https://doi.org/10.31891/2307-5732-2025-355-82
УДК 004.056.5:004.89:528.85

СНЄОСІКОВ ОЛЕГ
Харківський національний університет імені В. Н. Каразіна
https://orcid.org/0009-0001-9468-5965
e-mail: oleh.snieosikov@student.karazin.ua

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ КІБЕРАТАКАМ ТИПУ GPS SPOOFING І GPS JAMMING З ВИКОРИСТАННЯ AI ДЛЯ СИСТЕМ ДИФЕРЕНЦІЙНОЇ КОРЕКЦІЇ ТА ГЛОБАЛЬНОЇ НАВІГАЦІЙНОЇ СУПУТНИКОВОЇ СИСТЕМИ

Запропоновано гібридний підхід, який поєднує кластеризацію (K-Means, Fuzzy C-Means, Онлайн K-Means), сигнатурний аналіз (Random Forest) та прогнозування за допомогою рекурентної нейронної мережі (RNN) на основі GRU. Це дозволяє виявляти аномалії в реальному часі, класифікувати атаки та адаптивно реагувати на нові загрози.

Ключові слова: GPS, GNSS, спуфінг, кібербезпека.

SNIEOSIKOV OLEH
V. N. Karazin Kharkiv National University

METHODS FOR DETECTION AND COUNTERACTION OF CYBERATTACKS OF THE TYPE GPS SPOOFING AND GPS JAMMING USING AI FOR DIFFERENTIAL CORRECTION SYSTEMS AND GLOBAL NAVIGATION SATELLITE SYSTEM

An integrated approach combining clustering, signature analysis, and forecasting methods is proposed to effectively detect and neutralize cyberattacks in real time.

The purpose of the article is to develop methods for using artificial intelligence (AI) for cyber defense of Differential Global Positioning Systems (DGPSs) of global navigation satellite systems (GNSS), autonomous autonomous DGPS, against GPS spoofing and GPS jamming attacks.

Scientific novelty. For the first time, a hybrid methodology based on K-Means, Fuzzy C-Means, Online K-Means, Random Forest, and Recurrent Neural Network (RNN) algorithms using GRU layers is proposed. This technique allows not only to detect anomalies but also to adaptively update the model in response to new threats. A unique GNSS dataset was synthesized, including 500 samples for each class (normal signals, spoofing, jamming) with 8 critical features (signal strength, delay, acceleration, etc.). For the first time, post-quantum cryptography mechanisms are integrated to improve the system security.

Results. The study conducted a clustering analysis using K-Means and Fuzzy C-Means, which detected 66.7% of anomalies (100 out of 150 expected), while online K-Means showed better adaptability, detecting 204 anomalies. The distribution of clusters for K-Means was [100, 154, 1246], for Fuzzy C-Means - [1246, 154, 100], and for online K-Means - [924, 204, 372]. Signature analysis using Random Forest effectively filtered out false signals, the model was trained on 70% of the data and tested on 30%. Predicting attacks using GRU-based RNNs achieved an accuracy of 0.50 on the training set and 0.51 on the validation set, using 3 GRU layers of 128 neurons each, training was stopped after 32 epochs. Countermeasures included adaptive synchronization with a time correction of 0.14 ms, switching to inertial navigation when more than 50% of anomalies were detected, and simulating post-quantum key generation. Additional analyses revealed a correlation between power and signal latency of 0.54, and multisensory integration used an acceleration threshold of 0.5. Nine PNG graphs were generated to visualize various aspects of the analysis. Data processing included the use of 500 samples for each class (normal, spoofing, jamming) with 8 features, and data standardization for RNNs was applied.

Conclusions. The effectiveness of the proposed hybrid approach for protecting autonomous SDKs has been proved. Online K-Means showed the best results due to its ability to adapt to dynamic conditions. Further research should focus on using real GNSS data; improving the RNN architecture; expanding the feature set to improve accuracy.

Keywords: GPS, GNSS, spoofing, cybersecurity.

Стаття надійшла до редакції / Received 06.05.2025
Прийнята до друку / Accepted 06.06.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Глобальні навігаційні супутникові системи (Global navigation satellite systems, GNSS) відіграють ключову роль у сучасних технологіях, забезпечуючи точне позиціонування для авіації, морського транспорту, автономних транспортних засобів, а також систем диференційної корекції (СДК), зокрема автономних СДК (АСДК). Проте GNSS є вразливими до кібератак, таких як GPS spoofing (підміна сигналів) і GPS jamming (глушіння сигналів), які можуть призвести до серйозних наслідків, зокрема порушення навігації, втрати зв'язку або навіть аварій [1, 3, 6]. Особливо критичною ця проблема є для автономних систем, де людський контроль обмежений, а точність позиціонування напряму впливає на безпеку функціонування.

Сучасні методи виявлення атак на GNSS, такі як статистичний аналіз або геометричні методи, часто мають обмеження у швидкості реагування та адаптивності до нових типів атак [4, 6]. Наприклад, геометричний метод визначення GPS spoofing атак, запропонований Нетаврованою А., є ефективним для безпілотних літальних апаратів, але потребує значних обчислювальних ресурсів і не завжди підходить для реального часу [6]. У той же час, з розвитком штучного інтелекту (ШІ) з'явилися нові можливості для адаптивного виявлення та протидії кібератакам. Застосування методів машинного навчання, таких як кластеризація, сигнатурний аналіз і нейронні мережі, дозволяє виявляти аномалії в даних GNSS у реальному часі, а також прогнозувати потенційні атаки [2, 5].

Проблема кіберзахисту GNSS у контексті АСДК є важливою науковою і практичною задачею,

оскільки автономні системи дедалі частіше використовуються в критичних інфраструктурах, таких як транспорт, енергетика та військова сфера. У літературі, наприклад у роботах Сусукайла В.А., підкреслюється необхідність розробки моделей для дослідження кіберзлочинів, але конкретні рішення для GNSS залишаються недостатньо розвиненими [2]. Відсутність готових рішень для виявлення та протидії атакам у реальному часі зумовила необхідність розробки власного програмного коду для моделювання, аналізу та створення адаптивних методів захисту.

