

**Крючкова Лариса Петрівна**

доктор технічних наук, професор

професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0000-0002-8509-6659

l.kriuchkova@kubg.edu.ua

Ворохоб Нікіта Олександрович

магістр

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0009-0006-3623-7386

novorokhob.fitm24m@kubg.edu.ua

АДАПТИВНІ МЕТОДИ ПРОТИДІЇ АКТИВНИМ ШУМОВИМ ЗАВАДАМ

Анотація. Ефективність виконання польотної місії безпілотним літальним апаратом на заданій відстані вирішальним чином залежить від якісного управління, контролю телеметрії та передачі даних безпілотним літальним апаратом, які, в свою чергу, визначаються якістю радіозв'язку між наземною станцією управління та безпілотним літальним апаратом. Разом з тим, сучасні радіоелектронні системи військового призначення функціонують, як правило, в умовах складної радіоелектронної обстановки, обумовленої впливом як внутрішньосистемних і зовнішніх завад, так і засобів радіоелектронного подавлення противника. Застосовуються активні завади різного типу та призначення, спрямовані на виведення із ладу каналів управління, каналів навігації, каналів телеметрії та каналів передачі даних безпілотних літальних апаратів, зокрема FPV-дронів, що обумовлює необхідність пошуку та впровадження новітніх методів протидії, здатних забезпечити стабільне функціонування безпілотних літальних апаратів та FPV-дронів в умовах активного інформаційного протистояння. У статті розглянуто сучасні підходи до протидії активним шумовим завадам в системах управління FPV-дронами. Обґрунтовано актуальність проблеми, зумовлену зростанням масштабів використання безпілотних літальних апаратів у військовій та цивільній сферах, а також підвищенням ефективності засобів радіоелектронного подавлення. Проаналізовано традиційні методи захисту та виявлено їхні обмеження у динамічних умовах інформаційного протистояння. Представлено результати дослідження адаптивних фільтрів LMS та RLS, просторових методів селекції сигналів (MVDR, LCMV), а також застосування алгоритмів машинного навчання для виявлення й нейтралізації сигналів подавлення. Показано, що поєднання адаптивних та інтелектуальних методів забезпечує підвищення стійкості каналів зв'язку та зниження ризику втрати керування дронами. Зроблено висновок про доцільність використання гібридних рішень, які інтегрують класичні алгоритми цифрової обробки сигналів з методами штучного інтелекту.

Ключові слова: завадозахищеність; радіоподавлення; spoofing; jamming; радіоелектронна боротьба, методи протидії; методи захисту; системи CRPA.

ВСТУП

Стрімкий розвиток інформаційних технологій, засобів зв'язку та безпілотних систем обумовлює зростання масштабів і складності сучасних інформаційних протистоянь. У військовій, економічній та цивільній сферах дедалі більшого значення набуває поняття інформаційного конфлікту, у рамках якого сторони реалізують комплекс заходів, спрямованих на перехоплення, спотворення, знищення чи блокування інформаційних потоків. Основним інструментом у таких протистояннях виступають засоби



радіоелектронної боротьби (РЕБ), серед яких особливу загрозу становлять активні шумові завади.

У сучасних умовах застосування активних завад не обмежується лише військовими операціями. Подібні технології активно використовуються для перешкоджання роботі бездротових мереж, мобільного зв'язку, систем позиціонування та управління, що свідчить про універсальний характер даної загрози. Водночас, у військовій сфері проблема протидії активним шумовим завадам набула особливої актуальності у зв'язку з масовим використанням безпілотних літальних апаратів (БпЛА), зокрема FPV-дронів (First Person View). Ці апарати стали важливим елементом тактичної розвідки та виконання ударних завдань, проте їхня ефективність суттєво залежить від стійкості каналів радіозв'язку.

Викладене обумовлює необхідність пошуку та впровадження новітніх методів протидії, здатних забезпечити стабільне функціонування БпЛА та FPV-дронів в умовах активного інформаційного протиборства.

Постановка проблеми та її зв'язок із важливими науковими та практичними завданнями.

Забезпечення стійкості систем зв'язку та управління в умовах навмисного радіоелектронного впливу є однією з ключових проблем сучасних інформаційних технологій та воєнної науки. Сучасні засоби активного радіоелектронного подавлення характеризуються високим рівнем потужності, широкосмуговістю та здатністю до динамічної зміни спектральних параметрів. Це робить їх ефективними інструментами у процесі дезорганізації каналів зв'язку, що особливо критично у випадку використання як ударних БпЛА, так і FPV-дронів.

Серед найбільш поширених типів активних завад можна виокремити:

- широкосмуговий шум (Broadband Jammers), який перекриває широкий діапазон частот і здатний блокувати як канали відеопередачі, так і канали управління;
- прицільна завада (Directional Jammers), що створює локалізоване завадове поле у напрямку конкретної цілі;
- спуфінг-системи, які не лише блокують сигнал, але й підмінюють його, вводячи систему управління БпЛА в оману.

Традиційні підходи до захисту систем зв'язку від активних шумових завад базуються на використанні:

- методів частотного рознесення сигналів (frequency hopping, DSSS), які передбачають стрибкоподібну зміну робочих частот;
- корекційного кодування, спрямованого на зменшення впливу шумів та збереження корисної інформації;
- фільтраційних алгоритмів, що відсіюють завадові компоненти на основі попередньо відомих параметрів.

Однак зазначені підходи мають низку обмежень. По-перше, вони не враховують змінність параметрів завад у реальному часі. По-друге, такі методи потребують додаткових ресурсів – збільшення ширини смуги сигналу, складних схем синхронізації або потужних обчислювальних засобів, що не завжди прийнятно для малогабаритних та енергетично обмежених платформ, якими є FPV-дрони. По-третє, існує проблема адаптації зазначених методів до багатоканальних та багатопроменевих середовищ, характерних для міських і бойових умов.

Особливу складність становить також класифікація та ідентифікація завад. У реальних сценаріях протиборства спектральні характеристики завад можуть змінюватися випадково або цілеспрямовано, що ускладнює їх виявлення стандартними методами



спектрального аналізу. Це призводить до того, що система зв'язку витрачає надмірні ресурси на боротьбу з неактуальними або неправильно визначеними типами завад.

Зазначене дозволяє зробити висновок, що традиційні методи захисту, побудовані на використанні статичних алгоритмів фільтрації чи кодових методів підвищення завадостійкості, не гарантують належного рівня ефективності [1-7]. Їхня обмеженість пов'язана з тим, що характеристики завад є динамічними, а отже, необхідно застосовувати методи, які здатні оперативно адаптуватися до змін умов середовища.

Застосування адаптивних методів протидії активним шумовим завадам дозволяє:

- Автоматично виявляти характеристики активних шумових завад у режимі реального часу. Підлаштовувати параметри алгоритмів обробки сигналів залежно від спектральних, часових та статистичних властивостей завад.
- Оптимізувати співвідношення сигнал/шум (SNR) та забезпечувати мінімізацію ймовірності помилок (BER) у каналах передачі даних.
- Функціонувати в умовах обмежених ресурсів FPV-дронів – обчислювальних, енергетичних і частотних.

