



DOI 10.28925/2663-4023.2025.27.748

УДК 004.056.5

Биби́к Роман Тарасович

асистент кафедри захисту інформації

Національний Університет «Львівська Політехніка», Львів, Україна

ORCID ID: 0000-0002-9506-014X.

roman.t.bybyk@lpnu.ua**Опірський Іван Романович**

д.т.н., професор, завідувач кафедри захисту інформації

Національний Університет «Львівська Політехніка», Львів, Україна

ORCID ID: 0000-0002-8461-8996

ivan.r.opirskyi@lpnu.ua**ЕЛЕКТРОМАГНІТНІ ЗАГРОЗИ В СУЧАСНИХ КОНФЛІКТАХ:
АНАЛІЗ ХАРАКТЕРИСТИК ДЖЕРЕЛ РЕБ ТА ЇХ ВПЛИВ НА
ЕФЕКТИВНІСТЬ СИСТЕМ ЗАСОБІВ УРАЖЕННЯ**

Анотація. У статті досліджуються електромагнітні загрози, що виникають у сучасних військових конфліктах, зокрема ті, що створюються засобами радіоелектронної боротьби (РЕБ). Проаналізовано основні типи загроз, до яких належать заглушення, спотворення сигналу та перехоплення інформації. Розглянуто технічні характеристики джерел РЕБ, такі як частотний діапазон, потужність випромінювання, мобільність і функціональні можливості. Особливу увагу приділено впливу засобів РЕБ на ефективність сучасних систем ураження, включаючи системи протиповітряної оборони, безпілотні літальні апарати та високоточне озброєння. Окреслено методи протидії електромагнітним загрозам, які включають використання штучного інтелекту для адаптивного управління, застосування завадостійких технологій і впровадження новітніх засобів захисту апаратури. Проаналізовано перспективи розвитку технологій РЕБ, включаючи інтеграцію з автоматизованими системами та створення багатофункціональних платформ. У висновках наведено рекомендації щодо підвищення стійкості систем ураження до впливу засобів РЕБ, а також визначено напрями подальших досліджень у цій сфері.

Ключові слова: електромагнітні загрози; радіоелектронна боротьба; системи ураження; характеристики джерел РЕБ; протидія РЕБ; штучний інтелект; завадостійкі технології.

ВСТУП

Військові конфлікти характеризуються стрімким розвитком засобів радіоелектронної боротьби (РЕБ), які стають ключовим елементом ураження та протидії противнику. Електромагнітні загрози, створювані РЕБ, здатні суттєво впливати на ефективність систем управління озброєнням, порушуючи їхню роботу або повністю виводячи їх з ладу. У зв'язку зі збільшенням кількості конфліктів, де активно використовуються засоби РЕБ, дослідження їхніх характеристик, впливу на системи ураження та методів протидії є надзвичайно актуальним для забезпечення національної безпеки та обороноздатності. Основна проблема полягає у тому, що сучасні засоби РЕБ здатні нейтралізувати навіть найсучасніше озброєння, використовуючи широкий спектр електромагнітних впливів. Це знижує ефективність систем ураження та ускладнює виконання бойових завдань. Технічні характеристики джерел РЕБ, їх мобільність і функціональність ускладнюють виявлення та нейтралізацію цих загроз. Водночас наявні методи захисту часто виявляються недостатньо ефективними у швидкозмінних умовах сучасного бою.



Метою статті є аналіз характеристик джерел РЕБ, їх впливу на ефективність систем ураження та визначення перспективних методів протидії електромагнітним загрозам. Для досягнення цієї мети поставлено такі завдання:

- дослідити основні типи електромагнітних загроз та їх вплив на сучасні системи ураження;
- проаналізувати технічні характеристики та класифікувати джерела РЕБ;
- визначити вплив засобів РЕБ на ефективність виконання бойових завдань;
- запропонувати сучасні методи протидії електромагнітним загрозам із використанням технологій штучного інтелекту та завадостійких рішень;
- окреслити перспективи розвитку технологій РЕБ та вдосконалення систем захисту.