Аналіз досліджень та публікацій

У сучасних дослідженнях зосереджено увагу на застосуванні штучного інтелекту для виявлення та реагування на кіберзагрози, особливо в контексті систем GNSS. Зоря І. С. та Марущак А. В. [1] досліджують використання машинного навчання для аналізу аномалій у мережевих даних, підкреслюючи адаптивність таких методів. Сусукайло В. А. [2] розробляє модель системи дослідження кіберзлочинів, акцентуючи на необхідності комплексних моделей для захисту критичних систем. Петровський А. В. [3] описує алгоритм виявлення GPS spoofing, не використовуючи адаптивні методи ШІ. Волошин Д. Г. та Бульба С. С. [4] пропонують інтелектуальний метод виявлення GPS spoofing БПЛА, але без прогнозування атак за допомогою нейронних мереж. Мустафаєв О. В. [5] аналізує технології захисту від GPS spoofing, не охоплюючи адаптивні методи ШІ. Нетаврована А. [6] розробляє геометричний метод визначення GPS spoofing, не використовуючи гібридний підхід. Radoš K., Brkić M., Begušić D. [7] розглядають методи виявлення GPS jamming та GPS spoofing, але без прогнозування атак. Janiar S. та Wang P. [8] пропонують метод протидії GPS jamming, не зосереджуючись на комплексному виявленні аномалій. Alkhatib M. та ін. [9] досліджують класифікацію GPS jamming-атак, не використовуючи адаптивні методи. Mohanty A. та Gao G. [10] оглядають машинне навчання для покращення GNSS, не зосереджуючись на кіберзахисті, але підкреслюючи потенціал ШІ.

Таким чином, поточні дослідження підкреслюють потребу в комплексних та адаптивних методах ШІ для ефективного виявлення та протидії кібератакам у системах GNSS. Інтеграція різних підходів, таких як кластеризація, сигнатурний аналіз та нейронні мережі, може значно підвищити стійкість систем до атак типу GPS spoofing та GPS jamming.

Формулювання цілей статті

Метою роботи є розробка та дослідження методів штучного інтелекту для виявлення та протидії кібератакам типу GPS spoofing і GPS jamming у системах диференційної корекції (СДК) GNSS, зокрема в автономних СДК (АСДК). Для досягнення цієї мети було поставлено такі завдання:

1. Розробити синтетичні дані GNSS, які моделюють нормальні сигнали, а також сигнали, що зазнають атак GPS spoofing та GPS jamming.
2. Застосувати методи кластеризації (K-Means, Fuzzy C-Means, Онлайн K-Means) для виявлення аномалій у даних GNSS.
3. Використати сигнатурний аналіз на основі Random Forest для класифікації сигналів і фільтрації фальшивих сигналів.
4. Розробити модель рекурентної нейронної мережі (RNN) для прогнозування атак.
5. Запропонувати методи протидії атакам, включаючи адаптивну синхронізацію, перехід на інерційну навігацію та інтеграцію з пост-квантовою криптографією.
6. Провести кореляційний аналіз даних GNSS для оцінки зв’язків між характеристиками сигналів.

Виклад основного матеріалу

Запропонований підхід до кіберзахисту систем диференційної корекції (СДК) GNSS на мові програмування Python у Visual Studio Code, зокрема автономних СДК (АСДК), базується на інтеграції кількох методів штучного інтелекту, що дозволяє комплексно вирішувати проблему виявлення та протидії кібератакам типу GPS spoofing і GPS jamming. Основна ідея полягає у поєднанні кластеризації (K-Means, Fuzzy C-Means, Онлайн K-Means), сигнатурного аналізу (Random Forest) і прогнозування атак за допомогою рекурентної нейронної мережі (RNN) на основі GRU, що забезпечує багатошаровий аналіз даних GNSS. Такий гібридний підхід дає змогу не лише виявляти аномалії в реальному часі, а й адаптивно реагувати на нові загрози, що є критично важливим для автономних систем, де швидкість і точність реагування відіграють ключову роль.

Для дослідження було створено синтетичні дані GNSS, які моделюють нормальні сигнали, а також сигнали, що зазнають атак типу GPS spoofing і GPS jamming. Кожен клас даних (нормальні, GPS spoofing, GPS jamming) містив по 500 зразків, що забезпечило ідеальний баланс класів ([500, 500, 500]). Дані включали такі ознаки: потужність сигналу (power), затримка сигналу (delay), прискорення (accel), кількість видимих супутників (satellites), частота сигналу (frequency), рівень шуму (noise_level), доплерівське зміщення (doppler_shift) і кут приходу сигналу (angle_of_arrival). Для моделювання атак типу GPS spoofing і GPS jamming було змінено значення ознак, наприклад, потужність GPS jamming сигналів підвищувалася до 90 дБ, а GPS jamming сигнали мали знижену кількість супутників (0–3). Додатково було введено аугментацію даних шляхом додавання шуму для підвищення стійкості моделей до варіацій у реальних умовах.

Для виявлення аномалій було використано три методи кластеризації: K-Means, Fuzzy C-Means і Онлайн K-Means.

K-Means розділив дані на три кластери з розподілом [100, 154, 1246], визначивши аномальний кластер 0 з 100 точками (рис. 1). Очікувана кількість аномалій становила 150 (10% від загальної кількості зразків), тому K-Means виявив 66.7% аномалій.