Таким чином, дослідження адаптивних методів протидії активним шумовим завадам є складним і багатогранним завданням, яке поєднує в собі елементи радіотехніки, цифрової обробки сигналів, теорії інформації та кібербезпеки. Його результатом має стати створення алгоритмів і моделей, здатних забезпечити стійке функціонування FPV-дронів у складних умовах інформаційного протиборства, що, у свою чергу, відкриває перспективи для подальшого розвитку технологій захищеного зв'язку та систем автономного управління [8-10].

Наукова проблема полягає у розробці та вдосконаленні адаптивних методів протидії активним шумовим завадам, які забезпечать стабільність та ефективність функціонування БПЛА та FPV-дронів у реальних умовах інформаційного протиборства.

Дослідження проведено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022)."

Аналіз останніх досліджень і публікацій. Аналіз сучасних радіоелектронних засобів в аспекті постановки активних завад проведено на основі відкритих публікацій та відомостей із пошукових сайтів мережі Інтернет [1-17].

В даний час є кілька системних стратегій в частині формування радіозавад: широкосмугові загороджувальні завади; завади у частині смуги; слідкуючі, прицільні за частотою завади; імпульсні завади; ретрансльовані завади [1-17]. Різноманітність видів активних завад зумовлено прагненням розробників сконцентрувати обмежену потужність станцій завад у вузьких інтервалах частоти і часу.

Атаки з використанням подавлення корисних радіосигналів можна розділити на п'ять основних категорій залежно від схеми атаки:

- *Постійне подавлення:* сигнал подавлення безперервно передається на тій частоті, яку використовують пристрої, зв'язок яких вона хоче порушити [1].
- *Періодичне подавлення:* сигнал подавлення передається протягом певного періоду часу to n , а потім припиняється на інший період часу to ff . Зазначений цикл повторюється доти, доки атака не закінчиться [11].
- *Випадкове подавлення:* при випадковому подавленні сигнал подавлення активується у випадкові інтервали часу, перешкоджаючи передачі пакетів з ймовірністю p , заснованою на випадковому шаблоні [12].



- *Реактивне подавлення*: сигнал подавлення починає передаватись тільки після виявлення наявності енергії в каналі зв'язку, що вказує на те, що відбувається передача інформації. Очевидно, що зазначений тип атаки подавлення більш енергоефективний порівняно з іншими схемами атак [13].
- *Інтелектуальне подавлення*: полягає у здатності адаптувати сигнал подавлення для максимального порушення зв'язку між пристроями. Коригування схеми атаки забезпечується використанням модуля аналізу трафіку, який відслідковує особливості передачі цільових даних пристроїв і формує відповідний сигнал подавлення [14].

Виходячи з аналізу досліджень і публікацій, радіоелектронні конфлікти є однією з найактуальніших загроз для сучасних технологій управління БпЛА, а завдання дослідження адаптивних методів протидії активним шумовим завадам є актуальним і необхідним для підвищення стійкості радіоканалів управління та передачі даних.

Метою публікації є систематизація і аналітичний огляд методів адаптивної протидії активним шумовим завадам для виявлення перспективних напрямків їх розвитку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Методи розширення спектра сигналу

У загальному випадку метод розширення спектра сигналу є методом передачі інформації, при використанні якого радіосигнал займає смугу частот значно ширшу порівняно з мінімально необхідною для передачі інформації. При цьому на передавальній стороні здійснюється модуляція параметрів сигналу повідомлення функцією, що задається псевдовипадковою послідовністю, а на приймальній стороні – синхронна демодуляції сигналу відповідно такою ж функцією і відновлення переданого повідомлення [15].

Теоретичною основою застосування методу розширення спектра сигналу є фундаментальна формула К.Е. Шеннона, що зв'язує пропускну здатність каналу (C , біт/с), відведену смугу частот (W_s , Гц) та співвідношення сигнал/завада (P_s/P_i) [16]:

$$C = W_s \log_2(1 + P_s/P_i)$$

з якої було зроблено два важливі висновки. Перший полягає в тому, що підвищити пропускну здатність будь-якої системи зв'язку можна за рахунок відповідного збільшення відношення сигнал/шум, другий – в тому, що при певному розширенні смуги сигналу (каналу) відношення сигнал/шум може виявитися меншим 1, так зване "приймання під шумом".

Основними методами розширення спектра сигналу, які широко застосовуються в сучасних системах радіозв'язку, є [17]:

1. Метод псевдовипадкової перебудови робочої частоти – ППРЧ (метод FHSS), різновидом якого є метод адаптивної ППРЧ – АППРЧ.
2. Метод безпосередньої модуляції несучої псевдовипадковою послідовністю (метод DSSS). Наприклад, M -послідовності.
3. Метод псевдовипадкової часоімпульсної модуляції.
4. Комплексний метод – спільне застосування різних методів розширення спектра сигналу та ін.



Frequency Hopping Spread Spectrum (FHSS) [17] – метод розширення спектра сигналу, що базується на принципі псевдовипадкової перебудови робочої частоти. Передавач і приймач узгоджено змінюють несучу частоту сигналу відповідно до PRN-послідовності, відомої обом сторонам. У кожному часовому інтервалі передача здійснюється на іншій частоті в межах широкого діапазону, що дозволяє ефективно розподіляти енергію сигналу. Існують два режими реалізації методу: *Slow FHSS*, коли кілька біт передається на одній частоті, після чого відбувається стрибкоподібна зміна частоти, та *Fast FHSS*, у якому частота змінюється кілька разів під час передачі одного біта, що робить систему ще менш вразливою.

До переваг методу FHSS належить висока стійкість до вузькосмугових завад, оскільки для того, щоб зашкодити передачі інформації, активна завада має перекривати весь спектр. Варто зазначити, що метод FHSS забезпечує також захист інформації від перехоплення: без знання PRN-послідовності складно синхронізувати прийом і правильно відновити дані. Технологія FHSS підтримує мультимедіа (різні користувачі можуть працювати з різними кодами), а також зменшує вплив багатопроменевих спотворень, оскільки стрибкоподібна зміна частоти частоти дозволяє уникати глибоких провалів у спектрі (frequency fading).

Водночас метод FHSS має і недоліки. Основною проблемою є складність синхронізації, адже необхідне точне узгодження PRN-кодів між передавачем і приймачем. Метод FHSS залишається вразливим до широкосмугового шумового джеміну, якщо противник генерує суцільний шум у всьому робочому діапазоні. Крім того, метод обмежує швидкість передачі даних, оскільки тривалість стрибка (hop rate) напряму визначає максимальну пропускну здатність системи.

Direct Sequence Spread Spectrum (DSSS) [18] – розширення спектра сигналу методом прямої послідовності. Сутність методу полягає в підвищенні тактової частоти модуляції, при цьому кожному символу переданого повідомлення ставиться у відповідність деяка досить довга псевдовипадкова послідовність (PN-послідовність). Унаслідок цього сигнал розтягується на ширший спектр, а на приймальній стороні відновлення здійснюється через кореляцію з тією ж самою PN-послідовністю. Завдяки такому підходу DSSS має значно вищу швидкість і забезпечує більш досконалу обробку (10–30 дБ і більше), що фактично підвищує співвідношення сигнал/шум після декодування.

