УДК 681.3.06
DOI https://doi.org/10.32782/2663-5941/2025.1.2/12

Зилевіч М.О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Сваха Д.М.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ВИСОКОЕФЕКТИВНІ МЕТОДИ ПОСТАНОВКИ РАДІОЗАВАД НА ОСНОВІ АНАЛІЗУ КОМУНІКАЦІЙНОГО СИГНАЛУ

У статті розглянуто сучасні підходи до постановки радіозавад, що ґрунтуються на аналізі комунікаційного сигналу. Визначено проблеми традиційних методів радіопридушення в умовах швидко змінюваних радіочастотних середовищ та запропоновано нові рішення, спрямовані на підвищення ефективності роботи систем радіоелектронної боротьби (РЕБ). Окрему увагу приділено адаптивним підходам до аналізу та придушення сигналів, які враховують структуру, параметри та динаміку цільових систем зв'язку.

Ключовими аспектами дослідження виступає аналіз сучасних систем зв'язку та обмежень існуючих методів радіопридушення, зокрема стосовно систем із адаптивною модуляцією та частотним хопінгом. Розробка алгоритмів для ідентифікації та класифікації сигналів, які дозволяють створювати ефективні цілеспрямовані стратегії глушіння. Визначення енергоефективних методів, що мінімізують ризики впливу на дружні та цивільні системи.

У дослідженні представлено комплексний аналіз існуючих підходів до створення радіозавад, зокрема проактивних, реактивних, функціонально-специфічних та гібридних методів. Описано переваги та недоліки кожного з них, а також наведено класифікацію методів залежно від функціональності. Для підвищення ефективності було запропоновано використання програмно-визначених радіосистем (SDR), які забезпечують гнучкість, точність і високу швидкодію під час аналізу та постановки завад.

Запропонований метод поєднує радіорозвідку з постановкою радіозавад, що дозволяє адаптивно змінювати параметри в реальному часі, оптимізуючи ефективність перешкод. Основні переваги нового підходу включають точність налаштувань для націлювання на конкретні компоненти пакету, такі як преамбули або синхрослова. Гнучкість зміни параметрів завад залежно від динаміки каналу. Ефективне використання енергії завдяки адаптивному управлінню активністю пристроїв.

Запропонований підхід порівняно із традиційними методами. Основними перевагами є менше енергоспоживання, більша точність та швидкодія. Дослідження закладає основу для подальшого розвитку систем РЕБ, орієнтованих на інформаційну безпеку в умовах сучасного інформаційного протистояння.

Ключові слова: *радіопридушення, радіоелектронна боротьба, програмно-визначене радіо (SDR), енергоефективність, комунікаційні сигнали, частотний хопінг, адаптивна модуляці, радіорозвідка.*

Постановка проблеми. Стрімкий розвиток сучасних систем зв'язку зумовлює виникнення складних систем із вищими вимогами до безпеки та енергоефективності, що є викликом для традиційних методів постановки радіозавад. Зокрема, системи, що використовують широкосмугову передачу даних, адаптивну модуляцію та динамічне підлаштування параметрів сигналу, роблять застарілі методи глушіння, орієнтовані на фіксовані частоти або параметри сигналу, малоефективними. У зв'язку з цим виникають нові завдання для фахівців у галузі радіоелектронної боротьби, які спрямовані на забезпечення ефективного порушення ворожих комунікацій, мінімізуючи при цьому вплив на дружні системи та цивільну інфраструктуру.

Одна з основних проблем у постановці радіозавад загального призначення – це надмірне використання енергії, ризики створення перешкод для цивільних систем зв'язку та можливість ненавмисного втручання в союзні комунікації. У цьому контексті виникає нагальна потреба в розробці методів, що забезпечують точну і цілеспрямовану дію на ворожі системи зв'язку. Особливої актуальності дана тема набуває у військових та спеціалізованих системах, де радіоелектронна безпека є критично важливим елементом.

Для підвищення ефективності радіоелектронної боротьби (надалі – РЕБ) важливо досліджувати нові підходи до аналізу сигналів зв'язку. Це передбачає виявлення, класифікацію та адаптивну генерацію специфічних радіозавад, що спрямовані на порушення роботи цільових систем. Такий підхід забезпечує мінімальний вплив на суміжні канали та знижує енергоспоживання, що є ключовим фактором у сучасних військових операціях.

