

УДК 621.396:002.53

DOI <https://doi.org/10.36994/2788-5518-2025-02-10-05>

ЗАХИСТ ВІД АКТИВНИХ ЗАВАД БЕЗДРОТОВИХ СИСТЕМ ЗВ'ЯЗКУ З АДАПТИВНИМИ ФАЗОВАНИМИ АНТЕННИМИ РЕШІТКАМИ

Безрук В. М., д.т.н., проф., завідувач кафедри інформаційно-мережної інженерії Факультет інфокомунікацій, Харківський національний університет радіоелектроніки, Харків, Україна. <https://orcid.org/0000-0002-5482-9960>, valerii.bezruk@nure.ua

Голобородько Ю. М., к.т.н., доцент кафедри безпеки інформаційних технологій Факультет комп'ютерної інженерії та управління Харківський національний університет радіоелектроніки, Харків, Україна. <https://orcid.org/0009-0007-4040-9467>, yurii.holoborodko@nure.ua

Заболотний В. І., к.т.н., доцент, професор кафедри безпеки інформаційних технологій Факультет комп'ютерної інженерії та управління Харківський національний університет радіоелектроніки, Харків, Україна. <https://orcid.org/0000-0003-3258-8489>, volodymyr.zabolotnyi@nure.ua

Анотація. Актуальність та проблема. Надійність зв'язку є критично важливою для військових та силових структур, але бездротові системи вразливі до активних завад (глушіння, імітація). Ці завади мають ворожу природу, динамічно адаптуються та становлять пряму загрозу безпеці. Аналіз загроз показує, що активні перешкоди, на відміну від пасивних (тепловий шум, атмосферні), вимагають адаптивних рішень для збереження стійкості комунікацій у сучасному, насиченому радіоелектронному середовищі.

Мета роботи. Обґрунтування та дослідження методології захисту бездротових систем зв'язку від активних завад шляхом інтеграції адаптивних фазованих антенних решіток (АФАР) та засобів радіо- та радіотехнічної розвідки (РПТР). Дослідження зосереджено на використанні АФАР для динамічного керування діаграмою спрямованості (ДС) та ефективного пригнічення перешкод.

Методи дослідження. Запропонована методологія ґрунтується на просторово-частотній обробці сигналу з використанням АФАР. Підхід передбачає два ключові етапи: 1) використання засобів РПТР для оперативного виявлення, розпізнавання та пеленгування джерел активних завад; 2) адаптоване керування ДС АФАР (як приймальних, так і передавальних) для формування глибоких провалів («нулів») у напрямку перешкод та максимізації енергії корисного сигналу у напрямку кореспондента. Розглянуто різні алгоритми керування, включаючи методи на основі кореляційної матриці та градієнтні методи (математична оптимізація), які є найбільш ефективними для систем реального часу.

Основні результати та практичне значення. Доведено, що інтеграція АФАР із системами зв'язку є ефективним механізмом підвищення стійкості, що дозволяє зменшити вплив потужних перешкод ще до етапу демодуляції. Сумарний виграш від використання АФАР у порівнянні з всеспрямованою антеною може сягати 20–30 дБ, що складається з конструктивного виграшу (6–15 дБ) та виграшу від активного подавлення перешкод (10–20 дБ). Цей значний приріст у співвідношенні сигнал/перешкода забезпечує надійний зв'язок в умовах високої щільності завад. Розроблені рішення мають стратегічне значення для підвищення захищеності критично важливих комунікаційних систем.

Ключові слова: адаптивна фазована антенна решітка, активні завади, радіоелектронна боротьба (РЕБ), радіотехнічна розвідка (РПТР), динамічне керування, просторово-частотна обробка.

PROTECTION AGAINST ACTIVE INTERFERENCE OF WIRELESS COMMUNICATION SYSTEMS USING ADAPTIVE PHASED ARRAY ANTENNAS

Valerii Bezruk, Dr. habil, Prof., Head of Department of Information and Network Engineering of Faculty of Infocommunications of Kharkiv National University of Radio Electronics, Kharkiv, Ukraine. <https://orcid.org/0000-0002-5482-9960>, valerii.bezruk@nure.ua

Yurii Holoborodko, Ph.D., Ass. Prof of Department of Information Technology Security of Faculty of Computer Engineering and Control of Kharkiv National University of Radio Electronics, Kharkiv, Ukraine. <https://orcid.org/0009-0007-4040-9467>, yurii.holoborodko@nure.ua