Метод демонструє високу стійкість до вузькосмугових завад, адже після декодування вони рівномірно розподіляються по спектру й втрачають ефективність. Ще однією перевагою є захист від перехоплення: без знання PN-послідовності DSSS-сигнал сприймається як шум. Крім того, метод дозволяє реалізувати мультимедіа на основі CDMA, коли різні користувачі працюють із різними кодами, зберігаючи сумісність у спільному спектрі.

Разом з тим, технологія DSSS має і низку обмежень. По-перше, вона висуває високі вимоги до синхронізації як у часовій, так і у фазовій області, адже навіть невеликі похибки можуть зруйнувати кореляційне відновлення. По-друге, DSSS залишається вразливою до високоінтенсивних широкосмугових завад, хоча частково ця проблема компенсується за рахунок більш досконалої обробки. Ще однією складністю є генерація довгих і водночас ортогональних PN-послідовностей, особливо при великій кількості користувачів, що обмежує масштабованість системи.

Chirp Spread Spectrum (CSS) [19] – метод розширення спектру сигналу, що ґрунтується на використанні лінійно-частотної модуляції (ЛЧМ), коли частота сигналу змінюється у часі лінійно, як у напрямку зростання, так і спадання. Інформація кодується у зсуві початкової фази або частоти ЛЧМ, що створює унікальний часово-частотний



профіль сигналу. Яскравим прикладом реалізації цього принципу є технологія зв'язку LoRa (Long Range), у якій дані передаються шляхом зміщення у часово-частотному просторі ЛЧМ, що дозволяє забезпечувати надзвичайну стійкість до завад.

Серед головних переваг методу CSS варто відзначити його високу робастність до впливу шуму: навіть при дуже низькому співвідношенні сигнал/шум (LoRa здатна працювати при $\text{SNR} \approx -20$ дБ) приймач може відновити передану інформацію. До плюсів також належить простота реалізації, оскільки немає потреби у генерації довгих псевдовипадкових послідовностей, характерних для DSSS. CSS забезпечує високу дальність передачі при низькій швидкості даних, що робить його придатним для сенсорних і IoT-мереж, а також відрізняється стійкістю до мультипасажу, оскільки ЛЧМ має добру відокремлюваність навіть у складних канальних умовах.

Водночас метод має й обмеження. Найсуттєвіший недолік – низька швидкість передачі, оскільки вона навмисно зменшується задля досягнення робастності. Крім того, метод CSS є вразливим до спеціально синхронізованих завад, коли противник застосовує сигнали подавлення, синхронізовані з оригінальним сигналом. Також у CSS нижчий рівень захисту від перехоплення у порівнянні з FHSS чи DSSS, адже структура ЛЧМ є більш передбачуваною для сторонніх спостерігачів.

Time-Hopping Spread Spectrum (THSS) [20] – метод розширення спектра, у якому сигнал формується у вигляді дуже коротких імпульсів, а кожний імпульс передається у випадковому часовому інтервалі, що визначається псевдовипадковою послідовністю (PN-кодом). Завдяки такому підходу енергія сигналу розподіляється у часовій області, що робить його подібним шуму для стороннього спостерігача. Найчастіше THSS використовується в ультраширокопосмугових (UWB) системах, де надзвичайно широкі смуги частот поєднуються з надкороткими імпульсами тривалістю наносекунд.

Серед переваг THSS можна виділити низьку енергетичну спектральну щільність (PSD), завдяки якій сигнал виглядає як фоновий шум і стає важким для виявлення чи перехоплення. Метод також забезпечує високу стійкість до вузькосмугового джеміну, оскільки окремі імпульси розкидані в часі й не піддаються ефективному перекриттю вузькою завадою. Крім того, THSS має добру точність позиціонування, що особливо цінно для систем indoor-навігації на базі UWB.

Разом із тим, технологія має і суттєві недоліки. Найбільшим викликом є високі вимоги до синхронізації по часу, адже приймач має точно знати часові зсуви імпульсів для їх коректного прийому. Додатковою проблемою є складність апаратної реалізації, оскільки робота з наносекундними імпульсами потребує високошвидкісних схем. Також THSS демонструє низьку стійкість до широкопосмугового шуму, який може одночасно впливати на значну кількість імпульсів.

Щодо практичного застосування, THSS активно використовується в UWB-зв'язку (стандарти IEEE 802.15.4a, IEEE 802.15.6), а також у військових системах ближнього радіозв'язку з низькою помітністю, де важлива прихованість передачі й стійкість до спеціальних методів радіоелектронного подавлення.

Quadrature Spread Spectrum (QSS) [21] – метод розширення спектра, у якому використовується принцип ортогональних або квазіортогональних послідовностей для передачі сигналу. На відміну від класичного DSSS, у QSS дані розподіляються між I- та Q-каналами, кожен із яких модулюється власною PN-послідовністю. Такий підхід часто поєднується з модуляціями QPSK чи QAM, що дозволяє одночасно підвищувати ефективність використання спектра та досягати більшої швидкості передачі даних.

Серед головних переваг QSS варто відзначити ефективніше використання спектра в порівнянні з традиційним DSSS. Використання ортогональних послідовностей у I/Q-



каналом забезпечує вищу стійкість до багатопроменевих завад, оскільки приймач здатний розділяти канали й коректно відновлювати дані навіть у складному радіосередовищі. Крім того, QSS дає можливість збільшувати швидкість передачі, поєднуючи розширення спектра із сучасними модуляційними схемами.

Водночас існують і певні недоліки. По-перше, синхронізація значно складніша, оскільки потрібно узгоджувати як I/Q-канали, так і відповідні PN-послідовності. По-друге, система виявляється вразливою до міжсимвольних інтерференцій (ISI) у випадках сильного мультипасажу, що може погіршувати якість передачі.

Приклади практичного застосування QSS включають військові системи зв'язку, де використовуються DSSS/PSK-модуляції, а також дослідження в області MIMO-CDMA, де QSS дозволяє поєднати переваги багатокористувацького доступу й просторового рознесення.

Hybrid Spread Spectrum (FH/DSSS, FH/TH, DSSS/TH) [22] – метод розширення спектра, який базується на комбінуванні двох або більше технік, наприклад DSSS та FHSS. Такий підхід дозволяє одночасно отримати вигоду від використання різних принципів: DSSS забезпечує високий рівень завадостійкості завдяки кореляційній обробці сигналу, тоді як FHSS додає маскування через псевдовипадкову зміну робочих частот. У результаті утворюється багаторівневий захист, який підвищує ефективність системи в умовах складного спектрального середовища.

До основних переваг *Hybrid Spread Spectrum* належить високий рівень захищеності від різних типів джеміну: шумових, реактивних і вузькосмугових завад. Завдяки гнучкій архітектурі метод дозволяє адаптуватися під різні сценарії застосування, а також підтримує мультимедіа, використовуючи ортогональні коди та різні схеми перестрибування. Така комбінація робить *Hybrid Spread Spectrum* особливо ефективним у військових системах, де важлива робастність і надійність у середовищі з інтенсивною радіоелектронною протидією.