ЕЛЕКТРОМАГНІТНІ ЗАГРОЗИ В СУЧАСНИХ КОНФЛІКТАХ

Електромагнітні загрози є невід'ємною складовою сучасних військових конфліктів. Вони пов'язані з використанням радіоелектронних засобів, які впливають на функціонування систем зв'язку, управління, навігації та озброєння. Основною метою таких загроз є порушення інформаційного обміну між військовими підрозділами та зниження ефективності бойових систем. Електромагнітні загрози мають стратегічне значення, оскільки вони дозволяють отримати перевагу у конфлікті без прямого використання фізичного ураження [1], [3].

Таблиця 1

Ключові наслідки впливу електромагнітних загроз на військові системи

Сфера впливу	Наслідки електромагнітного впливу
Системи зв'язку	Заглушення або втрата сигналу, неможливість координації дій.
Навігаційні системи	Порушення роботи GPS, зниження точності навігації.
Системи озброєння	Зниження точності наведення, втрата керування.
Радари та сенсори	Спотворення даних, ускладнення виявлення цілей.

Системи радіоелектронної боротьби створюють широкий спектр електромагнітних загроз, серед яких найбільш відомими є глушіння, генерація високопотужних сигналів для створення перешкод у роботі радіо- або навігаційних систем, а також вплив на системи управління військовою технікою. Окрім того, вони здатні придушувати сигнали, вносячи хибні дані у канали зв'язку або навігації, а також створювати фальшиві цілі для радарів. Іншим важливим аспектом є перехоплення сигналів, що дає можливість втручатися у радіообмін для отримання розвідувальної інформації та впроваджувати дезінформацію з метою дезорієнтації противника.

Таблиця 2

Основні типи загроз, їхні методи реалізації та результати

Тип загрози	Методи реалізації	Результати впливу
Заглушення	Генерація шумових сигналів	Втрата зв'язку
Створення сигналу	Введення помилкових даних	Помилки навігації
Перехоплення сигналу	Розшифрування або злам радіоканалів	Розвідка, дезінформація

Сучасні військові операції вимагають радіоелектронної боротьби (РЕБ), оскільки вони дозволяють придушувати зв'язок противника, знижувати ефективність високоточної зброї та захищати власні системи управління. Війна між Україною та росією є однією з найбільш технологічно насичених війни, у якій широко застосовуються засоби РЕБ [4], [6].

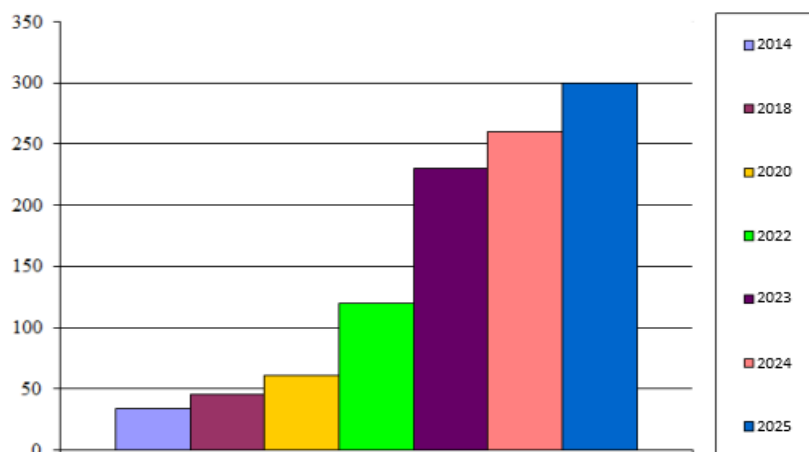


Рис. 1. Динаміка розширення типу перешкод, створюваних сучасними комплексами РЕБ

Використання РЕБ Україною у війні проти російської агресії

Україна активно розвиває власні системи РЕБ, які використовуються для нейтралізації ворожих БПЛА, захисту власного зв'язку та протидії навігаційним системам противника. Мобільні комплекси РЕБ, такі як «Буковель-AD» та «Анклав», широко застосовуються українськими військовими. Ці системи ефективно глушать канали управління та навігації ворожих безпілотників, що дозволяє запобігти атакам на військові та важливі об'єкти.



