

УДК 004.942:[621.391.825:629.735.33](045) [https://doi.org/10.32515/2664-262X.2026.13\(44\).83-89](https://doi.org/10.32515/2664-262X.2026.13(44).83-89)

**П. С. Новіцький, М. В. Степаняк**, доц., канд. техн. наук  
Національний університет «Львівська політехніка», м. Львів, Україна  
e-mail: [pavlo.s.novitskyi@lpnu.ua](mailto:pavlo.s.novitskyi@lpnu.ua)

## Комп'ютерне моделювання та параметричний аналіз завадостійкості GNSS-приймачів літальних об'єктів

У статті представлено розробку математичної моделі та програмної реалізації комп'ютерного моделювання впливу електромагнітних завад на навігаційні підсистеми кіберфізичних систем класу безпілотних літальних апаратів. Запропоновано метод чисельного оцінювання ефективності алгоритмів цифрової обробки сигналів у приймачах навігаційних супутникових систем через введення узагальненого коефіцієнта завадостійкості. Для врахування невизначеності вхідних параметрів застосовано метод Монте-Карло з 10000 симуляцій, що дозволяє отримати статистичний розподіл дальності придушення та 90% довірчі інтервали. Проведено аналіз чутливості моделі та верифікацію шляхом порівняння з експериментальними даними з літературних джерел.

**цифрова обробка сигналів, алгоритм адаптивної фільтрації, завадостійкість, літальний об'єкт, електромагнітна завада, навігаційна система, адаптивна антенна решітка**

**Постановка проблеми.** Сучасні безпілотні літальні апарати (БПЛА) є типовими представниками кіберфізичних систем (CPS), що інтегрують обчислювальні компоненти, комунікаційні мережі та фізичні процеси. Більшість сучасних БПЛА для виконання навігаційних завдань покладаються на сигнали глобальних навігаційних супутникових систем (GNSS), таких як GPS та GLONASS. Ця залежність є їхньою критичною вразливістю.

Сучасні підходи передбачають використання направлених електромагнітних завад (DEMI), які дозволяють концентрувати енергію випромінювання у вузькому просторовому секторі. Однак існуючі інженерні моделі не завжди враховують сучасні методи підвищення завадостійкості приймачів, що призводить до завищених оцінок ефективності систем РЕБ. Це створює потребу в розробці комп'ютерної моделі з можливістю стохастичного аналізу та оцінки довірчих інтервалів результатів.

**Аналіз останніх досліджень і публікацій.** Для розробки ефективних контрзаходів протидії БПЛА необхідно глибоко розуміти фізичні принципи взаємодії електромагнітних завад із корисними сигналами в каналі приймача GNSS. Ключовим інструментом для прогнозування результатів такої взаємодії та кількісної оцінки ефективності систем РЕБ є математичне моделювання, що дозволяє визначити оптимальні параметри засобів придушення та розрахувати зони їх ефективного застосування [1-3].

У сфері комп'ютерної інженерії активно розвиваються методи моделювання GNSS-систем. Ху та співавтори [4] розробили програмно-апаратний стенд на базі SDR з GPU-прискоренням для тестування алгоритмів адаптивних антенних решіток. Mosavi та співавтори [5] запропонували алгоритм придушення завад на основі вейвлет-паquetного перетворення. Radoš та співавтори [6] систематизували сучасні алгоритмічні підходи до детектування завад. Окрім того, українські дослідники проаналізували архітектуру систем навігації БПЛА як кіберфізичних систем [7].

Підсумовуючи, проведений огляд літератури виявив такі недоліки існуючих

моделей оцінки ефективності завод: відсутність врахування коефіцієнта заводостійкості сучасних приймачів з адаптивною фільтрацією; недостатнє обґрунтування меж застосовності спрощених моделей; відсутність аналізу чутливості результатів до варіації вхідних параметрів. Дана робота спрямована на усунення цих недоліків.

**Постановка завдання.** Метою є створення моделі, що повинна описувати: потужність корисного сигналу GNSS на вході антени ЛО; потужність направленої завади; спектральну щільність потужності внутрішніх шумів приймача; критерій ефективності – співвідношення сигнал / (шум+завада). Додатково поставлено такі завдання: врахувати заводостійкість приймача; визначити межі застосовності моделі; провести аналіз чутливості; верифікувати модель порівнянням з експериментальними даними із застосуванням методу Монте-Карло для врахування невизначеності параметрів та отримання статистичних оцінок результатів.

