УДК 621.396.967.4:004.056.55 **DOI: 10.31653/2306-5761.37.2025.109-122**

AUTHENTICATION OF AUTOMATIC IDENTIFICATION SYSTEM MESSAGES BASED ON THE USE OF DIGITAL WATERMARKING TECHNOLOGY

АВТЕНТИФІКАЦІЯ ПОВІДОМЛЕНЬ АВТОМАТИЧНОЇ ІДЕНТИФІКАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

O. Shyshkin, *D.Sc., professor,* **V. Konovets**, *PhD, Senior Research Officer*

О.В. Шишкін, *д.т.н., професор,* **В.І. Коновець,** *к.т.н., ст. наук. співробітник*

National University "Odessa maritime academy", Ukraine

Національний Університет «Одеська морська академія», Україна

ABSTRACT

The Automatic Identification System (AIS) is one of the key technologies in modern maritime navigation, enhancing both the safety and efficiency of maritime transportation. AIS transponder data improves situational awareness, overcomes the limitations of radar, and supports various maritime services. However, the open nature of AIS radio channels makes the system vulnerable to cyberattacks, particularly through data falsification, which poses risks to navigational safety. Message authentication is an effective countermeasure against such threats. This paper proposes a method for authenticating AIS messages using digital watermarking technology. The proposed method minimizes the overhead required to detect spoofed transmissions and AIS data substitution. The developed algorithm Carrier Reconstruction Watermark Decoding (CRWD) enables the integration of additional authentication data into the AIS signal without degrading its noise immunity and maintains compatibility with standard shipboard transponders. This authentication approach can be incorporated within the TESLA cryptographic protocol, which has become a de facto standard for maritime digital communication channels due to its combined advantages of symmetric and asymmetric cryptography.

Keywords: cryptography, message authentication code, radio channel, algorithm, transponder.

АНОТАЦІЯ

Суднова АІС є одним з важливих засобів сучасного судноплавства, яка сприяє навігаційної безпеці та ефективності морських перевезень. Дані від суднових транспондерів АІС доповнюють інформованість та усувають обмеження радарів, забезпечують різноманітні сервіси морської галузі. Але відкритість радіоканалів АІС робить цю систему вразливою до кібератак у вигляді фальшування даних, що створює ризики навігаційної безпеки. Автентифікація повідомлень АІС є дієвим механізмом протидії такого типу кібератак. В даній роботі запропонований спосіб автентифікації повідомлень АІС на основі використовування технології цифрових водяних знаків. Спосіб дозволяє зменшити необхідний обсяг даних накладних витрат для виявлення злочинних передавань та підміни даних АІС. Розроблений алгоритм декодування водяних знаків за допомогою реконструкції сигналу-носія (CRWD) дозволяє здійснити передавання додаткових даних коду автентифікації у складі сигналу АІС без погіршення завадостійкості та підтримує сумісність зі стандартними судновими транспондерами. Спосіб автентифікації може бути інтегрований в рамках криптографічного протоколу TESLA, який є де-факто стандартом,

поширеним на морські цифрові радіоканали обміну даними завдяки притаманним перевагам симетричної та асиметричної криптографії.

Ключові слова: криптографія, код автентифікації повідомлення, радіоканал, алгоритм, транспондер.

ПЕРЕЛІК СКОРОЧЕНЬ

BCH	Bose–Chaudhuri–Hocquenghem (codes)
CRWD	Carrier Reconstruction Watermark Decoding, Декодування водяних знаків на основі реконструкції носія (Абревіатура запропонована авторами)
DSSS	Direct Sequence Spread Spectrum, Розширення спектру за допомогою прямої послідовності
GMSK	Gaussian Minimum Shift Keying, Маніпуляція з мінімальним Гаусівим зсувом
GPS	Global Positioning System, Глобальна система позиціонування
MAC	Message Authentication Code, Код автентифікації повідомлення
MMSI	Maritime Mobile Service Identity, Ідентифікатор морської рухомої служби
SART	Search And Rescue Transponder, Пошуковий рятувальний маяк відповідач
TESLA	Timed Efficient Stream Loss-tolerant Authentication, Ефективна стійка до втрат автентифікація потоку
АБГШ	Адитивний білий Гаусів шум
АІС (AIS)	Автоматична ідентифікаційна система, Automatic Identification System
ЕЦП	Електронний цифровий підпис
ЗШПФ	Зворотне швидке перетворення Фур’є
ЦВЗ	Цифрові водяні знаки
ШПФ (FFT)	Швидке перетворення Фур’є, Fast Fourier Transform

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

Автоматична ідентифікаційна система (АІС) вважається одним з важливіших засобів навігації на морських і річкових маршрутах. Згідно Міжнародної конвенції з охорони людського життя́ на морі (SOLAS Chapter V, Regulation 19.2.4) усі судна валовою місткістю 300 реєстрових тон і більше, що здійснюють міжнародні рейси, і вантажні судна валовою місткістю 500 реєстрових тон і більше, які не здійснюють міжнародні рейси та пасажирські судна незалежно від розміру повинні бути оснащені АІС, починаючи з 2003 року. АІС в значній мірі сприяє безпеці судноплавства, зокрема усунення обмеженості суднових радіолокаційних станцій, щодо виявлення малих суден та навігації в акваторіях з обмеженою видимістю. Інформаційний міжсудновий обмін навігаційними параметрами по каналам АІС дозволяє забезпечити автоматичну ідентифікацію суден та знизити ризик зіткнення суден за рахунок прискорення прийняття рішень з маневрування в стислих водах. Супутниковий прийом сигналів АІС забезпечує глобальний моніторинг суден (так званий режим sat-AIS). Передавання АІС використовуються в пошуково-рятувальних операціях, в тому числі шляхом комплексування передавача АІС з радіолокаційним маяком відповідачем (AIS SART).

