УДК 004.056:004.75
DOI https://doi.org/10.32782/IT/2025-1-7

Сергій ДОРОЖИНСЬКИЙ
PhD, доцент кафедри кібербезпеки, інформаційних технологій та економіки, декан факультету інформаційних технологій та соціально-гуманітарних наук, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-5395-6423*
***Scopus author ID:** 57222147991*

Бібліографічний опис статті: Дорожинський, С. (2025). Захист радіомереж від впливу РЕБ: виклики та методи. Information *Technology: Computer Science, Software Engineering and Cyber Security*, 48–54, doi: https://doi.org/10.32782/IT/2025-1-7

ЗАХИСТ РАДІОМЕРЕЖ ВІД ВПЛИВУ РЕБ: ВИКЛИКИ ТА МЕТОДИ

У статті розглядаються актуальні проблеми захисту радіомереж від впливу засобів радіоелектронної боротьби (РЕБ), що становлять значну загрозу для сучасних кіберфізичних систем. Описано основні вектори атак, спрямованих на порушення цілісності, конфіденційності та доступності переданих даних у бездротових мережах, зокрема перехоплення сигналу, глушіння частот і внесення перешкод.

*Аналізуються ключові **методології** кіберзахисту, зокрема використання адаптивних алгоритмів модуляції, криптографічних засобів шифрування трафіку, динамічного розподілу спектра та технологій виявлення атак.*

***Метою** є впровадження машинного навчання та штучного інтелекту для ідентифікації аномалій у роботі мереж.*

***Висновки.** Обґрунтовано необхідність інтеграції методів радіоелектронного захисту із сучасними підходами до кібербезпеки для формування багаторівневих систем оборони критичної інфраструктури.*

***Ключові слова:** радіоелектронна боротьба, захист радіомереж, кібербезпека, штучний інтелект, критична інфраструктура.*

Serhii DOROZHYNSKYI
PhD, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Dean of the Faculty of Information Technology and Social Sciences and Humanities, Kyiv University of Intellectual Property and Law of the National University “Odesa Law Academy”, 210, Kharkivske highway, Kyiv, Ukraine, 02121, dorozhun1706@gmail.com
***ORCID:**0000-0002-5395-6423*
***Scopus author ID:** 57222147991*

To cite this article: Dorozhynskyi, S. (2025). Zakhyst radiomerezh vid vplyvu REB: vyklyky ta metody [Protection of radio networks from the effects of Electronic Warfare: challenges and methods]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 48–54, doi: https://doi.org/10.32782/IT/2025-1-7

PROTECTION OF RADIO NETWORKS FROM THE EFFECTS OF ELECTRONIC WARFARE: CHALLENGES AND METHODS

The article discusses the current problems of protecting radio networks from the effects of electronic warfare (EW), which pose a significant threat to modern cyber-physical systems. The main vectors of attacks aimed at violating the integrity, confidentiality and availability of transmitted data in wireless networks are described, including signal interception, frequency jamming and interference.

*Key **methods** of cyber defense are analyzed, including the use of adaptive modulation algorithms, cryptographic traffic encryption, dynamic spectrum allocation, and attack detection technologies.*

***The purpose.** Particular attention is paid to the introduction of machine learning and artificial intelligence to identify anomalies in the operation of networks.*

***Conclusions.** The necessity of integrating electronic warfare methods with modern approaches to cybersecurity to form multi-level defense systems for critical infrastructure is substantiated.*

Key words: electronic warfare, radio network protection, cybersecurity, artificial intelligence, critical infrastructure.

Вступ. У сучасних умовах розвитку інформаційно-комунікаційних технологій та широкого впровадження бездротових мереж радіоелектронна боротьба (РЕБ) стає одним із ключових інструментів у кіберконфліктах і гібридних війнах. Засоби РЕБ, спрямовані на порушення роботи радіомереж, становлять значну загрозу для забезпечення цілісності, конфіденційності та доступності переданих даних, особливо в критичних інфраструктурах. Технологічна еволюція методів глушіння, перехоплення сигналів і внесення перешкод вимагає розробки нових підходів до захисту радіомереж, які б дозволили ефективно нейтралізувати ворожий вплив. З огляду на це, актуальним є дослідження методів забезпечення стійкості радіомереж до деструктивних впливів засобів РЕБ, зокрема шляхом впровадження інноваційних технологій подавлення шуму та адаптивної фільтрації сигналів.

