COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.001

УДК 004.75; 004.8

ДОСЛІДЖЕННЯ ВПЛИВУ ЕЛЕКТРОМАГНІТНИХ ПЕРЕШКОД НА ФУНКЦІОНУВАННЯ СИСТЕМ ЗВ'ЯЗКУ ТА РАДІОЛОКАЦІЇ

Р. Т. Бибик, Ю. М. Наконечний

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: roman.t.bybyk@lpnu.ua, yurii.m.nakonechnyi@lpnu.ua

Розглянуто вплив електромагнітних перешкод на функціонування систем зв'язку та радіолокації. У сучасному військовому конфлікті ефективність комунікацій та розвідки є головними факторами успішності. За допомогою високоточних досліджень та експериментів, проведених у цій статті, розкрито основні аспекти впливу електромагнітних перешкод на здатність систем зв'язку та радіолокації працювати в умовах бойових дій. Розглянуто також різні типи перешкод, їх вплив та взаємодію із системами зв'язку, методи управління та зменшення впливу перешкод. Отримані результати є корисним доповненням до розуміння проблем радіочастотного спектру і забезпечення надійності систем зв'язку та радіолокації в умовах електромагнітної обстановки сучасного бойового театру. Мета статті – дослідити та систематизувати знання щодо впливу електромагнітних перешкод на системи зв'язку та радіолокації і надати читачам інформацію, яка може лягти в основу подальших розвідок та розробок у цій ділянці. У процесі дослідження широко проаналізовано літературу та статті, які надають інформацію про вплив електромагнітних перешкод на системи радіолокації.

Ключові слова: електромагнітна перешкода (ЕМП), радіоелектронна боротьба (РЕБ), радіоелектронне забезпечення, радіоелектронне придушення, радіоелектронний захист, перешкоди, радіолокатор.

Вступ

З огляду на технології, які швидко зростають, і на постійні інновації у галузі бездротового зв'язку та радіолокації тема впливу електромагнітних перешкод на їх функціонування стає надзвичайно актуальною. Сучасні суспільства все більше стають залежними від ефективної роботи систем зв'язку та радіолокації в різних сферах, від комерційних та технологічних інновацій до оборонної й екстреної допомоги.

Зростання кількості електронних пристроїв, що використовують радіосигнали, породжує інтенсивний конкурентний тиск за використання обмежених ресурсів електромагнітного спектра. Це викликає не лише технічні виклики для стійкості систем, але і можливі загрози від зловмисного використання електромагнітних перешкод, включно з радіоелектронними бойовими засобами (РЕБ).

Захист від електромагнітних перешкод і від РЕБ стає пріоритетом у забезпеченні національної та міжнародної безпеки. Оцінка ризиків та розробка ефективних стратегій захисту стають критичними завданнями для забезпечення неперервного та безперебійного функціонування систем зв'язку і радіолокації. З огляду на ці виклики важливо провести глибокий аналіз впливу електромагнітних перешкод на сучасні системи зв'язку та радіолокації, визначити ризики та розвинути ефективні засоби захисту. Ця стаття ставить за мету висвітлити основні аспекти цієї проблеми та запропонувати практичні рекомендації для подолання викликів, пов'язаних із впливом електромагнітних перешкод.

1. Огляд літературних джерел

Загальний аналіз останніх досліджень свідчить про зростання складності впливу електромагнітних перешкод на системи зв'язку та радіолокації. Дослідники активно працюють над розумінням нових видів атак, впроваджують штучний інтелект у системи захисту та розвивають технічні рішення для протидії електромагнітним втручанням. Цей аналіз слугує основою для подальших досліджень та вдосконалення стратегій захисту від РЕБ у сучасних телекомунікаційних системах.

У своїй праці В. Ю. Соколов надає важливий огляд останніх технологій в електронній боротьбі. Автор розглядає нові методи та технології, що використовуються у сучасних системах електронної боротьби, такі як перешкоджання, розвідка та контррозвідка, ідентифікація та протидія електронним загрозам. Також досліджує важливі питання безпеки та виклики, пов'язані з розвитком і застосуванням цих технологій у військових конфліктах сучасного світу [1].

У статті Р. Шохата розглянуто такі аспекти, як кібератаки, їх вплив на електронні системи зв'язку та радіолокації, методи захисту від кіберзагроз, а також можливості використання кіберзброї у межах радіоелектронної боротьби [2].

У праці М. А. Річардса, В. А. Холма, і Дж. А. Шіра подано фундаментальний огляд принципів сучасної радіолокації. Розглянуто такі аспекти, як теорія радіолокації, сигналопереоблення, алгоритми оброблення сигналів та їх застосування у сучасних радарних системах. У книжці висвітлено основні принципи та технічні аспекти, такі як формулювання та вивчення радіосигналів, процес формування та оброблення сигналів у радарних системах. А також обговорення сучасних тенденцій та інновацій у сфері радіолокації, які висвітлюються в праці [9].