Дослідження зосереджено на розробці інноваційних високоефективних методів аналізу сигналів зв'язку, що відповідають сучасним вимогам до точності, швидкодії та енергетичної ефективності. Одним із перспективних напрямів є застосування програмно-визначених радіосистем (Software-Defined Radio, SDR) для реалізації адаптивних завад. Зокрема, пристрої на кшталт BladeRF забезпечують можливість швидкої обробки сигналів, генерації цілеспрямованих завад та динамічної адаптації до змін параметрів комунікаційних систем.

Формування цілеспрямованих завад здійснюється шляхом аналізу структури сигналів, їх частотних спектрів і часових характеристик. Такий підхід дозволяє ефективно порушувати роботу критичних компонентів систем зв'язку, мінімізуючи при цьому побічні ефекти для суміжних систем. Таким чином, запропоновані методи відкривають нові можливості для оптимізації роботи сучасних комунікаційних технологій в умовах високої динаміки та складних технічних викликів. Значення цього дослідження полягає не лише у вирішенні актуальних завдань РЕБ, але й у створенні фундаментальної бази для розробки майбутніх технологій забезпечення інформаційної безпеки в умовах інформаційного протистояння.

Аналіз останніх досліджень і публікацій. Принцип роботи будь-якої системи радіоелектронної боротьби (РЕБ) спрямований на навмисне порушення бездротової передачі даних, зокрема шляхом зайняття середовища передачі або спотворення сигналів, що змушує передавачі втрачати зв’язок. Переважно такі дії спрямовані на фізичний рівень передачі пакетів, хоча можливі й міжрівневі атаки. Методи радіопридушення поділяються на прості та складні залежно від функціональності. У свою чергу, прості методи класифікуються на проактивні та реактивні. Складні методи поділяються на два підтипи: функціонально-специфічні та розумно-гібридні. Більш детальна класифікація представлена на рисунку 1.

Проактивні завади створюють сигнали перешкод незалежно від передачі даних у мережі. Вони надсилають пакети або випадкові дані заважаючи працювати всім вузлам на цьому каналі. Ці завади працюють на одному конкретному каналі. Існує три основні типи проактивних завад: постійні, оманливі та випадкові.

1. Метод постійної завади безперервно генерує випадкові біти, ігноруючи протокол CSMA [1]. Згідно з механізмом CSMA, перед передаванням даних легітимний вузол повинен перевірити стан бездротового середовища. Передавання дозволяється лише тоді, коли середовище залишається вільним протягом встановленого інтервалу DIFS (DCF Interframe Space). Якщо канал зайнятий під час цього інтервалу, вузол відкладає передавання. Постійний глушник створює постійну зайнятість бездротового середовища, блокуючи комунікацію між легітимними вузлами. Хоча така атака легко виявляється та не є енергоефективною, вона є досить простою