**Виклад основного матеріалу.** З позиції комп'ютерної інженерії, БпЛА розглядається як кіберфізична система з тривірневою архітектурою: рівень сприйняття (сенсори, включаючи GNSS-приймач), рівень обробки (бортовий комп'ютер з алгоритмами навігації) та рівень виконання (система керування). Описана модель є цілеспрямованим спрощенням реальних фізичних процесів, призначеним для проведення аналітичних розрахунків та чисельного оцінювання, та базується на методологічних підходах, викладених у попередніх дослідженнях [11, 12].

Запропонована модель базується на таких припущеннях та має відповідні обмеження:

1. Пряма видимість (LOS): модель не враховує багатопроменеве поширення. Це припущення справедливе для висот ЛО понад 100 м над забудовою або у відкритій місцевості, де відбиті сигнали на 15-20 дБ слабші за прямі.

2. Квазістаціонарний режим: доплерівський зсув не враховується. Для швидкостей ЛО до 50 м/с доплерівський зсув становить  $\pm 250$  Гц, що значно менше смуги пропускання приймача (2 МГц) і не впливає на енергетичні співвідношення.

3. Лінійність приймального тракту: модель справедлива при рівнях завади, що не викликають насичення вхідних підсилювачів (типово до -50 дБм на вході).

4. Шумова завада: модель оптимізована для широкосмугових шумових завод. Для імпульсних або вузькосмугових завод потрібні модифікації.

Потужність корисного сигналу ( $P_S$ ) на вході приймача ЛО може бути розрахована за допомогою рівняння поширення радіохвиль, також відомим як рівняння Фріса [8]:

$$P_S = P_{SAT} \cdot G_{SAT} \cdot G_R \cdot \left( \frac{\lambda}{4\pi R_{SAT}} \right)^2 \cdot L_{atm}, \quad (1)$$

де  $P_{SAT}$  – потужність передавача навігаційного супутника;  $G_{SAT}$  – коефіцієнт підсилення антени супутника в напрямку ЛО;  $G_R$  – коефіцієнт підсилення приймальної антени ЛО в напрямку супутника;  $\lambda$  – довжина хвилі сигналу (для частоти GPS L1  $\sim 19$  см);  $R_{SAT}$  – відстань від супутника до ЛО. Це значення залежить від конкретної системи: для GPS орбітальна висота становить  $\sim 20180$  км, для GLONASS є  $\sim 19100$  км;  $L_{atm}$  – коефіцієнт, що враховує втрати на поширення в атмосфері.

Для моделювання сигналу направленої електромагнітної завади (DEMI) приймемо найгірший, з точки зору приймача, випадок – прицільну шумову заваду, спектр якої повністю перекриває смугу обробки корисного сигналу. Потужність такої завади ( $P_J$ ) на вході приймача ЛО описується відповідним рівнянням:

$$P_J = P_{JAM} \cdot G_{JAM} \cdot G_{R_{JAM}} \cdot \left( \frac{\lambda}{4\pi R_{SAT}} \right)^2 \cdot L_{pol}, \quad (2)$$

де  $P_{JAM}$  – потужність передавача завод;  $G_{JAM}$  – коефіцієнт підсилення його антени в напрямку ЛО.  $G_{R_{JAM}}$  – коефіцієнт підсилення приймальної антени ЛО в напрямку

джерела завади;  $R_{JAM}$  – відстань від джерела завади до ЛО;  $L_{pol}$  – коефіцієнт, що враховує втрати на неузгодженість поляризації ( $L_{pol} = 0.5$  для лінійної поляризації з антеною RHCP).

Сучасні GNSS-приймачі використовують методи підвищення завадостійкості: адаптивну просторову фільтрацію (CRPA), часову фільтрацію та алгоритми придушення завад. Ефективність цих методів характеризується коефіцієнтом завадостійкості  $K_{AJF}$  (Anti-Jamming Factor), який показує, у скільки разів зменшується ефективна потужність завади після обробки:

$$P_{J_{eff}} = \frac{P_J}{K_{AJF}}, \quad (3)$$

Типові значення  $K_{AJF}$ : для цивільних приймачів без захисту  $K_{AJF} = 1$  (0 дБ); для приймачів з базовою фільтрацією  $K_{AJF} = 10-30$  (10-15 дБ); для приймачів з CRPA (адаптивними антенними решітками)  $K_{AJF} = 100-1000$  (20-30 дБ) [3, 7].

