УДК 621.391

О. М. Барсуков, В. П. Зинченко

УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ СУПУТНИКОВИХ СПУФІНГ-СИГНАЛІВ НА ОСНОВІ ЕФЕКТУ ДОПЛЕРА

Анотація. *Доповідь присвячена дослідженню методів виявлення супутникових спуфінг-сигналів у навігаційних системах безпілотних літальних апаратів (БпЛА). Проаналізовані основні варіанти формування спуфінг-сигналів, а також існуючи методи їх виявлення. Запропоновано удосконалення методу виявлення супутникових спуфінг-сигналів, з використанням доплерівської частоти зсуву.*

Ключові слова: *супутниковий сигнал, спуфінг-сигнал, виявлення, доплерівський ефект, радіоперешкода.*

Abstract. *The report is devoted to the study of methods for detecting satellite spoofing signals in the navigation systems of unmanned aerial vehicles (UAVs). The basic principles of spoofing signal generation are analyzed, as well as existing methods for spoofing signal detection. An improvement to the method of detecting satellite spoofing signals using the Doppler frequency shift is proposed.*

Keywords: *satellite signal, spoofing signal, detection, Doppler effect, radio interference.*

Вступ. Досвід сучасних збройних конфліктів [1-4] продемонстрував ключову роль застосування безпілотних літальних апаратів (БпЛА) під час виконання бойових завдань. Водночас дослідження свідчать, що ефективність застосування ударних БпЛА досягає лише 20-30% [1], а кількість їхніх втрат фіксується приблизно до 10 000 одиниць щомісяця.

Безумовно, що використання засобів та комплексів радіоелектронної боротьби (РЕБ) противника є однією з причин низької ефективності застосування БпЛА [1], яка обґрунтована недостатньою завадозахищеністю радіоканалів передачі навігаційних даних та є актуальною на сьогоднішній день.

Доповідь присвячена дослідженню методів виявлення радіоперешкод у бортових радіонавігаційних системах. Перший вид радіоперешкод (jamming, “джемінг”) [5] – це навмисно сформовані спеціальними радіоелектронними засобами електромагнітні випромінювання, які призначені для ускладнення прийому та (або) подавлення корисних радіосигналів. Другий вид – (spoofing, “спуфінг”) [2, 5-6] – це навмисно сформовані спеціальними радіоелектронними засобами електромагнітні випромінювання, які призначені для підміни радіосигналів з метою передачі хибної інформації.

Існує кілька варіантів формування супутникових спуфінг-сигналів. Розглянемо основні з них [2, 6-7]: спуфінг-сигнали на основі ретрансляції (Replay Spoofing Attack – RSA, “ретрансляційна спуфінгова атака”); спуфінг-сигнали на основі імітації (Forgery Spoofing Attack – FSA, “спуфінгова атака з підміною”); параметричні спуфінг-сигнали (Estimation Spoofing Attack – ESA “спуфінгова атака фальсифікації параметрів”) ; удосконалені спуфінг-сигнали – (Advanced Spoofing Attack – ASA, “удосконалена спуфінгова атака”).

Основний матеріал. Виходячи з варіантів формування спуфінг-сигналів існують методи їх виявлення.

1. Spoofing detection methods based on signal parameter statistics analysis (методи виявлення спуфінг-сигналу на основі статистичного аналізу параметрів сигналу). Наприклад, метод, з використанням, критерію Неймана-Пірсона, особливість якого полягає, як правило, у виборі порогу прийняття рішення. Однак, подібні методи виявлення потребують додаткових досліджень, стосовно використання у навігаційних системах БпЛА.

2. Spoofing detection methods based on arrival time and arrival time difference [7] (методи виявлення на основі оцінці часової різниці між прийнятими сигналами), наприклад, метод TDOA (Time Difference of Arrival). Основа методу TDOA полягає в оцінці характеристик супутникових сигналів, виходячи з того, що вони відповідають нормальному (гаусівському) розподілу, з урахуванням чого запропоновано статистичний метод перевірки гіпотез для виявлення спуфінг-

сигналів. В умовах дії спуфінг-сигналів в статистичному тесті використовуються критерій χ^2-статистики, тоді як за відсутності спуфінг-сигналів гаусівський розподіл не зберігається. Разом з цим, результати дослідження свідчать про залежність подібних методів від швидкості приймача.