Недоліками цієї технології є насамперед висока апаратна складність. Для реалізації потрібно синхронізувати кілька PN-послідовностей і координувати роботу частотних та часових стрибків. Це тягне за собою збільшені вимоги до енергоспоживання та ускладнює застосування в малогабаритних чи енергообмежених платформах, таких як FPV-дрони. Крім того, складність синхронізації кількох процесів одночасно підвищує ймовірність збоїв.

Прикладами застосування є система JTIDS/Link-16, яка використовується країнами НАТО, а також інші військові мережі зв'язку, де потрібна підвищена стійкість до завад і відповідність високим стандартам ECCM (Electronic Counter-Counter Measures).

Ultra-Wideband (UWB) [23] – технологія передачі даних, яка базується на використанні надзвичайно коротких імпульсів тривалістю наносекунди. За стандартом FCC, ширина спектра UWB перевищує 500 МГц, що робить сигнал надзвичайно широкосмуговим. Завдяки цьому він має вигляд випадкового шуму й дуже важко виявляється противником, що надає системам UWB властивість низької ймовірності перехоплення.

До основних переваг цієї технології належить висока скритність і завадостійкість: широкосмуговий сигнал практично неможливо ефективно заглушити вузькосмуговими засобами РЕБ. Крім того, UWB добре працює у складних умовах мультипасажу, оскільки відбиті сигнали легко розділяються у часі. Ще однією важливою перевагою є надзвичайно висока точність позиціонування — до кількох сантиметрів, що робить технологію унікальною для систем навігації та трекінгу.



Водночас UWB має низку суттєвих недоліків. Найважливішим є складність апаратної реалізації: потрібно генерувати наносекундні імпульси та використовувати ширококутові антени, що ускладнює і здорожчує апаратуру. Крім того, система має обмежену дальність дії, яка прямо залежить від рівня потужності випромінювання. Існують також жорсткі регуляторні обмеження (FCC, ЄС), які лімітують використання UWB у певних частотних діапазонах і обмежують рівень випромінюваної потужності.

Серед прикладів застосування можна виділити системи позиціонування і навігації всередині приміщень та відстеження рухомих об'єктів, де UWB дозволяє досягати сантиметрової точності позиціонування; військовий зв'язок ближньої дії, де важлива низька помітність та стійкість до завад; а також високоточні радарні системи, що працюють на принципах ультраширококутового аналізу відбитих імпульсів.

Multicarrier Spread Spectrum (MC-SS) [24] – метод передачі даних, що ґрунтується на використанні багатьох піднесучих (наприклад, у схемах OFDM), між якими енергія сигналу розподіляється псевдовипадковим чином. Такий підхід дозволяє не лише розширити спектр, а й забезпечити додаткову гнучкість у його використанні. Одним із відомих варіантів цього підходу є MC-CDMA (Multicarrier Code Division Multiple Access), де кодове розширення поєднується з багатонесучою структурою для підтримки багатокористувацького доступу.

Перевагами MC-SS є висока стійкість до багатопроменевих спотворень, можливість гнучкого керування спектром і висока пропускна здатність, що робить цей метод надзвичайно актуальним для сучасних безпроводових інформаційних систем. Недоліки методу: вразливість до синхронізованих сигналів подавлення, які можуть цілеспрямовано атакувати окремі піднесучі; складність апаратної реалізації, оскільки OFDM поєднується із кодовим розширенням; високий рівень PAPR (*peak-to-average power ratio*), що знижує енергоефективність і ускладнює проектування підсилювачів потужності.

Прикладами застосування MC-SS є системи LTE, 5G, Wi-Fi (особливо у військових модифікаціях), а також MC-CDMA, що використовується для забезпечення багатокористувацького доступу в ширококутових мережах.

Chaos-Based Spread Spectrum (CBSS) [25] – метод розширення спектра, який базується на використанні хаотичних нелінійних послідовностей, згенерованих нелінійними динамічними системами. На відміну від традиційних PN-послідовностей, хаотичні сигнали мають властивість надзвичайної чутливості до початкових умов, що робить їх майже неможливими для передбачення навіть у разі знання базового алгоритму. Сигнал у такій системі виглядає як некогерентний шум, проте між передавачем і приймачем, які мають однакові початкові параметри, можлива синхронізація, що дозволяє правильно відновлювати дані.

Основна перевага хаотичного розширення спектра – високий рівень скритності (*low probability of detection*, LPD) і низька ймовірність перехоплення (*low probability of intercept*, LPI). Для стороннього спостерігача сигнал виглядає випадковим, що суттєво ускладнює завдання його виявлення та демодуляції. Крім того, завдяки широкому спектру і непередбачуваності, CBSS має високу стійкість до цілеспрямованого подавлення й може витримувати навіть складні атаки, оскільки противник не знає точної структури сигналу. Додатковою перевагою є велика кількість можливих хаотичних функцій, що дає змогу будувати різноманітні системи з різними рівнями складності.

До недоліків варто віднести наступне. По-перше, генерація хаотичних сигналів вимагає надзвичайно високої точності апаратури, адже навіть невелика похибка у відтворенні початкових параметрів може призвести до втрати синхронізації. По-друге, на практиці виникають труднощі з відтворюваністю хаотичних послідовностей: теоретичний



хаос легко описується математично, але у реальному обладнанні він спотворюється шумами, неточністю генераторів і нестабільністю апаратних компонентів. Третім недоліком є відсутність стандартизації, що обмежує практичне використання методу.

Хаотичні методи застосовуються в експериментальних системах ECCM (*Electronic Counter-Counter Measures*), де головною метою є підвищення скритності та захищеності каналу зв'язку. CBSS також досліджується у сфері секретних комунікацій і UWB-системах, де хаотичні імпульси використовуються для формування сигналів із дуже низькою спектральною густиною потужності, які практично неможливо відрізнити від фонового шуму. Наукові розробки у цій галузі активно ведуться в університетських лабораторіях і дослідницьких центрах, але для масового впровадження потрібні як апаратні прориви, так і стандартизація.

Adaptive Spread Spectrum – перспективний підхід до побудови захищених систем зв'язку, який базується на когнітивному радіо та динамічній зміні техніки розширення спектра залежно від рівня і типу завад. Ідея полягає в тому, що система не обмежується одним методом (FHSS, DSSS, OFDM чи UWB), а може адаптивно перемикаватися між ними або комбінувати їх у реальному часі. Вибір здійснюється на основі аналізу середовища: система постійно оцінює якість каналу, спектральні характеристики завад і на основі цього приймає рішення про оптимальну стратегію.

Переваги цього підходу очевидні. По-перше, це максимальна гнучкість: система може підбирати метод розширення спектра під конкретний сценарій, забезпечуючи оптимальний баланс між стійкістю до подавлення, швидкістю передачі та енергоефективністю. По-друге, такі системи мають високу робастність у динамічному середовищі, де типи завад змінюються у реальному часі. По-третє, *Adaptive Spread Spectrum* розглядається як один із ключових напрямів розвитку ECCM і вже сьогодні активно вивчається в рамках програм НАТО та DARPA.