У своїй праці Марк Монтроуз пропонує вступний огляд принципів електромагнітної сумісності (EMI) та електромагнітної сумісності (EMC) з погляду дизайну друкованих плат. Також розглянуто у цій роботі, як проєктування друкованих плат з урахуванням електромагнітної сумісності, методи мінімізації електромагнітних перешкод та впливів на електронні пристрої, впровадження заходів електромагнітної сумісності під час розроблення продуктів [6].

Зростання як кількості, так і складності електромагнітних перешкод свідчить про постійне вдосконалення методів атак та потребу в постійному вдосконаленні захисних стратегій. Нові види атак як врахування нових можливостей атак, спрямованих на викривлення та перехоплення сигналів, свідчать про потребу швидкого реагування та розвитку нових методів захисту. Використання штучного інтелекту – провадження штучного інтелекту в системи захисту, є основним елементом в боротьбі із сучасними електромагнітними загрозами, забезпечуючи ефективніше розпізнавання та відсіювання перешкод. Розвиток технічних засобів захисту, таких як фільтри, екрани та автоматизовані системи реагування, підкреслює потребу не лише теоретичних аспектів захисту, а й практичних технологічних рішень. Орієнтація на 5G технології, де особлива увага до впливу перешкод на системи 5G свідчить про важливість забезпечення стійкості та надійності нових телекомунікаційних технологій. Цей аналіз стає фундаментом для подальших досліджень, спрямованих на розроблення та вдосконалення стратегій захисту від електромагнітних перешкод у сучасних телекомунікаційних системах. Із зростанням викликів у цій сфері постійне вдосконалення заходів захисту є основним елементом забезпечення безпеки та надійності інформаційних систем [5].

2. Мета та постановка завдання

Ця стаття присвячена дослідженню впливу електромагнітних перешкод на ефективність та надійність функціонування систем зв'язку та радіолокації. Мета полягає в розкритті механізмів взаємодії електромагнітних перешкод із зазначеними системами, а також у виявленні можливостей для покращення стійкості цих систем в умовах електромагнітного впливу.

Постановка завдання:

- Аналіз електромагнітних перешкод: дослідити різні види електромагнітних перешкод та їхні характеристики, які можуть впливати на системи зв'язку та радіолокації. Проаналізувати джерела цих перешкод та їх можливий вплив на ефективність систем.

- Взаємодія із системами зв’язку та радіолокаційними системами: дослідити взаємодію електромагнітних перешкод із різними типами систем зв’язку, включно з бездротовими мережами та супутниковим зв’язком. Розглянути вплив електромагнітних перешкод на точність та надійність роботи радіолокаційних систем. Дослідити методи підвищення стійкості радіолокаційних систем до електромагнітних втручань.
- Технічні рішення та інновації: проаналізувати наявні технічні рішення для захисту систем зв’язку та радіолокації від електромагнітних перешкод. Сформулювати висновки щодо вивчених аспектів впливу електромагнітних перешкод на системи зв’язку та радіолокації.
-

3. Електромагнітні перешкоди та їх вплив

Електромагнітні перешкоди (ЕМП) – це небажаний шум або перешкоди в електричному тракті чи ланцюзі, спричинені зовнішнім джерелом. Це також відомо як радіочастотна інтерференція. Електромагнітні перешкоди можуть спричинити погану роботу електроніки, несправність або повне припинення роботи.

Електромагнітні перешкоди можуть виникати в різних частотних діапазонах, від радіочастот до мікрохвильового та навіть інфрачервоного спектра. Різні джерела перешкод можуть генерувати сигнали з різною потужністю та модуляцією, що створює складну електромагнітну ситуацію.

Електромагнітні перешкоди (ЕМП) можуть призводити до різноманітних викликів для різних систем, таких як системи зв’язку та радіолокації. Розглянемо основні типи ЕМП та їх вплив на ці системи [6].