Рис. 2. Комплекс РЕБ - Буковель-AD

Система «Буковель AD» здатна виявляти ворожі БПЛА, такі як «Орлан-10», на відстані до 40 км, використовуючи пасивну технологію пеленгації. Після виявлення система може «глушити» їх на відстані 15–20 км від своїх позицій.

Обладнання «Буковель» легко монтується на кузові пікапа, де розміщується станція управління та модуль виявлення безпілотників. Розгортання системи займає всього дві хвилини.

Сучасна модифікація цієї системи здатна подавляти сигнали управління, передачі даних супутникової навігації GPS, ГЛОНАСС, Galileo і Beidou, а також створювати множину фальшивих сигналів. Окрім того, система протистоїть ворожим системам зв'язку, радіолокації та зброї з супутниковими системами наведення.



Рис. 3. Комплекс РЕБ — Анклав

Система РЕБ «Анклав» створює завади для приймачів, що працюють на частотах навігаційних систем ГЛОНАСС та GPS. Вона також здатна перешкоджати каналам управління та телеметрії, що використовуються в БПЛА та високоточному озброєнні. Завдяки цьому система придушує можливість передавання сигналів управління від оператора до самого апарату.

Система «Анклав» забезпечує захист зв'язку та управління військами, блокуючи спроби перехоплення мобільного зв'язку противника та створюючи безпечні канали комунікації для Збройних Сил України. Крім того, вона застосовується для придушення супутникової навігації, що ускладнює використання противником високоточної зброї, керованих ракет і безпілотників.

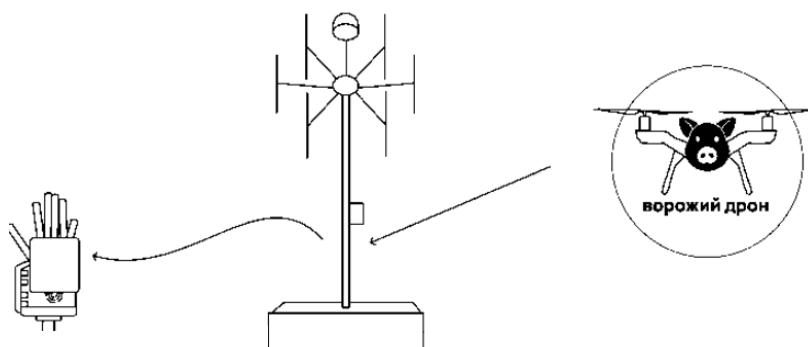


Рис. 4. Принцип роботи РЕБ

Використання Ізраїлем засобів РЕБ

Ізраїль активно використовує технології РЕБ для боротьби з терористичними угрупованнями та для захисту власного повітряного простору. Одним із таких комплексів є система «Drone Dome», яка застосовується для виявлення та нейтралізації ворожих дронів шляхом глушіння їхніх каналів управління.



Рис. 5. Комплекс РЕБ — Drone Dome

Drone Dome є повноцінним комплексом захисту від дронів «малого класу» і об'єднує засоби виявлення, придушення, а в додатковій версії — й фізичного знищення безпілотників. Всі три блоки можуть постачатися як разом, так і окремо, що дозволяє системі працювати автономно або інтегруватися в інші системи ППО. Система Drone Dome складається з радару RADA Electronic Industries RPS-42, системи зображення CONTROP Precision Technologies і детекторів радіосигналів. Радіолокаційна станція з оглядом 360 градусів дозволяє виявляти цілі з надмалим показником ЕПР — $0,002 \text{ м}^2$ на відстані до 3,5 км. Оптична система з нічним каналом відповідає за виявлення цілей на дальності до 3 км, автоматично знаходить і відслідковує їх. Додатково станція радіотехнічної розвідки пеленгує сигнали дронів у діапазоні від 70 МГц до 6 ГГц.

Комплекс «Scorpius» — це сучасна система РЕБ, яка створює електромагнітні перешкоди для авіації, радарів і систем зв'язку супротивника, при цьому не створюючи масових перешкод для власних військ.