Втім, *Adaptive Spread Spectrum* має і серйозні недоліки. По-перше, його реалізація вимагає створення повноцінної когнітивної радіосистеми, здатної в реальному часі аналізувати середовище, приймати рішення та перебудовувати власні параметри. Це створює високі вимоги до обчислювальних ресурсів і енергоспоживання, що особливо несприятливо для мобільних платформ, таких як дрони чи переносні радіостанції. По-друге, тестування таких систем у реальних бойових умовах є дуже складним: необхідно враховувати широкий спектр завад, мобільність, обмежені ресурси й непередбачувану поведінку противника.

Прикладом застосування *Adaptive Spread Spectrum* є військові когнітивні системи зв'язку (програми DARPA, стандарти НАТО), де від системи вимагається стійкість навіть у найскладніших умовах радіоелектронного протистояння. У цивільній сфері адаптивні методи розглядаються як один із базових елементів 6G, де когнітивні мережі повинні забезпечувати не лише високу пропускну здатність, а й робастність до завад і гнучке керування спектром.

Адаптивні методи обробки сигналів

Важливим напрямом підвищення стійкості радіосистем до активних завад є застосування *адаптивних методів обробки сигналів*, які дозволяють автоматично налаштовувати параметри системи для мінімізації впливу завад. Найбільш поширеними є *методи адаптивної фільтрації сигналів* (LMS, RLS) та *методи просторово-частотного рознесення сигналів* (MVDR, LCMV).



Методи адаптивної фільтрації сигналів

Метод найменших середніх квадратів (Least Mean Squares, LMS) належить до найпростіших і найпоширеніших алгоритмів адаптивної фільтрації. Його принцип роботи полягає у поступовому коригуванні вагових коефіцієнтів фільтра пропорційно до похибки між вихідним сигналом і бажаним (опорним) сигналом. LMS відзначається низькою обчислювальною складністю, однак має порівняно повільну швидкість збіжності та чутливість до статистичних властивостей шуму.

Алгоритм рекурсивних найменших квадратів (RLS — Recursive Least Squares) є більш точним і швидкодіючим. Він мінімізує суму зважених квадратів похибок за весь період роботи, що забезпечує кращу адаптацію до змінних умов середовища, зокрема при наявності інтенсивних активних завад. За даними сучасних досліджень [26], алгоритм RLS демонструє вищу ефективність у подавленні завад порівняно з LMS, хоча вимагає більших обчислювальних ресурсів. У [27] підкреслюється, що розвиток адаптивних фільтрів спрямовується на підвищення швидкості збіжності та стабільності роботи в нестационарних умовах. Зокрема, досліджуються варіанти фільтрів зі змінною довжиною імпульсної характеристики (*variable tap-length*) і вдосконалені версії RLS із меншою чутливістю до флуктуацій шуму.

Методи просторово-частотного рознесення сигналів

Для подавлення (компенсації) спрямованих активних завад застосовуються *методи адаптивного формування діаграми спрямованості антенних решіток CRPA (Controlled Reception Pattern Antenna)*. Адаптивна просторова селекція корисного сигналу на фоні завад за допомогою антенних решіток реалізується за рахунок відмінностей у просторових структурах електромагнітних хвиль сигналу та завад і забезпечується адаптивними алгоритмами, зокрема MVDR (*Minimum Variance Distortionless Response*) і LCMV (*Linearly Constrained Minimum Variance*), у якості цільової функції автоматичного функціонування яких виступає досягнення мінімуму середньоквадратичного відхилення вихідного сигналу. При цьому, окрім подавлення завад також максимізується відношення сигнал/шум.

Алгоритм MVDR забезпечує мінімізацію потужності сигналу завад при одночасному збереженні сигналу в напрямку корисного джерела. У свою чергу, LCMV вводить додаткові лінійні обмеження, що дозволяє контролювати форму діаграми спрямованості для одночасного прийому кількох корисних сигналів або зниження рівня побічних пелюсток.

Принципи функціонування адаптивних пристроїв подавлення завад висвітлено в роботі [28]. Реалізація адаптивного алгоритму у більшості випадків забезпечується у цифровому вигляді з використанням програмно реалізованих трансверсальних фільтрів. З високою ймовірністю можна сказати, що саме таким чином побудований приймач GNSS «Комета–М» (до складу якого включено 4-елементну антенну решітку).

В [29] авторами запропоновано метод просторової селекції сигналів, блок-схему якого зображено на рис. 1.

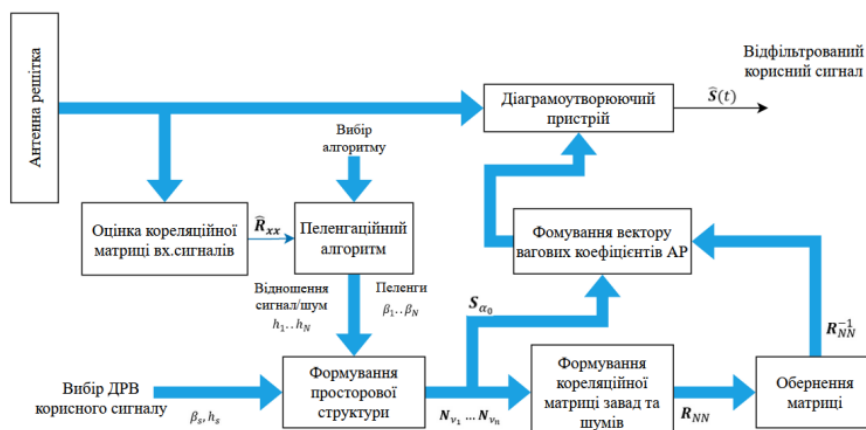


Рис. 1. Блок-схема методу просторової селекції.

Сучасні дослідження демонструють активне використання зазначених алгоритмів у поєднанні з методами машинного навчання та оптимізації. Наприклад, у роботі [30] показано, що застосування *Reconfigurable Intelligent Surface* (RIS) та глибокого навчання значно підвищує стійкість UAV-комунікацій до завад і спроб перехоплення. У дослідженні [31] продемонстровано використання рухомої антенної решітки з підтримкою глибокого навчання для адаптивного формування променя, що дозволяє ефективно знижувати співвідношення сигнал/завада навіть при наявності кількох сигналів подавлення.

Інші сучасні підходи поєднують адаптивне формування променя з оптимізаційними алгоритмами – наприклад, використання *Particle Swarm Optimization* (PSO) або генетичних алгоритмів [32].

Інтелектуальні технології подавлення активних завад у системах зв'язку.

Еволюцію парадигм протидії навмисним активним завадам від класичних адаптивних методів до сучасних інтелектуальних стратегій, що базуються на машинному навчанні, когнітивних технологіях та автономних рішеннях, викладено в [33]. Головна ідея полягає в переході від *реактивної протидії* (тобто реагування на вже наявну заваду) до *проактивної*, коли система *передбачає, розпізнає та адаптує свою поведінку* ще до того, як завада повністю вплине на роботу каналу.

Інтелектуальна протидія спирається на концепцію *когнітивного радіо* (CRS), яка включає три базові функції:

- *Аналіз спектра* (*Spectrum Sensing*): система постійно аналізує середовище, фіксуючи сигнали завад, їхню потужність, тип і частоту.
- *Прийняття рішень* (*Decision-Making*): на основі зібраної інформації система обирає оптимальну стратегію протидії – зміну частоти, модуляції, потужності чи навіть топології мережі.
- *Адаптація* (*Reconfiguration*): миттєва зміна параметрів радіосистеми без переривання зв'язку.

