Технічні науки

УДК 621.396.96:004.89

Сидорів Максим Сергійович

студент кафедри інформаційних систем та мереж

Національного університету «Львівська політехніка»

Sydoriv Maksym

Student of the Department of Information Systems and Networks

Lviv Polytechnic National University

АНАЛІЗ MLP МЕРЕЖІ ДЛЯ РОЗПІЗНАВАННЯ СПУФІНГУ СИНХРОННИХ GPS-СИГНАЛІВ

ANALYSIS OF THE MLP NETWORK FOR RECOGNIZING SYNCHRONOUS GPS SPOOFING

Анотація. *У статті розглянуто використання багатошарової перцептронної мережі (MLP) для задачі виявлення синхронного GPS-спуфінгу, однієї з найбільш небезпечних форм атак на глобальні навігаційні супутникові системи (GNSS). Показано, що класичні методи перевірки сили сигналу або геометричних параметрів мають обмеження в умовах складних динамічних сценаріїв. Для експерименту використано еталонний набір даних TEXBAT (сценарій ds7), який моделює поступове захоплення сигналу атакувальником. Архітектура MLP включала каскад щільних шарів із активацією ReLU та сигмоїдальним вихідним шаром, що дозволило досягти accuracy = 0.92, precision = 0.92, recall = 0.93 та F1-score = 0.93. Отримані результати підтверджують ефективність застосування MLP для автоматичного виявлення спуфінгових атак без складної часової обробки. Показано, що модель забезпечує баланс між точністю та обчислювальною ефективністю, а подальші дослідження мають бути*

спрямовані на гібридні архітектури (MLP+CNN/Transformer) для узагальнення на інші типи атак.

Ключові слова: *GPS-спуфінг, GNSS, MLP, нейронні мережі, машинне навчання, TEXBAT, виявлення аномалій, радіоелектронна боротьба.*

Summary. *The paper investigates the application of a multilayer perceptron (MLP) neural network for detecting synchronous GPS spoofing, one of the most dangerous types of attacks on Global Navigation Satellite Systems (GNSS). It is shown that traditional detection methods based on signal strength or geometric consistency checks are limited in complex dynamic environments. The experiment used the benchmark TEXBAT dataset (scenario ds7), which simulates a realistic synchronous signal takeover by an attacker. The proposed MLP architecture consists of several dense layers with ReLU activation and a sigmoid output layer, achieving accuracy = 0.92, precision = 0.92, recall = 0.93, and F1-score = 0.93. The results confirm the effectiveness of MLP in automatically identifying spoofing attacks without complex temporal processing. The model demonstrates a balanced trade-off between detection accuracy and computational efficiency. Future research should focus on hybrid architectures (MLP+CNN/Transformer) to improve generalization to other spoofing scenarios.*

Key words: *GPS spoofing, GNSS, MLP, neural networks, machine learning, TEXBAT, anomaly detection, electronic warfare.*

Постановка проблеми. Супутникова навігація на основі GPS давно стала основою сучасних цивільних і військових технологій. Вона забезпечує безперервний доступ до глобальних координат і точного часу, що необхідно для роботи транспортних систем, телекомунікацій, фінансових мереж, енергетики та логістики. У військовій сфері GPS використовується для управління бойовою технікою, наведення

високоточного озброєння, синхронізації дій підрозділів і стратегічного планування операцій. Водночас відкритість структури сигналів GPS створює вразливість до підробки та маніпуляцій, які стають усе більш поширеним інструментом гібридної війни та радіоелектронної боротьби.