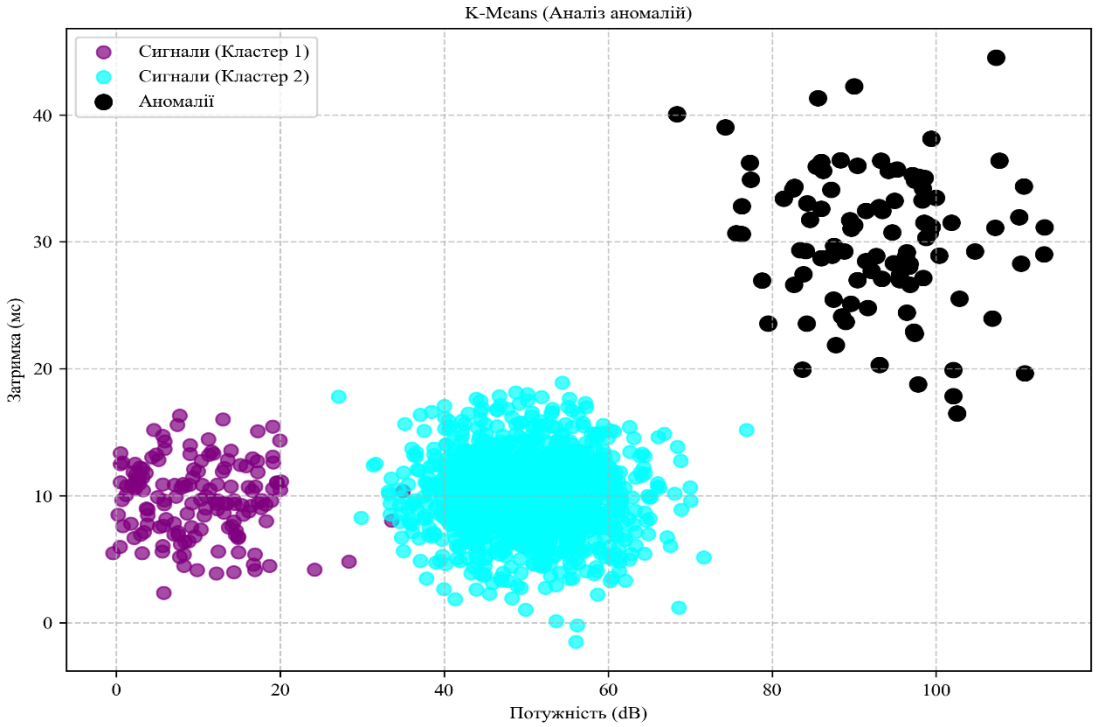

Рис. 1. Результати кластеризації K-Means
Джерело: авторська розробка

Fuzzy C-Means показав схожий результат із розподілом [1246, 154, 100], визначивши аномальний кластер 2 з 100 точками (рис. 2). Кількість виявлених аномалій також склала 66.7% від очікуваної.

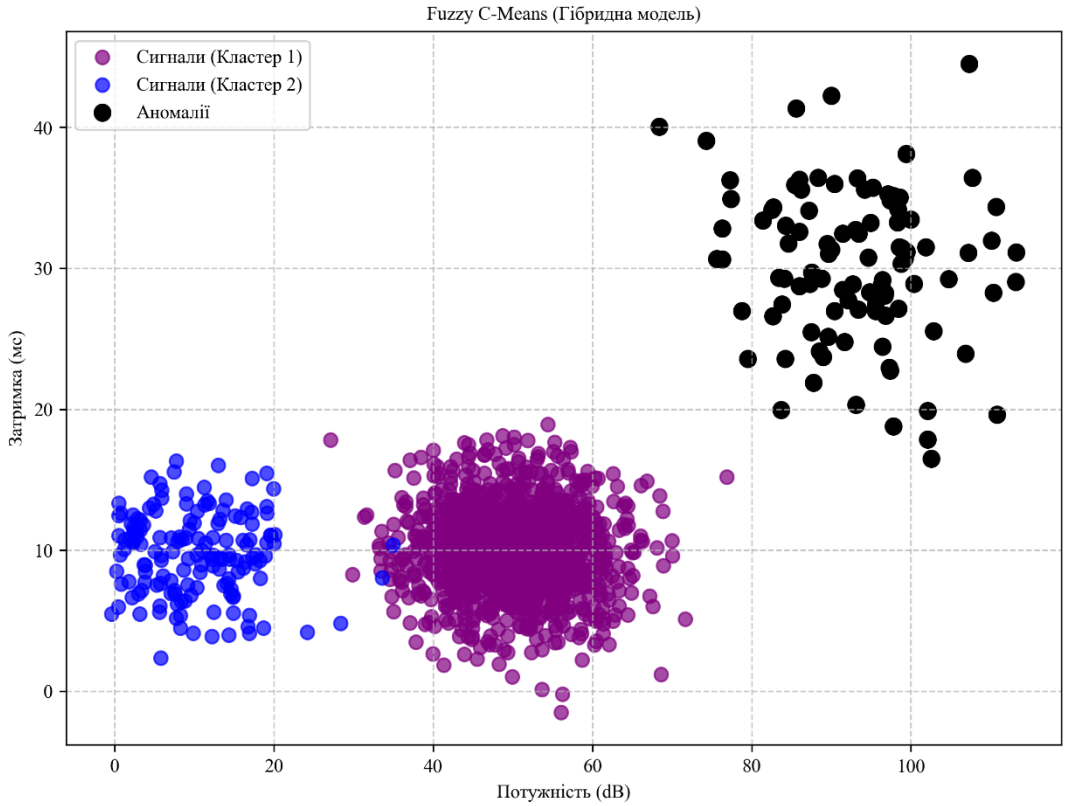

Рис. 2. Результати кластеризації Fuzzy C-Means
Джерело: авторська розробка

Онлайн K-Means моделював поступове надходження даних, розділивши їх на дві частини. Розподіл кластерів склав [924, 204, 372], а аномальний кластер 1 містив 204 точки (рис. 3). Це ближче до очікуваної кількості аномалій (150), що свідчить про адаптивність методу до умов реального часу.