Рис. 6. Комплекс РЕБ — Scorpius



Систему Scorpius пропонують у кількох виконаннях. Сухопутна версія Scorpius G призначена для виявлення й усунення наземних та повітряних загроз і може базуватися на автомобільному шасі. Модифікація для флоту, Scorpius N, призначена для захисту кораблів ВМС від протикорабельних крилатих ракет та БПЛА. Великий радіус дії системи забезпечує раннє виявлення загроз та ураження цілей. Модуль Scorpius SP використовується для самозахисту літаків, а Scorpius SJ — для створення перешкод радіоелектронним комплексам противника як у повітрі, так і на землі. У разі використання на літаках система працює автономно, не відволікаючи пілота від виконання бойових завдань.

Характеристики джерел РЕБ

Сучасні засоби радіоелектронної боротьби (РЕБ) розробляються з урахуванням вимог багатофункціональності, високої ефективності та адаптивності до змінних умов бойових дій. Основними технічними характеристиками є частотний діапазон, потужність випромінювання та мобільність. Засоби РЕБ охоплюють широкий спектр частот від декількох мегагерц до десятків гігагерц, що дозволяє їм впливати на різні типи сигналів. Потужність випромінювання варіюється від кількох ватів до сотень кіловат, що забезпечує ефективне заглушення сигналів на значних відстанях. Для забезпечення мобільності використовуються різні платформи — стаціонарні, мобільні наземні комплекси, авіаційні системи та морські носії.

Таблиця 3

Технічні характеристики засобів РЕБ

Параметр	Значення
Частотний діапазон	1 МГц – 40 ГГц
Потужність випромінювання	До 200 кВт
Дальність дії	До 300 км
Тип платформи	Стаціонарні, мобільні, авіаційні, морські

Джерела РЕБ можна класифікувати за їхнім призначенням та способом впливу на противника. Засоби радіопридушення призначені для блокування або значного ускладнення радіозв'язку супротивника. Прикладом є українські комплекси «Анклав», що використовуються для подавлення сигналів зв'язку та мобільних мереж противника. Засоби протидії безпілотним апаратам виявляють і придушують канали управління дронами. Наприклад, комплекс «Буковель-AD» може ефективно порушити зв'язок між оператором і дроном, змушуючи його здійснити аварійну посадку або повернутися до точки запуску [8].

Засоби радіотехнічної розвідки та перехоплення виявляють джерела випромінювання противника, аналізують сигнали та можуть здійснювати вибіркове придушення. Одним із прикладів є американський літак EC-130H Compass Call, що використовується для радіопридушення та збору інформації про радіосистеми противника. Засоби боротьби з навігаційними системами орієнтовані на глушіння сигналів супутникової навігації (GPS, ГЛОНАСС, Galileo). Багато сучасних комплексів, зокрема турецький KORAL, використовуються для створення перешкод навігаційним системам противника, що ускладнює застосування високоточної зброї [8], [10].

**Особливості використання мобільних, стаціонарних та авіаційних платформ РЕБ**

Мобільні комплекси РЕБ встановлюються на автомобілях, бронетехніці або спеціалізованих транспортних платформах. Їхня головна перевага — це мобільність і можливість швидкого зміни місця розташування. Прикладом є український комплекс «Nota», який може ефективно впливати на канали зв'язку противника та працювати в складі розвідувально-ударних груп.

Стаціонарні комплекси РЕБ використовуються для створення радіоелектронного захисту стратегічно важливих об'єктів, таких як командні пункти, бази, критична інфраструктура. Вони мають потужніші передавачі та більш широкі можливості аналізу радіосигналів. Як приклад, можна навести американську систему AN/FSQ-214, яка застосовується для придушення сигналів супутникового зв'язку та радіолокаційних систем.

Авіаційні платформи РЕБ встановлюються на літаках і безпілотної, що дозволяє здійснювати придушення радіоелектронних систем противника на великій відстані. Основними завданнями є забезпечення переваги в повітрі та створення «електромагнітних коридорів» для безпечного застосування авіації. Наприклад, американський EA-18G Growler використовується для придушення систем ППО противника [3].