Одним із найбільш небезпечних методів впливу є спуфінг GPS-сигналів – навмисне генерування хибних сигналів, що імітують справжні супутникові передачі. Приймач, не маючи внутрішніх засобів автентифікації, сприймає підроблені сигнали як реальні, унаслідок чого відбувається зміщення визначених координат або часу. Для військових застосувань це може означати хибну навігацію техніки, зрив операцій чи втрату боєздатності підрозділів. Для цивільного сектору – аварії в авіації та автомобільному транспорті, помилки в морській навігації, збої у фінансових транзакціях та порушення роботи критичної інфраструктури, що базується на точному часі. Масштаби ризиків свідчать про те, що спуфінг становить загрозу не лише безпеці окремих систем, а й національній та міжнародній стабільності.

Традиційні методи виявлення спуфінгу, що ґрунтуються на перевірці сили сигналу, аналізі геометричних характеристик супутників або простих кореляційних перевірках, мають суттєві обмеження. Вони часто неефективні у складних сценаріях, де спуфер адаптивно підлаштовує свої сигнали під реальне оточення. Крім того, у випадках багатопроменевого поширення чи активного використання противником засобів радіоелектронної боротьби, класичні методи не здатні забезпечити ні оперативність, ні достатню точність виявлення. Це особливо критично в умовах сучасних військових конфліктів, де навіть короткочасна дезорієнтація навігаційних систем може мати стратегічні наслідки.

У цьому контексті зростає потреба у впровадженні нових, більш гнучких та інтелектуальних підходів. Використання методів машинного навчання та нейронних мереж дозволяє здійснювати багатовимірний аналіз

сигналів, виявляти приховані аномалії та формувати більш надійні механізми ідентифікації атак. Такий підхід здатний не лише підвищити рівень захисту військових систем управління й наведення, але й зміцнити безпеку цивільних сервісів, які критично залежать від GPS. Таким чином, розробка ефективних алгоритмів виявлення GPS-спуфінгу є актуальною науковою та прикладною задачею, що стоїть на перетині інтересів оборони, транспорту та інфраструктурної безпеки.

Аналіз останніх досліджень і публікацій. Класичні методи детекції GNSS-спуфінгу охоплюють моніторинг якості сигналу (SQM), перевірки узгодженості код/фаза/доплер, багатоантенні схеми кута приходу (AoA/DoA), а також перехресні PNT-перевірки з інерціальними/мережевими джерелами [13, с. 1258–1270]. Паралельно розвиваються «активні» засоби – криптографічна автентифікація навігаційних повідомлень, зокрема Galileo OSNMA (операційний сервіс із 24 липня 2025 р.) та перспективна концепція GPS CHIMERA для L1C [4; 3, с. 1–10]. Ці рішення істотно зменшують площу атаки, але не усувають потреби у виявленні складних сценаріїв (ретрансляція/затримка, комбіновані атаки), тож практичні системи комбінують криптографію з дано-орієнтованими детекторами [10].

Найпоширенішою лінією робіт у сфері НН є підхід, де вхід формують як «зображення» (STFT-спектрограми, кореляторні карти, частотні ознаки) і застосовують CNN для бінарної/мультикласової детекції спуфінгу; показано високу чутливість як на БпЛА, так і на наземних приймачах [9]. Дослідження 2024–2025 рр. також переходять до Transformer-архітектур для моделювання довгих залежностей у послідовностях (доплер, різниці фаз, динаміка кореляцій), а гібриди CNN+Transformer знижують хибні спрацьовування на мультишляху [12, с. 5156–5168]. Поряд із цим, для відтворюваних порівнянь де-факто стандартом лишається TEXBAT це публічна батарея реалістичних спуфінг-сценаріїв (у т. ч. ds7/ds8), широко

застосовувана як класичними, так і DL-методами; спільнота водночас підкреслює потребу в ширших відкритих наборах для валідної оцінки генералізації [15; 14; 8; 7, с. 2314–2325].