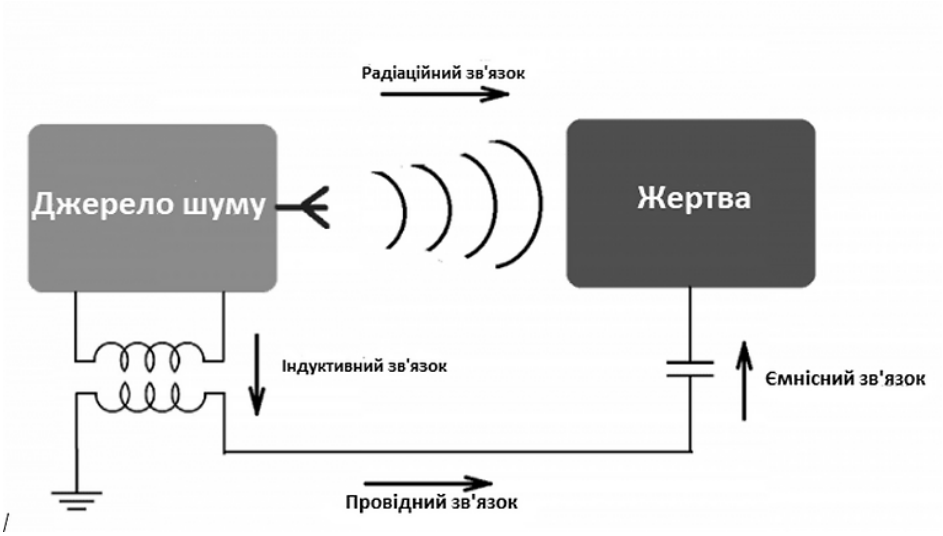

Рис. 1. Електромагнітна перешкода (ЕМП)

ЕМП – електромагнітні перешкоди можуть виникати з багатьох джерел, не залежно від того, чи створені людиною, чи природні. Категоризація ЕМП здійснюється з огляду на те, як вона була створена:

- Електромагнітна перешкода, створена людиною: зазвичай виникає від інших електронних ланцюгів, хоча деяка електромагнітна перешкода може виникати внаслідок перемикання великих струмів і т. ін.
- Природна електромагнітна перешкода: виникає з різних джерел, таких як космічний шум, а також блискавка та інші атмосферні види шуму.

Є багато способів, якими електромагнітна перешкода може передаватися від джерела шуму до потерпілого пристрою [6]. Розуміння того, який метод зв’язку призводить до перешкоджання для потерпілого, є основним для можливості розв’язання проблеми.

Категорії ЕМП за тривалістю часу:

- Імпульсний шум: цей вид ЕМП може бути створений людиною або мати природне походження. Блискавка, електростатичний розряд (ESD) та перемикальні системи роблять свій внесок в імпульсний шум.
- Постійне втручання: цей вид ЕМП зазвичай виникає від джерела, такого як ланцюг, який випромінює постійний сигнал. Проте постійний фоновий шум може бути створений різними способами: чи штучними, чи природними.

Категорії ЕМП за її шириною смуги:

- Вузькосмуговий ЕМП: зазвичай ця форма ЕМП може бути джерелом одного несучого сигналу, ймовірно, створеного якимось генератором. Ще однією формою вузькосмугового ЕМП є випадкові сигнали, спричинені інтермодуляцією та іншими формами спотворень у передавачі, такому як мобільний телефон чи Wi-Fi-маршрутизатор. Ці випадкові сигнали можуть з'являтися в різних точках спектра і можуть викликати перешкоди для іншого користувача радіочастотного спектра. Отже, ці випадкові сигнали мають бути утримані в тісних межах.
- Широкосмуговий ЕМП: є багато форм широкосмугового шуму, які можна виявити. Він може виникати з великої кількості джерел. Широкосмугове штучне втручання може виникати від джерел, таких як дугові зварювальники, де іскра генерується безперервно [6].

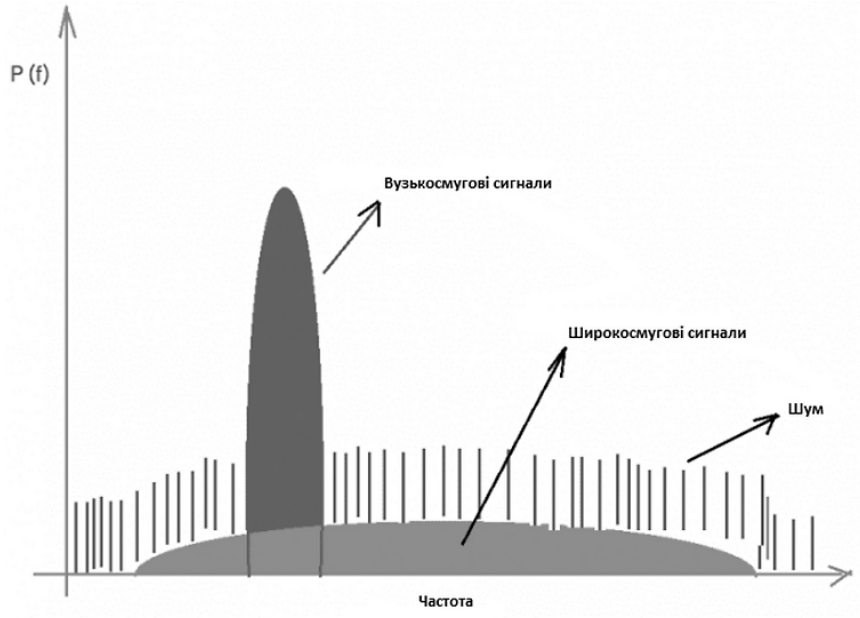

Рис. 2. ЕМП (електромагнітне втручання) за його шириною смуги (частотним діапазоном)