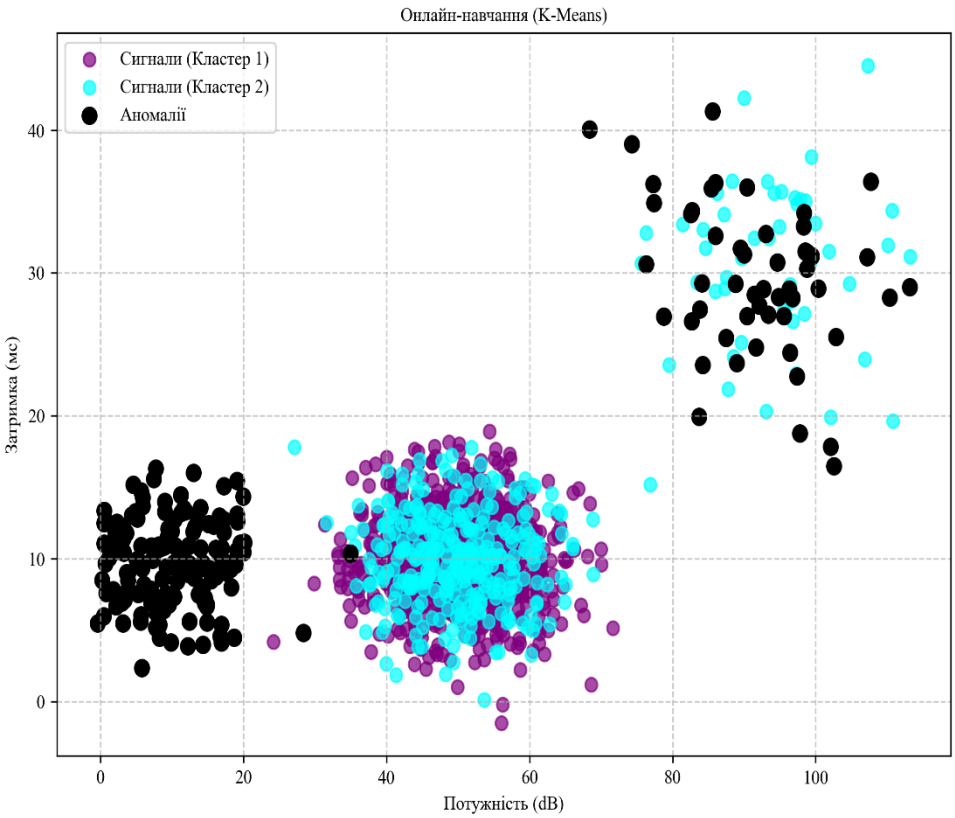

Рис. 3. Результати Онлайн K-Means
Джерело: авторська розробка

Для класифікації сигналів на нормальні та аномальні було використано алгоритм Random Forest із 100 деревами. Модель була навчена на 70% даних і протестована на 30%. Результати класифікації використано для фільтрації фальшивих сигналів, що показано на рис. 4.

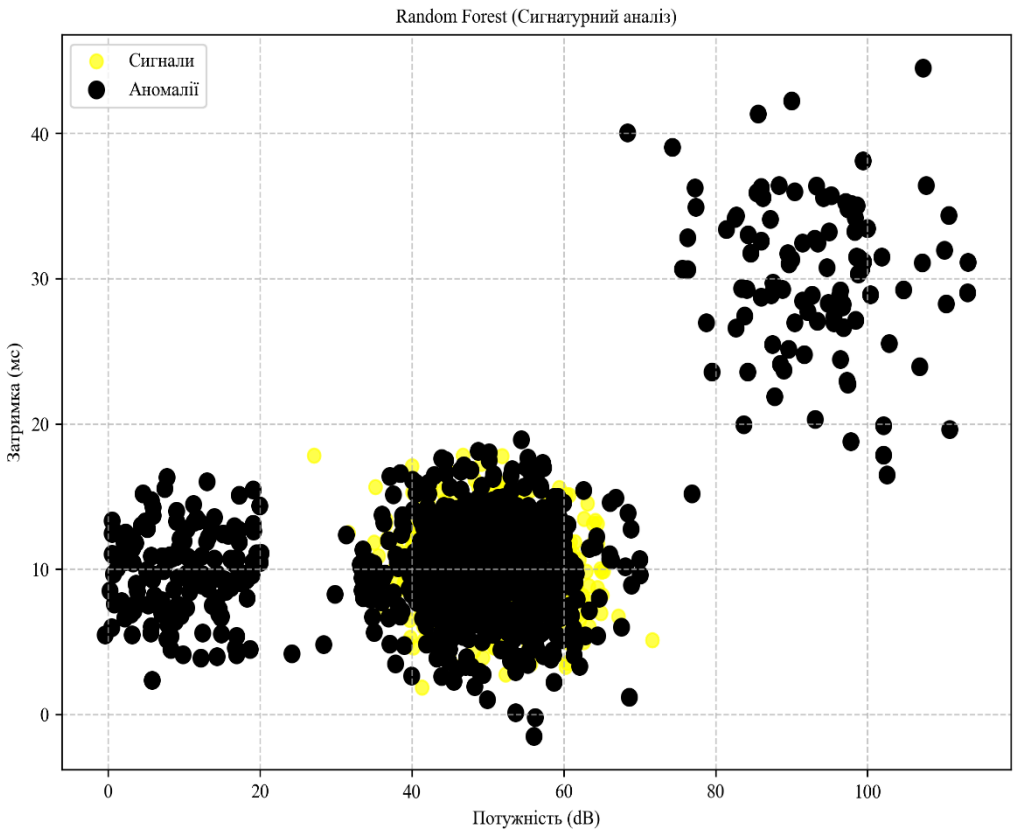

Рис. 4. Результати сигнатурного аналізу Random Forest

Джерело: авторська розробка

Для виявлення аномалій на основі даних акселерометра було використано порогове значення прискорення 0.5. Аномалії, визначені за допомогою багатосенсорної інтеграції, показано на рис. 5.