3. Spoofing detection method based on antenna array (метод виявлення спуфінг-сигналів на основі антенних решіток для розрізнення супутникових та спуфінгових сигналів. Основний принцип полягає в тому, що спуфінгові сигнали від одного передавача передаються до всіх елементів антенної решітки з однакового напрямку, тоді як сигнали різних супутників мають різні кути прийому [4]. Недолік методу полягає у необхідності додаткового апаратного забезпечення, пов'язаного з калібруванням і удосконаленням приймача, що підвищує вартість та вагу обладнання.

4. Метод виявлення спуфінг-сигналу на основі нев'язки (residual signal detection – RSD). Метод ґрунтується на аналізі різниці (похибок) оцінок параметрів між супутниковим та спуфінговим сигналами [7], виходячи з того, що супутниковий сигнал не повністю спотворюється спуфінг-сигналом. Слід зазначити, що недоліками цього методу, є потреба у збільшенні часу на обробку даних, складність реалізації алгоритму, а також деградації характеристик GNSS приймача, які можуть впливати на порогові значення (перевірку гіпотез) внаслідок зростання похибок.

5. Spoofing detection methods based on Doppler shift (методи виявлення спуфінг-сигналу на основі допплерівського зсуву частоти). Нижче за текстом розглядаються метод виявлення спуфінг-сигналу [2, 8]. Розглянемо алгоритм вимірювання допплерівської $f_{\mathrm{D}}^{(s)}$ зсуву частоти супутникового сигналу, яка визначається за формулою (1) [8]:

$$f_{\mathrm{D}}^{(s)} = \frac{(\mathrm{v} - \mathrm{v}^{(s)}) \cdot \iota^{(s)}}{\lambda} = \frac{f}{c}(\mathrm{v} - \mathrm{v}^{(s)}) \cdot \iota^{(s)}, \quad (1)$$

де: f – несуча частота і λ – довжина хвилі несучої частоти f та c – швидкість світла; $\mathrm{v} = [\mathrm{v}_x, \mathrm{v}_y, \mathrm{v}_z]^{\mathrm{T}}$ – вектор швидкості приймача на БпЛА; $\mathrm{v}^{(s)} = [\mathrm{v}_x^{(s)}, \mathrm{v}_y^{(s)}, \mathrm{v}_z^{(s)}]^{\mathrm{T}}$ – вектор швидкості супутника яка обчислена, з використанням його ефемерид; $\iota^{(s)} = [\iota_x^{(s)}, \iota_y^{(s)}, \iota_z^{(s)}]^{\mathrm{T}}$ – одиничний вектор, спрямований вздовж лінії прямої видимості від БпЛА до супутника.

Спираючись на те, що доплерівський ефект [8] супутникового сигналу спостерігається як на несучої так і у псевдовипадковій кодовій послідовності (ПвКП) частотах, то у такому разі отримаємо вираз співвідношення [8]:

$$\frac{f_{Дн}}{f_{ДПвКП}} = \frac{f_н}{f_{ПвКП}}, \quad (2)$$

де $f_{Дн}$ – доплерівська частота зсуву несучої частоти, $f_{ДПвКП}$ – доплерівська частота зсуву ПвКП, $f_н$ – несуча частота, $f_{ПвКП}$ – ПвКП частота. Отже, для супутникового сигналу співвідношення $f_н/f_{ПвКП}$ = 1575,42·10^6 (Гц)/1,023·10^6 (Гц) = 1540 раз, розуміють як постійній коефіцієнт, у разі впливу спуфінг-сигналу він змінюється. В процесі моделювання було визначено поріг прийняття рішення про наявність спуфінг-сигналу на вході супутникового приймача, який складатиме 2% (±30,8), опираючись на те, що при відхиленні значення у співвідношенні (2) біля 1% у приймальному тракті супутниковий сигнал ідентифікується як похибка вимірювання.