Загальні джерела ЕМП:

DC/DC-перетворювачі, або просто DC/DC-конвертери, є електронними пристроями, які використовуються для зміни рівня напруги (Voltage) та/або струму (Current) постійного струму (Direct Current, DC) [7]. Ці пристрої відіграють основну роль у різних електронних системах, забезпечуючи стабільне живлення для різноманітних пристроїв та систем. Основні характеристики та використання DC/DC-перетворювачів такі:

- Висока ефективність: DC/DC-перетворювачі вирізняються високою ефективністю перетворення енергії. Це дає можливість економити електроенергію та зменшує втрати енергії в системі.
- Зміна напруги: DC/DC-перетворювачі забезпечують можливість зміни рівня напруги. Це особливо важливо, коли потрібно забезпечити правильний рівень напруги для живлення конкретного електронного пристрою або системи.

- Стабілізація вихідної напруги: DC/DC-перетворювачі можуть стабілізувати вихідну напругу навіть під час змін напруги у вхідному джерелі.
- Захист від перенапруги: деякі DC/DC-перетворювачі містять механізми захисту від перенапруги, що робить їх надійними в умовах нестабільного живлення.
- Регульована потужність: DC/DC-перетворювачі дають змогу регулювати потужність залежно від вимог системи.

Загалом DC/DC-перетворювачі є невід'ємною частиною сучасних електронних систем, забезпечуючи стабільне живлення та оптимальне використання електроенергії у різних галузях, від промисловості до побуту.

Перемикальні інтегральні схеми (Switching Integrated Circuits або Switching ICs) – клас електронних пристроїв, які здатні швидко перемикати сигнали або створювати імпульси для керування електричними колами. Ці ICs широко використовуються в різноманітних застосуваннях і галузях, зокрема в електроніці, електропостачання, телекомунікації та інших [1, 2]. Основні характеристики та функції перемикальних інтегральних схем такі:

- Перемикальні регулятори напруги (Switching Voltage Regulators): застосовуються для конвертації напруги з одного рівня в інший з використанням перемикальних елементів, таких як транзистори, для ефективного регулювання вихідної напруги.
- Перемикальні джерела живлення (Switching Power Supplies): ці пристрої використовуються для забезпечення стабільного та ефективного живлення електронних пристроїв, зокрема у промисловості, вбудованих системах та побутових пристроях.
- Перемикальні масштабатори частоти (Switching Frequency Scalers): здатні перетворювати частоту сигналу на виході відповідно до заданого вхідного сигналу. Використовуються в радіосистемах та інших системах зв'язку.
- Перемикальні підсилювачі (Switching Amplifiers): використовуються для ефективного посилення сигналів, особливо в авдіосистемах та системах звукового відтворення.
- Перемикальні ключі (Switches): вони дають можливість чи блокують потік електричного струму у системі.
- Лінійні та логічні буфери (Switching Linear and Logic Buffers): забезпечують підсилення або підтримку сигналів у системах лінійного або логічного оброблення.

Multiple Clock Frequencies вказує на сценарій у цифровій системі, де різні компоненти або секції працюють із відмінними частотами годинника. Однак у деяких складних системах може бути вигідно або навіть потрібно працювати з різними блоками із різними частотами годинника [9]. Основні моменти, пов'язані з кількома частотами годинника, такі [6]:

- Домен годинника: це частина цифрового ланцюга, яка працює на підставі конкретного сигналу годинника. Різні розділи складної системи можуть бути призначені різним доменам годинника.
- Частоти годинника: у кожного домену годинника є власна частота годинника, яка представляє швидкість зміни сигналів та виконання операцій у цьому домені. Ці частоти вимірюються в герцах (Гц).
- Переходи між доменами годинника (CDC): коли сигнали мають перейти з одного домену годинника в інший, треба вживати спеціальних заходів для уникнення проблем, пов'язаних із порушеннями часу, метастабільністю та цілісністю даних.
- Асинхронні інтерфейси: у системах із кількома частотами годинника часто трапляються асинхронні інтерфейси, де дані передаються між різними доменами годинника. Часто використовуються асинхронні FIFO (перший прийшов – перший вийшов) та протоколи рукостискання для управління такими інтерфейсами.