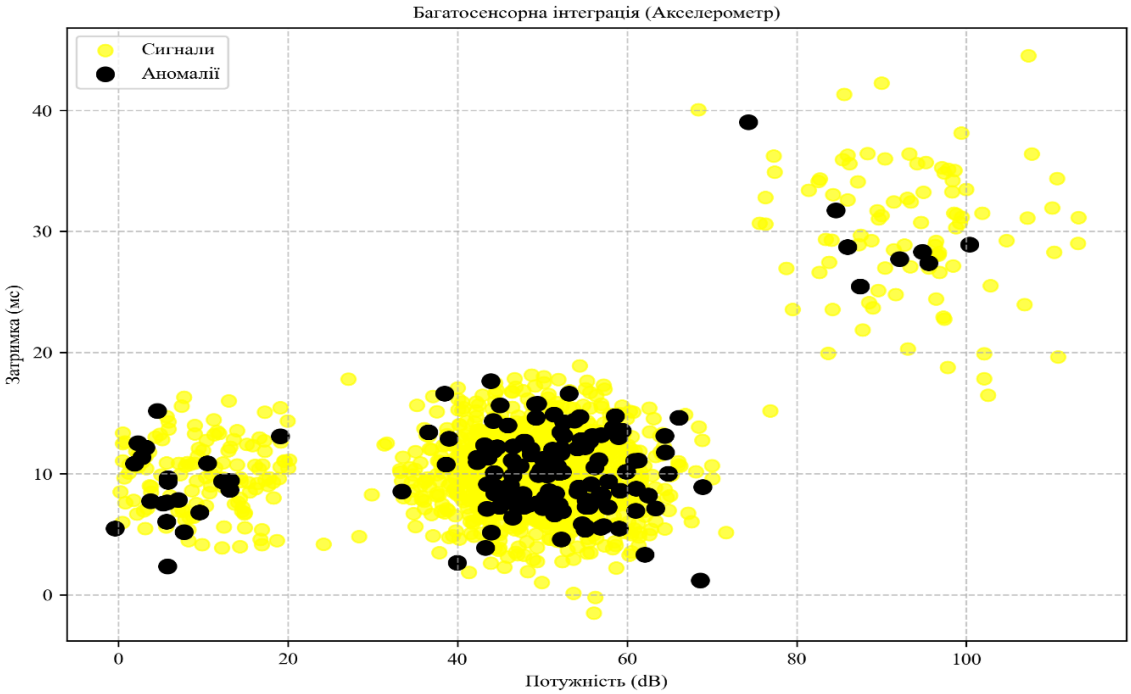

Рис. 5. Результати багатосенсорної інтеграції
Джерело: авторська розробка

Для прогнозування атак було розроблено рекурентну нейронну мережу (Recurrent neural network – RNN) на основі трьох шарів GRU (128 нейронів у кожному шарі), з L2-регуляризацією (коефіцієнт 0.02), Dropout (0.5) і швидкістю навчання 0.0005. Модель навчалася протягом 32 епох (з максимальних 100) із застосуванням Early Stopping (patience=30). Точність на тренувальному наборі склала 0.50, а на валідаційному — 0.51. Динаміка навчання зображена на рис. 6 (точність) і рис. 7 (втрати). Результати прогнозування атак показано на рис. 8.

