УДК 623.61:621.396

В. О. Тимошенко

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ТАКТИЧНОГО РАДІОЗВ'ЯЗКУ В УМОВАХ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Анотація. *Проаналізовано загрози тактичному радіозв'язку з боку засобів радіоелектронної боротьби противника та порівняно основні методи забезпечення його стійкості за принципом дії, ефективністю та обмеженнями. Показано, що жоден із методів окремо не забезпечує стійкості, та обґрунтовано напрями її комплексного підвищення.*

Ключові слова: *тактичний радіозв'язок, радіоелектронна боротьба, завадостійкість, ППРЧ, розширення спектра, MANET, радіомаскування, пеленгування.*

Abstract. *The threats posed by enemy electronic warfare to tactical radio communications are analysed, and the main methods of ensuring their resilience are compared by operating principle, effectiveness and limitations. It is shown that no single method ensures resilience on its own, and directions for its comprehensive improvement are substantiated.*

Keywords*: tactical radio communications, electronic warfare, jamming resistance, frequency hopping, spread spectrum, MANET, emission control, direction finding.*

Вступ

Стійкість тактичного радіозв'язку безпосередньо визначає здатність підрозділів до управління в бою. У російсько-українській війні радіоелектронна боротьба (РЕБ) набула масового характеру: за оцінкою RUSI, у 2023 р. противник мав щонайменше один потужний комплекс РЕБ на кожні 10 км фронту, а його засоби забезпечували перехоплення в реальному часі навіть шифрованого тактичного радіообміну [1].

Російська доктрина розглядає РЕБ як ланку циклу «виявлення – ураження»: засоби радіоелектронної розвідки виявляють джерела випромінювання для їх подальшого придушення або знищення [2]. Досвід війни підтверджує дієвість такого підходу: українські підрозділи використовували перехоплення, придушення та пеленгування незахищених російських радіомереж для наведення засобів ураження [3]. Тактична радіоелектронна розвідка забезпечує до 90 % первинної розвідувальної інформації, а сучасні переносні пеленгатори мають похибку менше 0,5° [4]. Отже, радіостанція в ефірі стає не лише об'єктом придушення, а й ціллю для вогневого ураження.

Класичні методи підвищення завадостійкості — псевдовипадкова перебудова робочої частоти (ППРЧ) і розширення спектра — добре досліджені [5, 6], однак в умовах щільного РЕБ і пеленгування жоден із них окремо не забезпечує стійкості зв'язку, що зумовлює актуальність комплексного підходу.

Мета роботи — на основі аналізу досвіду війни та наукових джерел оцінити ефективність основних методів забезпечення стійкості тактичного радіозв'язку в умовах РЕБ і обґрунтувати напрями її підвищення.

Методи дослідження: аналітичний огляд відкритих аналітичних звітів і наукових публікацій 2011–2025 рр.; порівняльний аналіз методів захисту радіозв'язку за принципом дії, ефективністю та обмеженнями.

Результати дослідження

Аналіз джерел дає змогу виділити чотири складові впливу противника на тактичний радіозв'язок: придушення радіоліній завадами; перехоплення змісту радіообміну; пеленгування джерел випромінювання з подальшим вогневим ураженням; виведення з ладу окремих вузлів мережі. Так, комплекс «Борисоглібськ-2», імовірно основний тактичний засіб РЕБ сухопутних військ РФ, поєднує радіорозвідку з постановкою завад радіозв'язку, супутниковому зв'язку й навігації [2]. Відповідно, стійкість радіозв'язку слід розглядати як сукупність завадостійкості, скритності, криптостійкості та живучості мережі.

ППРЧ змушує противника розподіляти потужність завади за всім діапазоном: проти загороджувальної завади виграш обробки визначається числом частотних каналів N як $G_п = 10 \lg N$ [6]; для діапазону 30–88 МГц із кроком сітки 25 кГц (N = 2320) він становить близько 33,7 дБ. Водночас за

повільної ППРЧ противник може застосовувати завади з відстеженням частоти [5], а надійність системи визначається швидкістю і стійкістю синхронізації [7]. Моделювання радіоканалу ОВЧ/УВЧ показує, що правильний вибір азимутів і типу діаграм спрямованості антен суттєво підвищує завадозахищеність навіть за кількох джерел навмисних завад [8].

У тактичних мережах MANET адаптивне керування швидкістю передачі та потужністю підвищувало пропускну здатність в умовах дії завад до 150 %, тоді як сама лише ППРЧ забезпечувала обмежений захист; багатошляхова маршрутизація підвищує живучість мережі в разі втрати вузлів [9]. Порівняльну характеристику методів наведено в таблиці 1.