Але, з певних причин, зокрема, через використання відкритих каналів зв’язку, широкомовного режиму передавання повідомлень, відсутності за технічним стандартом [17]

шифрування інформації, повідомлення АІС можуть бути сфальшовані з будь-яких міркувань. Зважаючи на широкий обсяг застосунків, які ґрунтуються на використанні даних АІС, існує велика кількість сценаріїв злочинних дій у вигляди протизаконних втручань – атак на радіоканали АІС [4, 5, 6]. Зважаючи на важливість отримання дійсних даних для підтримання безпеки судноплавства, вирішення проблеми автентифікації, тобто встановлення справжності повідомлень АІС, набуває зростаючої актуальності з огляду на поширення інструментів кіберзлочинності на морському транспорті [20].

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

Загально відомим підходом забезпечення автентичності даних в інформаційно-комунікаційних технологіях, включно канали зв’язку АІС, є використання електронного цифрового підпису (ЕЦП) повідомлень що передаються [6, 11, 14]. Сутність такого рішення полягає в тому, що ЕЦП формується у вигляді криптографічного перетворення власне повідомлення та ключа – у формі контрольної суми (хеша). Цей хеш має назву код автентифікації повідомлень (Message Authentication Code, MAC). У подальшому використаємо англомовне скорочення MAC як найбільш поширене скорочення у спеціальній літературі з криптографії. Дані MAC додаються якимось чином до самого повідомлення аналогічно звичайному підпису паперового документу.

Величезна добірка наукових публікацій стосовно морської кібербезпеки, включно автентифікації АІС наведена в електронній книзі Gary C. Kessler, Steven D. Shepard (2025) [11].

Різноманітні сценарії втручань в радіоканали АІС проаналізовані в роботі Goudosis A., Katsikas S. (2022) [11].

Алгоритми автентифікації з використанням відкритого (публічного) ключа досліджені в статті Wimpenny G. та ін. (2022) [21].

Публікація Wimpenny G. та ін. (2025) [22] присвячена дослідженням методів автентифікації повідомлень у системі обміну повідомленнями в УКХ діапазоні (VDES).

Використання технології ЦВЗ у різних аспектах морської кібербезпеки запропоновано та досліджується в публікаціях Anderson J. та ін. (2022, 2024) [2, 3], Shyshkin O. (2022) [19].

Аналіз літературних джерел дозволяє зробити висновок про те, що найбільш розповсюдженими сценаріями кібервтручань є передавання вигаданих повідомлень АІС від неіснуючого, примарного судна або свідоме спотворення інформації в повідомленнях, начебто переданих реальним судном [6]. Через доступність транспондерів суднового призначення анонімні кібератаки на АІС набувають все більшого поширення, що підриває довіру вахтового офіцера до даних транспондерів АІС з потенційними наслідками зниження безпеки судноплавства.

Існуючі рішення автентифікації повідомлень АІС базуються на використанні криптографічних алгоритмів захисту даних, які так чи інакше потребують передавання додаткової інформації, необхідної для виявлення фальшувань. Наприклад, система автентифікації Auth-AIS [18] може працювати в двох режимах конфігурації: детермінована безпека, що вимагає обсягу накладних витрат даних до 75% на повідомлення, або імовірнісна безпека, що зменшує накладні витрати на повідомлення до 35,7%.

Формулювання цілей статті (постановка завдання)

Ціллю статті є розробка способу автентифікації повідомлень АІС, який забезпечує зменшення накладних витрат у вигляді додаткових даних, необхідних для здійснення процедури автентифікації при збереженні сумісності з існуючим штатним судновим обладнанням АІС. Для досягнення цілі обрана технологія цифрових водяних знаків для

передавання даних автентифікації у складі основного повідомлення AIC, що потребує розроблення завадостійкого алгоритму ЦВЗ, який забезпечує надійне передавання даних AIC і автентифікації.

ЦВЗ – це технологія непомітного вбудовування певного обсягу даних в цифровий продукт різного фізичного призначення (аудіо, відео, зображення, сигнали, тощо). ЦВЗ зазвичай застосовується для захисту авторських прав, виявлення фальсифікацій, контролю розповсюдження [8], або захисту повідомлень, зокрема у глобальних навігаційних супутникових системах (ГНСС) [2]. В нашому дослідженні ЦВЗ використовується як спосіб передавання додаткових даних у складі стандартного повідомлення AIC.

Виклад матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Протокол TESLA автентифікації широкомовних передач

Протокол TESLA (Timed Efficient Stream Loss-tolerant Authentication, Ефективна стійка до втрат автентифікація потоку) – це алгоритм, який забезпечує автентифікацію регулярних широкомовних повідомлень [1, 22]. (Абревіатура не має нічого спільного з електромобілями, через те протокол з’явився раніше за відповідну компанію). Перевагами протоколу є:

- низки обчислювальні витрати і накладні розходи на здійснення автентифікації;
- використання методу симетричного шифрування (секретний ключ) одночасно з перевагами асиметричного шифрування (пара публічний - секретний ключі);
- допустимість втрат інформаційних пакетів;
- здатність роботи в широкомовному режимі без обмежень кількості приймачів.

Основна ідея TESLA полягає в тому, що він використовує симетричну криптографію, більш швидку за асиметричну, але робить це за допомогою часової синхронізації та відкладеного розкриття ключів, щоб забезпечити автентифікацію повідомлень, начебто використовувалася асиметрична криптографія [1].

Просте використання стандартного механізму автентифікації «точка-точка» шляхом додавання коду автентифікації повідомлення (MAC) до кожного пакету, обчисленого за допомогою однакового для відправника і отримувача секретного ключа, не забезпечує безпечну широкомовну автентифікацію. Проблема полягає в тому, що будь-який отримувач із секретним ключем може підробити дані та видати себе за відправника. Отже, потрібне рішення, засноване на асиметричній криптографії, щоб запобігти цьому.