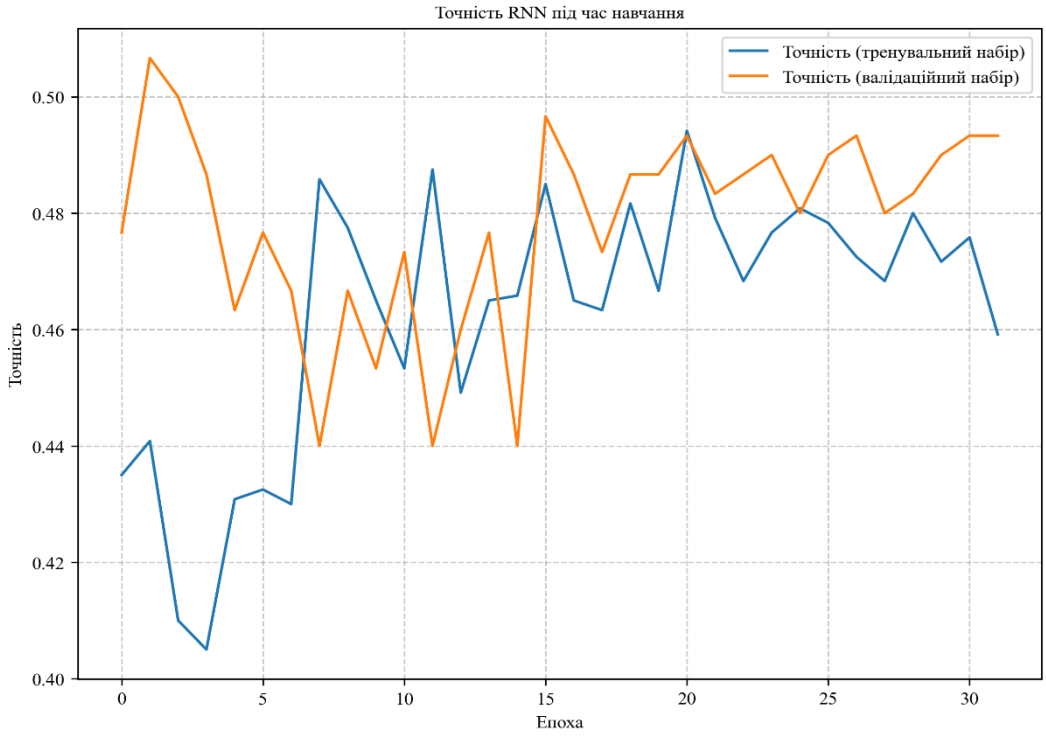

Рис. 6. Динаміка точності під час навчання
Джерело: авторська розробка

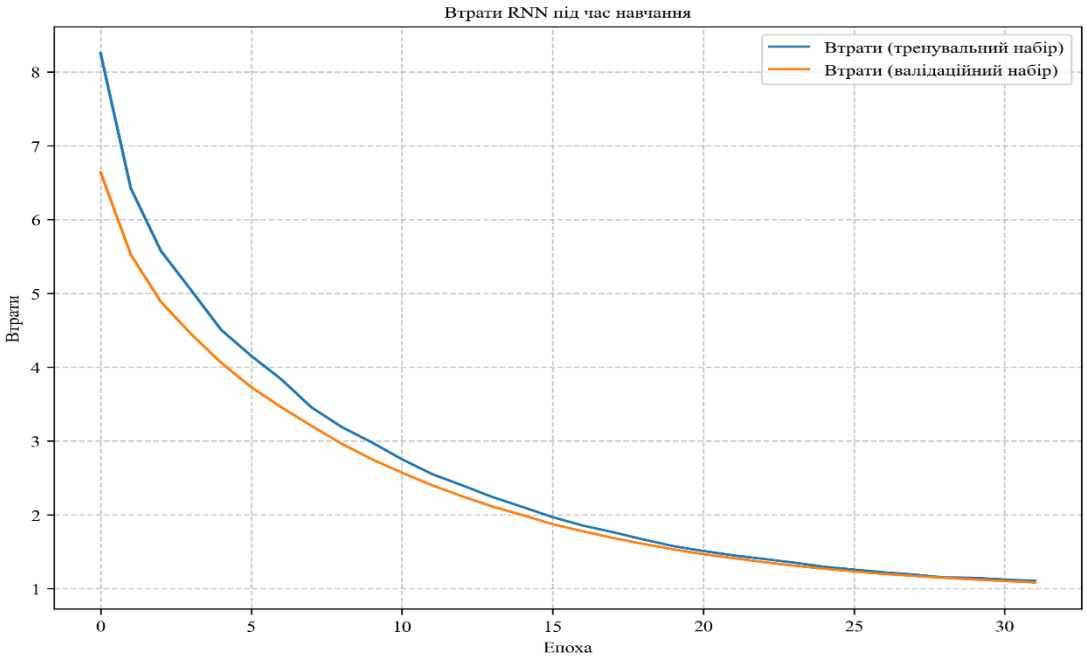

Рис. 7. Динаміка втрат під час навчання
Джерело: авторська розробка

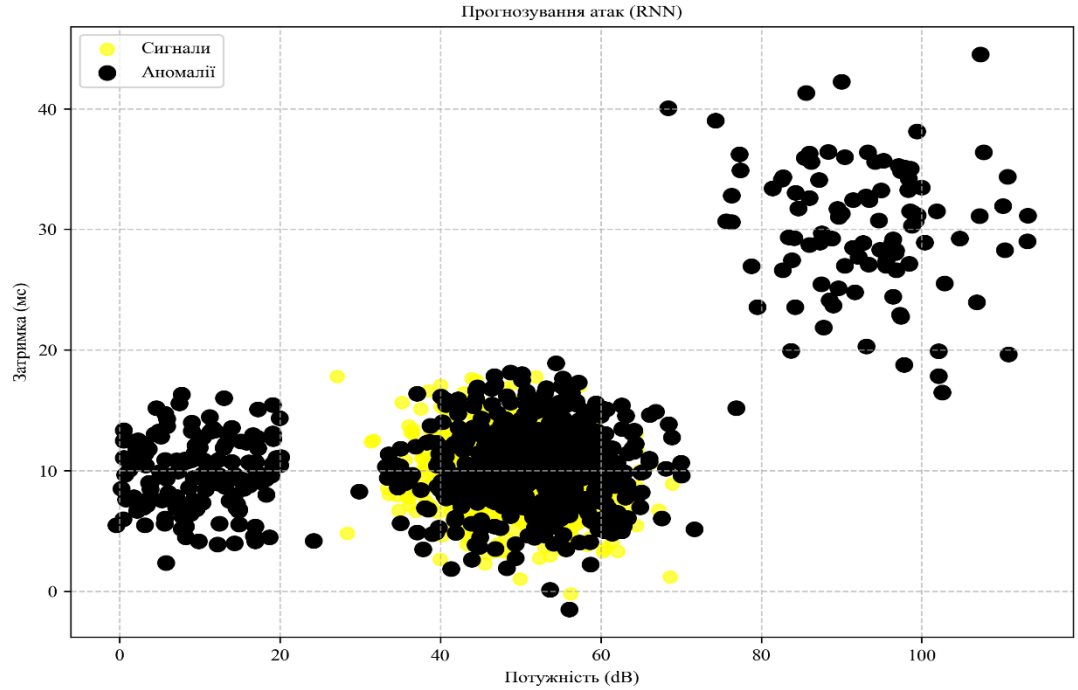

Рис. 8. Прогнозування атак за допомогою RNN
Джерело: авторська розробка

На основі результатів Random Forest було виконано фільтрацію фальшивих сигналів. Порівняння даних до і після фільтрації показано на рис. 9.

У разі виявлення значної кількості аномалій (понад 50% даних) передбачено перехід на інерційну навігацію, що забезпечує безперервність роботи АСДК.

Для компенсації затримок, спричинених спуфінгом, було реалізовано адаптивну синхронізацію. У фінальному запуску корекція часу склала 0.14 мс.

Для захисту даних GNSS від майбутніх загроз було імітуровано генерацію пост-квантового ключа (перші 10 бітів: [0 0 0 0 1 1 0 1 1 0]).

Кореляційний аналіз показав помірний зв’язок між потужністю і затримкою сигналів (коефіцієнт кореляції 0.54). Повна кореляційна матриця зображена на рис. 10.