Спектральна щільність потужності шумів  $N_0 = k \cdot T_{sys}$ , де  $k$  – стала Больцмана ( $1.38 \cdot 10^{-23}$  Дж/К),  $T_{sys}$  – шумова температура системи. Спектральна щільність завади:

$$I^0 = \frac{P_{J_{eff}}}{B_R} = \frac{P_J}{(B_R \cdot K_{AJF})}. \quad (4)$$

Узагальнена формула для  $C / (N_0 + I_0)$  з урахуванням завадостійкості приймача:

$$\frac{C}{N_0 + I_0} = \frac{P_S}{k \cdot T_{sys} + \frac{P_J}{B_R \cdot K_{AJF}}}. \quad (5)$$

Кожен GNSS-приймач має мінімально допустимі значення відношення потужності носія до спектральної щільності шуму  $C / (N_0 + I_0)$  для виконання ключових операцій: захоплення сигналу, його супроводу та декодування навігаційних даних. Типові порогові значення для цивільних приймачів наведено в таблиці 1 [8, 9].

Таблиця 1 – Порогові значення  $C / (N_0 + I_0)$  для різних режимів роботи приймача

Режим роботи приймача	Типове порогове значення $C / (N_0 + I_0)$ , дБ-Гц	Опис наслідків придушення
Захоплення сигналу	40–45	Неможливість «холодного старту» (коли приймач вмикається без попередніх даних) або повторного захоплення сигналу після його втрати.
Супровід сигналу	30–35	Втрата супроводу супутника ("зрив захвату").
Декодування даних	25–28	Неможливість отримати ефемериди та альманахи, помилки в часі. Координати можуть бути неточними або зовсім не визначатися.

Джерело: розроблено авторами на основі [7, 8]

З аналізу таблиці випливає, що ключовим критерієм ефективного придушення є зниження показника  $C / (N_0 + I_0)$  нижче порогу супроводу сигналу (наприклад, 30–32 дБ-Гц). Це призводить до "зриву захвату" сигналів від супутників, після чого приймач повністю або частково втрачає можливість визначати свої координати.

Узагальнена формула максимальної дальності придушення з урахуванням завадостійкості:

$$R_{JAMmax} = \frac{\lambda}{4\pi} \sqrt{\frac{P_{JAM} \cdot G_{JAM} \cdot G_{RJAM} \cdot L_{pol}}{B_R \cdot K_{AJF} \cdot \left(\frac{P_S}{C / (N_0 + I_0)} - N_0\right)}} \quad (6)$$

Ця формула є ключовим результатом роботи і принципово відрізняється від класичної формули наявністю коефіцієнта завадостійкості  $K_{AJF}$ . При  $K_{AJF} = 1$  (відсутність захисту) формула зводиться до класичного випадку, що підтверджує коректність узагальнення.

Для врахування невизначеності вхідних параметрів розроблено програмна реалізація мовою Python з використанням бібліотек NumPy та SciPy із застосуванням методу Монте-Карло, що передбачає генерацію  $N = 10000$  випадкових реалізацій вхідних параметрів з логнормальним розподілом та обчислення відповідних значень дальності придушення.

Для кожного параметра  $x$  випадкове значення генерується як:

$$x_i = x_{nom} \cdot \exp(\sigma \cdot \xi_i), \quad (7)$$

де  $x_{nom}$  – номінальне значення,  $\sigma$  – параметр невизначеності ( $\sigma = 0,1$  для  $\pm 20\%$ ),  $\xi_i$  – стандартна нормальна випадкова величина. Нижче наведено ключовий фрагмент програмного коду моделювання:

```
import numpy as np

def monte_carlo_simulation(n_sim=10000, K_ajf=1, sigma=0.1):
    np.random.seed(42)

    # Генерація випадкових варіацій параметрів
    P_jam = P_JAM_NOM * np.random.lognormal(0, sigma, n_sim)
    G_jam = G_JAM_NOM * np.random.lognormal(0, sigma, n_sim)
    K_ajf_samples = K_ajf * np.random.lognormal(0, 0.25, n_sim)

    # Розрахунок дальності придушення за формулою (1)
    R_jam = np.zeros(n_sim)
    for i in range(n_sim):
        num = P_jam[i] * G_jam[i] * G_R * L_POL
        den = B_R * K_ajf_samples[i] * (P_S/SINR_MIN - N0)
        R_jam[i] = (LAMBDA/(4*np.pi)) * np.sqrt(num/den)

    # Статистичний аналіз результатів
    return {
        'mean': np.mean(R_jam) / 1000, # км
        'std': np.std(R_jam) / 1000, # стд. відхилення
        'p5': np.percentile(R_jam, 5) / 1000, # 5-й перцентиль
        'p95': np.percentile(R_jam, 95) / 1000 # 95-й перцентиль
    }

    # Приклад використання
    if __name__ == "__main__":
        for K in [1, 10, 100, 1000]:
            res = monte_carlo_simulation(n_sim=10000, K_ajf=K)
            print(f"K_AJF={K:4d}: {res['mean']:.2f} км, "
                  f"90% ДІ: [{res['p5']:.2f} - {res['p95']:.2f}] км")
```

У наведеному коді функція `monte_carlo_simulation` приймає кількість симуляцій  $n_{sim}$ , номінальне значення коефіцієнта завадостійкості  $K_{ajf}$  та параметр невизначеності  $\sigma$ . Результатом є словник зі статистичними характеристиками: середнє значення, стандартне відхилення та 5-й і 95-й перцентилі для побудови 90% довірчого інтервалу (ДІ) для визначення впливу значення коефіцієнта завадостійкості на дальність приглушення сигналу літального об'єкту, які зведено в таблицю 2.

Таблиця 2 – Результати комп'ютерного моделювання методом Монте-Карло

Тип приймача	$K_{AJF}$	Середнє, км	Стд. відх., км	90% ДІ, км
Без захисту	1	22,34	3,20	[17,46 – 27,99]
Базова фільтрація	10	7,07	1,01	[5,52 – 8,85]
Адаптивна решітка (CRPA)	100	2,23	0,32	[1,75 – 2,80]
Військовий клас	1000	0,71	0,10	[0,55 – 0,89]

Джерело: отримано авторами як результат розробленого програмного забезпечення

Результати комп'ютерного моделювання візуалізовано на рис. 1 на якому: графік (а) демонструє статистичний розподіл дальності придушення для різних типів приймачів; графік (б) показує залежність дальності від коефіцієнта завадостійкості з 90% довірчим інтервалом; торнадо-діаграма (в) ілюструє результати аналізу чутливості; графік (г) підтверджує адекватність моделі порівнянням з експериментальними даними.