Volodymyr Zabolotnyi, Ph.D., Ass. Prof., Prof of Department of Information Technology Security of Faculty of Computer Engineering and Control of Kharkiv National University of Radio Electronics, Kharkiv, Ukraine. <https://orcid.org/0000-0003-3258-8489>, volodymyr.zabolotnyi@nure.ua

Abstract. Relevance and Problem. Communication reliability is vital for military and security operations, but wireless systems are susceptible to active interference (jamming, spoofing). Such interference is hostile, dynamically adapts, and poses a direct security threat. The analysis shows that active interference, unlike

passive noise, necessitates adaptive solutions to maintain communication resilience in today's saturated radio-electronic environment.

Objective. To substantiate and investigate a methodology for protecting wireless communication systems against active interference by integrating Adaptive Phased Array Antennas (APAA's) with Radio and Radiotechnical Reconnaissance (RRTR) assets. The study focuses on using APAA's for dynamic control of the radiation pattern (RP) to effectively suppress interference.

Methods. The proposed methodology is based on spatial-frequency signal processing using APAA's. The approach involves two key stages: 1) utilization of RRTR assets for operational detection, recognition, and direction finding (DF) of active interference sources; 2) adaptive control of the APAA's RP (for both transmitting and receiving) to form deep nulls in the direction of interference and maximize the energy of the useful signal towards the correspondent. Various control algorithms are discussed, including correlation matrix-based methods and gradient methods (mathematical optimization), which are most efficient for real-time systems.

Main Results and Practical Significance. The integration of APAA's into communication systems is proven to be an effective mechanism for enhancing resilience, allowing for the mitigation of powerful interference before the demodulation stage. The total gain from using APAA's, compared to an omnidirectional antenna, can reach 20–30 dB, comprising the constructive gain (6–15 dB) and the gain from active interference suppression (10–20 dB). This significant increase in the signal-to-interference ratio ensures reliable communication under high interference density. The developed solutions are of strategic importance for strengthening the security of critical communication systems.

Key words: *adaptive phased array antenna, active interference, electronic warfare (EW), radio-technical reconnaissance (RRTR), dynamic control, spatial-frequency processing.*

Вступ

Надійний зв'язок є критично важливим для успіху військових операцій та функціонування силових структур, забезпечуючи синхронізацію дій, оперативне виявлення загроз та стратегічну координацію. З розвитком сучасних технологій та широким впровадженням цифрових систем, залежність озброєння та бойової техніки від сенсорів та обміну інформацією постійно зростає, що підкреслює вирішальну роль радіоелектронної боротьби (РЕБ). У цьому контексті, ефективність армії майбутнього значною мірою визначається її здатністю гнучко адаптувати доктрини, структури та методи підготовки до розвитку РЕБ [1; 2].

Особливе значення в РЕБ має радіо- та радіотехнічна розвідка (РПТР), яка відповідає за виявлення, пеленгування та аналіз джерел електромагнітного випромінювання противника [3]. Якщо стратегічна РПТР зосереджена на підготовці до операцій, то тактична РПТР ведеться безперервно під час бойових дій, надаючи критично важливу інформацію для управління військами та озброєнням. Однак бездротові системи зв'язку, попри свої переваги (передача інформації на великі відстані, обмін даними через важкодоступну місцевість, швидке встановлення зв'язку та мовлення багатьом кореспондентам), є вразливими до низки факторів. До них належать атмосферні перешкоди, можливість пеленгування та перехоплення інформації противником, а головне – подавлення радіозв'язку засобами РЕБ противника, що призводить до низької якості та пропускну здатності каналів зв'язку.

Декаметровий (короткохвильовий, КХ/ВЧ, 3,0–30,0 МГц) радіозв'язок, що забезпечує зв'язок на значні відстані завдяки відбиттю від іоносфери, є особливо чутливим до нестабільності середовища поширення та активних завад [3; 4]. Сучасні радіосистеми поділяються на неадаптивні, що вимагають постійного ручного налаштування оператором, та адаптивні, які автоматизують процеси встановлення та ведення зв'язку, що значно підвищує їхню ефективність. Попри переваги адаптивних систем, неадаптивні системи все ще використовуються, що створює потребу в універсальних рішеннях для підвищення стійкості до завад.