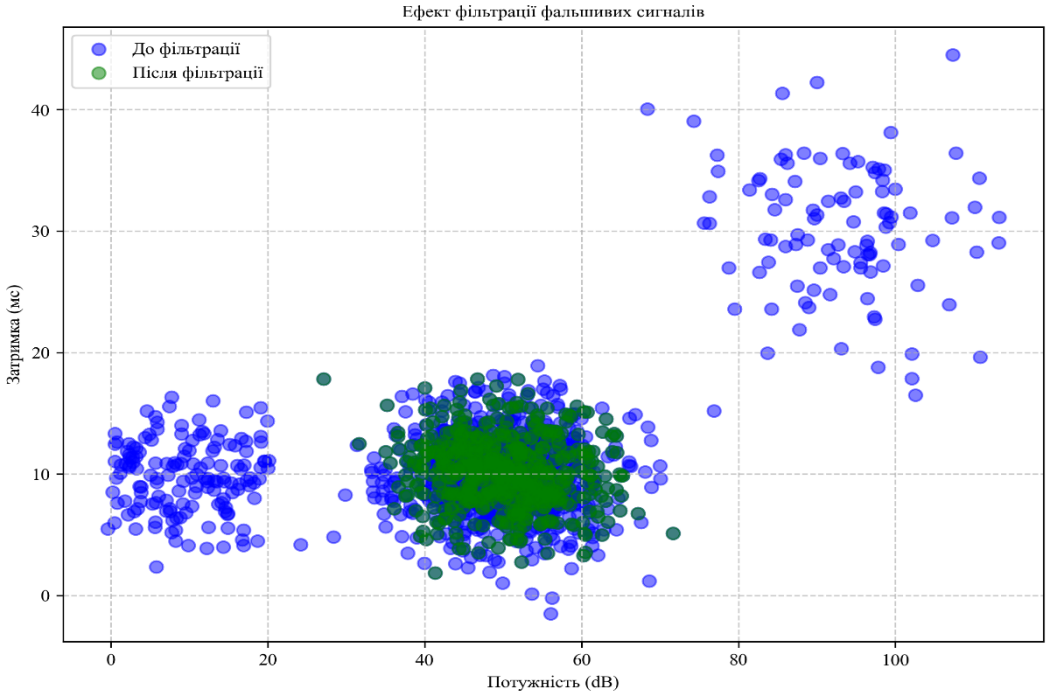

Рис. 9. Ефект фільтрації фальшивих сигналів
Джерело: авторська розробка

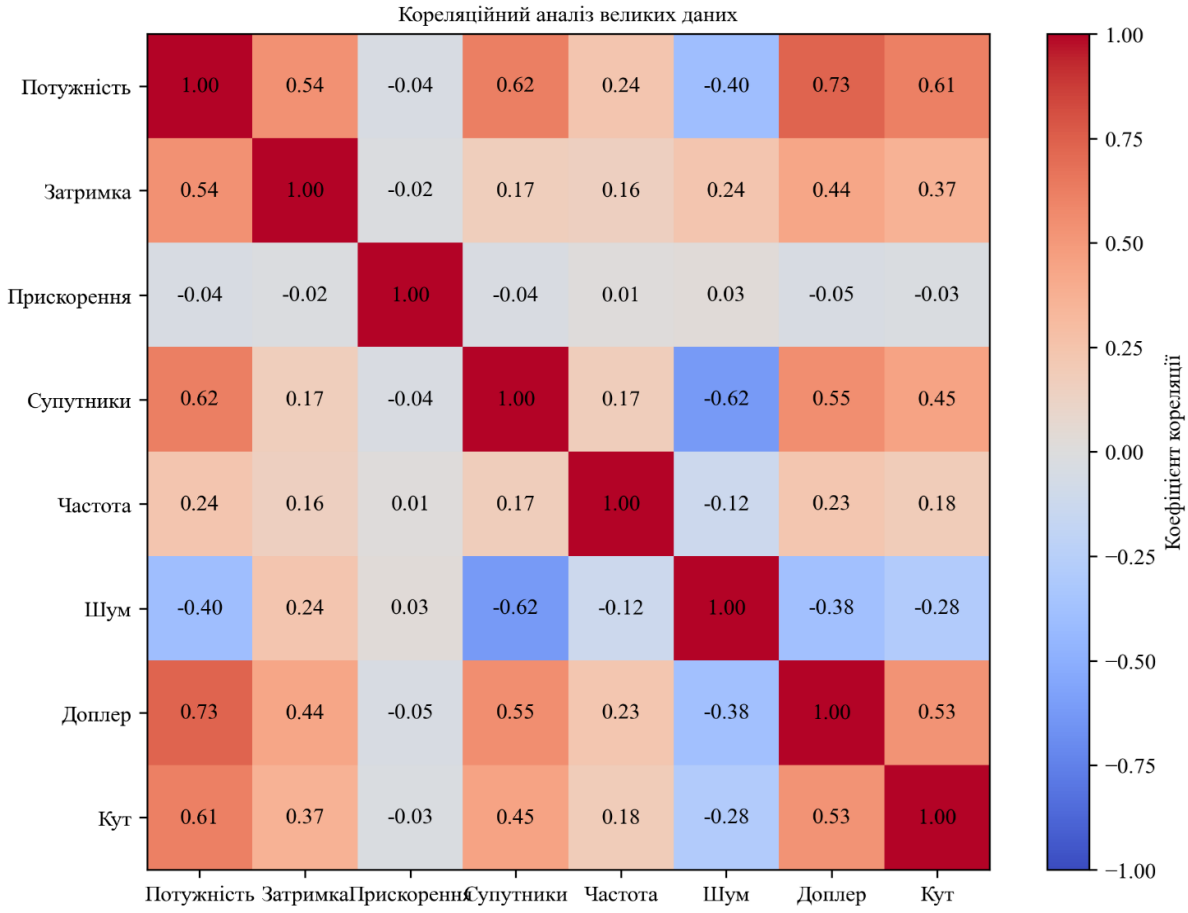

Рис. 10. Кореляційний аналіз великих даних
Джерело: авторська розробка

Методи кластеризації (K-Means, Fuzzy C-Means, Онлайн K-Means) і Random Forest показали прийнятні результати для виявлення аномалій, хоча точність RNN залишилася низькою (0.51). Це може бути пов'язано з обмеженою інформативністю синтетичних даних. Онлайн K-Means виявився найбільш адаптивним для умов реального часу, що є важливим для АСДК.

Унікальність підходу полягає в адаптивності та орієнтації на реальний час, що досягається завдяки

використанню Онлайн K-Means для поступового оновлення моделі кластеризації під час надходження нових даних. На відміну від традиційних методів, таких як статистичний аналіз або геометричні підходи, які часто потребують значних обчислювальних ресурсів і не завжди ефективні в динамічних умовах, запропонований метод дозволяє моделі "навчатися на ходу", що робить його придатним для АСДК, де дані надходять безперервно. Крім того, інтеграція пост-квантової криптографії для захисту даних GNSS додає додатковий рівень безпеки, враховуючи майбутні загрози, пов'язані з розвитком квантових обчислень.

Відмінність підходу також полягає у використанні синтетичних даних із розширеним набором ознак (потужність, затримка, прискорення, кількість супутників, частота, рівень шуму, доплерівське зміщення, кут приходу сигналу), що дозволяє моделювати різноманітні сценарії атак і підвищувати стійкість моделей до варіацій у реальних умовах. На відміну від існуючих рішень, які часто зосереджуються на одному методі (наприклад, лише класифікація або лише кластеризація), запропонований підхід поєднує сильні сторони різних алгоритмів, забезпечуючи комплексний захист: кластеризація виявляє аномалії, Random Forest фільтрує фальшиві сигнали, а RNN прогнозує атаки, що дає змогу системі не лише реагувати на поточні загрози, а й передбачати майбутні.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У роботі розроблено методи штучного інтелекту для виявлення та протидії кібератакам типу GPS spoofing і GPS jamming у системах диференційної корекції GNSS, зокрема в автономних СДК. Кластеризація (K-Means, Fuzzy C-Means) виявила 66.7% аномалій, а Онлайн K-Means показав кращий результат (204 аномалії з очікуваних 150). Random Forest ефективно використано для сигнатурного аналізу і фільтрації фальшивих сигналів. RNN на основі GRU досягла точності 0.51 на валідаційному наборі, що вказує на необхідність використання більш інформативних даних. Запропоновано методи протидії, включаючи адаптивну синхронізацію (корекція часу 0.14 мс) і інтеграцію з пост-квантовою криптографією. Кореляція між потужністю і затримкою склала 0.54, що може бути використано для створення додаткових ознак. Майбутні дослідження можуть включати використання реальних даних GNSS і гібридних моделей (наприклад, RNN із трансформерами) для підвищення точності прогнозування атак.