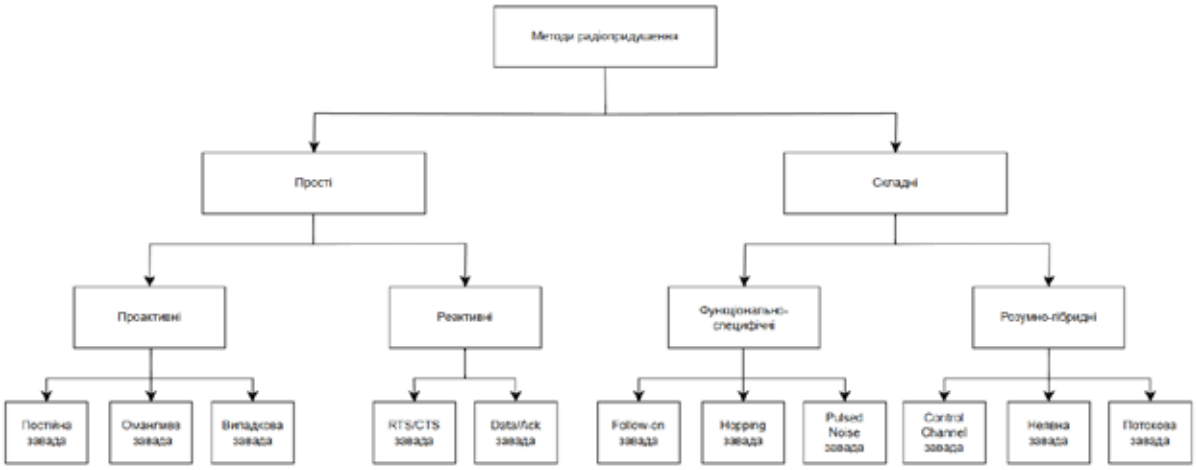

Рис. 1. Класифікація методів радіопридушення

в реалізації та здатна повністю паралізувати комунікацію між вузлами мережі.

2. Метод оманливої завади постійно передає стандартні пакети, замість випадкових бітів, як це відбувається у випадку постійних завад. Він вводить інші вузли в оману, створюючи ілюзію легітимної передачі даних, через що вони залишаються в режимі приймання, доки завада не припиниться або не буде усунена. У порівнянні з постійною завадою, виявити оманливу заваду складніше, оскільки вона використовує звичайні пакети, а не випадкові біти. Проте, подібно до постійних завад, оманливі також не є енергоефективними через безперервну передачу [1].

3. Метод випадкових перешкод періодично передає випадкові біти або звичайні пакети. Він чергує фази активності і сну для економії енергії. Цей підхід є компромісом між енергоефективністю та ефективністю постанови радіозавди, оскільки він не може створювати радіозавади під час фази сну [1].

Постановка реактивних завад ґрунтується на активації засобу радіопридушення тоді, коли виявлено мережеву активність на певному каналі [1], і має на меті порушити приймання повідомлень. Застосування даного методу доцільне по відношенню як до малих, так і до великих пакетів, але є менш енергоефективним, ніж метод випадкових перешкод, оскільки вимагає постійного моніторингу радіо ефіру. Однак виявити реактивну заваду важче, ніж проактивну, через складність точного вимірювання коефіцієнта надсилання пакетів (PDR). Існує два методи постановки реактивних перешкод:

1. Метод завад RTS/CTS активується при виявленні RTS-повідомлення. Він спотворює RTS, запобігаючи отриманню відповіді CTS від одержувача, що змушує відправника припинити передачу. Крім того, даний метод може створювати перешкоди після отримання RTS і до відправлення CTS, не даючи відправнику можливості передавати дані [2].

2. Метод завад Data/ACK націлений на пакети даних або ACK-пакети. Активується при детектуванні початку передачі даних, а потім пошкоджує дані або пакети ACK, змушуючи їх повторно передаватися.Якщо дані пошкоджені або ACK-пакети втрачені, відправник повторно передає дані [2].

Функціонально-специфічні завади розробляються з наперед визначеною функцією і можуть бути як проактивними, так і реактивними. Вони можуть працювати на одному каналі для економії енергії або охоплювати кілька каналів для більшої пропускної здатності перешкод, незалежно від споживання енергії. Навіть якщо вони зосереджені на одному каналі – можливе перемикання між каналами залежно від їхньої функціональності. Існує три методи постановки функціонально-специфічних завад:

1. Метод завад Follow-on швидко перемикається між каналами (тисячі разів на секунду), створюючи перешкоди в кожному з них на короткий проміжок часу. Він перемикає канали при виявленні завад і може використовувати псевдовипадкові послідовності, щоб зменшити можливість впливу на свою роботу з боку методів протидії завадам, таких як частотна модуляція з розширеним спектром (FHSS) [3].

2. Метод завад зі стрибкоподібною перебудовою каналів (Hopping) проактивно перестрибує між каналами, перекриваючи алгоритм CSMA. Такий метод може блокувати декілька каналів одночасно, використовуючи псевдовипадкову послідовність, і залишається прихованим під час фази виявлення [4, 5].

3. Метод імпульсно-шумових завад може перемикатися між каналами і смугами частот, заощаджуючи енергію, вмикаючись і вимикаючись за розкладом. На відміну від базових випадкових завад, такий метод може впливати на кілька каналів одночасно [6].