Висновки. Таким чином, у результаті запропонованого вдосконалення методу виявлення спуфінг-сигналу на основі аналізу доплерівського зсуву частоти було визначено поріг прийняття рішення, який дозволяє навігаційній системі розрізняти вплив спуфінг-сигналу та похибки в обчисленнях як наслідок дії ненавмисних шумів.

Список використаних джерел:

1. Таршин В. А., Дрозд К. А. Комплексування мультимодальної інформації на основі фільтрів Калмана для навігації та побудови маршрутів ударних безпілотних літальних апаратів. *Наука і техніка Повітряних Сил Збройних Сил України.* 2026. № 1(62). С. 37-49. https://doi.org/10.30748/nitps.2026.62.10.

2. Chen Y., Jiang Y., Wen C., Liu Y., Wang L., He X., Jiang Y., Peng X., Liu X., Yang R.,

Yi J. GNSS spoofing detection via self-consistent verification of receiver's clock state. *Sensors.* 2026. Vol. 26. Article 397. P. 1-22. https://doi.org/10.3390/s26020397.

3. Барсуков О.М., Бойко М.М., Шевчук О.Ю., Лукашенко Т.С. Метод підвищення скритності сигналу в каналі передачі даних безпілотного літального апарату. *Збірник наукових праць Державного науково-дослідного інституту авіації.* 2023. № 16(26). С. 49-53. https://doi.org/10.54858/dndia.2023-19-6.

4. Barsukov O., Zynchenko V. Analysis of the impact of enemy radio interference on radionavigation signals and control channels of second- and third-class UAVs. *Новітні технології – для захисту повітряного простору:* зб. тез доп. XXII міжнар. наук. конф. Харківського національного університету Повітряних Сил ім. І. Кожедуба. Харків: ХНУПС ім. І. Кожедуба, 2026. С. 205-206.

5. Настанова виконання заходів радіо-, радіотехнічного контролю окремим спеціальним центром радіоелектронної боротьби (окремим вузлом радіоелектронної боротьби) у ході застосування військ (сил). ВКДП 10-27(56).01. Київ: Управління радіоелектронної боротьби Командування Сил підтримки Збройних Сил України, 2020. 83 с.

6. Humphreys T. E., Ledvina B. M., Psiaki M. L., O'Hanlon B. W., Kintner P. M., Jr. 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): conference paper. Savannah, GA : Institute of Navigation, 2008. P. 2314-2325.

7. Wu Z., Zhang Y., Yang Y., Liang C., Liu R. Spoofing and anti-spoofing technologies of global navigation satellite system: A Survey. *IEEE Access.* 2020 Vol. 8. P. 165444-165496. https://doi.org/10.1109/ACCESS.2020.3022294.

8. Tao H., Wu H., Li H. and Lu M. GNSS spoofing detection based on consistency check of velocities. *Chinese Journal of Electronics*. 2019. Vol. 28, No. 2. P. 437-444. https://doi.org/10.1049/cje.2019.01.006.

Барсуков Олександр Миколайович *– кандидат технічних наук, доцент, начальник кафедри радіоелектронного обладнання літальних апаратів, Харківський національний університет Повітряних Сил ім. Івана Кожедуба, м. Харків, e-mail: bars07@meta.ua. ORCID https://orcid.org/0000-0002-9129-2285.*

Зинченко Володимиир Павлович *– магістр, ад'юнкт кафедри радіоелектронного обладнання літальних апаратів, Харківський національний університет Повітряних Сил ім. Івана Кожедуба, м. Харків, e-mail: zynchenkovolodymyr@gmail.com. ORCID https://orcid.org/0009-0004-6040-7600.*

Barsukov Oleksandr Mykolayovych *– Candidate of Technical Sciences, Associate Professor, Head of the Department of Radioelectronic Aircraft Equipment, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, e-mail: bars07@meta.ua. ORCID https://orcid.org/0000-0002-9129-2285.*

Zynchenko Volodymyr Pavlovych *– Master, Postgraduate Student (Adjunct) at the Department of Radioelectronic Aircraft Equipment, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, e-mail: zynchenkovolodymyr@gmail.com. ORCID https://orcid.org/0009-0004-6040-7600.*