Когнітивна платформа є базисом для більш досконалих стратегій, зокрема тих, що використовують машинне навчання.

Інтелектуальні системи протидії завадам базуються на машинному навчанні, когнітивних технологіях і колективній взаємодії. Цей підхід дає змогу створювати

самонавчальні, автономні та проактивні системи, здатні протистояти навіть адаптивним і складним атакам.

Архітектуру інтелектуальної системи захисту від завад наведено на рис. 2.

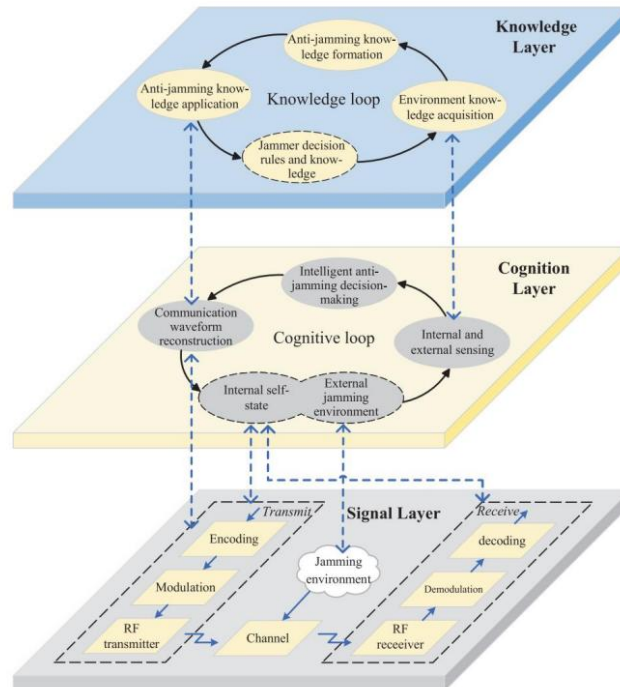


Рис.2. Архітектура інтелектуальної системи захисту від завад.

Ключові стратегії інтелектуальної антизавадової системи, які формують основу сучасних підходів:

1. *Навчання з підкріпленням (Reinforcement Learning, RL):*

- Система моделюється як агент, що взаємодіє з радіосередовищем.
- На основі винагороди за успішну передачу агент поступово навчається ухвалювати оптимальні рішення — змінювати частоту, модуляцію або антенну конфігурацію.
- Особливо ефективні методи: Q-Learning, Deep Q-Network (DQN), Multi-Agent RL.

2. *Глибоке навчання (Deep Learning, DL):*

- Використовується для класифікації типів завад, розпізнавання складних патернів DRFM, реактивного подавлення тощо.
- Конволюційні мережі (CNN) застосовуються для обробки спектрограм, рекурентні мережі (RNN, LSTM) – для часових послідовностей.

3. *Ігрова теорія (Game Theory):*

- Протидія подавленню розглядається як гра між двома сторонами, атакуючим і захисником.
- Використання рівноваги Неша дозволяє системі знаходити стабільні стратегії навіть за умови непередбачуваної поведінки противника.

4. *Колективне навчання:*

- Обмін знаннями між кількома вузлами (наприклад, між групою дронів) без необхідності централізованого сервера.
- Підвищує швидкість адаптації та робастність системи до нових типів завад.



Очікуваний ефект:

- зниження обчислювальних вимог без втрати точності;
- підвищення робастності до складних і адаптивних атак;
- прискорення навчання та реакції системи за рахунок кооперації вузлів і попереднього навчання;
- реалізація проактивного захисту – система не лише реагує, а й передбачає поведінку противника.

В [34] обговорюється перспектива інтеграції наземних сотових мереж 5G/6G з мережами БпЛА та переваги використання передового штучного інтелекту для виявлення атак глушіння.

Незважаючи на значні виклики – високу ресурсоемність, чутливість до даних та складність практичної реалізації – інтелектуальні методи представляють стратегічний напрям розвитку засобів захисту БпЛА і систем зв'язку нового покоління.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Стрімкий розвиток методів завадового впливу на радіоелектронні засоби та зростання масштабів застосування різного виду радіозавад, спрямованих на перехоплення, спотворення, знищення чи блокування інформаційних потоків, являються найнебезпечнішими загрозами для сучасних засобів радіозв'язку. Зростання доступності та потужності засобів радіоелектронної боротьби створює серйозні ризики для багатьох секторів економіки, транспорту, оборони та суспільства загалом.

Удосконалення і подальший розвиток адаптивних методів протидії активним шумовим завадам є складним і багатогранним завданням, яке поєднує в собі елементи радіотехніки, цифрової обробки сигналів, теорії інформації та кібербезпеки. Результатом наукових досліджень має стати створення алгоритмів і моделей, здатних забезпечити стійке функціонування радіоелектронних засобів у складних умовах інформаційного протистояння, що, у свою чергу, відкриває перспективи для подальшого розвитку технологій захищеного зв'язку та систем автономного управління.

Аналіз динаміки удосконалення методів формування активних завад, зокрема із використанням штучного інтелекту, обумовлює необхідність залучення штучного інтелекту для вирішення задач протидії впливу активних завад. Незважаючи на високу ресурсоемність, чутливість до даних та складність практичної реалізації інтелектуальні методи представляють стратегічний напрям розвитку засобів забезпечення стабільності і захисту радіозв'язку в умовах впливу активних завад.

Перспективним напрямком є застосування методів адаптивного розширення спектру сигналів, адаптивних фільтрів (LMS, RLS), просторових методів селекції сигналів (MVDR, LCMV), методів машинного навчання і штучного інтелекту для автоматичного виявлення, класифікації і протидії різноманітним типам завад, включаючи складні та раніше невідомі завадові впливи.

Майбутні зусилля мають бути спрямовані на створення більш універсальних та адаптивних систем протидії, здатних ефективно працювати в складних електромагнітних умовах. Окрім технічних рішень, важливими є організаційні заходи, такі як навчання персоналу, регулярне оновлення програмного забезпечення та міжнародна співпраця.