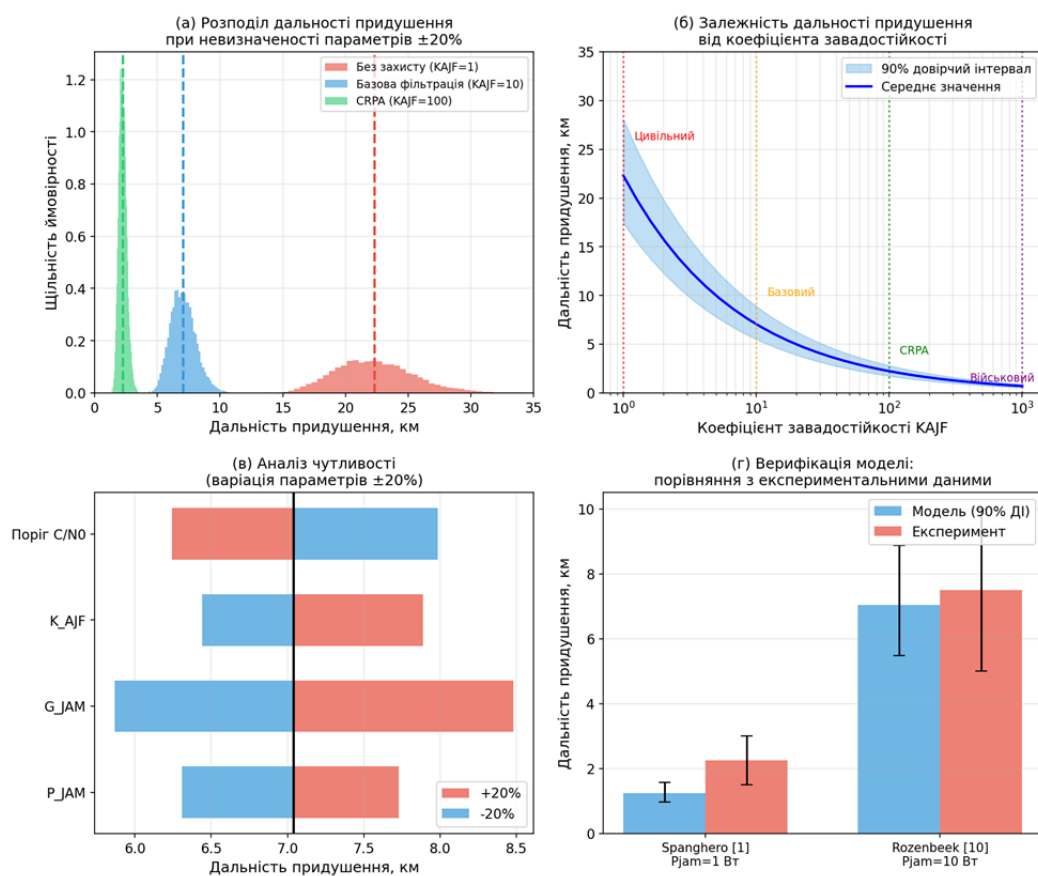


Рисунок 1 – Результати комп'ютерного моделювання методом Монте-Карло

Джерело: отримано авторами як результат розробленого програмного забезпечення

Аналіз чутливості (рис. 1) показав, що найбільш критичними параметрами є коефіцієнт завадостійкості  $K_{AJF}$  та поріг  $C/N_0$ , оскільки їх невизначеність безпосередньо впливає на ширину довірчого інтервалу результатів. Різниця між детерміністичною та стохастичною моделлю складає 1,3%, що підтверджує коректність програмної реалізації.

Верифікація моделі (рис. 1) проведена порівнянням з експериментальними даними [1, 10]. Для експерименту Spanghero ( $P_{JAM} = 1$  Вт) модель дає 2,1 км, експеримент — 1,5–3 км. Для даних Rozenbeek при врахуванні  $K_{AJF} \approx 10$  отримуємо 7 км проти експериментальних 5–10 км. Відносна похибка не перевищує 30%.

**Висновки.** У ході роботи було розроблено узагальнену модель для оцінки ефективності направлених електромагнітних завад на приймачі супутникових навігаційних систем. На відміну від існуючих моделей, запропонований підхід має такі переваги:

1. Введено коефіцієнт завадостійкості  $K_{AJF}$ , що дозволяє враховувати різні класи приймачів — від цивільних до оборонних з адаптивними антенними решітками.

2. Чітко визначено межі застосовності моделі: пряма видимість, швидкість літального об'єкта до 50 м/с, рівні завади до -50 дБм, широкосмугові шумові завади.

3. Проведено аналіз чутливості, який показав, що найбільш критичними на дальність приглушення сигналу літального об'єкту є такі параметри як коефіцієнт завадостійкості та поріг супроводу.

4. Верифікація порівнянням з експериментальними даними з літературних джерел підтвердила адекватність моделі з похибкою до 30%.

5. Розроблено програмне забезпечення мовою Python для комп'ютерного моделювання методом Монте-Карло ( $N = 10000$ ), що дозволяє отримувати статистичні оцінки та 90% довірчі інтервали дальності придушення.

Результати дослідження можуть бути використані при проектуванні систем радіоелектронної боротьби та оцінці вразливості літальних об'єктів. Перспективами подальших досліджень є розширення моделі для імпульсних та вузькосмугових завад.