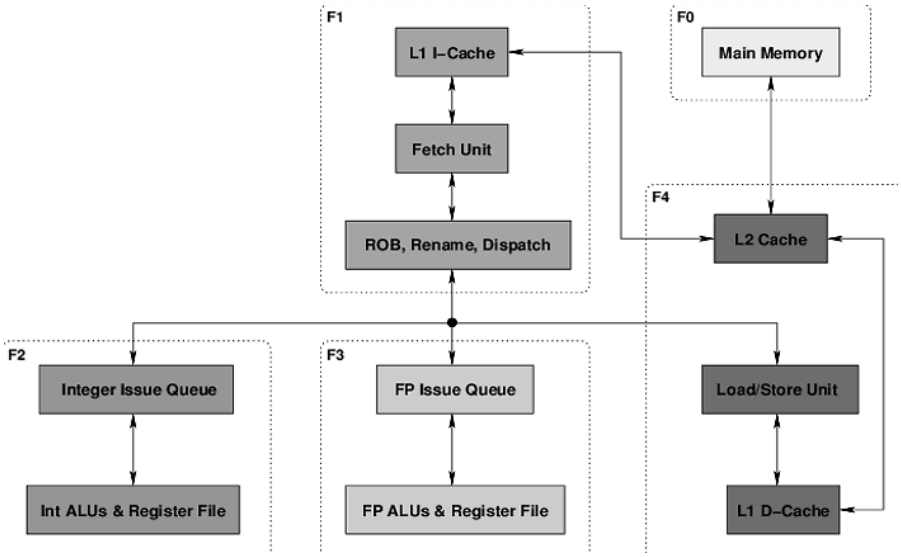

Рис. 3. Блок-схема процесора з кількома доменами годинника

Електромагнітні перешкоди (ЕМП) можуть серйозно впливати на системи зв'язку та радіолокації, завдаючи шкоди їх функціонуванню та надійності [6]. Механізми взаємодії ЕМП із такими системами містять декілька аспектів:

- Поглиблення сигналів: ЕМП може спричинити поглиблення сигналів у системах зв'язку, особливо на великих частотах. Це може викликати зниження якості зв'язку та збільшення рівня шуму.
- Затухання сигналів: ЕМП може призводити до затухання сигналів на шляху їх поширення. Затухання може бути особливо важливим під час використання мікрохвильового чи міліметрового діапазону для радіолокації.
- Множинне розсіювання (Multipath Fading): ЕМП може викликати явище множинного розсіювання, коли сигнали відображаються від різних поверхонь та приходять до антени з різних напрямків.
- Інтерференція: ЕМП може викликати інтерференцію з сигналами у системах зв'язку та радіолокації. Інші електронні пристрої чи самі системи можуть стати джерелами інтерференції, що може призвести до втрати сигналу або спотворення інформації.
- Змішування сигналів: ЕМП може викликати необмежене змішування сигналів, особливо у високочастотних системах. Це може створити нові сигнали, які не були задумані і можуть вплинути на правильне функціонування системи.
- Перешкоджання у чутливих ділянках спектра: ЕМП може бути спрямованим так, щоб впливати на конкретні чутливі частоти у спектрі системи. Це може призводити до великих проблем, оскільки ці частоти можуть бути основними для правильної роботи системи.

У військових застосуваннях може бути важливим розуміння та контроль взаємодії ЕМП із системами зв'язку та радіолокації, оскільки це може визначати ефективність та безпеку таких систем у реальних умовах [4].

4. Оцінка ризику та наслідки для систем зв'язку і радіолокації

Електромагнітні перешкоди (ЕМП) можуть становити значний ризик для систем зв'язку та радіолокації, викликаючи різні проблеми та порушення їхньої нормальної роботи. Ось деякі конкретні ризики, пов'язані з ЕМП, які можуть впливати на ці системи [9]:

Імпульси ЕМП:

- Втрата даних: велика потужність імпульсів ЕМП може призвести до втрати або пошкодження інформації, яка передається каналами зв'язку.

● Пошкодження комунікаційної Інфраструктури: ЕМП може викликати перенапругу в проводках та обладнанні, що може призвести до його знищення або неправильної роботи.