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 24(2), 767–809. <https://doi.org/10.1109/COMST.2021.3126481>
2. V. Sokolov, P. Skladannyi, A. Platonenko, Video Channel Suppression Method of Unmanned Aerial Vehicles, in: IEEE 41st International Conference on Electronics and Nanotechnology (2022) 473–477. doi: 10.1109/ELNANO54667.2022.9927105
3. V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.
4. V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.
5. V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.
6. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421
7. V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi: 10.1109/AICT61584.2023.10452687.
8. Kriuchkova, L., et al. (2023). Experimental research of the parameters of danger and protective signals attached to high-frequency imposition. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3550, pp. 261–268).
9. Kriuchkova, L., et al. (2024). Influence of protective signals on dangerous signals of high-frequency imposition. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3654, pp. 419–425).
10. Kriuchkova, L., et al. (2024). Experimental determination of protective signal parameters for effective “swinging” of the carrier frequency of high-frequency imposition. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 251–259).
11. Lu, Z., Wang, W., & Wang, C. (2014). Modeling, evaluation and detection of jamming attacks in time-critical wireless applications. *IEEE Transactions on Mobile Computing*, 13(8), 1746–1759. <https://doi.org/10.1109/TMC.2013.108>
12. Firouzbakht, K. (2015). *Packetized wireless communication under jamming: A game theoretic approach* (Doctoral dissertation, Northeastern University). Boston, MA. <https://repository.library.northeastern.edu/files/neu:rx916241c/fulltext.pdf>
13. Boualouache, A., & Engel, T. (2023). A survey on machine learning-based misbehavior detection systems for 5G and beyond vehicular networks. *IEEE Communications Surveys & Tutorials*, 25(2), 1128–1172. <https://doi.org/10.1109/COMST.2023.3244143>
14. Feng, S., & Haykin, S. (2019). Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks. *IEEE Transactions on Vehicular Technology*, 68(10), 9920–9934. <https://doi.org/10.1109/TVT.2019.2933719>
15. Ström, E., Ottosson, T., & Svensson, A. (2002). *An introduction to spread spectrum systems* (Report No. R016/2002). Department of Signals and Systems, Chalmers University of Technology.
16. Proakis, J. G., & Salehi, M. (2008). *Digital communications* (5th ed.). New York, NY: McGraw-Hill.
17. Wang, J., & Chen, L. (2023). Adaptive frequency hopping and direct sequence hybrid approach for anti-interference communications. *Electronics*, 12(5), 1142. <https://doi.org/10.3390/electronics12051142>
18. Stojanović, N. M., Todorović, B. M., Ristić, V. B., & Stojanović, I. V. (2024). Direct sequence spread spectrum: History, principles and modern applications. *Vojnotehnički glasnik (Military Technical Courier)*, 72(2), 790–813. <https://doi.org/10.5937/vojtehg72-46847>
19. Maleki, A., Nguyen, H. H., Bedeer, E., & Barton, R. (2024). A tutorial on chirp spread spectrum for LoRaWAN: Basics and key advances. *IEEE Open Journal of the Communications Society*, 5, 4578–4612. <https://doi.org/10.1109/OJCOMS.2024.3410603>



20. Win, M. Z., & Scholtz, R. A. (2000). Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications. *IEEE Transactions on Communications*, 48(4), 679–691. <https://doi.org/10.1109/26.843135>
21. De Almeida, I. B. F., Chafii, M., Nimr, A., & Fettweis, G. (2020, December). In-phase and quadrature chirp spread spectrum for IoT communications. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2020)* (pp. 1–6). Taipei, Taiwan. <https://doi.org/10.1109/GLOBECOM42002.2020.9322294>
22. Ma, L. (2023). Overview of commonly used spread spectrum techniques. *Academic Journal of Engineering and Technology Science*, 6(12), 83–92.
23. Zheng, C., Ge, Y., & Guo, A. (2023). Ultra-wideband technology: Characteristics, applications and challenges. *arXiv preprint arXiv:2307.13066*. <https://arxiv.org/abs/2307.13066>
24. Farhang-Boroujeny, B., Sego, T. C., Holschuh, T. V., Moradi, H., & Haab, D. (2023). *Multicode signaling in a filter bank multicarrier spread spectrum system and its application to HF communications* (STI No. INL/JOU-22-68674-Revision-0). Idaho National Laboratory.
25. Singh, D. (2021). *A brief survey of chaos theory in spread spectrum system*. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3865453>
26. Chiheb, A., & Khelladi, H. (2024). Performance comparison of LMS and RLS algorithms for ambient noise attenuation. *International Journal of Electrical and Computer Engineering Research*, 4(1), 14–19. <https://doi.org/10.53375/ijecer.2024.001>
27. Haykin, S. (2014). *Adaptive filter theory* (5th ed.). Pearson.
28. Panchenko, I. V., Bondarenko, D. M., Lypskyi, O. A., Stefanyshyn, Ya. I., & Ushakov, V. D. (2024). Analysis of the approach to protecting UAV satellite navigation receivers from interference. *Communication, Informatization and Cybersecurity Systems and Technologies*, (5), 108–118.
29. Kulykivska, N. I., Avdeienko, H. L., & Yakornov, Ye. A. (2022). Development of a spatial signal selection method based on radiation source direction-finding algorithms. *Infocommunication and Computer Technologies*, (2), 184–206. http://nbuv.gov.ua/UJRN/ict_2022_1_13
30. Zou, C., Li, C., Li, Y., & Yan, X. (2023). RIS-assisted robust beamforming for UAV anti-jamming and eavesdropping communications: A deep reinforcement learning approach. *Electronics*, 12(21), 4490. <https://doi.org/10.3390/electronics12214490>
31. Tang, X., Jiang, Y., Liu, J., Du, Q., Niyato, D., & Han, Z. (2024). Deep learning-assisted jamming mitigation with movable antenna array. *arXiv preprint arXiv:2410.20344*. <https://arxiv.org/abs/2410.20344>
32. Nipo, A., Islam, R. A., & Islam, M. I. (2025). Adaptive beamforming of linear array antenna system using particle swarm optimization and genetic algorithm. *International Journal of Wireless and Microwave Technologies*, 15(5). <https://www.mecspress.org/ijwmt/ijwmt-v15-n5/v15n5-1.html>
33. Zhou, Q., & Niu, Y. (2024). From adaptive communication anti-jamming to intelligent communication anti-jamming: 50 years of evolution. *Advanced Intelligent Systems*. <https://doi.org/10.1002/aisy.202300853>
34. *A lightweight AI-based approach for drone jamming detection*. (2024). *Sensors*, 24, 112–125. <https://doi.org/10.3390/s24010112>

**Larysa Kriuchkova**

Doctor of technical sciences, Professor

Professor of the Volodymyr Buriachok Department of Information and Cyber Security

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID: 0000-0002-8509-6659

l.kriuchkova@kubg.edu.ua

Nikita Vorokhob

master

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID: 0009-0006-3623-7386

novorokhob.fitm24m@kubg.edu.ua

ADAPTIVE METHODS TO COUNTER ACTIVE NOISE JAMMING

Abstract. The effectiveness of performing a flight mission by an unmanned aerial vehicle at a given distance crucially depends on the quality of control, telemetry control and data transmission by the unmanned aerial vehicle, which, in turn, are determined by the quality of radio communication between the ground control station and the unmanned aerial vehicle. At the same time, modern military radio-electronic systems operate, as a rule, in a complex radio-electronic environment, caused by the influence of both internal and external interference, as well as enemy electronic suppression means. Active interference of various types and purposes is used, aimed at disabling control channels, navigation channels, telemetry channels and data transmission channels of unmanned aerial vehicles, in particular FPV drones, which necessitates the search and implementation of new countermeasure methods capable of ensuring the stable functioning of unmanned aerial vehicles and FPV drones in conditions of active information confrontation. The article considers modern approaches to counteracting active noise interference in FPV drone control systems. The relevance of the problem is substantiated, due to the increasing scale of the use of unmanned aerial vehicles in the military and civilian spheres, as well as increasing the effectiveness of electronic jamming. Traditional protection methods are analyzed and their limitations in dynamic conditions of information warfare are identified. The results of the study of adaptive LMS and RLS filters, spatial signal selection methods (MVDR, LCMV), as well as the use of machine learning algorithms for detecting and neutralizing jamming signals are presented. It is shown that the combination of adaptive and intelligent methods provides increased stability of communication channels and reduces the risk of loss of drone control. The conclusion is made about the feasibility of using hybrid solutions that integrate classical digital signal processing algorithms with artificial intelligence methods.