Проблема захисту бездротових систем зв'язку від активних завад є критично важливою не лише для військових, але й для правоохоронних органів (СБУ, МВС) та регуляторних органів (НКРЕ), які стикаються з викликами контролю за радіочастотним спектром, протидії злочинним угрупованням та забезпечення чистоти урядових каналів зв'язку. У зв'язку з цим, методи захисту, що ґрунтуються на використанні адаптивних фазованих антенних решіток (АФАР), набувають особливої актуальності. Ці технології дозволяють динамічно керувати діаграмою спрямованості антени, максимізуючи прийом корисного сигналу та мінімізуючи вплив активних завад, що є ключовим для підвищення надійності та безпеки бездротових комунікацій в умовах сучасного інформаційного середовища.

Виконання досліджень

Одним із найважливіших чинників, що впливають на якість та надійність бездротових телекомунікаційних систем, є вплив шумових завад. У контексті рухомих об'єктів ці фактори стають ще критичнішими, адже зв'язок має підтримуватися в умовах змінного середовища, різної швидкості об'єкта

та можливого навмисного зовнішнього втручання. Загалом за характером джерела всі перешкоди поділяються на пасивні та активні.

Пасивні перешкоди виникають внаслідок природних або стохастичних процесів, без спрямованого наміру порушити роботу системи. Вони є невід'ємною частиною будь-якого реального фізичного каналу зв'язку. До основних типів пасивних перешкод належать:

1. Тепловий шум (Johnson-Nyquist noise): Виникає внаслідок теплового руху носіїв заряду в провіднику або напівпровіднику. Характеризується рівномірним спектром і присутній у будь-якому електронному колі. Його потужність прямо пропорційна температурі та смузі пропускання.

2. Адитивний білий гаусівський шум (AWGN): Теоретична модель випадкового шуму, який нормально розподілений і широко використовується для тестування телекомунікаційних систем як наближення до природного фону.

3. Фононний або фотонний шум: Характерний для оптоелектронних і квантових пристроїв, з'являється у високочастотних підсистемах, де теплові флуктуації взаємодіють з фотонними процесами (наприклад, у сенсорах, лазерах).

4. Атмосферні перешкоди: Включають перешкоди від блискавок, сонячної активності, а також радіовипромінювання земного та космічного походження.

Такі перешкоди не є ворожими, проте здатні призводити до зниження відношення сигнал / шум (SNR), втрати пакетів та збільшення помилок, особливо за низької потужності сигналу. У русі цей ефект посилюється через зміну кута падіння хвилі, доплерівський зсув та багатопроменевість.

Активні перешкоди – це навмисне створення завад з метою впливу на канал зв'язку. Їх джерелом може бути як інша техніка, так і зловмисник, який має на меті порушити передачу, заглушити сигнал, перехопити або змінити дані. Основні типи активних шумових перешкод:

1. Шум випромінювання: Електромагнітне випромінювання пристроїв або спеціально створене джерело перешкоди, що працює у тому ж частотному діапазоні (наприклад, використання генератора білого шуму для придушення Wi-Fi сигналу).

2. Імпульсні перешкоди: Короточасні інтенсивні сплески напруги або випромінювання. Можуть виникати при запуску двигунів, переключенні реле або цілеспрямованому електромагнітному імпульсі (EMI).

3. Глушіння (Jamming): Навмисне створення потужного сигналу на робочій частоті каналу для його блокування. Існують різні типи: безперервне, псевдовипадкове, імпульсне, направлене, адаптивне глушіння.

4. Імітаційні перешкоди (Spoofing): Створення сигналу, що імітує легітимне джерело, з метою обману системи виявлення або навігації (наприклад, GPS spoofing).

Активні перешкоди становлять реальну загрозу інформаційній безпеці, оскільки призводять не лише до завад, а й до порушення функцій зв'язку – зниження доступності, збільшення затримки, втрати керованості. У випадку безпілотних систем або автономних транспортних засобів це може призвести до аварій або порушень навігації.