Таблиця 1 — Порівняльна характеристика методів забезпечення стійкості тактичного радіозв'язку в умовах РЕБ

Метод	Принцип дії	Від якого впливу захищає	Обмеження
ППРЧ (FHSS) [5–7]	Стрибкоподібна зміна несучої частоти за псевдовипадковим законом	Вузькосмугові та загороджувальні завади; ускладнює виявлення і пеленгування	Вразливість повільної ППРЧ до завад з відстеженням; потреба в синхронізації
Розширення спектра (DSSS) [5, 6]	Розподіл енергії сигналу в широкій смузі частот	Вузькосмугові завади; знижує ймовірність виявлення сигналу	Потреба в широкій смузі; ефективність падає за великої потужності завади
Просторова селекція [8]	Спрямовані антени, вибір азимутів, багатоантенні (MIMO) системи	Завади з відомого напрямку; зменшує зону доступності для радіорозвідки	Складність для рухомих абонентів; потреба в орієнтуванні антен
Адаптивні мережі (MANET) [9]	Автоматичний вибір параметрів, багатоскачкова маршрутизація в обхід придушених вузлів	Локальне придушення, втрата окремих вузлів	Затримки, зростання службового трафіку, складність керування
Радіомаскування [2–4]	Мінімізація тривалості, потужності та регулярності випромінювання	Радіорозвідка, пеленгування й подальше вогневе ураження	Обмежує обсяг обміну; залежить від дисципліни особового складу
Криптографічний захист [1, 3]	Шифрування та регулярна зміна ключів	Перехоплення змісту радіообміну	Не захищає від придушення і пеленгування; потребує налагодженої розсилки ключів

Дані таблиці свідчать, що жоден метод не забезпечує стійкості радіозв'язку самостійно: методи підвищення завадостійкості не захищають від пеленгування, а криптографічний захист — від придушення. Досвід війни показує, що найвразливішою ланкою часто є не техніка, а організація зв'язку: проблеми з розсилкою криптоключів змушували російські підрозділи переходити на незахищені цивільні радіостанції, а неузгоджене застосування власних засобів РЕБ призводило до придушення своїх же мереж [3]. Тому стійкість має забезпечуватися поєднанням технічних методів з організаційними заходами радіомаскування.

Висновки

Сучасна РЕБ противника є щільною (щонайменше один потужний комплекс на 10 км фронту) і поєднує придушення, перехоплення та пеленгування з вогневим ураженням, тому стійкість тактичного радіозв'язку слід оцінювати комплексно: за завадостійкістю, скритністю, криптостійкістю та живучістю мережі.

Жоден із методів окремо не забезпечує стійкості: ППРЧ і розширення спектра не захищають від пеленгування, а криптографічний захист — від придушення.

Найбільший ефект дає поєднання ППРЧ із просторовою селекцією, адаптивним керуванням параметрами та мережевою маршрутизацією (MANET), що дає змогу обходити придушені ділянки мережі.

Напрями вдосконалення: оснащення підрозділів радіостанціями з адаптивним вибором частот і підтримкою MANET; застосування спрямованих антен і керування потужністю; дотримання радіомаскування та підготовка особового складу; резервування каналів (проводові, супутникові); своєчасна розсилка криптоключів.

Список використаних джерел:

1. Watling J., Reynolds N. Meatgrinder: Russian tactics in the second year of its invasion of Ukraine. London : Royal United Services Institute, 2023. URL: https://rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine (дата звернення: 28.10.2026).
2. Kjellén J. Russian electronic warfare: the role of electronic warfare in the Russian armed forces : FOI-R--4625--SE. Stockholm : Swedish Defence Research Agency (FOI), 2018. 105 p.
3. McCrory D. Electronic warfare in Ukraine: preliminary lessons for NATO air power capability development. JAPCC Journal. 2023. Edition 36. URL: https://www.japcc.org/?p=17102 (дата звернення: 28.10.2026).
4. Майборода І., Власов К., Глущенко М. Застосування і перспективи розвитку мобільних засобів радіоелектронної розвідки тактичної ланки сил сектору безпеки і оборони України. Честь і закон. 2024.

№ 2 (89). С. 83–90. URL: https://chiz.nangu.edu.ua/article/download/309207/300739/714448 (дата

звернення: 28.10.2026).
5. Poisel R. A. Modern communications jamming principles and techniques. 2nd ed. Boston : Artech House, 2011. 870 p.
6. Torrieri D. Principles of spread-spectrum communication systems. 4th ed. Cham : Springer, 2018. 727

p. DOI: https://doi.org/10.1007/978-3-319-70569-9.
7. Синхронізація та надійність систем зв'язку з псевдовипадковим перелаштуванням робочої частоти / В. В. Ткачук та ін. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2025. №

61. С. 256–263. DOI: https://doi.org/10.36910/6775-2524-0560-2025-61-35.
8. Малюк В. Г. Комп'ютерний аналіз умов завадозахищеності радіоканалу VHF/UHF діапазону з урахуванням зон електромагнітної доступності джерел радіовипромінювання. Збірник наукових праць Національної академії Національної гвардії України. 2025. Вип. 2 (46). С. 78–85. URL: https://znp.nangu.edu.ua/article/download/352575/339295/817418 (дата звернення: 28.10.2026).
9. ARSENAL: a cross layer architecture for secure resilient tactical mobile ad hoc networks : final report

/ K. Levitt et al. Davis : University of California, 2016. URL: https://apps.dtic.mil/sti/pdfs/AD1053217.pdf (дата звернення: 28.10.2026).

Тимошенко Віталій Олександрович – викладач кафедри військової підготовки Вінницького національного технічного університету, м. Вінниця, вул. Хмельницьке шосе, буд. 95, інд. 20021, E-mail: vitaliktymoshenko@gmail.com ORCID: https://orcid.org/0009-0009-8352-3299

Tymoshenko Vitalii Oleksandrovych – Lecturer at the Department of Military Training, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse St., Building 95, Ind. 20021, E-mail: vitaliktymoshenko@gmail.com ORCID: https://orcid.org/0009-0009-8352-3299