Література

1. Зоря, І. С., & Марущак, А. В. (2023). *Застосування штучного інтелекту для виявлення та реагування на кіберзагрози*. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3&isAllowed=y (дата звернення: 24.03.2025).

2. Сусукайло, В. А. (2024). *Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем* (Дисертація на здобуття ступеня доктора філософії, Національний університет «Львівська політехніка»). https://lpnu.ua/sites/default/files/2024/radaphd/27650/disertaciya-susukailo-va-1.pdf (дата звернення: 24.03.2025).

3. Петровський, А. В. (2019). Алгоритм виявлення впливу спуфінгу під час виконавчої прокладки програмними засобами електронної картографічної навігаційно-інформаційної системи. *Проблеми інформаційних технологій, 25*, 30–38. https://doi.org/10.35546/2313-0687.2019.25.30-38

4. Волошин, Д. Г., & Бульба, С. С. (2022). Інтелектуальний метод виявлення спуфінгу БПЛА. *Сучасні інформаційні системи, 6*(1), 88–96. https://doi.org/10.20998/2522-9052.2022.1.15

5. Мустафаєв, О. В. (2024). Сучасні технології захисту від GPS спуфінгу у системах навігації. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки, 35*(74), №5, 58–61. https://doi.org/10.32782/2663-5941/2024.5.1/10

6. Нетаврована, А. (2023). Геометричний метод визначення GPS spoof атак на безпілотні літальні апарати. У *Матеріали конференцій МЦНД (22.12.2023, Одеса, Україна)* (с. 316–321). https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/954 (дата звернення: 24.03.2025).

7. Radoš, K., Brkić, M., & Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. *Sensors, 24*(13), 4210. https://doi.org/10.3390/s24134210

8. Siavash, J., & Ping, W. (2024). Intelligent anti-jamming based on deep reinforcement learning and transfer learning. *IEEE Transactions on Vehicular Technology*, 1–10. https://doi.org/10.1109/TVT.2024.3359426

9. Alkhatib, M., McCormick, M., Williams, L., Leon, A., Camerano, L., Al, K., Devabhaktuni, V. K., Kaabouch, N., Svm, D., & Regularization, L. (2024). Classification and source location indication of jamming attacks targeting UAVs via multi-output multiclass machine learning modeling. У *2024 IEEE International Conference on Consumer Electronics (ICCE)* (с. 1–5). https://ieeexplore.ieee.org/document/10444388

10. Mohanty, A., & Gao, G. (2024). A survey of machine learning techniques for improving global navigation satellite systems. *EURASIP Journal on Advances in Signal Processing*, 1–40. https://asp-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13634-024-01167-7.pdf

References

1. Zoria, I. S., & Marushchak, A. V. (2023). Zastosuvannia shtuchnoho intelektu dlia vyiavlennia ta reahuvannia na kiberzahrozy. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3&isAllowed=y (data zvernennia: 24.03.2025).

2. Susukailo, V. A. (2024). Rozroblennia modeli systemy doslidzhennia kiberzlochyniv dlia skladovykh infrastruktury informatsiinykh system (Dysertatsiia na zdobuttia stupenia doktora filosofii, Natsionalnyi universytet «Lvivska politekhnika»). https://lpnu.ua/sites/default/files/2024/radaphd/27650/disertaciya-susukailo-va-1.pdf (data zvernennia: 24.03.2025).

3. Petrovskyi, A. V. (2019). Alhorytm vyiavlennia vplyvu spufinhu pid chas vykonavchoi prokladky prohramnymy zasobamy elektronnoi kartohrafichnoi navihatsiino-informatsiinoi systemy. Problemy informatsiinykh tekhnolohii, 25, 30–38. https://doi.org/10.35546/2313-0687.2019.25.30-38

4. Voloshyn, D. H., & Bulba, S. S. (2022). Intelektualnyi metod vyiavlennia spufinhu BPLA. Suchasni informatsiini systemy, 6(1), 88–96. https://doi.org/10.20998/2522-9052.2022.1.15

5. Mustafaiev, O. V. (2024). Suchasni tekhnolohii zakhystu vid GPS spufinhu u systemakh navihatsii. Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky, 35(74), №5, 58–61. https://doi.org/10.32782/2663-5941/2024.5.1/10

6. Netavrovana, A. (2023). Heometrychnyi metod vyznachennia GPS spoof atak na bezpilotni litalni aparaty. U Materialy konferentsii MTsND (22.12.2023, Odesa, Ukraina) (s. 316–321). https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/954 (data zvernennia: 24.03.2025).

7. Radoš, K., Brkić, M., & Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. Sensors, 24(13), 4210. https://doi.org/10.3390/s24134210

8. Siavash, J., & Ping, W. (2024). Intelligent anti-jamming based on deep reinforcement learning and transfer learning. IEEE Transactions on Vehicular Technology, 1–10. https://doi.org/10.1109/TVT.2024.3359426

9. Alkhatib, M., McCormick, M., Williams, L., Leon, A., Camerano, L., Al, K., Devabhaktuni, V. K., Kaabouch, N., Svm, D., & Regularization, L. (2024). Classification and source location indication of jamming attacks targeting UAVs via multi-output multiclass machine learning modeling. U 2024 IEEE International Conference on Consumer Electronics (ICCE) (s. 1–5). https://ieeexplore.ieee.org/document/10444388

10. Mohanty, A., & Gao, G. (2024). A survey of machine learning techniques for improving global navigation satellite systems. EURASIP Journal on Advances in Signal Processing, 1–40. https://asp-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13634-024-01167-7.pdf