Радіоелектронна боротьба (РЕБ) – це комплекс узгоджених дій, спрямованих на використання електромагнітної енергії для управління спектром, впливу на радіоелектронні системи противника та захисту власних засобів. Згідно з керівними документами Армії США, радіоелектронна війна (РЕВ) охоплює радіоелектронну атаку, радіоелектронний захист та забезпечення ведення РЕВ, підкреслюючи її роль як елемента інформаційних операцій. У Збройних Силах України термін РЕБ [3] включає організацію виконання завдань щодо планування кібероборони України, планування та ведення радіоелектронної боротьби та кіберборотьби, управління радіочастотним спектром (далі – РЧС), розвитком відповідних спроможностей.

РРТР, як невід'ємна частина РЕБ, відіграє ключову роль у виявленні, розпізнаванні та визначенні місцезнаходження джерел активних завад. Вона забезпечує збір оперативних даних про ворожі радіовипромінювання, що є основою для подальших дій РЕБ. Радіоелектронне подавлення, своєю чергою, передбачає безпосередній вплив на радіоелектронні системи противника шляхом електромагнітного випромінювання, застосування оманних цілей, дезінформуючих повідомлень, імітації роботи або зміни умов поширення радіохвиль.

Висновки з аналізу загроз: Проведений аналіз показує, що пасивні перешкоди, хоч і є невід'ємною частиною будь-якого каналу зв'язку, здебільшого піддаються математичному моделюванню та компенсації. Активні перешкоди, навпаки, мають ворожу природу і можуть динамічно адаптуватися до параметрів сигналу, що робить їх надзвичайно небезпечними, особливо для систем з рухомими об'єктами. Традиційні методи боротьби з такими перешкодами мають обмежену ефективність [6]. Це обґрунтовує нагальну потребу у використанні адаптивних фазованих антенних решіток (АФАР), які здатні динамічно змінювати напрямок прийому та випромінювання, формувати провали в діаграмі спрямованості на джерело завади та відновлювати надійний зв'язок навіть у складних умовах.

Для подолання проблем, пов'язаних із частотним дефіцитом, впливом завад та високою щільністю користувачів у мобільних мережах, перспективним напрямом є використання адаптивних антен-

них систем. Ці системи забезпечують динамічне керування діаграмою спрямованості (ДС) антенних решіток залежно від місцеположення джерел сигналу та завад, потужності сигналу та поточних радіоумов. Вони дозволяють формувати вузькі направлені промені у бік абонента, одночасно мінімізуючи випромінювання в напрямку джерел завад. Такий підхід забезпечує просторове розділення користувачів, зменшує рівень міжканальних інтерференцій та безпосередньо підвищує якість сервісу й надійність передачі даних [5; 7; 8].

З точки зору захисту інформації та зменшення вразливості до завад, адаптивні антени дозволяють не лише фокусувати сигнал у потрібному напрямку, а й активно пригнічувати небажані сигнали шляхом формування «нулів» у діаграмі спрямованості у визначених напрямках. Це створює просторовий бар'єр для потенційних злоумисників, відкриваючи широкі можливості для застосування таких систем у військових, критично важливих та спеціалізованих комунікаційних системах, де питання безпеки та захищеності є пріоритетними.

У запропонованому дослідженні розглядається методологія захисту, що базується на використанні просторово-частотної обробки сигналу з АФАР. Підхід передбачає поєднання таких ключових технік:

1) використання засобів РРТР для виявлення, розпізнавання та визначення напрямків на джерела пасивних та активних перешкод;

2) адаптоване керування діаграмою спрямованості антенних решіток засобів зв'язку (як приймальних, так і передавальних) для придушення високопотужних сигналів перешкод та формування максимуму випромінювання сигналу у бік розташування приймальної сторони.

Такий підхід дозволяє зменшити вплив потужних перешкод ще до етапу демодуляції та одночасно збільшити ефективну потужність випромінювання корисного сигналу. Розвиток цифрової техніки обробки сигналів дає змогу будувати складні антенні системи, вихідний сигнал яких формується в результаті обробки сигналів, прийнятих кожним елементом антени [7; 8]. Ця обробка покращує характеристики антени та співвідношення сигнал/перешкода порівняно з антенами без такої обробки. Зокрема, алгоритми обробки дозволяють автоматично пригнічувати перешкоди, що діють у ділянці бічних пелюсток ДС антени, формуючи «провали» у їхньому напрямку. Найважливішими якісними показниками для алгоритмів придушення бічних пелюсток є швидкість адаптації та ступінь придушення перешкод. Отриманий вииграш у співвідношенні сигнал/перешкода залежить від потужностей сигналу та перешкод, їхньої кількості та просторового розташування.