Особливу увагу привертає використання алгоритмів машинного навчання та глибокого навчання, які відкривають нові можливості для виявлення джерел перешкод і динамічного налаштування параметрів роботи мережі. Інтеграція таких технологій із сучасними підходами до кібербезпеки може суттєво підвищити рівень захищеності радіомереж і мінімізувати ризики, пов'язані з кіберзагрозами.

Метою даної роботи є обґрунтування нової методології подавлення шуму для захисту радіомереж, її теоретична розробка та практична перевірка ефективності. Результати дослідження спрямовані на формування комплексного підходу до протидії загрозам у радіоелектронному та цифровому середовищах, що є критично важливим для забезпечення стійкості сучасних кіберфізичних систем.

Радіомережі, як ключовий елемент сучасних інформаційно-комунікаційних систем, залишаються вразливими до широкого спектра атак, що реалізуються засобами радіоелектронної боротьби. Одним із найбільш поширених типів атак є **перехоплення сигналів**, що спрямоване на отримання несанкціонованого доступу до переданих даних. Такі атаки здебільшого базуються на використанні спеціалізованого обладнання для моніторингу частотного спектра, аналізу параметрів сигналу та розшифрування інформації, що створює загрози конфіденційності й сприяє можливим подальшим вторгненням у систему.

Другим типом є **глушіння сигналу**, що реалізується шляхом навмисного створення надпотужних радіосигналів у тих самих частотних діапазонах, які використовуються цільовою мережею. Така діяльність призводить до деградації сигналу, втрати пакунків даних або повної недоступності зв'язку. Глушіння є особливо небезпечним для критичних інфраструктур, таких як військові системи, авіаційні мережі або медичні телеметричні системи, де порушення зв'язку може мати катастрофічні наслідки.

Ще одним поширеним методом є **внесення перешкод**, що включає створення штучного шуму або маніпулювання сигналом таким чином, щоб порушити його цілісність або дезорієнтувати приймальний пристрій. Перешкоди можуть бути як випадковими, так і спрямованими, зокрема, з використанням адаптивних методів, які ускладнюють їх виявлення та нейтралізацію. Особливу небезпеку становить комбінація цих атак у комплексних сценаріях, де вони використовуються синхронізовано для одночасного порушення кількох аспектів роботи радіомережі.

Вразливості сучасних бездротових технологій. Сучасні бездротові технології, що формують основу радіомереж, вирізняються високою гнучкістю, масштабованістю та швидкістю передачі даних, однак водночас залишаються вразливими до широкого спектра загроз, пов'язаних із радіоелектронною боротьбою. Однією з головних вразливостей є **обмежена захищеність протоколів зв'язку**, особливо в контексті відкритого доступу до радіочастотного спектра. Багато протоколів, таких як Wi-Fi, Zigbee, Bluetooth, використовують заздалегідь визначені діапазони частот, що спрощує для зловмисників моніторинг і глушіння сигналу.

Іншим суттєвим недоліком є **залежність від обмежених ресурсів пристроїв**, таких як обчислювальна потужність і енергетична ефективність. Наприклад, IoT-пристрої часто не здатні реалізувати складні криптографічні алгоритми чи адаптивні методи захисту від атак через обмеження апаратних можливостей. Це створює передумови для успішної реалізації атак, таких як внесення перешкод або навмисне перевантаження мережі.

Вразливістю також є **відсутність динамічного управління частотним спектром** у багатьох системах. Статичне використання частот робить їх прогнозованими для атак глушіння або перехоплення. Незважаючи на зусилля щодо впровадження методів когнітивного радіо, багато систем ще не підтримують технології, здатні динамічно змінювати параметри сигналу для уникнення ворожих впливів. Крім того, значну роль відіграє **недосконалість систем виявлення аномалій** у радіомережах. Більшість існуючих засобів моніторингу

не забезпечують достатнього рівня точності для виявлення малопотужних або адаптивних перешкод. Це дає змогу зловмисникам застосовувати складні методи атак із низьким енергетичним профілем, які залишаються непоміченими протягом тривалого часу. На додаток до технічних аспектів, вразливості також обумовлені **людським фактором**, включаючи недоліки у налаштуванні мереж, відсутність регулярних оновлень програмного забезпечення та використання стандартних параметрів безпеки. Це спрощує для зловмисників використання експлойтів для доступу до мережі.