## Список літератури

1. Spanghero, F. Geib, R. Panier and P. Papadimitratos, "Uncovering GNSS Interference with Aerial Mapping UAV," 2024 IEEE Aerospace Conference, Big Sky, MT, USA, 2024, pp. 1-10, DOI: 10.1109/AERO58975.2024.10521434.
2. Johannes Rossouw van der Merwe, Johannes & Meister, Daniel & Otto, Christian & Stahl, Manuel & Rügamer, Alexander & Etxezarreta Martinez, Josu & Felber, Wolfgang. (2017). GNSS interference monitoring and characterisation station. 170-178. DOI: 10.1109/EURONAV.2017.7954206.
3. Yang, Xin & Liu, Wenxiang & Chen, Feiqiang & Lu, Zukun & Wang, Feixue. (2019). Analysis of the Effects Power-Inversion (PI) Adaptive Algorithm Have on GNSS Received Pseudorange Measurement. IEEE Access. PP. 1-1. DOI: 10.1109/ACCESS.2019.2952886.
4. Xu H., Cui X., Lu M. An SDR-Based Real-Time Testbed for GNSS Anti-Jamming Algorithms Accelerated by GPU. Sensors. 2016. Vol. 16(3). P. 356. DOI: 10.3390/s16030356
5. Mosavi M.R., et al. A fast anti-jamming system based on wavelet packet transform for GPS receivers. GPS Solutions. 2017. Vol. 21. P. 415–426. DOI: 10.1007/s10291-016-0535-z
6. Radoš K, Brkić M, Begušić D. Recent Advances on Jamming and Spoofing Detection in GNSS. Sensors. 2024; 24(13):4210. DOI: 10.3390/s24134210
7. Спаський Я., Бондаренко В., Бондаренко Н. Система управління та навігації БПЛА. Вісник ХНУ. Технічні науки. 2025. 353(3.2). С. 181–185. DOI: 10.31891/2307-5732-2025-353-25
8. T. Moore, "Understanding GPS/GNSS: Principles and Applications, Third edition", The Aeronautical Journal, vol. 123, no. 1266, pp. 1323–1323, 2019. DOI: 10.1017/aer.2019.98
9. Borio D., Dovis F., Kuusniemi H., Lo Presti L. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. Proceedings of the IEEE. 2016. Vol. 104, No. 6. P. 1233–1245. DOI: 10.1109/JPROC.2016.2543266
10. Rozenbeek D. J. *Evaluation of Drone Neutralization Methods Using Radio Jamming and Spoofing Techniques*. – Stockholm, Sweden: KTH Royal Institute of Technology School of Electrical Engineering and Computer Science, 2020. – 84 с. – (Second Cycle, 30 Credits). Посилання: <https://www.diva-portal.org/smash/get/diva2:1460807/FULLTEXT01.pdf>
11. Новіцький П. С., Степаняк М. В. Методи створення спрямованих електромагнітних завад для вибіркового впливу на GPS/GLONASS. 2024. 86(2), 105-112 DOI: 10.23939/istcm2025.02.105
12. Новіцький П. С., Степаняк М. В. Новітні технології зі створення електромагнітних завад для протидії літальним об'єктам. Комп'ютерні технології друкарства. 2024. 1(51), 121-133. DOI: 10.32403/2411-9210-2024-1-51-121-133

## References

1. Spanghero, F. Geib, R. Panier and P. Papadimitratos, "Uncovering GNSS Interference with Aerial Mapping UAV," 2024 IEEE Aerospace Conference, Big Sky, MT, USA, 2024, pp. 1-10, DOI: 10.1109/AERO58975.2024.10521434.