На рис. 1 зображено структурну схему системи зв'язку з використанням АФАР з адаптивним керуванням діаграмами спрямованості.

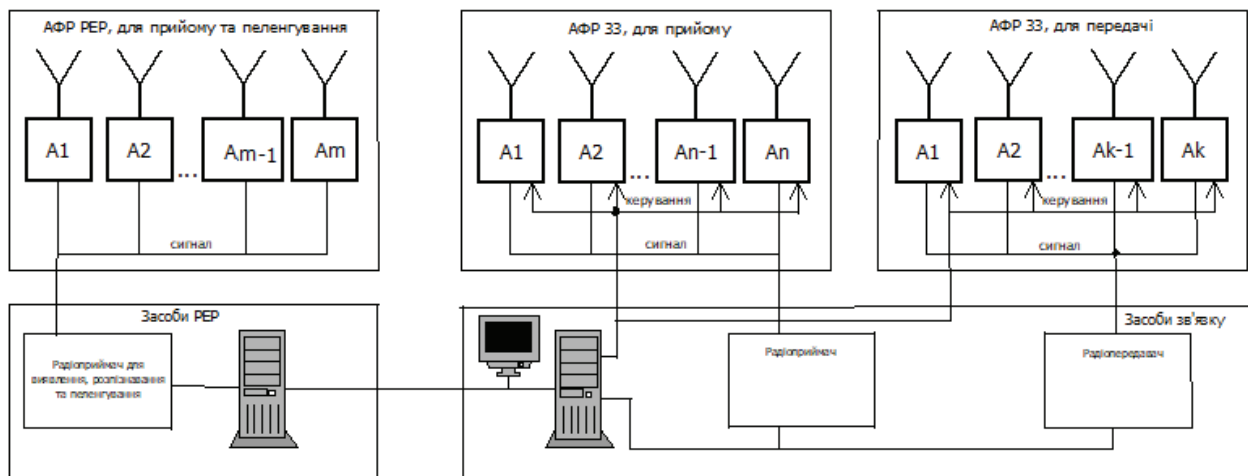


Рис. 1. Структурна схема системи зв'язку з використанням АФАР з адаптивним керуванням діаграм спрямованості

Система зв'язку складається з:

- системи РРТР (радіоелектронної розвідки);
- засобів зв'язку (ЗЗ).

Система РРТР включає:

- антенну систему, яка може бути реалізована як антенною решіткою з елементів $A_1 \dots A_m$, так і просто пеленгаційною антеною;
- радіоприймач, що сканує та виконує функції пеленгування [3];
- систему обробки та керування, призначену для виявлення, розпізнавання та визначення напрямків на джерела активних перешкод, а також передачі цих даних до засобів зв'язку.

Засоби зв'язку включають:

- АФАР з елементів $A_1 \dots A_n$ для прийому;
- АФАР з елементів $A_1 \dots A_k$ для передачі;
- радіоприймач;
- радіопередавач;

– систему обробки та керування, яка отримує дані про джерела активних перешкод, розраховує за цими даними оптимальні діаграми спрямованості АФАР, керує фазообертачами елементів АФАР для формування необхідних ДС, а також управляє радіоприймачем та радіопередавачем.

Принцип дії АФАР полягає в динамічному керуванні характеристиками випромінювання окремих активних антенних елементів. Головна мета – забезпечити максимальну чутливість антени у напрямку корисного сигналу, одночасно мінімізуючи рівень прийому завадових сигналів з інших напрямків. В ідеалі, у напрямках перешкод діаграма спрямованості повинна мати нульове значення, що відповідає повному пригніченню завад. Хоча на практиці досягти абсолютного нуля неможливо, у технічній термінології використовується поняття «нульова характеристика» у напрямку джерел шуму та перешкод.

Для реалізації такого керування характеристиками адаптивного антенного масиву застосовуються спеціальні алгоритми, які можна розділити на кілька основних категорій, зазначених нижче.

1. Алгоритми на основі кореляційної матриці.

Кожен активний елемент антенного масиву оснащений власним приймачем. На основі сигналів, прийнятих усіма елементами, формується кореляційна матриця, за якою розраховуються оптимальні вагові коефіцієнти, що максимізують співвідношення корисного сигналу до сумарних перешкод і шуму (SINR). Цей підхід є одним із найефективніших, оскільки використовує повну інформацію про прийняті сигнали, проте вимагає більшої кількості приймачів та регулярної калібровки.