Схема ЕЦП на основі асиметричного криптографічного протоколу дозволяє вирішити цю проблему. Підписання кожного пакета даних секретним ключем, якій має тільки відправник, забезпечує безпечну широкомовну автентифікацію. Але спосіб асиметричної криптографії пов'язаний з високими накладними витратами даних та часу для здійснення процедури автентифікації. В результаті класична асиметрична криптографія «з’їдає» доступний обсяг передавань, якого вже не вистачає в районах інтенсивного судноплавства.

Принцип TESLA заснований на тому, що відправник додає до кожного пакету даних, що передаються, MAC обчислений за допомогою секретного ключа k, відомого лише йому самому. В контексті AIC пакет даних може складатися з даних слотів, що передаються впродовж, наприклад, одної хвилини. Одержувач накопичує отриманий пакет, не маючи можливості відразу його автентифікувати. Наступним кроком відправник розкриває ключ k, і одержувач може автентифікувати пакет. Отже, одного MAC на пакет достатньо для забезпечення широкомовної автентифікації за умови, що одержувач заздалегідь синхронізував свій годинник із відправником.

Протокол TESLA не потребує участі третьої довіреної сторони, що розподіляє та оновлює ключі, як це притаманне для класичної симетричної криптографії. Дійсно секретний ключ генерується відправником автоматично, тому третя сторона взагалі не потрібна. В кінцевому рахунку TESLA використає симетричну криптографію, але з перевагами, що належать до асиметричного шифрування. Платою за отримання цих переваг є деяка затримка в здійсненні автентифікації і наявність часової синхронізації, яка за визначенням доступна в AIC. У настанові IALA G1117 розглядається використання VDES для розширення повідомлень AIS з метою надання додаткової інформації для автентифікації з використанням протоколу TESLA [10]. Це дозволяє підвищити довіру до даних і забезпечити безпечне прийняття рішень на основі цих повідомлень.

Автентифікація повідомлень з використанням MAC

Код автентифікації повідомлень (Message Authentication Code, MAC) - це криптографічна контрольна сума (або хеш), якій додається до повідомлення та розповсюджується в мережі або радіоканалі з метою перевірки його цілісності і автентичності [13]. MAC гарантує, що передане повідомлення надійшло від зазначеного відправника і не було змінено під час передачі випадково чи навмисно. MAC іноді називають тегом через те, як він додається якимось чином до повідомлення, яке він посвідчує. Принцип застосування MAC показаний на Рис. 1.

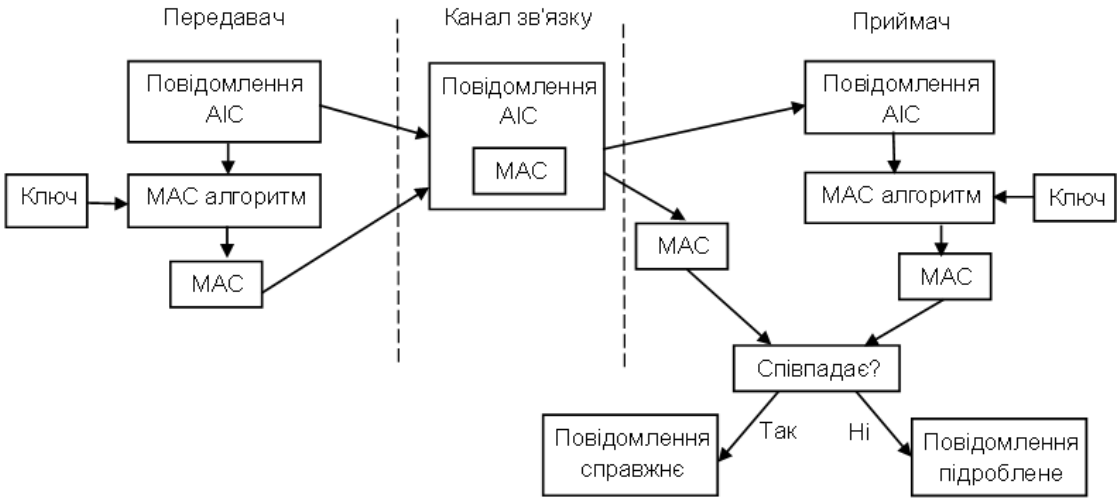


Рис. 1. Принцип використання MAC

Важливо зазначити, що MAC алгоритм використає однаковий секретний ключ у передавачі і приймачі – це так звана симетрична схема шифрування. Недоліки симетричної схеми очевидні через необхідність наявності третьої сторони крім передавача і приймача, яка повинна розподіляти/міняти ключі та можливість фальшування даних будь-якім учасником мережі. Отримання ключа злочинцем ламає усю систему захисту. В мережах/радіоканалах з широкомовним передаванням даних, тобто коли один передавач працює на чисельну кількість приймачів, MAC алгоритм взагалі втрачає працездатність. Будь-який власник секретного ключа може передати сфальшовані дані.

Для подолання цього недоліку розроблена асиметрична схема шифрування, яка застосовує два типи ключів – секретний та публічний, відкритий ключ. Секретним ключем володіє тільки одна особа, власник такого ключа. На основі секретного ключа формується відкритий ключ, але тільки в одну сторону, зворотна операція отримання секретного ключа,

знаючи відкритий ключ – неможлива (обчислювальне важка та визначається довжиною ключа у випадку перебору варіантів). Будь-яка особа з використанням відкритого ключа може тільки зашифрувати повідомлення, але розшифрувати його може тільки власник секретного ключа.

Довжина MAC обирається з огляду отримання балансу між безпекою та ефективністю у кількості 128 біт, що вважається досить безпечним у практичних застосуванням [14]. Можливе зменшення довжини MAC до 80 біт в умовах обмеження пропускної спроможності каналу зв'язку.