Мета статті – дослідити придатність багатошарової перцептронної мережі (MLP) для задачі виявлення синхронного GPS-спуфінгу на рівні приймача, порівнявши її ефективність із базовими методами (порогові SQM-індикатори, логістична регресія) та оцінити вплив вибору ознак й налаштувань навчання на точність і робастність детектора. У рамках цієї статті ми сформулюємо наступні цілі:

- Обрати метрики для оцінювання MLP для поставленої задачі;
- Перетворити вхідні дані в IQ форматі в числові значення параметрів;
- Провести оцінку параметрів GPS сигналів та виділити параметри, які найкраще відображають різницю між оригінальним і підробленим сигналом. Провести нормалізацію даних і фільтрацію невалідних рядків;
- Провести комп'ютериний експеримент та порівняти продуктивність розробленою моделі згідно з раніше обраними метриками. Оцінити ефективність виявлення синхронних спуфінгових атак і переспективу використання мережі для інших типів спуфінгу,таких як статичний, динамічний, спуфінг час-зсут і т.д..

Досягнення даної мети дозволить нам оцінити наскільки MLP мережа актуальна для даної задачі і перспективи подальшого розвитку задачі для інших типів атак.

Виклад основного матеріалу. Для оцінювання ефективності багатошарової перцептронної мережі (MLP) у задачах класифікації було використано стандартні метрики якості - Accuracy(Точність), Precision (прецизійність), Recall (повнота) та F1-score (F1-міра). Ці метрик у

комплексі дає змогу всебічно оцінити продуктивність MLP, забезпечуючи коректне порівняння з базовими методами та підвищуючи надійність висновків щодо здатності моделі виявляти GPS-спуфінг.

Точність класифікації (Accuracy) відображає частку правильно класифікованих прикладів серед усієї вибірки та надає загальне уявлення про результативність моделі, хоча може бути недостатньо інформативною у випадку незбалансованих класів. Розраховується за формулою:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN), \quad (1)$$

де:

TP – кількість істотно позитивних прикладів, правильно класифікованих моделлю(виявлений спуфінг).

TN – кількість істотно негативних прикладів(правильно виявлені автентичний сигнал GPS).

FP – кількість хибнопозитивних класифікацій (помилково визначений спуфінг).

Кількість хибнонегативних класифікацій (спуфінг класифікований як автентичний сигнал). Прецензійність або precision показує, яка частка об'єктів, передбачених як позитивні, насправді є позитивними. Високе значення Precision означає, що модель робить мало хибнопозитивних помилок, що є важливим у задачах, де "помилкова тривога" має велику ціну:

$$\Pr e\,cision = TP/(TP + FP), \quad (2)$$

Повнота або Recall відображає частку правильно виявлених позитивних прикладів серед усіх фактичних позитивних об'єктів. Високий Recall означає, що модель рідко пропускає спуфінгові сигнали. Розраховується за формулою:

$$Recall = TP/(TP + FN), \quad (3)$$

F1-score – це гармонійне середнє між Precision і Recall. Використовується для досягнення балансу між здатністю моделі уникати

помилкових спрацювань та її здатністю виявляти всі релевантні приклади. Формула для розрахунку:

$$F1 = 2 \cdot \frac{\mathrm{Pr}\,ecision \cdot Recall}{\mathrm{Pr}\,ecision + Recall}, \quad (4)$$

TEXBAT (Texas Spoofing Test Battery) є еталонним набором даних для дослідження уразливостей супутникових навігаційних систем (GNSS) до атак типу спуфінг. Цей набір створений для оцінювання та порівняння алгоритмів виявлення спуфінгу в контрольованих і відтворюваних умовах. Дані TEXBAT були зібрані під час експериментів, у яких на приймачі GPS впливали штучно згенерованими сигналами, що імітують справжні навігаційні дані. Таким чином, дослідники отримали можливість перевіряти поведінку приймачів у різних сценаріях атак, включаючи поступове захоплення сигналу, синхронний та несинхронний спуфінг.