2. Алгоритми, засновані на апріорній інформації про джерело перешкод.

Базуються на точних відомостях про напрямок джерела перешкод та характеристики елементів антени (атенюаторів, фазообертачів). На основі цієї інформації система математично визначає ваги, які формують «нуль» у напрямку завади. Цей метод ефективний за наявності достовірних даних про джерело перешкоди, для отримання яких пропонується використовувати засоби РРТР.

3. Алгоритми випадкового перебору.

Передбачають випадковий перебір різних варіантів налаштування вагових коефіцієнтів для антенного масиву. Хоча теоретично цей метод може призвести до оптимального рішення, він вимагає значного часу на обчислення, що робить його непридатним для систем реального часу.

4. Алгоритми математичної оптимізації (градієнтні методи).

Вагові коефіцієнти елементів антени обираються так, щоб мінімізувати загальну потужність на виході адаптивної системи. Зазвичай для цього формується вектор градієнта, який послідовно підбирає вагові коефіцієнти для досягнення мінімуму потужності, знижуючи рівень шуму та перешкод.

Таким чином, адаптивні алгоритми забезпечують ефективне управління характеристиками антенного масиву, підвищуючи якість прийому корисного сигналу навіть у складних умовах із наявністю значних перешкод.

Висновки

Проведене дослідження підтверджує, що використання адаптивних фазованих антенних решіток (АФАР) є ефективним методом для значного підвищення стійкості бездротових систем зв'язку до впливу активних завад. Завдяки здатності до динамічного керування діаграмою спрямованості, АФАР посилює корисний сигнал та ефективно пригнічує перешкоди, що є особливо критичним в умовах швидкоплинних змін у радіоелектронному середовищі.

Як показують попередні дослідження (або: за результатами проведеного аналізу /моделювання), сумарний виграш від адаптивних фазованих антенних решіток у системах мобільного чи супутникового зв'язку може сягати:

- 6–15 дБ за рахунок спрямованості (конструктивний виграш);
- 10–20 дБ за рахунок активного подавлення перешкод.

Таким чином, загальний виграш у системі може становити 20–30 дБ при використанні АФАР у порівнянні з всеспрямованою антеною. Це суттєво покращує стійкість до завад, ефективність передачі та захист від цілеспрямованих атак. Інтеграція АФАР із системами РРТР для оперативного виявлення та пеленгування джерел завад є ключовим фактором для реалізації їх повного потенціалу.

Перспективи подальших досліджень можуть включати наступне.

Проведення додаткових експериментів для оцінки ефективності запропонованих захисних механізмів у різних реальних сценаріях.

Удосконалення програмних моделей та алгоритмів керування адаптивними фазованими антенними решітками з метою підвищення їх продуктивності та швидкості адаптації.

Придільнення особливої уваги інтеграції захисних рішень на фізичному та програмному рівнях для створення комплексних систем захисту з підвищеним рівнем безпеки та надійності.

Загалом, подальший розвиток цієї галузі сприятиме значному посиленню захищеності бездротових систем зв'язку та підвищенню їх ефективності в умовах сучасного, насиченого інформаційного середовища.

Література

1. Головне управління радіоелектронної та кібербороти. *Офіційний веб-сайт МО*. URL: <https://www.mil.gov.ua/ministry/struktura-generalnogo-shtabu/golovne-upravlinnya-radioelektronnoi-ta-kiberborotbi.html>
2. Довідник військового зв'язківця. Засоби радіоелектронної боротьби та розвідки, які використовуються російською федерацією. Київ : ЦУЛ, 2024. 64 с.
3. Голобородько Ю. М., Радіоконтроль діапазону Short Waves, Research in Science, Technology and Economics : collection of Scientific Papers. *International Scientific Unity* : Proceedings of the 2nd International Scientific and Practical Conference (March 5–7, 2025. Luxembourg). Luxembourg. 397 p. Pp. 275–278. ISBN 979-8-89704-985-1 (series). DOI: <https://doi.org/10.70286/ISU-05.03.2025>.
4. Короткохвильовий радіозв'язок : настанова. Київ : ЦУЛ, 2024. 83 с.
5. Omelchenko V. A. Balabanov V. V. Bezruk V. M. Goloborod'ko Ju. N. Detection of Changes in the Random Signal Properties by Spectral Methods Under the Conditions of A Priori Uncertainty. *Telecommunications and Radio Engineering*. 1999. 53 (9–10). P. 1–10.
6. Заславець В. П., Долина М. П., Чечуй О. В. Особливості розрахунку завадозахищеності ліній радіозв'язку в умовах радіоподавлення (радіоелектронного конфлікту). DOI: <https://doi.org/10.30748/soivt.2020.61.01>.
7. Пресняков І. М., Ситник О. В. Алгоритм адаптивного формування діаграми напрямленості антенної решітки в умовах інтенсивних сигналів і перешкод. *Радіотехніка* : міжвідомчий науково-технічний збірник. 1988. Вип. 87. С. 71–78.
8. Плющ О. Г., Рибидайло А. А. Алгоритм налаштування адаптивної антенної решітки, який не потребує присутності опорного сигналу. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2019. № 2 (66). С. 108–114.