Keywords: anti-jamming capability; radio jamming; spoofing; jamming; electronic warfare; countermeasure methods; protection techniques; CRPA systems.

REFERENCES

1. Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 24(2), 767–809. <https://doi.org/10.1109/COMST.2021.3126481>
2. V. Sokolov, P. Skladannyi, A. Platonenko, Video Channel Suppression Method of Unmanned Aerial Vehicles, in: IEEE 41st International Conference on Electronics and Nanotechnology (2022) 473–477. doi: 10.1109/ELNANO54667.2022.9927105
3. V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.
4. V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.



5. V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.
6. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421
7. V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi: 10.1109/AICT61584.2023.10452687.
8. Kriuchkova, L., et al. (2023). Experimental research of the parameters of danger and protective signals attached to high-frequency imposition. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3550, pp. 261–268).
9. Kriuchkova, L., et al. (2024). Influence of protective signals on dangerous signals of high-frequency imposition. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3654, pp. 419–425).
10. Kriuchkova, L., et al. (2024). Experimental determination of protective signal parameters for effective “swinging” of the carrier frequency of high-frequency imposition. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 251–259).
11. Lu, Z., Wang, W., & Wang, C. (2014). Modeling, evaluation and detection of jamming attacks in time-critical wireless applications. *IEEE Transactions on Mobile Computing*, 13(8), 1746–1759. <https://doi.org/10.1109/TMC.2013.108>
12. Firouzbakht, K. (2015). *Packetized wireless communication under jamming: A game theoretic approach* (Doctoral dissertation, Northeastern University). Boston, MA. <https://repository.library.northeastern.edu/files/neu:rx916241c/fulltext.pdf>
13. Boualouache, A., & Engel, T. (2023). A survey on machine learning-based misbehavior detection systems for 5G and beyond vehicular networks. *IEEE Communications Surveys & Tutorials*, 25(2), 1128–1172. <https://doi.org/10.1109/COMST.2023.3244143>
14. Feng, S., & Haykin, S. (2019). Cognitive risk control for anti-jamming V2V communications in autonomous vehicle networks. *IEEE Transactions on Vehicular Technology*, 68(10), 9920–9934. <https://doi.org/10.1109/TVT.2019.2933719>
15. Ström, E., Ottosson, T., & Svensson, A. (2002). *An introduction to spread spectrum systems* (Report No. R016/2002). Department of Signals and Systems, Chalmers University of Technology.
16. Proakis, J. G., & Salehi, M. (2008). *Digital communications* (5th ed.). New York, NY: McGraw-Hill.
17. Wang, J., & Chen, L. (2023). Adaptive frequency hopping and direct sequence hybrid approach for anti-interference communications. *Electronics*, 12(5), 1142. <https://doi.org/10.3390/electronics12051142>
18. Stojanović, N. M., Todorović, B. M., Ristić, V. B., & Stojanović, I. V. (2024). Direct sequence spread spectrum: History, principles and modern applications. *Vojnotehnički glasnik (Military Technical Courier)*, 72(2), 790–813. <https://doi.org/10.5937/vojtehg72-46847>
19. Maleki, A., Nguyen, H. H., Bedeer, E., & Barton, R. (2024). A tutorial on chirp spread spectrum for LoRaWAN: Basics and key advances. *IEEE Open Journal of the Communications Society*, 5, 4578–4612. <https://doi.org/10.1109/OJCOMS.2024.3410603>
20. Win, M. Z., & Scholtz, R. A. (2000). Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications. *IEEE Transactions on Communications*, 48(4), 679–691. <https://doi.org/10.1109/26.843135>
21. De Almeida, I. B. F., Chafii, M., Nimr, A., & Fettweis, G. (2020, December). In-phase and quadrature chirp spread spectrum for IoT communications. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2020)* (pp. 1–6). Taipei, Taiwan. <https://doi.org/10.1109/GLOBECOM42002.2020.9322294>
22. Ma, L. (2023). Overview of commonly used spread spectrum techniques. *Academic Journal of Engineering and Technology Science*, 6(12), 83–92.
23. Zheng, C., Ge, Y., & Guo, A. (2023). Ultra-wideband technology: Characteristics, applications and challenges. *arXiv preprint arXiv:2307.13066*. <https://arxiv.org/abs/2307.13066>
24. Farhang-Boroujeny, B., Sego, T. C., Holschuh, T. V., Moradi, H., & Haab, D. (2023). *Multicode signaling in a filter bank multicarrier spread spectrum system and its application to HF communications* (STI No. INL/JOU-22-68674-Revision-0). Idaho National Laboratory.
25. Singh, D. (2021). *A brief survey of chaos theory in spread spectrum system*. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3865453>



26. Chiheb, A., & Khelladi, H. (2024). Performance comparison of LMS and RLS algorithms for ambient noise attenuation. *International Journal of Electrical and Computer Engineering Research*, 4(1), 14–19. <https://doi.org/10.53375/ijecer.2024.001>
27. Haykin, S. (2014). *Adaptive filter theory* (5th ed.). Pearson.
28. Panchenko, I. V., Bondarenko, D. M., Lypskyi, O. A., Stefanyshyn, Ya. I., & Ushakov, V. D. (2024). Analysis of the approach to protecting UAV satellite navigation receivers from interference. *Communication, Informatization and Cybersecurity Systems and Technologies*, (5), 108–118.
29. Kulykivska, N. I., Avdeienko, H. L., & Yakornov, Ye. A. (2022). Development of a spatial signal selection method based on radiation source direction-finding algorithms. *Infocommunication and Computer Technologies*, (2), 184–206. http://nbuv.gov.ua/UJRN/ict_2022_1_13
30. Zou, C., Li, C., Li, Y., & Yan, X. (2023). RIS-assisted robust beamforming for UAV anti-jamming and eavesdropping communications: A deep reinforcement learning approach. *Electronics*, 12(21), 4490. <https://doi.org/10.3390/electronics12214490>
31. Tang, X., Jiang, Y., Liu, J., Du, Q., Niyato, D., & Han, Z. (2024). Deep learning-assisted jamming mitigation with movable antenna array. *arXiv preprint arXiv:2410.20344*. <https://arxiv.org/abs/2410.20344>
32. Nipo, A., Islam, R. A., & Islam, M. I. (2025). Adaptive beamforming of linear array antenna system using particle swarm optimization and genetic algorithm. *International Journal of Wireless and Microwave Technologies*, 15(5). <https://www.mecspress.org/ijwmt/ijwmt-v15-n5/v15n5-1.html>
33. Zhou, Q., & Niu, Y. (2024). From adaptive communication anti-jamming to intelligent communication anti-jamming: 50 years of evolution. *Advanced Intelligent Systems*. <https://doi.org/10.1002/aisy.202300853>
34. A lightweight AI-based approach for drone jamming detection. (2024). *Sensors*, 24, 112–125. <https://doi.org/10.3390/s24010112>