Набір TEXBAT включає кілька різних сценаріїв, представлених у вигляді окремих файлів (ds1–ds9), кожен із яких відповідає певному типу або конфігурації атаки. Зокрема, у датасетах зафіксовано: чистий прийом справжнього сигналу без спуфінгу (референтний сценарій), просте накладання сигналу-спуфера, поступове зміщення фази та часу, синхронний захоплюючий спуфінг, а також складні комбінації з багатопроменевими ефектами. Кожен сценарій містить оцифровані I/Q-семпли на високій частоті дискретизації, що робить ці дані придатними для аналізу як на рівні сигналів, так і на рівні обробки в приймачах.

У даній роботі використовується датасет ds7, який відповідає сценарію синхронного спуфінгу із поступовим захопленням приймача. У цьому сценарії атакуючий сигнал починає точно збігатися з легітимним по фазі та часу, після чого поступово змінює параметри несучої та кодової затримки, змушуючи приймач перейти на підроблений сигнал. Це робить ds7 одним із найбільш релевантних наборів для дослідження методів виявлення синхронного GPS-спуфінгу, оскільки він відображає реалістичну

і складну для виявлення атаку, близьку до практичних сценаріїв у реальних системах навігації.

Як вже було сказкано раніше, для експериментів використано записи TEXBAT у форматі комплексних IQ. Це реалістичні сценарії спуфінгу GPS L1 C/A, що містять як «чисті» епізоди, так і інтервали атаки. Мітка цілі spoof∈{0,1} формувалась за сценарними анотаціями: 1 – інтервали спуфінгу, 0 – номінальний сигнал.

Оброблення IQ здійснювалося за допомогою gnss-sdr – SDR-приймача GNSS із модульною архітектурою і відкритим кодом. Для зчитування TEXBAT налаштовано Signal_Source = File_Signal_Source з частотою дискретизації 25 MSPS (25 мегасемплів/с), подальшим захопленням і стеженням за каналом L1 C/A. На виході використано трекінгові логи приймача, з яких сформовано табличне подання ознак, записане в декілька csv файлів.

Опрацювавши дані з допомогою gnss-sdr, отримаємо наступний набір полів: CN0_SNV_dB_Hz, PRN, PRN_start_sample_count, Prompt_I, Prompt_Q, abs_E, abs_L, abs_P, abs_VE, abs_VL, acc_carrier_phase_rad, aux1, aux2, carr_error_filt_hz, carr_error_hz, carrier_doppler_hz, carrier_doppler_rate_hz, carrier_lock_test, code_error_chips, code_error_filt_chips, code_freq_chips, code_freq_rate_chips.

Для тренування моделі використаємо наступний набір даних (див. табл. 1).

Таблиця 1

Опис даних для тренування MLP мережі

Назва	Пояснення
CN0_SNV_dB_Hz	Якість сигналу (дБ-Гц); чутлива до зміни SNR під час підміни
Prompt_I, Prompt_Q	(реальна/уявна частини), безпосередній слід узгодженості сигналу
acc_carrier_phase_rad	накопичена фаза несучої (рад)
carr_error_filt_hz, carr_error_hz	помилка несучої (Гц)
carrier_doppler_hz	Доплер (Гц)

code_error_chips, code_error_filt_chips	помилка коду (chips)
code_freq_chips	частота коду (chips/s)

Нижче наведено також колонки, які не використовуються і причини, чому вони не підходять для тренування (див. табл. 2).

Таблиця 2

Відкинуті поля

Назва	Характеристика	Подія
PRN, PRN_start_sample_count	Ідентифікатори	Неінформативне для детекції
abs_VE, abs_VL	Абсолют VE та VL компоненти	Майже константне/незмінне в наборі
abs_E, abs_L	Амплітуда на early та late кореляторах	Сильний перекіс розподілу; погіршує стабільність без спец. трансформацій
abs_P	Амплітуда на prompt-кореляторі	Надлишкова: відтворюється з Prompt_I_0,Prompt_Q_0
carrier_doppler_rate_hz	Швидкість зміни доплера	Низька варіативність у фрагментах; мінімальна користь для базової MLP
carrier_lock_test	Прапор утримання несучої	Майже константа (часто =1); мало дискримінативний
code_freq_rate_chips	Швидкість зміни частоти коду	Мала варіативність; не дає приросту якості в базовій моделі

Запропонована модель MLP мережі здійснює автоматичне виявлення спуфінгу на основі даних з Таблиці 1., тобто бінарну класифікацію повертаючи мітки 0 - якщо спуфінг не виявлено, та 1 - якщо спуфінг виявлено.