Радіоелектронна боротьба має суттєвий вплив на функціонування кіберфізичних систем, які інтегрують фізичні процеси з цифровими технологіями, забезпечуючи їхню взаємодію через радіомережі. Деструктивний вплив засобів РЕБ не лише порушує роботу комунікацій, але й створює серйозні ризики для безпеки даних, що передаються в таких системах. Основною загрозою є **порушення конфіденційності даних** через перехоплення та аналіз радіосигналів. Засоби радіоелектронної розвідки здатні фіксувати характеристики сигналу, що дозволяє зловмисникам не лише отримувати доступ до інформації, але й ідентифікувати джерела передачі та їхнє місцезнаходження.

Крім того, атаки типу **глушіння сигналів** призводять до порушення доступності даних, коли передача інформації між компонентами кіберфізичної системи стає неможливою. Це особливо критично для систем реального часу, таких як автоматизовані системи управління транспортом, енергетичні мережі або системи охорони здоров'я, де затримка у передачі даних може спричинити серйозні наслідки, включаючи збої або аварії.

Не менш небезпечним є **внесення перешкод із метою спотворення даних**, що може спричинити порушення цілісності інформації. Введення штучного шуму або зміна параметрів сигналу може призвести до помилкових рішень у системах автоматичного управління, зокрема у військових системах чи промислових виробництвах, де алгоритми працюють на основі отриманих даних у реальному часі.

Комплексний вплив РЕБ також включає **створення умов для реалізації багаторівневих кібератак**, де радіоелектронні методи застосовуються разом із традиційними методами компрометації мережі. Наприклад, глушіння може бути використане для відволікання уваги або створення тимчасової «дірки» у захисті, через яку зловмисники впроваджують шкідливе програмне забезпечення.

Окремо варто зазначити, що вплив РЕБ на кіберфізичні системи ускладнюється їхньою архітектурою, яка часто включає розподілені компоненти з різним рівнем захищеності. Це створює додаткові можливості для зловмисників використовувати слабкі ланки в системі. Особливо це стосується IoT-пристроїв, які можуть слугувати як точками входу для атак, так і джерелами поширення вразливостей у мережі.

Сучасні радіомережі потребують впровадження високоефективних методів захисту, які здатні протидіяти складним загрозам, створеним засобами радіоелектронної боротьби. Найкращими визнані ті підходи, які демонструють високий рівень адаптивності, стійкості до атак та інтеграції з інноваційними технологіями:

1. Адаптивні методи модуляції та кодування сигналів. Ці методи забезпечують динамічну зміну параметрів сигналу, таких як частота, амплітуда та модуляційна схема, що ускладнює роботу засобів РЕБ. Використання технік когнітивного радіо дозволяє мережам аналізувати стан спектра в реальному часі й оперативно змінювати параметри передачі для уникнення перешкод або глушіння. Зокрема, використання модуляції типу OFDM (ортогональне частотне мультиплексування) з динамічним керуванням частотами значно підвищує стійкість систем до перешкод.

2. Криптографічний захист трафіку. Впровадження сучасних криптографічних протоколів, таких як AES-256 або ECC (еліптичні криві), забезпечує високий рівень конфіденційності даних навіть за умов їхнього перехоплення. Для бездротових мереж також перспективними є протоколи, що реалізують захист на фізичному рівні, наприклад, через хаотичне шифрування сигналу, яке інтегрує криптографічні підходи у процес генерації радіосигналу.

3. Методи динамічного розподілу спектра. Цей підхід ґрунтується на принципах когнітивного радіо та передбачає аналіз доступності частотного ресурсу для ефективного уникнення зон впливу засобів РЕБ. Технологія спектрального сканування в режимі реального часу дозволяє визначати «чисті» частотні діапазони й оперативно перемикати передачу сигналу, мінімізуючи ризики глушіння.