*Таблиця 4***Вплив РЕБ на точність різних систем ураження**

Система озброєння	Тип впливу РЕБ	Результат впливу
Протиракетні системи	Заглушення радарів	Неможливість виявлення цілей
Високоточні ракети	Спотворення сигналу GPS	Відхилення від курсу
БПЛА	Заглушення команд	Втрата керування, аварії

Приклади впливу РЕБ на сучасні системи озброєння

Радіоелектронна боротьба має значний вплив на сучасні системи озброєння, змінюючи тактику їхнього застосування та ефективність. Вона може суттєво впливати на протиповітряну оборону, зокрема на системи типу «Патріот» чи «Бук», створюючи фальш-цілі для їхніх радарів. Це дозволяє противнику здійснювати атаки, залишаючись непоміченим. Однією з тактик є масований запуск хибних цілей, що провокує витрати боєприпасів та дозволяє виявити активні позиції ППО. Також фальш-цілі можуть запускатися разом із бойовими ракетами або дронами, створюючи перешкоди для ідентифікації справжніх загроз. Крім того, РЕБ здатна формувати хибне уявлення про масштаби чи напрямки атаки, що дезорієнтує системи оборони [4], [5].

Безпілотні літальні апарати, які використовуються для розвідки та ударів, є вразливими до заглушення навігаційних і командних сигналів. Спеціальні засоби РЕБ можуть не лише переривати зв'язок між оператором і БПЛА, а й здійснювати злом каналів управління, що потенційно дозволяє перехоплювати контроль над апаратом або виводити його з ладу.

Високоточне ракетне озброєння також значною мірою залежить від роботи супутникових навігаційних систем. Ракети, які використовують GPS-наведення, можуть стати неефективними через спотворення або повне заглушення сигналу. Під час сучасних конфліктів, зокрема в Україні, засоби РЕБ часто блокували роботу високоточних ракет противника, суттєво знижуючи їхню ефективність. Це підтверджує ключову роль радіоелектронної боротьби у протидії сучасним високоточним озброєнням і необхідність розвитку нових методів захисту від таких загроз [5].



Таблиця 5

Вплив українських засобів РЕБ на різні системи озброєння

Тип озброєння	Засоби РЕБ	Ефект
Протиповітряна оборона (ППО)	«Канон», «Nota»	Створення помилкових цілей, зниження точності наведення ракет ППО
Безпілотні літальні апарати (БПЛА)	«Буковель-AD», «Анклав»	Втрата сигналу управління, аварійна посадка або повернення на базу
Високоточні ракети	«Nota», «Канон»	Відхилення від курсу, зменшення ефективності навігаційних систем

Ці приклади підкреслюють стратегічну важливість засобів РЕБ у сучасних конфліктах та їхній значний вплив на ефективність навіть найсучаснішого озброєння.

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ РЕБ

Швидкий розвиток штучного інтелекту та автоматизації відкриває нові можливості для вдосконалення засобів РЕБ. Використання алгоритмів ШІ дозволяє аналізувати електромагнітний спектр у реальному часі, автоматично виявляти джерела випромінювання та класифікувати їх за типом. Це значно підвищує ефективність розпізнавання та оцінки загроз. Адаптивне управління системами РЕБ забезпечує автоматичне налаштування параметрів їхньої роботи залежно від умов бойової обстановки. Використання навчальних моделей сприяє прогнозуванню дій противника та проактивному створенню перешкод. Інтеграція з безпілотними платформами дозволяє швидко реагувати на зміни у спектрі та створювати локалізовані перешкоди, а рої дронів з елементами штучного інтелекту забезпечують ефективну колективну роботу у складних умовах.

Сучасні конфлікти вимагають універсальних рішень, що сприяє створенню багатофункціональних платформ. Системи РЕБ стають більш гнучкими, забезпечуючи можливість одночасної роботи в різних діапазонах частот та інтеграції функцій заглушення, спотворення, перехоплення й аналізу сигналів. Модульна конструкція дозволяє швидко адаптувати платформи до нових умов бойових дій, інтегруючи новітні технології без потреби у повній заміні обладнання. Мобільність відіграє ключову роль у підвищенні ефективності засобів РЕБ, що сприяє розробці легких і компактних систем, які можуть бути встановлені на мобільних та авіаційних платформах. Зростає популярність транспортних засобів із комбінованими можливостями радіоелектронної боротьби та розвідки.