У цьому дослідженні було реалізовано комп'ютерний експеримент, метою якого було навчання мережі MLP для виявлення синхронного спуфінгу, на основі даних, отриманих з TEXBAT набору, що розділені

маркером на дві катеорії - наявність спуфінгу та відсутність спуфінгу (див. рис. 1).

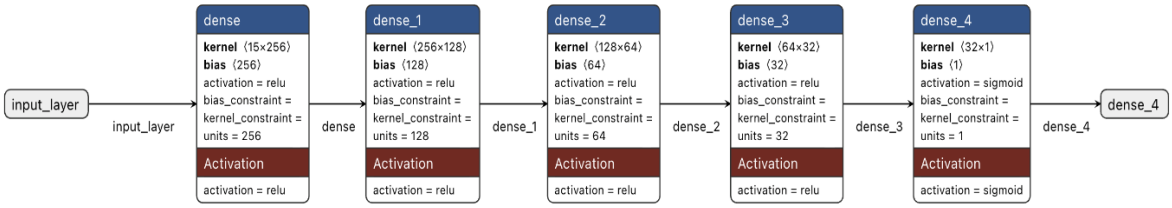

Рис. 1. Архітектура мережі

Запропонована вище модель є багатошаровим перцептроном (MLP) для класифікації табличних ознак приймача GNSS. На вхід подається вектор нормалізованих параметрів (уніфікованих у діапазоні [−1;1]), що описують миттєвий стан трекінгу: якість сигналу (C/N_0), компоненти prompt-корелятора (I/Q), фазові та частотні похибки PLL/DLL, доплер та частоту коду.

Архітектура побудована як каскад щільних шарів із нелінійною активацією ReLU, які послідовно зменшують розмірність простору ознак і формують ієрархію представлень: спершу виділяються грубі міжознакові залежності (256 нейронів), далі — більш компактні та спеціалізовані патерни (128 → 64 → 32 нейрони). Така структура дає змогу моделі вловлювати характерні поєднання ознак, притаманні синхронному спуфінгу (наприклад, нетипова узгодженість фазово-частотних величин на тлі стабільного доплера чи C/N_0).

Вихідний шар є однонейронним із сигмоїдальною активацією, що інтерпретується як ймовірність наявності спуфінгу для даного вектору вимірювань. Навчання здійснюється методом адаптивної градієнтної оптимізації (типу Adam) з бінарною крос-ентропією як функцією втрат. Для підвищення стабільності збіжності використовується адаптивне зниження швидкості навчання за відсутності покращення на валідаційному наборі.

Оцінювання проводиться за класичними метриками бінарної класифікації (точність, precision, recall) із подальшим аналізом звіту класифікації та матриці неточностей. У такій постановці MLP виступає легкою та придатною до вбудування альтернативою послідовним/конволюційним моделям, зосереджуючись на миттєвих сигнальних індикаторах і забезпечуючи належний компроміс між якістю детекції та обчислювальною вартістю.