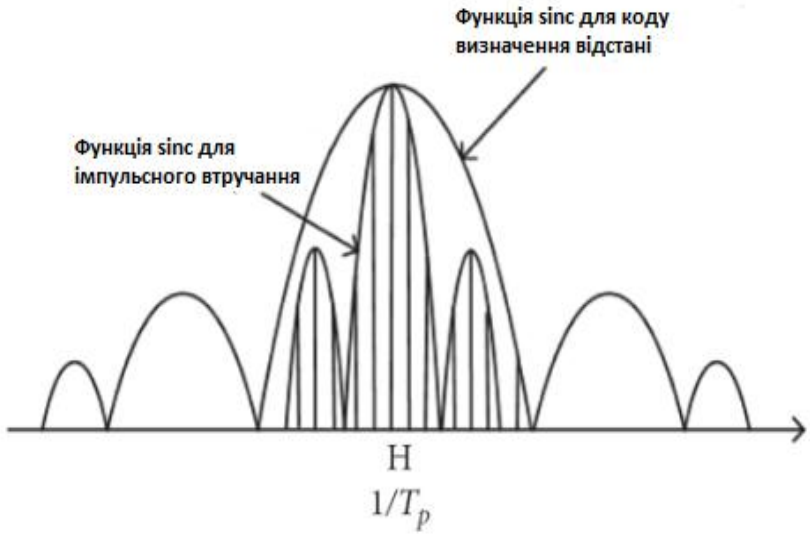

Рис. 4. Аналіз ефекту електромагнітних перешкод
від імпульсних перешкод на приймач навігації

Радіоелектронна боротьба (РЕБ):

● Перехоплення та втручання в комунікаційні сигнали: активне використання РЕБ може призвести до перехоплення та втручання в комунікаційні сигнали, що може порушити конфіденційність та цілісність інформації [5].

● Зміна орієнтації антен: РЕБ може вплинути на роботу антен, змінюючи їх орієнтацію та спрямованість, що може вплинути на якість зв’язку та радіолокації.

●

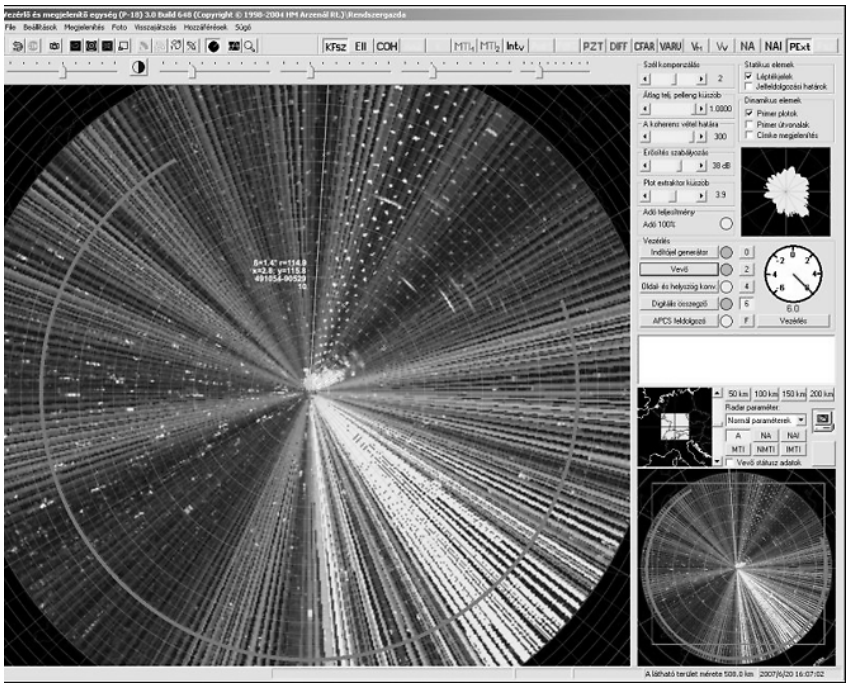

Рис. 5. Перешкоджання з модульованим шумом, інтерферент
на 150° (радар СВЧ-діапазону)

Навмисне випромінювання:

- Електромагнітне шпигунство: навмисне випромінювання ЕМП може бути використане для шпигунства і вивчення характеристик систем зв'язку та радіолокації.
- Джемінг: намагання завадити роботі систем створенням інтенсивних електромагнітних сигналів, які перешкоджають роботі систем.

Забезпечення захисту від цих ризиків містить ефективні технічні засоби захисту, криптографічні методи, а також стратегії фізичної та логічної безпеки. Також важливо проводити авдит безпеки і регулярні перевірки для виявлення та усунення можливих вразливостей [9, 3].

Електромагнітні перешкоди (ЕМП) можуть мати серйозні наслідки для систем зв'язку та радіолокації, викликаючи різні проблеми, які впливають на їхню ефективність та надійність.

Втрата зв'язку:

- Перерви та зникнення сигналу: ЕМП може призвести до перерв у переданні сигналів, що призводить до втрати зв'язку між об'єктами та системами.
- Погіршення якості зв'язку: інтенсивні ЕМП можуть спричиняти шум та спотворення в сигналах, знижуючи якість зв'язку.

Порушення роботи радіолокації:

- Втрата точності визначення розташування: ЕМП може впливати на роботу систем радіолокації, призводячи до неточності визначення розташування об'єктів.
- Зміна характеристик сигналів: перешкоди можуть змінювати характеристики високочастотних сигналів, ускладнюючи процес визначення об'єктів та їхніх параметрів.