Спосіб автентифікації повідомлень AIC на основі використання ЦВЗ

У розробленому алгоритмі використається технологія ЦВЗ, яка передбачає приховане вбудовування даних MAC в сигнал-носій GMSK [16]. Зазвичай у мережевих технологіях MAC передається цілком, але в умовах коли рапорти AIC передаються регулярно з часовим інтервалом від 2 секунд (швидкість судна більше 23 вузлів та зміна курсу) до 3 хвилин (судно на якорі або дрейфує зі швидкістю не більше 3 вузлів) [17, Table 1]. Тому немає потреби передати увесь MAC на кожний рапорт. Достатньо перевіряти збіг обмеженої кількості бітів для перевірки одного рапорту. З кожним наступним повідомленням довіра до джерела рапортів буде тільки підвищуватись, асимптотичне наближуючись до одиниці для справжніх рапортів. У разі хоча б одного незбігу довіра до такого передавача, як джерела підроблених даних (атаки), повинна піддаватися сумніву.

Імовірності правильного виявлення атаки P_{TP} (True – Positive) та пропуску атаки P_{FN} (False – Negative) пов'язані наступним співвідношенням:

$$P_{\text{TP}} = 1 - P_{\text{FN}}. \tag{1}$$

Рішення про наявність атаки формується шляхом порівняння кодів автентифікації – прийнятого безпосередньо та обчисленого як показано на Рис. 1. Випадок помилкового рішення (False – Negative) відповідає збігу кодів за умови наявності атаки. Для кількісної оцінки імовірності P_{FN} такої події будемо розглядати MAC як послідовність Бернуллі з однаковими імовірностями нульових та одиничних бітів $p = 0,5$. Таке припущення може бути прийняте виходячи з властивостей криптографічних хеш-функцій.

За умови передавання обмеженої кількості *b* бітів MAC одного повідомлення імовірність пропуску атаки буде співпадати з імовірністю вгадування усіх відповідних b бітів і дорівнювати значенню $P_{\text{FN}} = 2^{-b}$. Впродовж обробки *M* повідомлень AIC, що використані для автентифікації того ж самого передавача, імовірність виявлення атаки з урахованням (1) визначається за формулою:

$$P_{\text{TP}} = 1 - 2^{-bM}. \tag{2}$$

Наприклад, за умов $b = 4$, $M = 1; 2; 3; 4; 5$ імовірність виявлення атаки покроково приймає значення: $P_{\text{TP}} = 0,937500;\ 0,996094;\ 0,999756;\ 0,999985;\ 0,999999$. Таким чином, зважаючи на потоковий характер рапортів AIC, відбувається зростання P_{TP}, тобто довіри до прийнятих повідомлень. В протилежному випадку, у разі незбігу хоча б одного розряду з b розрядів MAC, обраних для перевірки, буде зафіксована атака і передавач з MMSI, зазначеним у повідомленні, набуває статусу порушника.

Вбудовування бітів MAC в сигнал-носій відбувається за технологією ЦВЗ наступним чином. У суднових пристроях AIC (транспондерах) для передавання даних використають метод модуляції з мінімальним Гаусівим зсувом частот (англ. Gaussian Minimum Shift Keying, GMSK). В нашому застосуванні низькочастотний сигнал з GMSK модуляцією окрім основної

своєї функції передавання даних AIC використається як носій додаткових даних, які непомітним чином додається в сигнал-носій.

Алгоритм ЦВЗ

Алгоритм ЦВЗ виконує процедуру вбудовування певним чином даних MAC в сигнал-носій GMSK за рахунок мінімального його спотворення. Вбудовування даних виконується у частотній області ШПФ сигналу-носія. Використання амплітудного спектру ШПФ для вбудовування даних забезпечує їх стійкість до фазових спотворень з огляду на властивості ШПФ [8, 15]. Попередньо дані частки MAC піддаються завадостійкому кодуванню та розширенню спектра методом DSSS [7].

Для реалізації алгоритму використається IQ модель представлення сигналів у квадратурах коли відліки сигналу представляються синфазною I та квадратурною Q складовими. Така модель запроваджується в сучасних пристроях цифрової обробки сигналів та програмно-керованого радіо (англ. Software Defined Radio SDR) [7]. У стислому вигляді алгоритм представляється операціями та формулами, наведеними у Таблиці 1.

Таблиця 1. Алгоритм вбудовування даних MAC

Дія	Формула
Кодування даних ЦВЗ завадостійким кодом BCH	$y = \mathrm{ENCOD}(data\_WM)$ (3)
Розширення спектру за методом DSSS	$wm\_tx = R * y$ (4)
Швидке перетворення Фур'є (ШПФ)	$F = \mathrm{FFT}(gmsk)$ (5)
Амплітудна модуляція відліків спектру	$Fwm(I) = (1 + \rho * wm\_tx).*F(I)$ (6)
Зворотне ШПФ для отримання сигналу з вбудованими даними	$gmsk\_wm = \mathrm{FFT}^{-1}(Fwm)$ (7)

Позначення:

$data\_WM$ – дані ЦВЗ (частка MAC з b бітів);
y – завадостійкий код BCH;
wm_tx – мультиплексований сигнал з розширеним спектром DSSS;
$gmsk$ – низькочастотний сигнал з GMSK модуляцією;
ENCOD – процедура кодування;
I – індекси відліків спектру, які піддаються модуляції;
R – матриця м-послідовностей;
F – спектр сигналу $gmsk$;
Fwm – спектр сигналу $gmsk$ з вбудованими даними;
ρ – індекс амплітудної модуляції.

Для підвищення завадостійкості даних ЦВЗ застосовується код BCH [7], здатний виявляти та виправляти помилки. Код BCH дозволяє виправляти похибки, які обумовлені впливом завад в каналі передавання. За позначенням код BCH (n, k, t) має довжину блоку n біт, з яких k ($k<n$) являються власне даними, решта бітів – надлишкові для здійснення виправлення можливих помилок. Кількість виправлених помилок позначається t. Приклади параметрів кодів BCH з довжиною блоку n = 7; 15; 31 наведені нижче:

n	*k*	*t*	*n*	*k*	*t*	*n*	*k*	*t*
7	4	1	15	11	1	31	26	1
			15	7	2	31	21	2
			15	5	3	31	16	3
						31	11	5
						31	6	7

Наприклад, код (31, 16, 3) має довжину блоку $n = 31$, складається з $k = 16$ інформаційних бітів, решта 15 – перевірочні, та здатний виправляти до 3-х помилок на блок. Код, що виправляє одну помилку на блок, називають також кодом Хеммінга, якій е окремим випадком кодів BCH зі здатністю корекції одної помилки на блок $t = 1$.