References

1. Holovne upravlinnia radioelektronnoi ta kiberborotby. *Ofitsiyni veb-sait MO* [Main Directorate of Radio Electronic and Cyber Warfare. *Official website of the Ministry of Defense*]. URL: <https://www.mil.gov.ua/ministry/struktura-generalnogo-shtabu/golovne-upravlinnya-radioelektronnoi-ta-kiberborotbi.html> [in Ukrainian].
2. Dovidnyk viiskovoho zv'iazkivtsia. Zasoby radioelektronnoi borotby ta rozvidky, yaki vykorystovuiutsia rosiiskoiu federatsiiei. Kyiv : "TsUL", [Military Signaller's Handbook. Electronic Warfare and Intelligence Means Used by the Russian Federation. Kyiv : "TsUL"], 2024. 64 p. [in Ukrainian].
3. Holoborodko Y. M., Radiokontrol' diapazonu Short Waves. [Short Wave Radio Monitoring]. Research in Science, Technology and Economics : collection of Scientific Papers. *International Scientific Unity* : Proceedings of the 2nd International Scientific and Practical Conference (March 5–7, 2025. Luxembourg). Luxembourg. 397 p. Pp. 275–278. ISBN 979-8-89704-985-1 (series). DOI: <https://doi.org/10.70286/ISU-05.03.2025>.
4. Korotkikhvyl'nyi radiozviazok: nastanova. Kyiv : "TsUL", [Shortwave radio communication: a guide. Kyiv : "TsUL"] 2024. 83 p. [in Ukrainian].
5. Omelchenko V. A. Balabanov V. V. Bezruk V. M. Goloborod'ko Ju. N., Detection of Changes in the Random Signal Properties by Spectral Methods Under the Conditions of A Priori Uncertainty. *Telecommunications and Radio Engineering*. 1999. 53 (9–10). Pp. 1–10.
6. Zaslavets V. P., Dolyna M. P., Chechui O. V. Osoblyvosti rozrakhunku zavadozakhyshchenosti linii radiozviazku v umovakh radiopodavleniia (radioelektronnoho konfliktu) [Peculiarities of calculating the interference immunity of radio communication lines in conditions of radio suppression (radioelectronic conflict)]. URL: <https://doi.org/10.30748/soivt.2020.61.01> [in Ukrainian].
7. Presniakov I. M., Sytnyk O. V. Alhorytm adaptynoho formuvannia diahramy napriamlenosti antennoi reshitky v umovakh intensyvnykh syhnaliv i pereshkod [Algorithm for adaptive formation of the antenna array directivity diagram in conditions of intense signals and interference]. *Radio engineering, interdepartmental scientific and technical collection*. 1988. 87. P. 71–78 [in Ukrainian].
8. Pliushch O. H., Rybydailo A. A. Alhorytm nalashtuvannia adaptynoi antennoi reshitky, yakyi ne potrebuie prysutnosti opornoho syhnalu [Adaptive antenna array tuning algorithm that does not require the presence of a reference signal]. *Collection of scientific papers of the Center for Military and Strategic Studies of the Ivan Chernyakhovsky National Defense University of Ukraine* 2019. № 2 (66). P. 108–114 [in Ukrainian].

Дата першого надходження статті до видання: 27.10.2025
 Дата прийняття статті до друку після рецензування: 26.11.2025
 Дата публікації (оприлюднення) статті: 26.12.2025