is proposed. This architecture integrates signal-level, navigation-level, and network-level detection mechanisms into a unified framework, providing a comprehensive and adaptive defense against spoofing attacks. The technical prerequisites for its effective implementation are also defined, including requirements for sensor integration, data synchronization, and system interoperability.

Keywords: *GNSS spoofing, maritime navigation, GPS security, anomaly detection, Kalman filter, machine learning, AIS, navigation system protection architecture.*

Стаття прийнята 29.01.2026