Паралельно з розвитком засобів РЕБ зростає потреба у вдосконаленні захисту систем ураження. Використання метаматеріалів сприяє зменшенню впливу електромагнітного випромінювання, а наноматеріали можуть забезпечити додатковий рівень захисту обладнання від ворожих завад. Інноваційні програмні рішення включають адаптивні алгоритми штучного інтелекту, що дозволяють швидко відновлювати працездатність систем після впливу РЕБ, а також створення систем самодіагностики, здатних виявляти пошкодження. Посилення завадостійкості досягається шляхом застосування криптографічних технологій для захисту каналів передачі даних та використання багаторазового частотного перестроювання для уникнення заглушення. Інтеграція резервних систем управління забезпечує надійність функціонування військових структур навіть за умов інтенсивного впливу РЕБ, що досягається за рахунок альтернативних каналів зв'язку та децентралізованих мереж, які знижують вразливість до атак противника.



Також, одним із перспективних напрямів є когнітивна радіоелектронна боротьба, яка базується на застосуванні технологій машинного навчання для адаптивного налаштування систем РЕБ у реальному часі. Когнітивні системи здатні самостійно аналізувати параметри радіочастотного середовища, знаходити оптимальні стратегії заглушення та коригувати власні дії залежно від тактики противника. Це значно підвищує ефективність боротьби з новими загрозами та ускладнює роботу ворожих засобів зв'язку та навігації.

Окрему увагу слід приділити розвитку квантових технологій, які можуть суттєво змінити підходи до інформаційної безпеки та захисту від електронних атак. Зокрема, квантова криптографія забезпечує абсолютно захищений зв'язок, який неможливо перехопити або підробити традиційними методами. Використання квантових сенсорів у військових системах навігації також відкриває нові можливості для протидії засобам РЕБ, оскільки вони не залежать від сигналів супутникових систем, що робить їх менш вразливими до заглушення.

Важливим є також розвиток методів електромагнітного маскування, що спрямовані на зменшення помітності об'єктів у широкому спектрі частот. Використання спеціальних покриттів, здатних поглинати або змінювати характеристики відбитого сигналу, дозволяє значно ускладнити виявлення військової техніки засобами розвідки противника. Іншим перспективним напрямом є технології динамічного управління випромінюванням, які дозволяють мінімізувати радіочастотний слід та оперативно змінювати частотні характеристики сигналів, ускладнюючи їхнє виявлення та заглушення.

Крім того, інтеграція засобів РЕБ у мережево-центричні бойові системи відкриває нові можливості для координації дій у реальному часі. Поєднання засобів розвідки, РЕБ та вогневого ураження в єдину інформаційно-аналітичну систему дозволяє значно підвищити точність і швидкість реагування на загрози. Використання штучного інтелекту та великих масивів даних у таких системах дає змогу не лише прогнозувати дії противника, а й автоматично обирати оптимальні методи впливу на нього.

У комплексі всі ці технології дозволяють створювати більш стійкі та ефективні системи управління військовими операціями, що забезпечують перевагу у сучасному електромагнітному протистоянні. Поєднання когнітивних технологій, квантових рішень, методів маскування та мережево-центричних підходів формує нову концепцію ведення радіоелектронної боротьби, що дозволяє адаптуватися до швидкозмінних умов бойових дій та ефективно протидіяти сучасним загрозам.

Таблиця 6

**Ключові характеристики сучасних українських
багатофункціональних платформ РЕБ**

Назва комплексу	Частотний діапазон	Призначення	Тип платформи	Основні можливості
«Буковель-AD»	900 МГц – 5,8 ГГц	Придушення каналів управління БПЛА	Мобільний (автомобіль)	Блокування зв'язку дронів, GPS-придушення
«Анклав»	30 МГц – 3 ГГц	Глушіння мобільного зв'язку противника	Мобільний/стаціонарний	Блокування зв'язку GSM, 3G, 4G
«Nota»	1 ГГц – 6 ГГц	Придушення зв'язку та навігації	Мобільний (бронетехніка)	Дезорієнтація навігаційних систем, перешкоди для РЛС



«Канон»	100 МГц – 4 ГГц	Протидія радіолокаційним системам	Авіаційний/стаціонарний	Радіолокаційні перешкоди, створення помилкових цілей
«Полонез»	500 МГц – 8 ГГц	Придушення ППО та ракетних систем	Мобільний (автомобіль)	Дезорієнтація систем наведення, глушіння РЛС