За підсумками тестування на 488 375 зразках модель MLP досягла точності 0.92, із precision 0.92, recall 0.93 та F1-score 0.93. Якість по класах збалансована: для класу «0» (nominal) — precision = 0.93, recall = 0.92, F1 = 0.92 (support = 238 565); для класу «1» (spoof) — precision = 0.92, recall = 0.93, F1 = 0.93 (support = 249 810). Матриця помилок вказує на 19 569 FP (помилкові спрацьовування) та 17 486 FN (пропуски), що підтверджує збалансований компроміс між чутливістю та специфічністю за порогу 0.5. Сукупно це свідчить, що навіть без складної часової обробки MLP на нормалізованих канальних ознаках здатна надійно відрізняти синхронний спуфінг від номінального сигналу.

Динаміка навчання (див. рис. 2.) показує монотонне зростання точності та спадання втрат із виходом на плато без вираженої розбіжності між навчальною та валідаційною кривими — ознака відсутності суттєвого перенавчання.

Зниження швидкості навчання на плато (ReduceLROnPlateau) стабілізує збіжність наприкінці тренування. Загальний час експерименту склав 3 655.85 с, після чого виконано оцінювання на тесті та побудовано звіти (classification report, confusion matrix). У прикладних сценаріях поріг 0.5 може бути зміщено для мінімізації FN або FP залежно від вимог (наприклад, зменшення пропусків спуфінгу за рахунок збільшення кількості тривог).

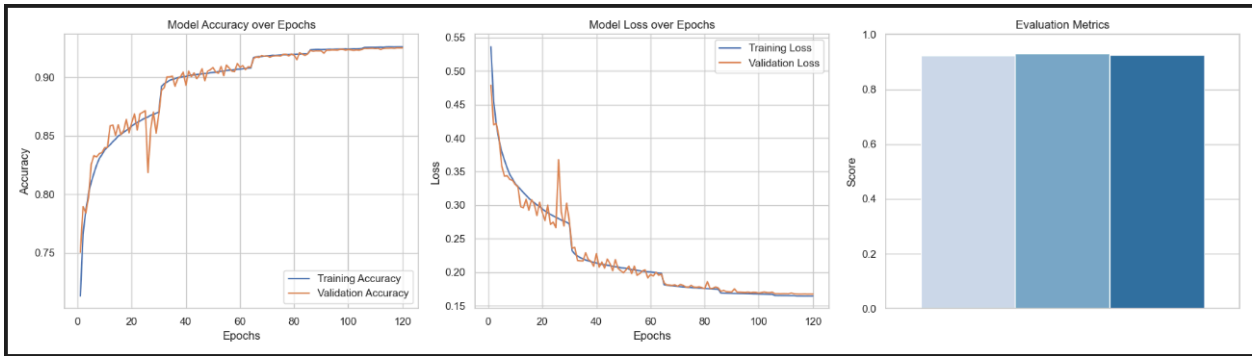

Рис. 2. Графіки точності та витрати

Висновки. Розроблено та досліджено модель MLP для виявлення синхронного GPS-спуфінгу на основі табличних ознак трекінгу приймача GNSS (C/N₀, Prompt I/Q, фазові та частотні похибки PLL/DLL, доплер, частота коду). Для оцінювання застосовано метрики Accuracy, Precision, Recall, F1-score. За підсумками тестування на 488 375 зразках отримано accuracy = 0.92, precision = 0.92, recall = 0.93, F1-score = 0.93. Матриця плутанини засвідчує збалансованість помилок: TP = 232 324, TN = 218 996, FP = 19 569, FN = 17 486 за порогу 0.5, що підтверджує надійну відмінність між номінальним сигналом і синхронним спуфінгом навіть без складної часової обробки.

Проведено попереднє опрацювання даних: нормалізацію ознак до [−1;1], очищення від аномальних значень, сценарно-усвідомлене розбиття вибірок без витоків. Навчання здійснювалось адаптивною оптимізацією з контролем збіжності (зниження швидкості навчання на плато). Графіки "Model Accuracy over Epochs" та "Model Loss over Epochs" демонструють стале підвищення якості та згасання втрат із виходом на плато без ознак суттєвого перенавчання, що узгоджується з підсумковими метриками на тесті.