4. Виявлення аномалій за допомогою штучного інтелекту. Алгоритми машинного навчання (ML) та машинного навчання (DL) використовуються для моніторингу роботи радіомереж і виявлення аномальних дій, таких як глушіння, внесення перешкод або несанкціоноване сканування спектра. Зокрема, нейронні мережі здатні аналізувати великі обсяги даних

у реальному часі, що дає змогу швидко ідентифікувати джерела атак та адаптувати захисні заходи.

5. Використання спрямованих антенних систем. Технологія формування спрямованих променів у системах MIMO (багатовхідний та багатовихідний зв'язок) дозволяє створювати вузьконаправлені сигнали, які зменшують ймовірність перехоплення або глушіння. Зокрема, використання адаптивних антенних решіток забезпечує зміну напрямку передачі сигналу залежно від рівня виявлених перешкод.

6. Інтеграція захисних систем із багаторівневою архітектурою. Найбільш ефективними є підходи, що об'єднують кілька захисних механізмів у єдину багаторівневу систему. Наприклад, поєднання методів динамічного розподілу спектра, криптографічного шифрування та адаптивної модуляції створює багатошарову оборону, здатну ефективно протидіяти одночасно кільком типам атак.

Основними недоліками існуючих методів є енергетична ефективність, інтеграційна здатність та спроможність протидії комбінованим атакам. Тому пропонується нова методологія подавлення шуму, що базується на адаптивному підході до аналізу та обробки радіосигналів у реальному часі. Її мета – забезпечення стійкого функціонування радіомереж в умовах впливу радіоелектронної боротьби шляхом динамічного виявлення перешкод і мінімізації їх впливу на якість зв'язку. Основні кроки реалізації цієї методології включають:

• **Моделювання радіочастотного середовища.** На першому етапі система створює математичну модель середовища, яка враховує особливості частотного спектра, потужність сигналів і можливі джерела перешкод. Це дозволяє оцінити потенційні загрози та адаптуватися до динаміки середовища. Формула для оцінки ефективності частотного спектра в умовах шуму:

$$S(f, t) = P_{сигнал}(f, t) - P_{шум}(f, t),$$

де $S(f, t)$ – сила сигналу на частоті f у часі t, $P_{сигнал}(f, t)$ – потужність корисного сигналу на частоті f у часі t, $P_{шум}(f, t)$ – потужність шуму на частоті f у часі t.

• **Спектральний аналіз і виявлення перешкод.** Використання когнітивних технологій та алгоритмів машинного навчання дозволяє визначити джерела перешкод шляхом аналізу аномалій у спектрі сигналів. Завдяки цьому мережа в реальному часі може визначати активність засобів РЕБ та оцінювати рівень загрози. Формула для виявлення аномалій у спектрі, що використовує порівняння очікуваної та фактичної потужності сигналу:

$$A(f,t) = \left| \frac{P_{фактичний}(f,t) - P_{очікуваний}(f,t)}{P_{очікуваний}(f,t)} \right|,$$

де $A(f, t)$ – коефіцієнт аномалії на частоті f у часі t, $P_{фактичний}(f, t)$ – фактична потужність сигналу на частоті f у часі t, $P_{очікуваний}(f, t)$ – очікувана потужність сигналу на частоті f у часі t.

• **Динамічне налаштування параметрів сигналу.** Після виявлення перешкод система адаптує параметри передачі, такі як частота, модуляція або кодування, щоб уникнути зон впливу засобів РЕБ. Використання методів когнітивного радіо забезпечує автоматичний вибір оптимальних параметрів для передачі даних. Формула для динамічного коригування модуляції в залежності від рівня шуму:

$$M(t) = arq\left(\sum_f [SNR(f,t) - \gamma]^2\right),$$

де $M(t)$ – обрана модуляція в часі t, $SNR(f, t)$ – співвідношення сигнал/шум на частоті f у часі t, γ – пороговий рівень для вибору оптимальної модуляції.