За пропонованим алгоритмом загальний сигнал ЦВЗ формується шляхом мультиплексування окремих сигналів, отриманих за методом DSSS. У якості послідовностей розширення використовуються м-послідовності, які зазвичай використають в системах зв'язку і супутникової навігації. Наприклад, в GPS використають м-послідовності довжиною 1023 біт. В нашому випадку використовуються послідовності довжиною 255 біт. Довжина L м-послідовностей співпадає з кількістю гармонік спектру, які використовуються для вбудовування ЦВЗ.

Приклад м-послідовності довжиною 15 наведений нижче.

-1 1 -1 -1 -1 1 1 1 1 -1 1 -1 1 1 -1.

Мультиплексований сигнал ЦВЗ wm_tx обчислюється як сума усіх модульованих м-послідовностей. Математично ця операція представляється матричним добутком за формулою (4), де R - матриця $\left(L \times n\right)$ м-послідовностей.

Матриця R формується одноразово з циклічних зсувів базової м-послідовності і зберігається в паняті передавача і приймача.

Наприклад, для даних ЦВЗ [0 1 1 0] і коду (7, 4, 1) кодовий блок на виході кодера буде мати вигляд для формату логічного представлення даних: [0 1 1 0 0 0 1]. Тоді операція мультиплексування за формулою (4) демонструється у форматі фізичного 1/-1 відображення даних наступним чином:

Для компактності запису матриці R використані позначення +/- для даних 1/-1 відповідно. В нашому випадку довжина м-послідовностей складає $L = 255$ біт.

$$R = \begin{bmatrix} - & - & + & + & - & + & - \\ + & - & - & + & + & - & + \\ - & + & - & - & + & + & - \\ - & - & + & - & - & + & + \\ - & - & - & + & - & - & + \\ + & - & - & - & + & - & - \\ + & + & - & - & - & + & - \\ + & + & + & - & - & - & + \\ + & + & + & + & - & - & - \\ - & + & + & + & + & - & - \\ + & - & + & + & + & + & - \\ - & + & - & + & + & + & + \\ + & - & + & - & + & + & + \\ + & + & - & + & - & + & + \\ - & + & + & - & + & - & + \end{bmatrix} \quad y = \begin{bmatrix} -1 \\ +1 \\ +1 \\ -1 \\ -1 \\ -1 \\ +1 \end{bmatrix} \quad wm\_tx = \begin{bmatrix} -1 \\ -3 \\ -1 \\ +3 \\ +1 \\ -3 \\ -1 \\ +5 \\ +1 \\ +1 \\ -5 \\ -1 \\ -1 \\ -1 \\ +5 \end{bmatrix}$$

Таким чином, вбудовування ЦВЗ у сигнал-носій здійснюється у частотній області шляхом обчисленням ШПФ, модуляції амплітуд гармонік спектру за формулою (6) та обчислення зворотного ШПФ. Для модуляції використають обмежену множину *I* гармонік в основній смузі спектру, яка співпадає з довжиною м-послідовностей та дорівнює в нашому випадку 255. Фази спектральних відліків залишаються незмінними.

Алгоритм декодування MAC

Дані MAC у розробленому способі автентифікації [16] передаються за технологією ЦВЗ, тобто приховано вбудовуються в сигнал-носій. Для декодування вбудованих даних на приймальному боці розроблений алгоритм декодування на основі реконструкції сигналу-носія (англ. Carrier Reconstruction Watermark Decoding, CRWD). Алгоритм дозволяє здійснювати декодування даних AIC і даних MAC без взаємного негативного впливу сигналів носія (дані AIC) і сигналу ЦВЗ (дані MAC). Математично алгоритм описується сукупністю формул (8) – (19) зведених у Таблиці 2.

Таблиця 2. Алгоритм декодування CRWD

Крок	Дія	Формула	
0	Попередні обчислення		
	Демодуляція вхідного сигналу	$data\_AIS = \mathrm{DEMOD}(gmsk\_rx)$	(8)
	Обчислення ШПФ вхідного сигналу	$X\_rx = \mathrm{FFT}(gmsk\_rx)$	(9)
1	Обчислення даних ЦВЗ		
	Реконструкція сигналу GMSK за прийнятими даними	$gmsk\_rec = \mathrm{MOD\_GMSK}(data\_AIS)$	(10)
	Обчислення ШПФ реконструйованого сигналу	$X\_rec = \mathrm{FFT}(gmsk\_rec)$	(11)
	Обчислення сигналу ЦВЗ	$WM\_rec = \mathrm{abs}(X\_rx) - \mathrm{abs}(X\_rec)$	(12)
	Оцінка коду BCH	$y\_rec = sign(R^{\mathrm{T}} * WM\_rec)$	(13)
	Оцінка даних ЦВЗ	$data\_WM = \mathrm{DECOD}(y\_rec)$	(14)
2	Обчислення даних AIC		
	Обчислення завадостійкого коду за даними ЦВЗ	$y\_rec = \mathrm{ENCOD}(data\_WM)$	(15)
	Реконструкція сигналу ЦВЗ	$WM\_rec = R * y\_rec$	(16)
	Обчислення оцінки спектру сигналу без ЦВЗ	$X\_rec = (1 - \rho * WM\_rec).* X\_rx$	(17)
	Обчислення сигналу GMSK шляхом ЗШПФ	$gmsk\_rec = \mathrm{FFT}^{-1}(X\_rec)$	(18)
	Демодуляція сигналу GMSK	$data\_AIS = \mathrm{DEMOD}(gmsk\_rec)$	(19)

Позначення:

DEMOD – процедура демодуляції сигналу;
data _ AIS – прийняті дані AIC;
data _WM – декодовані дані ЦВЗ;
MOD_GMSK – процедура модуляції методом GMSK;
gmsk _ rx – прийнятий GMSK сигнал, включно ЦВЗ та шум;
gmsk _ rec – реконструйований GMSK сигнал без впливу ЦВЗ та шуму;

WM_rec – реконструйований сигнал ЦВЗ;
y_rec – кодовані дані ЦВЗ;
ENCOD – процедура кодування даних;
X_rx – спектр прийнятого сигналу;
X_rec – реконструйований спектр сигналу GMSK (без ЦВЗ);

Схема моделювання алгоритму CRWD наведена на Рис. 2. Сигнал-носій позначений вектором $\boldsymbol{x}$, сигнал ЦВЗ, значно слабкішій від носія, позначений $\boldsymbol{w}$. Для спрощення операції ШПФ та ЗШПФ на рисунку не показані. Сумарний сигнал $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{w}$ піддається впливу адитивного білого Гаусіва шуму (АБГШ).

На приймальному боці обробляється сигнал $\boldsymbol{z}$, з додатковою складовою у вигляді АБГШ. Обробка здійснюється покрокове, $i = 0, 1, 2, ...$ на основі прийнятого сигнальному вектору $\boldsymbol{z}$ з урахуванням оцінок сигналу ЦВЗ $\hat{\boldsymbol{w}}$ та сигналу-носія GMSK $\hat{\boldsymbol{x}}$. На початковому кроці $i = 0$ приймаємо $\hat{\boldsymbol{w}}[0]=0$. За алгоритмом обробки (Таблиця 2) отримуємо оцінки прийнятих даних повідомлення АІС $\hat{d}_x$ та даних МАС $\hat{d}_w$.

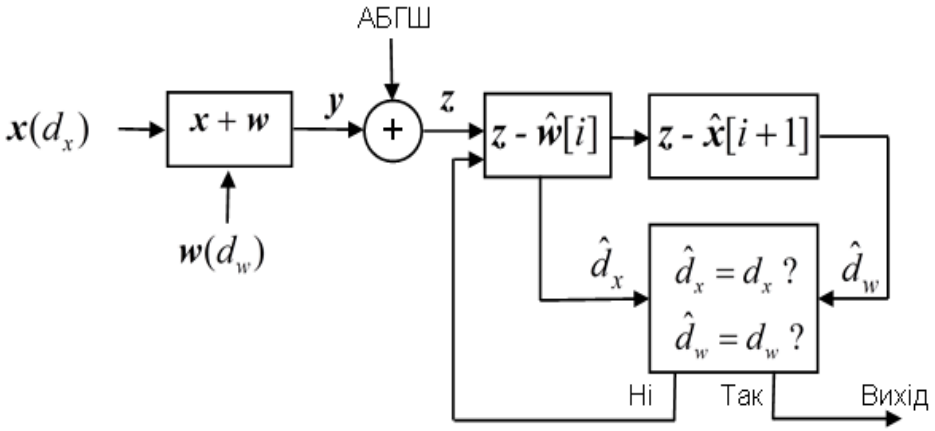


Рис. 2. Схема моделювання алгоритму CRWD передавання даних МАС

Під впливом шуму прийняті дані можуть відрізнятися від переданих даних. Якщо прийняті дані не співпадають с переданими, то виконуються наступні кроки алгоритму. Ключовим моментом алгоритму CRWD є те, що на кожному кроці, починаючи з першого, почергово здійснюється реконструкція сигналів $\hat{\boldsymbol{x}}$ та $\hat{\boldsymbol{w}}$ за оцінками даних відповідно $\hat{d}_x$ та $\hat{d}_w$. В результаті, якщо, наприклад, дані АІС отримані без помилок (про що свідчить контрольна сума передбачена форматом повідомлення АІС), то реконструйований сигнал GMSK $\hat{\boldsymbol{x}}$ має бути віднятий з прийнятого сигналу $\boldsymbol{z}$ як завада для декодування даних МАС. Навпаки, сигнал $\hat{\boldsymbol{w}}$ має бути віднятий на кроці демодуляції даних АІС $\hat{d}_x$. Цілісність даних МАС гарантується використанням завадостійкого кодування BCH.

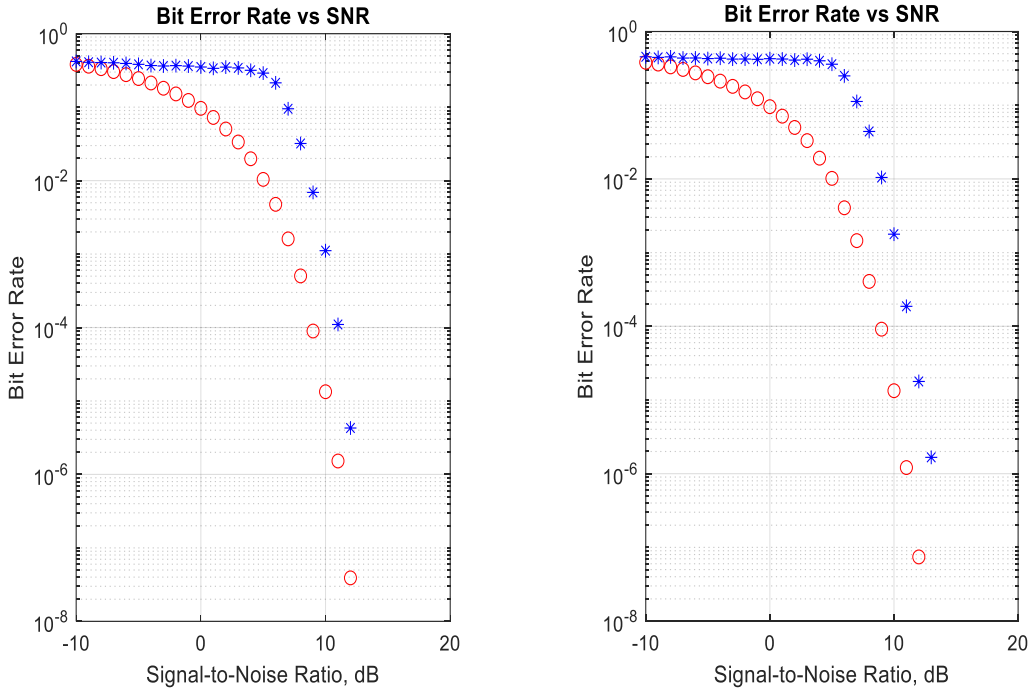
Вихід з процедури декодування даних АІС та МАС здійснюється якщо: а) дані $\hat{d}_x$ та $\hat{d}_w$ співпадають з переданими відповідно, або б) досягнута межа кроків $i = i_{max}$. Експериментально встановлено що вже при $i_{max} = 6$ алгоритм CRWD дозволяє отримати вірні дані, або взагалі не досягає результату, що трапляється у разі низького відношення сигнал-шум у каналі передачі.