Розумно-гібридні завади є ефективними та дієвими у створенні перешкод, розроблені для максимального впливу з одночасним збереженням енергії. Ці методи можуть працювати як у проактивному, так і у реактивному режимах, націлюючись на всю мережу або значні її частини у великих мережах. Розглянуто три основних методи розумно-гібридних перешкод:

1. Метод керуючого каналу націлюється на відповідний канал у багатоканальних мережах, порушуючи координацію. У цьому випадку випадкові завади можуть значно погіршити продуктивність, тоді як безперервні завади можуть повністю заблокувати доступ [7].

2. Метод неявного глушіння використовує алгоритм адаптації швидкості, що використовується в бездротових мережах, викликаючи відмову в обслуговуванні на інших вузлах, коли точка доступу зосереджує свою увагу на зв'язку з вузлом зі слабким сигналом [8].

3. Метод глушіння потоку вимагає використання декількох пристроїв для зменшення потоку трафіку, як в централізованих, так і в децентралізованих моделях. При централізованому управлінні пристрій постановки використовує розраховану потужність для ефективності, в той час як

в децентралізованих моделях пристрої обмінюються інформацією для оптимізації атаки [9].

Постановка завдання. Метою цієї роботи є розробка ефективних методів аналізу сигналів зв'язку та реалізації методів цілеспрямованого радіопридушення. Основна мета полягає в ефективному виведенні з ладу систем зв'язку противника з одночасним мінімізацією споживання енергії та зменшенням перешкод для суміжних систем. Для досягнення цієї мети дослідження зосереджене на кількох ключових напрямках:

1. Проведення аналізу сучасних систем зв'язку та методів динамічної модуляції сигналів, що дозволить виявити обмеження існуючих методів радіозавад, зокрема проти систем з адаптивною модуляцією.

2. Розробка алгоритму для ідентифікації та класифікації сигналів зв'язку, що стане основою для створення більш точних стратегій їхнього нейтралізування.

3.Створення методів глушіння, які забезпечуватимуть енергоефективність і мінімізуватимуть ризики виникнення перешкод для дружніх систем або цивільної інфраструктури.

Запропонований підхід сприятиме підвищенню ефективності сучасних методів радіопридушення в умовах динамічно змінюваного радіочастотного середовища.

Виклад основного матеріалу. Радіо пакети є основою для передачі інформації в будь-якій системі бездротового зв'язку, включаючи системи з частотним хопінгом та складними схемами модуляції. Розуміння структури пакету на фізичному рівні є ключовим для створення ефективних методів глушіння, які можуть націлювати перешкоди на критичні компоненти пакету, блокуючи комунікацію. Пакет в радіоефірі зазвичай складається з кількох основних елементів:

1. **Преамбула (Preamble)** є першою частиною пакету, яка допомагає приймаючому пристрою визначити початок пакету та синхронізувати свої параметри для прийому сигналу. Преамбула містить повторювані біти або спеціальні символи, які дозволяють приймачеві налаштуватися на конкретні параметри, як то часова синхронізація чи частотне зміщення. Преамбула часто використовується для визначення частотного зміщення та інших параметрів каналу зв'язку.

2. **Синхрослово (Synchronization Word).** Після преамбули слідує синхрослово, яке є важливим елементом для точної синхронізації між передавачем і приймачем. Синхрослово допомагає приймачеві визначити точний момент початку передачі даних і уточнити час та частоту для коректного прийому. Воно є унікальним набором бітів, що відрізняється від інших частин пакету, що дозволяє приймачеві чітко розпізнати цей сигнал серед шумів або перешкод.

3. **Дані (Payload) та опціональні поля.** Основна частина пакету – це дані або payload. Це безпосередньо корисні дані, що передаються через канал зв'язку. Розмір і структура цих даних можуть змінюватися в залежності від стандарту або технології зв'язку. В системах з пакетною комутацією ці дані можуть бути поділені на кілька сегментів, які передаються окремо, а потім збираються разом у приймачі. Опціональні поля містять додаткову інформацію, яка може бути необхідна для коректної роботи системи. Це можуть бути поля для корекції помилок, перевірки цілісності даних (наприклад, CRC – циклічний контрольний код), а також інструкції або параметри конфігурації для пристрою прийому або передачі.