Порушення безпеки та конфіденційності:

- Перехоплення та розкриття інформації: ЕМП може збільшити ризик перехоплення та розкриття конфіденційної інформації, передаваної через зв'язок.
- Вразливість до кібератак: ЕМП може робити системи зв'язку та радіолокації більш вразливими до кібератак, особливо через порушення нормального функціонування.

Обмеження функціональності:

- Пошкодження електронних компонентів: інтенсивний ЕМП може призвести до пошкодження електронних компонентів систем, обмежуючи їхню функціональність.
- Втрата здатності до локалізації: вища потужність ЕМП може призводити до тимчасової втрати можливості локалізації об'єктів за допомогою радіолокації.

Забезпечення захисту та стійкості систем зв'язку та радіолокації від ЕМП – використання електромагнітностійких матеріалів, екранування та застосування технологій, які зменшують вразливість до електромагнітних перешкод [3, 4, 9].

5. Системи захисту від РЕБ

Радіоелектронна боротьба (РЕБ) відіграє основну роль у сучасних воєнних конфліктах, що полягає у захисті від радіоелектронних засобів противника, які можуть використовуватися для завад комунікацій, контролю та розвідки. Цей процес є критичним для обох сторін у військових конфліктах. Основні завдання радіоелектронної боротьби – розгром управління військами противника, підтримання низької ефективності ворожої розвідки та застосування бойової техніки й зброї, а також забезпечення надійної роботи власних систем управління військами та зброєю [2].

Системи захисту від радіоелектронної боротьби (РЕБ) використовують різноманітні технічні засоби для забезпечення надійності та ефективності електронних систем в умовах можливих електромагнітних перешкод. Технічні засоби захисту містять такі компоненти, як фільтри, екрани та екранування. Основні технічні засоби захисту від РЕБ такі [9]:

Фільтри:

- Фільтрація частот: використання фільтрів для виділення частот допустимого діапазону та приглушення сигналів, які перебувають за межами цього діапазону.

● Фільтрація шуму: застосування фільтрів для зменшення впливу електромагнітних перешкод та шуму на сигнали в системі.

Екрани:

● Електромагнітно стійкі матеріали: використання спеціальних матеріалів, які мають високі властивості екранування та зменшують проникнення електромагнітних полів.

● Екрановані кабелі: застосування кабелів з екранами для захисту від електромагнітних перешкод та зменшення викидів сигналів.

Екранування:

● Електромагнітне екранування обладнання: використання спеціальних конструкцій та матеріалів для екранування окремих компонентів електронних систем від зовнішніх впливів.

● Електромагнітно стійкі корпуси: застосування корпусів обладнання, які мають високу ефективність екранування для захисту внутрішніх компонентів.

Захист від ЕМП:

● ЕМП-стійкі компоненти: використання компонентів, які можуть витримувати імпульси електромагнітного випромінювання без пошкоджень.

● Системи захисту подання енергії: застосування захисних систем, які від'єднують електромережу від обладнання в разі спостереження потужного ЕМП.

Ізоляція та інтерфейси:

● Оптичні ізолятори: використання оптичних ізоляторів для відокремлення електричних сигналів та захисту від перенесення електромагнітних перешкод.

● Гальванічна ізоляція: застосування гальванічної ізоляції для подання електроенергії та передання сигналів, щоб уникнути перенесення електромагнітних перешкод.

Захист кабелів та вводів–виводів:

● Скрутка кабелів: використання техніки скрутки кабелів для зменшення ефекту індукції та уникнення електромагнітних перешкод.

● Фільтри на входах–виходах: встановлення фільтрів та дроселів на входах–виходах для захисту від високочастотних сигналів.

Ці технічні засоби захисту допомагають забезпечити ефективний захист від РЕБ та зберегти працездатність електронних систем у невизначених електромагнітних умовах.

В сучасних умовах, де електронні системи стають все більш вразливими до радіоелектронної боротьби, використання алгоритмів та програмного забезпечення стає основним елементом для виявлення та протидії електромагнітним перешкодам (ЕМП). Нижче подано огляд алгоритмів та програмного забезпечення, які використовуються для забезпечення ефективності та безпеки в умовах РЕБ [7, 10].

Алгоритми детекції ЕМП:

● Спектральний аналіз: використання алгоритмів спектрального аналізу для виявлення незвичайних частотних компонентів, що можуть свідчити про наявність ЕМП.

● Кореляційний аналіз: визначення кореляційних зв'язків між сигналами, що надходять, та типовими сигналами перешкод.

● Методи машинного навчання: застосування алгоритмів машинного навчання для виявлення аномальних патернів в електромагнітному спектрі.