Результати комп'ютерного моделювання

З метою підтвердження працездатності розробленого алгоритму CRWD та отримання кількісних показників виконане комп'ютерне моделювання в середовищі Matlab. Досліджувався вплив АБГШ на GMSK сигнал з вбудованими даними, які у контексті загальної проблеми що вирішується, представляють частку коду автентифікації MAC.

Моделювання проводилось за методом Монте-Карло з випадковим обранням даних повідомлення AIC d_x та даних MAC d_w, що вбудовуються в сигнал-носій.

Результати моделювання представлені на Рис. 3 у вигляді графіків завадостійкості - залежності імовірностей правильного декодування даних AIC та MAC від відношення сигнал-шум. По осі X відкладені значення відношення сигнал/шум у дБ в діапазоні (- 10 … 20) дБ, по осі Y відкладені значення імовірності помилки у логарифмічному масштабі в діапазоні (10^0 … 10^{-8}). Кружечками показані значення імовірності помилок у даних AIC, а зірочками - значення імовірності помилок у даних MAC для параметрів ρ, n, k як вказано на Рис. 3.



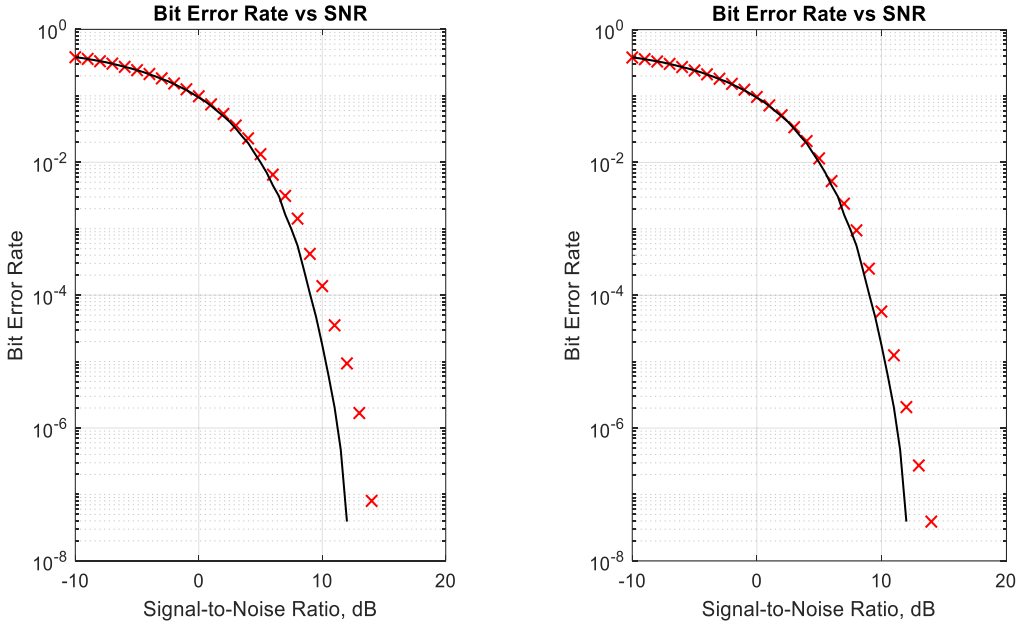
а) б)

Рис. 3. Імовірність бітової помилки (Bit Error Rate) даних AIC (червоні кружечки) та даних MAC (блакитні зірочки) у залежності від відношення сигнал-шум (Signal-to-Noise Ratio) для параметрів: а) $\rho = 0,02$, $n = 15$, $k = 7$; *б)* $\rho = 0,01$, $n = 31$, $k = 6$.

Графіки демонструють високу завадостійкості даних MAC для зазначених прикладів параметрів. За рахунок використання алгоритму з почерговим декодування даних AIC та MAC характерною рисою є подібний на водоспад вигляд графіку, що пояснюється тим, що при низькому відношенні с/ш приблизно до значення 8 дБ завадостійкий код не справляється з корекцією помилок. Тому імовірність помилок залишається на стабільно низькому рівні. Якщо с/ш перевищує 8 дБ, імовірність помилок різко зменшується за рахунок спроможності коду виправляти помилки.

Сумісність алгоритму зі стандартними судновими транспондерами AIC без опції автентифікації демонструється графіками на Рис. 4. Суцільною лінією показані графіки

завадостійкості сигналу GMSK без накладання сигналу ЦВЗ або з ЦВЗ у вигляді даних MAC в алгоритмі CRWD. Хрестиками наведені графіки завадостійкості у разі приймання сигналу з вбудованими даними MAC штатними транспондерами AIC без опції автентифікації. Звичайно, сигнал ЦВЗ, завдяки якому передаються дані MAC, є додатковою завадою яка негативно впливає на декодування даних AIC. Але цей вплив відбувається в незначній мірі в межах 2 – 3 дБ тільки для транспондерів без опції автентифікації. Для транспондерів з алгоритмом CRWD погіршення завадостійкості даних AIC не відбувається.