Розвиток цих напрямків забезпечить зростання ефективності систем ураження, навіть у умовах інтенсивного використання засобів РЕБ противником [4] – [6].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті проведено аналіз електромагнітних загроз, що виникають у сучасних військових конфліктах, із особливим акцентом на засоби радіоелектронної боротьби (РЕБ) та їхній вплив на ефективність систем ураження. Дослідження підтвердило, що засоби РЕБ є потужним інструментом дестабілізації роботи ключових військових систем, оскільки вони охоплюють широкий спектр впливів, включаючи генерацію завадових сигналів, спотворення даних, перехоплення та аналіз радіообміну. Використання таких технологій дозволяє суттєво знизити ефективність систем управління військовою технікою, навігаційних комплексів, систем зв'язку та високоточного озброєння. Зокрема, засоби РЕБ можуть перешкоджати роботі безпілотних літальних апаратів, викликати збої у системах наведення ракет, а також створювати хибні цілі для систем протиповітряної оборони, що значно ускладнює виконання бойових завдань.

Аналіз характеристик джерел РЕБ показав, що їхні можливості значною мірою залежать від таких параметрів, як частотний діапазон, потужність випромінювання, мобільність та функціональні можливості. Розвиток сучасних засобів РЕБ йде в напрямку підвищення їхньої автономності, інтеграції зі штучним інтелектом для адаптивного аналізу електромагнітного середовища, а також використання багатофункціональних платформ, здатних одночасно здійснювати подавлення, розвідку та створення хибних сигналів. Встановлено, що традиційні методи боротьби з РЕБ в умовах інтенсивного електромагнітного впливу стають недостатньо ефективними, що зумовлює необхідність розробки нових підходів до захисту військових систем.

Одним із перспективних напрямів протидії електромагнітним загрозам є використання адаптивних алгоритмів обробки сигналів, які дозволяють в режимі реального часу аналізувати та нівелювати вплив завад. Впровадження завадостійких технологій у системи навігації та зв'язку, зокрема технологій просторово-часового та просторово-частотного орієнтування, забезпечує підвищену стійкість до впливу перешкод. Значні перспективи також відкриває використання штучного інтелекту для автоматизованого аналізу електромагнітної обстановки, прогнозування можливих атак з боку РЕБ і динамічного коригування параметрів роботи систем ураження.

Подальший розвиток технологій РЕБ, зокрема їхня інтеграція з автоматизованими системами управління військами, створює нові виклики у сфері електромагнітної безпеки. Це вимагає розробки комплексних методів захисту, що включають багаторівневі заходи, такі як використання малопомітних антенних систем, розподілених мереж зв'язку з підвищеною завадостійкістю та методів активного маскування сигналів. З огляду на постійне зростання загроз у сфері РЕБ, необхідність подальших досліджень та впровадження інноваційних підходів до протидії електромагнітним атакам є одним із ключових напрямів забезпечення ефективності сучасних систем ураження.



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shohat, R. (2019). Cyber Electronic Warfare. *Cyber Defense Review*, 4(2), 5–11. <https://doi.org/10.18462/cdr.2019.0402.02>
2. Lozynskyi, V. V. (2018). Electronic Warfare in the System of Preparation and Conduct of Combat Operations of the Armed Forces of Ukraine. *Armament and Military Equipment*, 2(14), 48–57.
3. Schleher, D. C. (2019). Electronic warfare in the 21st century: challenges, threats and opportunities. *IET Radar, Sonar & Navigation*, 13(3), 328–333. <https://doi.org/10.1049/iet-rsn.2018.5344>
4. Sokolov, V. Y. (2015). Latest Technologies of Electronic Warfare. *Armament and Military Equipment*, 2(14), 48–50.
5. McPeak, W. M., et al. (2015). Design of nanostructured metamaterials for optical magnetometry. *Nature materials*, 14(4), 395–400. <https://doi.org/10.1038/nmat4221>
6. Balanis, C. A. (2016). *Antenna Theory: Analysis and Design*. 4th ed. Hoboken: Wiley
7. Opirskyy I., Bybyk R. (2023). Research on modern methods of Electronic Warfare (EW) and methods and means of its counteraction. *Ukrainian Scientific Journal of Information Security*, 29(2), 88–97. <https://doi.org/10.18372/2225-5036.29.17873>
8. Adamczyk, B. (2017). Rapidly Varying Electromagnetic Fields. *Foundations of Electromagnetic Compatibility: with Practical Applications*, 439–452. <https://doi.org/10.1002/9781119120810.ch15>
9. Voytenko, V. I. (2018). *Fundamentals of Electronic Warfare*. Kyiv: Army of Ukraine.
10. Wiley, R. G. (2006). *Electronic Intelligence: The Analysis of Radar Signals*. Norwood: Artech House.