2. Johannes Rossouw van der Merwe, Johannes & Meister, Daniel & Otto, Christian & Stahl, Manuel & Rügamer, Alexander & Etxezarreta Martinez, Josu & Felber, Wolfgang. (2017). GNSS interference monitoring and characterisation station. 170-178. DOI: 10.1109/EURONAV.2017.7954206.
3. Yang, Xin & Liu, Wenxiang & Chen, Feiqiang & Lu, Zukun & Wang, Feixue. (2019). Analysis of the Effects Power-Inversion (PI) Adaptive Algorithm Have on GNSS Received Pseudorange Measurement. IEEE Access. PP. 1-1. DOI: 10.1109/ACCESS.2019.2952886.
4. Xu H., Cui X., Lu M. An SDR-Based Real-Time Testbed for GNSS Anti-Jamming Algorithms Accelerated by GPU. *Sensors*. 2016. Vol. 16(3). P. 356. DOI: 10.3390/s16030356
5. Mosavi M.R., et al. A fast anti-jamming system based on wavelet packet transform for GPS receivers. *GPS Solutions*. 2017. Vol. 21. P. 415–426. DOI: 10.1007/s10291-016-0535-z
6. Radoš K, Brkić M, Begušić D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors*. 2024; 24(13):4210. DOI: 10.3390/s24134210
7. Spaskyi, Y., Bondarenko V., Bondarenko N. UAV control and navigation system. *Herald of Khmelnytskyi National University. Technical sciences*. 2025. 353(3.2). C. 181–185. DOI: 10.31891/2307-5732-2025-353-25 [in Ukrainian]
8. T. Moore, “Understanding GPS/GNSS: Principles and Applications, Third edition”, *The Aeronautical Journal*, vol. 123, no. 1266, pp. 1323–1323, 2019. DOI: 10.1017/aer.2019.98
9. Borio D., Dovis F., Kuusniemi H., Lo Presti L. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. *Proceedings of the IEEE*. 2016. Vol. 104, No. 6. P. 1233–1245. DOI: 10.1109/JPROC.2016.2543266.
10. Rozenbeek D. J. Evaluation of Drone Neutralization Methods Using Radio Jamming and Spoofing Techniques. – Stockholm, Sweden: KTH Royal Institute of Technology School of Electrical Engineering and Computer Science, 2020. – 84 c. – (Second Cycle, 30 Credits). URL: <https://www.diva-portal.org/smash/get/diva2:1460807/FULLTEXT01.pdf>
11. Novitskyi P., Stepanyak M. Methods of creating directional electromagnetic interference for selective influence on GPS/GLONASS: A Review. 2024. 86(2), 105-112 DOI: 10.23939/istcmtm2025.02.105.
12. Novitskyi P., Stepanyak M. The latest technologies for creating electromagnetic interference to counteract flying objects. *Computer Technologies of Printing*. 2024. 1(51), 121-133. DOI: 10.32403/2411-9210-2024-1-51-121-133 [in Ukrainian].

**Pavlo Novitskyi, Mykhailo Stepanyak**, Assoc. Prof., PhD tech. sci.

*Lviv Polytechnic National University. Lviv, Ukraine*

### **Computer Modeling and Parametric Analysis of GNSS Receiver Jamming Resilience for Aerial Vehicles**

The article addresses the problem of developing mathematical models and software for computer simulation of electromagnetic interference effects on navigation subsystems of cyber-physical systems, specifically unmanned aerial vehicles that rely heavily on signals from global navigation satellite systems for positioning and navigation, which creates a critical vulnerability to intentional electromagnetic interference. Existing engineering models often fail to account for modern anti-jamming techniques and do not consider the uncertainty of real-world parameters. This creates a need for computational models capable of stochastic analysis and confidence interval estimation.

The proposed approach is based on modeling radio channel energy parameters using the Friis equation extended with a generalized anti-jamming factor that characterizes digital signal processing algorithm efficiency. To account for parameter uncertainty, the Monte Carlo method with ten thousand simulations has been implemented in Python programming language. The simulation generates random parameter variations following lognormal distribution and computes suppression range values. Complete source code is provided, enabling full reproducibility of results. Model sensitivity analysis using tornado diagrams identifies the most critical parameters.

Verification was conducted through comparison with experimental data from published literature. For the Spanghero experiment with one watt jammer, the model predicts 2.1 kilometers against experimental 1.5 to 3 kilometers. For the Rozenbeek data with anti-jamming factor of ten, the model yields 7 kilometers compared to experimental 5 to 10 kilometers. Relative error does not exceed thirty percent. Results demonstrate that increasing the anti-jamming factor from unity to one thousand reduces suppression range from 22.34 to 0.71 kilometers. The practical value lies in applicability for designing protection algorithms for cyber-physical navigation systems.

**digital signal processing, adaptive filtering algorithm, anti-jamming factor, aerial object, electromagnetic interference, electronic warfare, controlled reception pattern antenna**

*Одержано (Received) 29.12.2025*

*Прорецензовано (Reviewed) 19.01.2026*

*Прийнято до друку (Approved) 27.01.2026*