Для наочності на рисунку 2 наведено формат пакета для радіомодуля RFM66

За результатами проведеного аналізу пропонується енергоефективний метод глушіння, який поєднує в собі дві ключові складові: радіорозвідку та постановку радіозавад на основі отриманих даних. На першому етапі проводиться аналіз параметрів каналу зв'язку з використанням SDR (Software Defined Radio) технологій, що дозволяє виявити важливі елементи сигналу, такі як частоти, синхрослово та преамбулу. Отримані результати використовуються для точного налаштування завад націлених на конкретні частоти та компоненти пакету, що забезпечить високу ефективність і мінімізацію впливу на інші сигнали. Цей підхід дає змогу глушити лише ті канали зв'язку, які використовуються для передавання важливих

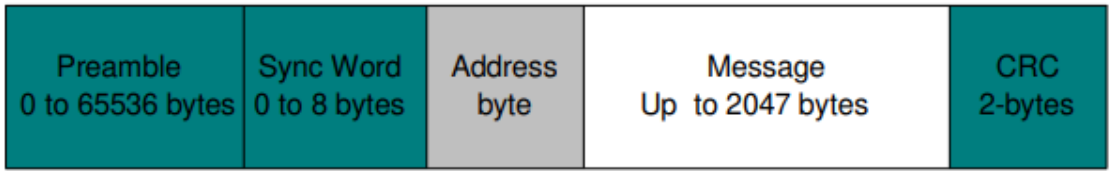

Рис. 2. Формат пакету для радіомодуля RFM66

даних, знижуючи ймовірність випадкового блокування інших бездротових систем.

1. **Радіорозвідка (Signal Intelligence).** На першому етапі SDR-пристрій проводить радіорозвідку для визначення параметрів каналу, включаючи частоти, на яких відбувається передача сигналу, типи модуляції, а також використання частотного хопінгу. Після проведення аналізу, необхідно зібрати таблицю частот, по яких відбувається комунікація, а також виявити синхрослово, що дозволяє точно визначити структуру пакету. Цей етап дає змогу зрозуміти, як виглядає передача, що дає основу для подальшої постанови завади.

2. **Аналіз параметрів сигналу.** Виявивши параметри передачі, необхідно налаштувати характеристики для синхронізації з каналом зв'язку. Визначення частотного хопінгу дозволяє створити таблицю частот, по яким передається цільовий комунікаційний сигнал. Важливим етапом є визначення розміру та значення синхрослова, довжини та значення преамбули, що дозволяє точно спрямовувати перешкоди на ключові компоненти пакету.

3. **Постановка завад на основі аналізу каналу.** Після збору необхідної інформації, SDR-пристрій активізує постановку завади, шляхом надсилання пакетів, що використовуватимуть визначені параметри та саме на тих частотах, які були визначені під час радіорозвідки. Дані перешкоди зможуть порушувати синхронізацію та перешкоджати коректному обміну пакетами між вузлами мережі.

Порівняння з іншими методами постановки завад. Традиційні методи, не завжди є ефективними, оскільки їхня основна мета максимально займати місце в одному або декількох каналах, для придушення корисного сигналу. Також через те, що при використанні традиційних методів намагаються створювати завади на максимальній потужності, такі пристрої не є енергоефективними.

У порівнянні з традиційними методами, метод на основі SDR має кілька переваг:

- **Точність налаштування**: SDR дозволяє націлюватися безпосередньо на конкретні частоти, синхрослова та преамбули, що робить постановку завад точнішим.
- **Гнучкість**: Завдяки програмному налаштуванню, можна швидко змінювати параметри завади в залежності від зміни каналу.
- **Радіорозвідка**: Можливість аналізувати канал та визначати його параметри до початку постановки завади значно підвищує ефективність впливу.

Висновки. У даній роботі розглянуто методи радіопридушення, спрямовані на створення перешкод для передачі інформації через радіоканали. Проведено аналіз наявних рішень у цій галузі та оцінено їхню ефективність у залежності від умов середовища та характеристик сигналу. Досліджено вплив параметрів сигналу, умов середовища та технічних характеристик засобів радіопридушення на їхню ефективність. Розглянуто можливість адаптації параметрів радіопридушення в реальному часі для підвищення ефективності перешкод і зменшення впливу на ненавмисні цілі. Запропоновано енергоефективний підхід, заснований на аналізі комунікаційного сигналу. Цей підхід дозволяє оптимізувати параметри роботи засобів радіопридушення для досягнення максимального рівня ефективності при мінімальному енергоспоживанні. Це є ключовим аспектом у розробці сучасних систем радіоелектронної боротьби.