Напрямками подальших досліджень є розгляд альтернативних архітектур нейронних мереж, насамперед CNN (для опрацювання часово-частотних представлень та кореляторних «карт») і, за потреби, їхніх гібридів із простими послідовними блоками. Окремим вектором стане

розширення постановки завдання на інші типи спуфінгових атак, представлені в TEXBAT (зокрема сценарії з різною динамікою, затримками/ретрансляцією та комбінованими впливами), щоб оцінити узагальнюваність підходу поза синхронним спуфінгом і визначити, яка архітектура (MLP/CNN/гібрид) забезпечує найкращий компроміс між якістю та обчислювальною вартістю.

Література

1. Anderson J. M., Carroll K. L., DeVilbiss N. P., Gillis J. T., Hinks J. C., O'Hanlon B. W., Rushanan J. J., Scott L., Yazdi R. A. *Chips-Message Robust Authentication (CHIMERA) for GPS civilian signals. Proceedings of ION GNSS+*. 2017. URL: https://www.ion.org/ (дата звернення: 01.10.2025).

2. Bishop C. M. Pattern recognition and machine learning. New York : Springer, 2006. 738 p.

3. European Commission. Galileo's OSNMA authentication service now operational. 25 серпня 2025 р. URL: https://defence-industry-space.ec.europa.eu/ (дата звернення: 01.10.2025).

4. European Union. Galileo Open Service Navigation Message Authentication (OSNMA): Service Definition Document (Issue 1.0). Luxembourg : Publications Office of the European Union, 2025. URL: https://www.gsc-europa.eu/ (дата звернення: 01.10.2025).

5. Goodfellow I., Bengio Y., Courville A. Deep learning. Cambridge (MA) : MIT Press, 2016. 800 p.

6. Haykin S. Neural networks: A comprehensive foundation. 2nd ed. Upper Saddle River (NJ) : Prentice Hall, 1999. 842 p.

7. Humphreys T. E., Ledvina B. M., Psiaki M. L., O'Hanlon B. W., Kintner P. M. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS)*. 2008. P. 2314–2325.

8. Humphreys T. E. TEXBAT data sets 7 and 8: Description and usage (Technical report). Austin (TX) : The University of Texas at Austin, Radionavigation Laboratory, 2016. URL: https://rnl-data.ae.utexas.edu/ (дата звернення: 01.10.2025).

9. Korium M. S., Saber M. та ін. Image-based intrusion detection system for GPS spoofing cyberattacks in UAVs. *Ad Hoc Networks*. 2024. Vol. 163. Art. 103597. DOI: https://doi.org/10.1016/j.adhoc.2024.103597

10. Meng L., Wei Z., Meng X., Li B. A survey of GNSS spoofing and anti-spoofing technology. *Remote Sensing.* 2022. Vol. 14, No. 19. Art. 4826.

11. Misra P., Enge P. Global Positioning System: Signals, measurements, and performance. 2nd ed. Lincoln (MA) : Ganga-Jamuna Press, 2011. 600 p.

12. Niu B., Zhuang X., Lin Z., Zhang L. Navigation spoofing interference detection based on a Transformer model in the acquisition stage. *Advances in Space Research.* 2024. Vol. 74, No. 10. P. 5156–5168.

13. Psiaki M. L., Humphreys T. E. GNSS spoofing and detection. *Proceedings of the IEEE*. 2016. Vol. 104, No. 6. P. 1258–1270.

14. UT Radionavigation Laboratory. TEXBAT: Texas Spoofing Test Battery. The University of Texas at Austin, [б.р.]. URL: https://radionavlab.ae.utexas.edu/texbat/

15. Wesson K. D., Shepard D. P., Bhatti J. A., Humphreys T. E. The Texas Spoofing Test Battery: Toward a standard for evaluating GPS signal authentication techniques. *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS).* 2012. P. 3569–3583.