а) б)

Рис. 4. Імовірність бітової помилки (Bit Error Rate) даних AIC (червоні хрестики) у штатних транспондерах AIC, які не підтримують опцію автентифікації у порівнянні з такими, що підтримують функцію автентифікації (суцільна крива) для параметрів:

Висновки і перспектива подальшої роботи по даному напрямку

Результати дослідження свідчать про доцільність використання розробленого способу автентифікації повідомлень AIC на основі використання технології ЦВЗ. Вбудовування даних, необхідних для автентифікації, в сигнал повідомлень AIC дозволяє знизити накладні витрати даних для передавання криптографічних ключів в протоколі автентифікації. Розроблений алгоритм на основі реконструкції сигналу-носія CRWD забезпечує декодування даних AIC і даних MAC без їхнього взаємного негативного впливу в мережі пристроїв с функцією автентифікації. Сумісність зі штатними транспондерами AIC забезпечується з втратою завадостійкості передавання даних AIC на рівні 2-3 дБ, що є платою за передавання додаткових даних.

Запропонований спосіб автентифікації природним шляхом може бути інтегрований в рамках загально прийнятого протоколу TESLA в морських радіоканалах обміну даними. Напрямками подальших досліджень може бути оптимізація параметрів алгоритму CRWD та визначення можливостей впровадження розробленого способу в системи цифрового зв’язку з відмінними від GMSK видами модуляції.

REFERENCES

[1] Anderson, J., Lo, S., & Walter, T. (2022, January). Cryptographic Ranging Authentication with TESLA, Rapid Re-keying, and a PRF. 2022 International Technical Meeting of The Institute of Navigation, Long Beach, California, pp. 43-55. DOI: 10.33012/2022.18226

[2] Anderson, J., Lo, S., & Walter, T. (2022, January). Efficient and Secure Use of Cryptography for Watermarked Signal Authentication. 2022 International Technical Meeting of The Institute of Navigation, Long Beach, California, pp. 68-82. DOI: 10.33012/2022.18228

[3] Anderson, J., Lo, S., & Walter, T. (2024, September). Authentication Security of Combinatorial Watermarking for GNSS Signal Authentication. NAVIGATION, 71(3). DOI: 10.33012/navi.655

[4] Androjna, A., Perkovič, M., Pavic, I., Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. Applied Sciences. 11(11):5015.

[5] Androjna, A., Pavić, I., Gucma, L., Vidmar, P., & Perkovič, M. (2023, December 19). AIS Data Manipulation in the Illicit Global Oil Trade. Journal of Marine Science and Engineering, 12(1), 6. DOI: 10.3390/jmse12010006

[6] Balduzzi, M., Pasta, A., & Wilhoit, K. (2014, December). A Security Evaluation of AIS Automated Identification System. 30th Annual Computer Security Applications Conference (ACSAC '14), New Orleans, Louisiana, December 8-12, 2014, pp. 436-445.

[7] Bernard Sklar. Digital Communications: Fundamentals and Applications, Ed. 3, Pearson, 2021, 1136 p.

[8] Cox, I., Miller, M., Bloom, J., Fredrich, J., and Kalker, T. (2008). Digital Watermarking and Steganography, Second Edition. Elsevier Science. doi: 10.1016/B978-012372585-1.50015-2

[9] Duan, Y., Huang, J., Lei, J., Kong, L., Lv, Y., Lin, Z., Chen, G., & Kha, M.K. (2023, February). AISChain: Blockchain-Based AIS Data Platform With Dynamic Bloom Filter Tree. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2332-2343. DOI: 10.1109/TITS.2022.3188691

[10] G1117 - VHF Data Exchange System (VDES) / IALA, Edition 3.0, December 2022,

[11] Goudosis, A., Katsikas, S. (2022). Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation. Journal of Marine Science and Engineering. 10(6):805.

[12] International Standard ISO/IEC 29192-6 Reference number ISO/IEC 29192-6:2019(E) Information technology - Lightweight cryptography - Part 6: Message authentication codes (MACs)

[13] International standard ISO/IEC 29192-6. Information technology - Lightweight cryptography - Part 6: Message authentication codes (MACs), 2019

[14] Kessler, G. & Shepard, S. Maritime Cybersecurity. (2025). A Guide for Leaders and Managers, Second Edition (v2.3, 01/2025).

[15] Kumari, R. & Mustafi, A. (2022). The spatial frequency domain designated watermarking framework uses linear blind source separation for intelligent visual signal processing. Front. Neurorobot. 16:1054481. doi: 10.3389/fnbot.2022.1054481.

[16] Patent Application № a202500460, 06/02/2025, UANIPIO. Sposib avtentyfikatsii peredavan povidomlen sudnovoi avtomatychnoi identyfikatsiinoi systemy, Shyshkin O.V., Konovets V.I.

[17] Recommendation ITU-R M.1371–5 (2014) Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band.

[18] Sciancalepore, S., Tedeschi, P., Aziz, A., Di Pietro, R. (2022). Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts. IEEE Transactions on Dependable and Secure Computing, Vol. 19/ 4, pp 2709 – 2726. DOI: 10.1109/TDSC.2021.3069428

[19] Shyshkin, O. (2022, November). Cybersecurity Providing for Maritime Automatic Identification System. IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, October 10-14, pp. 736-740. DOI: 10.1109/ELNANO54667.2022.9926987

[20] Westbrook Tegg. (2025). Lethal empowerment and electronic crime: A focus on radio-frequency interference capabilities // Security and Defence Quarterly. – DOI: 10.35467/sdq/196515

[21] Wimpenny, G., Šafář, J., Grant, A., Bransby, M. (2022). Securing the Automatic Identifica-tion System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility, NAVIGATION, 75(2).

[22] Wimpenny, G., Lázaro, F., Šafář, J., Raulefs, R. (2025). A pragmatic approach to VDES authentication. NAVIGATION, 72(1).