Список літератури:

1. Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05). Association for Computing Machinery, New York, NY, USA, 2005, pp.46–57. https://doi.org/10.1145/1062689.1062697

2. K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245-257, Second Quarter 2011, doi: 10.1109/SURV.2011.041110.00022.

3. A. Mpitziopoulos, D. Gavalas, G. Pantziou and C. Konstantopoulos, "Defending Wireless Sensor Networks from Jamming Attacks," 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Athens, Greece, 2007, pp. 1-5, doi: 10.1109/PIMRC.2007.4394775.

4. Ghada Alnifie and Robert Simon. A multi-channel defense against jamming attacks in wireless sensor networks. In Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks (Q2SWinet '07). Association for Computing Machinery, New York, NY, USA, 2007, pp.95–104. https://doi.org/10.1145/1298239.1298257

5. Alnifie, Ghada & Simon, Robert. MULEPRO: A multi-channel response to jamming attacks in wireless sensor networks. Wireless Communications and Mobile Computing. 2010. DOI:10. 704-721. 10.1002/wcm.734.

6. Muraleedharan, Rajani & Osadciw, Lisa. Jamming attack detection and countermeasures in wireless sensor network using ant system. Proceedings of SPIE – The International Society for Optical Engineering. 2006. DOI:10.1117/12.666330.

7. Loukas Lazos, Sisi Liu, and Marwan Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the second ACM conference on Wireless network security (WiSec '09). Association for Computing Machinery, New York, NY, USA, 2009., pp. 169–180. https://doi.org/10.1145/1514274.1514299

8. Broustis, Ioannis & Pelechrinis, Konstantinos & Syrivelis, Dimitris & Krishnamurthy, Srikanth & Tassiulas, Leandros. FIJI: Fighting implicit jamming in 802.11 WLANs. № 19., 2009., pp. 21-40. 10.1007/978-3-642-05284-2_2.

9. Tague, Patrick & Slater, David & Poovendran, Radha & Noubir, Guevara. Linear Programming Models for Jamming Attacks on Network Traffic Flows. 2008. pp. 207 – 216. DOI: 10.1109/WIOPT.2008.4586066.

Zylevich M.O., Svakha D.M. HIGHLY EFFICIENT METHODS OF DETERMINING RADIO INTERFERENCE BASED ON COMMUNICATION SIGNAL ANALYSIS

The article considers modern approaches to jamming based on communication signal analysis. The problems of traditional jamming methods in rapidly changing radio frequency environments are identified, and new solutions are proposed to improve the efficiency of electronic warfare (EW) systems. Special attention is paid to adaptive approaches to signal analysis and suppression that consider target communication systems' structure, parameters, and dynamics.

The key aspects of the study are the analysis of modern communication systems and the limitations of existing jamming methods, particularly systems with adaptive modulation and frequency hopping. Development of algorithms for signal identification and classification that allow for the creation of effective targeted jamming strategies. Determination of energy-efficient methods that minimize the impact risks on friendly and civilian systems.

The study presents a comprehensive analysis of existing approaches to jamming, including proactive, reactive, functionally specific, and hybrid methods. The advantages and disadvantages of each of them are described, and the methods are classified depending on their functionality. To increase efficiency, it was proposed to use software-defined radio systems (SDR), which provide flexibility, accuracy, and high speed during analysis and jamming.

The proposed method combines radio reconnaissance with jamming, which allows adaptively changing parameters in real-time, optimizing the effectiveness of jamming. The main advantages of the new approach include the accuracy of settings for targeting specific packet components, such as preambles or syncwords. Flexibility in changing jamming parameters depending on channel dynamics. Efficient use of energy due to adaptive control of device activity.

The proposed approach is compared to traditional methods. The main advantages are lower power consumption, greater accuracy, and speed. The study lays the foundation for the further development of electronic warfare systems focused on information security in the conditions of modern information confrontation.

Key words: *radio jamming, electronic warfare, software-defined radio (SDR), energy efficiency, communication signals, frequency hopping, adaptive modulation, radio intelligence.*