**Roman Bybyk**

Assistant of the Department of Information Protection

Lviv Polytechnic National University, Lviv, Ukraine

ORCID ID: 0000-0002-9506-014X.

roman.t.bybyk@lpnu.ua**Ivan Opriskyy**

Doctor of Technical Sciences, Professor, Head of the Department of Information Protection

Lviv Polytechnic National University, Lviv, Ukraine

ORCID ID: 0000-0002-8461-8996

ivan.r.opirskyy@lpnu.ua**ELECTROMAGNETIC THREATS IN MODERN CONFLICTS:
ANALYSIS OF EW SOURCES CHARACTERISTICS AND THEIR
IMPACT ON THE EFFECTIVENESS OF STRIKE SYSTEMS**

Abstract. This article examines electromagnetic threats arising in modern military conflicts, particularly those created by electronic warfare (EW) systems. The main types of threats, including jamming, signal distortion, and information interception, are analyzed. The technical characteristics of EW sources, such as frequency range, radiation power, mobility, and functional capabilities, are considered. Special attention is given to the impact of EW systems on the effectiveness of modern strike systems, including air defense systems, unmanned aerial vehicles, and precision-guided weapons. Methods of countering electromagnetic threats are outlined, including the use of artificial intelligence for adaptive control, the application of anti-jamming technologies, and the implementation of advanced hardware protection measures. The prospects for the development of EW technologies are analyzed, focusing on integration with automated systems and the creation of multifunctional platforms. The conclusions provide recommendations for enhancing the resilience of strike systems against EW influence and identify directions for further research in this field.

Keywords: electromagnetic threats; electronic warfare; strike systems; EW sources characteristics; EW countermeasures; artificial intelligence; anti-jamming technologies.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shohat, R. (2019). Cyber Electronic Warfare. *Cyber Defense Review*, 4(2), 5–11. <https://doi.org/10.18462/cdr.2019.0402.02>
2. Lozynskyy, V. V. (2018). Electronic Warfare in the System of Preparation and Conduct of Combat Operations of the Armed Forces of Ukraine. *Armament and Military Equipment*, 2(14), 48–57.
3. Schleher, D. C. (2019). Electronic warfare in the 21st century: challenges, threats and opportunities. *IET Radar, Sonar & Navigation*, 13(3), 328–333. <https://doi.org/10.1049/iet-rsn.2018.5344>
4. Sokolov, V. Y. (2015). Latest Technologies of Electronic Warfare. *Armament and Military Equipment*, 2(14), 48–50.
5. McPeak, W. M., et al. (2015). Design of nanostructured metamaterials for optical magnetometry. *Nature materials*, 14(4), 395–400. <https://doi.org/10.1038/nmat4221>
6. Balanis, C. A. (2016). *Antenna Theory: Analysis and Design*. 4th ed. Hoboken: Wiley
7. Opriskyy I., Bybyk R. (2023). Research on modern methods of Electronic Warfare (EW) and methods and means of its counteraction. *Ukrainian Scientific Journal of Information Security*, 29(2), 88–97. <https://doi.org/10.18372/2225-5036.29.17873>
8. Adamczyk, B. (2017). Rapidly Varying Electromagnetic Fields. *Foundations of Electromagnetic Compatibility: with Practical Applications*, 439–452. <https://doi.org/10.1002/9781119120810.ch15>
9. Voytenko, V. I. (2018). *Fundamentals of Electronic Warfare*. Kyiv: Army of Ukraine.
10. Wiley, R. G. (2006). *Electronic Intelligence: The Analysis of Radar Signals*. Norwood: Artech House.



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.