• **Фільтрація та відновлення сигналу.** Система використовує адаптивні фільтри для зменшення впливу шуму та спотворень. При цьому алгоритми машинного навчання допомагають ефективно відновлювати корисний сигнал, забезпечуючи збереження цілісності даних.

$$\hat{S}(t) = \sum_{n=0}^{N} \omega_n(t) \cdot x(t-n),$$

де $\hat{S}(t)$ – відновлений сигнал у часі t, $\omega_n(t)$ – коефіцієнти адаптивного фільтра на кроку n у часі t, $x(t - n)$ – значення вхідного сигналу в часі $t - n$, N – кількість етапів фільтру.

• **Моніторинг і зворотній зв'язок.** Постійний контроль стану радіомережі дозволяє оперативно оцінювати ефективність захисту та вносити необхідні корективи для забезпечення стійкості мережі в умовах змінних загроз. Формула для визначення ефективності зворотного зв'язку на основі постійного моніторингу параметрів:

$$E(t) = \sum_f \left(\frac{\left| P_{сигнал}(f,t) - P_{цільовий}(f) \right|}{P_{цільовий}(f)} \right),$$

де $E(t)$ – показник ефективності у часі t, $P_{сигнал}(f, t)$ – потужність сигналу на частоті f у часі t, $P_{цільовий}(f, t)$ – цільова потужність сигналу на частоті f.

Запропонована методологія подавлення шуму базується на використанні математичних

моделей і алгоритмів, що забезпечують автоматизацію процесу виявлення, фільтрації та відновлення сигналу в умовах радіоелектронної боротьби. Ключовими аспектами реалізації цієї методології є розробка точних моделей для оцінки радіочастотного середовища, адаптивне управління параметрами сигналу та інтеграція механізмів зворотного зв'язку для оптимізації процесів захисту.

Розроблена методологія подавлення шуму для захисту радіомереж демонструє значний потенціал у забезпеченні їх стійкості в умовах радіоелектронної боротьби. Її ефективність базується на інтеграції адаптивних алгоритмів, спектрального аналізу та механізмів зворотного зв'язку, що дозволяють не лише протидіяти існуючим перешкодам, але й швидко адаптуватися до динамічно змінюваних загроз. Одним із ключових аспектів методології є можливість її використання у широкому спектрі радіомереж, включаючи як традиційні комунікаційні системи, так і сучасні мережі з когнітивними функціями. Завдяки здатності до динамічного управління параметрами сигналу та ефективного фільтрування, методологія забезпечує високу якість передачі даних навіть за умов значного радіочастотного навантаження.

Перспективи впровадження методології охоплюють не лише військові, а й цивільні застосування. Зокрема, вона може бути інтегрована в системи забезпечення зв'язку для критичної інфраструктури, мобільні мережі нового покоління (5G і 6G), а також у системи інтернету речей (IoT), які є вразливими до впливу зовнішніх перешкод. Подальший розвиток методології передбачає її адаптацію до нових умов радіочастотного середовища, підвищення енергоефективності обчислювальних алгоритмів та інтеграцію з іншими технологіями кіберзахисту. Це дозволить створити універсальний інструмент для захисту радіомереж, що відповідає викликам сучасної інформаційної епохи.

Для оцінки ефективності запропонованої методології було змодельовано два типи атак, що характерні для сучасних радіомереж за допомогою **GNU Radio** – безкоштовної платформи з відкритим кодом для симуляції радіомереж і обробки сигналів: вузькосмугове радіоелектронне глушіння та широкосмугове подавлення сигналу. Нижче наведено опис цих сценаріїв та процес застосування методології для їхньої нейтралізації.

Сценарій 1: Вузькосмугове глушіння сигналу

У першому сценарії противник здійснює спрямоване вузькосмугове глушіння, націлене на конкретну частоту, яка використовується для передачі сигналу. Атака має на меті суттєве зниження співвідношення сигнал/шум (SNRSNRSNR) у вузькому діапазоні, що ускладнює або унеможливлює коректну передачу даних.

Для нейтралізації цієї атаки методологія виконує такі дії:

1. **Моніторинг спектра.** Алгоритм аналізує частотний спектр у реальному часі та ідентифікує вузькосмугові перешкоди за допомогою когнітивних методів.

2. **Динамічна зміна частоти.** Виявивши зону перешкоди, система автоматично переводить сигнал на сусідню частоту з кращими умовами передачі.

3. **Фільтрація залишкових перешкод.** Адаптивні фільтри зменшують вплив шуму, дозволяючи зберегти прийнятний рівень якості сигналу.

Результатом застосування методології стає відновлення стабільного зв'язку із мінімальними затримками, навіть у випадках активного глушіння.

Сценарій 2: Широкосмугове подавлення сигналу.

У другому сценарії противник застосовує широкосмугове подавлення, генеруючи високий рівень шуму на значній частині частотного спектра, що охоплює декілька каналів одночасно. Така атака має на меті порушити функціонування всієї мережі.

Методологія реагує наступним чином:

1. **Аналіз характеристик шуму.** Система визначає структуру широкосмугових перешкод, оцінюючи їх інтенсивність і розподіл по спектру.

2. **Адаптивне налаштування параметрів сигналу.** Для мінімізації втрат даних застосовується зміна модуляції, що дозволяє підвищити стійкість сигналу до шуму.

3. **Оптимізація потужності передачі.** Система збільшує потужність передавача на окремих ділянках спектра, щоб забезпечити коректний прийом сигналу навіть у зоні шуму.

4. **Впровадження резервних каналів.** У разі тривалих перешкод активується механізм перенаправлення сигналу через альтернативні частоти або канали.

Завдяки запропонованій методології мережа зберігає функціональність навіть за умов інтенсивного широкосмугового шуму, забезпечуючи надійний зв'язок для критично важливих завдань.

Подальший розвиток дослідження запропонованої методології подавлення шуму та захисту радіомереж передбачає інтеграцію

інноваційних підходів та адаптацію системи до сучасних викликів у сфері радіоелектронної боротьби. Впровадження методів машинного навчання дозволить створити когнітивні моделі для прогнозування динаміки атак і автоматизації адаптації параметрів системи, таких як частота, модуляція та потужність сигналу, що підвищить швидкість і точність реагування на перешкоди. Розробка багатовузлових систем захисту із динамічним обміном даними між вузлами дозволить забезпечити кооперативне подавлення шуму в умовах децентралізованих мереж, таких як IoT. Дослідження роботи методології в різних частотних діапазонах, включаючи міліметрові хвилі та ультраширокосмугові сигнали, відкриє нові можливості для її застосування в умовах високочастотного середовища та дозволить врахувати вплив природних факторів на ефективність захисту. Інтеграція алгоритмів у програмно-визначені радіосистеми (SDR) і випробування в польових умовах дадуть змогу перевірити практичну цінність методології в умовах активного радіоелектронного протистояння. Оцінка ефективності системи для протидії новим видам атак, таким як spoofing або replay attacks, забезпечить її адаптацію до сучасних загроз, а розробка енергетично ефективних алгоритмів підвищить її застосовність для пристроїв із низьким енергоспоживанням. Крім того, створення інструментів для автоматизованої оцінки ефективності в реальному часі дозволить побудувати систему моніторингу атак і стану мережі, забезпечуючи надійність зв'язку навіть у найскладніших умовах.

Висновки. Представлений підхід до адаптивного подавлення шуму забезпечує підвищення стійкості радіозв'язку за рахунок інтеграції алгоритмів аналізу спектральних характеристик сигналів, виявлення перешкод та їх фільтрації. Реалізація когнітивного підходу, включаючи динамічне налаштування частот і параметрів сигналу, значно підвищує ефективність захисту навіть у випадках цілеспрямованих атак, таких як вузькосмугове глушіння та широкосмугове подавлення. Випробування методології на симульованих сценаріях демонструють її здатність зберігати функціональність мережі та забезпечувати мінімізацію втрат даних, що підтверджує її потенціал для впровадження у практичні системи зв'язку. Перспективи подальшого розвитку методології полягають у її вдосконаленні за рахунок застосування методів машинного навчання для автоматизації виявлення атак і адаптації захисту в реальному часі, розробці багатовузлових систем захисту з кооперативним подавленням шуму, а також інтеграції в програмно-визначені радіосистеми. Крім того, забезпечення енергетичної ефективності запропонованого підходу робить його застосовним для пристроїв з обмеженими ресурсами, таких як IoT, а дослідження у сфері широкосмугового спектра та нових частотних діапазонів сприятиме його універсальності. Представлена методологія є важливим внеском у підвищення надійності та безпеки радіомереж, що робить її перспективною для застосування як у військових, так і в цивільних системах.

ЛІТЕРАТУРА:

1. Боголій С. М. Методи і засоби забезпечення стабільності та захищеності радіозв'язку в умовах низького співвідношення сигнал/шум. *Вісник Національного університету «Львівська політехніка»*. Серія: Радіоелектроніка та телекомунікації. 2024. № 101. С. 101–109.

2. Перепелицин С. Технологія налаштовування радіомережі в умовах електромагнітного протиборства: дис. … канд. техн. наук. Національний авіаційний університет, 2024.

3. Шолохов С. М., Самборський І. І., Вакуленко О. В., Ніколаєнко Б. А. Завадозахист радіоелектронних засобів. Частина 1. Основи завадозахисту систем зв'язку: навчальний посібник. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021.

4. Зелепукіна О. В. Дослідження методів зниження коефіцієнта шуму в радіоприймальних пристроях: магістерська дис. Київ : КПІ ім. Ігоря Сікорського, 2019.

5. Нестеренко В. П., Ковтун В. В., Фаль А. С. Інтелектуальні системи і технології: навчальний посібник. Київ : НАУ, 2018.

6. Ткачук Р., Сікора Л. Логіко-когнітивні моделі формування управлінських рішень: навчально-методичний посібник. Львів : ЛДУ БЖД, 2010.

7. Довбиш А. С., Васильєв А. В., Любчак В. О. Інтелектуальні інформаційні технології в освіті: монографія. Суми : Сумський державний університет, 2012.

REFERENCES:

1. Boholiy, S. M. (2024). Metody i zasoby zabezpechennya stabil'nosti ta zakhyshchenosti radiozvy"yazku v umovakh nyzkogo spivvidnoshennya syhnal/shum [Methods and means of ensuring

stability and security of radio communications in conditions of low signal-to-noise ratio]. *Vísnyk Natsional'noho universytetu "L'vivs'ka politekhnika"*. Seriya: Radioelektronika ta telekomunikaciyi, 101, 101–109. [in Ukrainian].

2. Perepelytsyn, S. (2024). Tekhnologiya nalashtovuvannya radiomerezhi v umovakh elektromahnitnoho protyborystva [Radio network configuration technology in electromagnetic interference conditions] (Dys. kand. tekhn. nauk). Natsional'nyy aviatsiynyy universytet. [in Ukrainian].

3. Sholokhov, S. M., Sambors'kyy, I. I., Vakulenko, O. V., & Nikolyayenko, B. A. (2021). Zavadozakhyst radioelektronnykh zasobiv [Interference protection of radio electronic devices]. Chastyna 1. Osnovy zavadozakhystu system zvyazku: navchal'nyy posibnyk. Kyiv : ISZZI KPI im. Ihorya Sikors'koho. [in Ukrainian].

4. Zelepukina, O. V. (2019). Doslidzhennya metodiv znyzhennya koefitsiyenta shumu v radiopriymal'nykh prystroyakh [Research on methods for reducing noise coefficient in radio receiving devices] (Mahisters'ka dys.). Kyiv : KPI im. Ihorya Sikors'koho. [in Ukrainian].

5. Nesterenko, V. P., Kovtun, V. V., & Fal', A. S. (2018). Intelektual'ni systemy i tekhnolohiyi [Intelligent systems and technologies]: navchal'nyy posibnyk. Kyiv: NAU. [in Ukrainian].

6. Tkachuk, R., & Sikora, L. (2010). Loho-kohnityvni modeli formuvannya upravlins'kykh rishen' [Logical-cognitive models of management decision-making]: navchal'no-metodychnyy posibnyk. L'viv : LDU BZHD. [in Ukrainian].

7. Dovbysh, A. S., Vasyl'yev, A. V., & Lyubchak, V. O. (2012). Intelektual'ni informatsiyni tekhnolohiyi v osviti [Intelligent information technologies in education]: monohrafiya. Sumy: Sumskyy derzhavnyy universytet. [in Ukrainian].