Алгоритми розпізнавання та ідентифікації сигналів:

● Ідентифікація звичайних та аномальних сигналів: використання алгоритмів для розпізнавання типових сигналів і виділення аномальних, що можуть бути пов'язані з ЕМП.

● Системи класифікації сигналів: впровадження систем класифікації для відокремлення корисних сигналів від шумів та перешкод.

Програмне забезпечення захисту від перешкод:

● Алгоритми фільтрації: використання алгоритмів фільтрації для виділення корисних сигналів та приглушення електромагнітних перешкод.

● Динамічне програмне забезпечення: розроблення програмного забезпечення, яке може динамічно адаптуватися до змін у спектрі електромагнітних сигналів.

Системи автоматичного реагування:

● Автоматичне визначення рівня загрози: реалізація алгоритмів, які автоматично визначають рівень загрози від ЕМП та активують захисні заходи.

● Системи автоматичного відновлення: Використання програмного забезпечення для автоматичного відновлення роботи систем після виявлення перешкод або атак.

Алгоритми контррозвідки:

● Виявлення систем РЕБ: розробка алгоритмів для виявлення та ідентифікації засобів радіоелектронної боротьби.

● Методи спротиву ідентифікації: розроблення алгоритмів, які спрямовані на ускладнення ідентифікації та локалізації систем РЕБ.

Сучасні технології, використовувані для захисту від радіоелектронної боротьби (РЕБ), постійно розвиваються, охоплюючи широкий спектр аспектів, від апаратних засобів до програмного забезпечення та алгоритмів. Деякі з основних технологій у цій ділянці містять [13, 15]:

Активне управління спектром:

● Когерентне перепрограмування: технологія, що дає можливість перепрограмувати радіочастотні пристрої для адаптації до змінних умов та уникнення перешкод.

● Адаптивне використання частот: системи, які динамічно визначають оптимальні частоти для уникнення інтерференцій та підвищення надійності зв’язку.

Методи штучного інтелекту та машинного навчання:

● Класифікація сигналів: використання алгоритмів машинного навчання для класифікації сигналів і виявлення аномалій, що може вказувати на електромагнітні перешкоди.

● Системи прогнозування: застосування алгоритмів штучного інтелекту для прогнозування можливих сценаріїв РЕБ та розроблення відповідних стратегій захисту.

Системи контррозвідки:

● Виявлення активних засобів РЕБ: використання радіоприймачів та антен для виявлення активних засобів РЕБ і реагування на їх дії.

● Системи розпізнавання загроз: використання технологій, які розпізнають типи та джерела електромагнітних перешкод.

Системи шифрування та криптографії:

● Квантова криптографія: використання принципів квантової механіки для забезпечення безпеки зв’язку та запобігання перехопленню сигналів.

● Диференціальне шифрування: застосування методів шифрування, що змінюються динамічно, для ускладнення розкриття шифрів.

Розроблення імунних до ЕМП компонентів:

● Електромагнітно стійкі матеріали: використання спеціальних матеріалів, що поглинають або відбивають електромагнітні хвилі, зменшуючи їхні наслідки.

● Спеціалізовані інтегральні схеми: розроблення електронних компонентів, які менш чутливі до електромагнітних перешкод.

Комплексні системи захисту:

● Інтегровані системи: розроблення комплексних систем, що об’єднують різні технічні та програмні засоби для забезпечення повноцінного захисту.

● Системи виявлення та реагування: використання сенсорів і систем автоматизованого реагування для оперативного виявлення та протидії перешкодам.

Ці технології взаємодіють для створення сучасних і надійних систем захисту від РЕБ, здатних адаптуватися до змінних умов та загроз електромагнітного середовища [3].

6. Приклади практичних застосувань

Вплив електромагнітних перешкод на системи зв'язку і радіолокації стає актуальним у різноманітних контекстах, які варіюються від військових операцій до цивільних та комерційних систем. Розглянемо кілька прикладів практичних застосувань і випадків використання:

- Військовий контекст: електронна боротьба (РЕБ) – у військовому середовищі використання електромагнітних перешкод стає основною складовою частиною електронної боротьби. Ворожі сили можуть використовувати перешкоди для маскування власних сигналів, спотворення сигналів противника та перехоплення комунікацій.
- Комерційні застосування – у місцях з високою щільністю електронних пристроїв, таких як офісні будівлі чи торгові центри, можуть виникати конфлікти між пристроями, що використовують різні комунікаційні стандарти. Використання електромагнітних перешкод може розв'язати проблеми взаємовпливу та покращити стабільність зв'язку.
- Авіаційні системи – захист від радарів у сучасній авіації: електромагнітні перешкоди використовуються для захисту від радарних систем. Авіаційні апарати можуть випромінювати електромагнітні сигнали або використовувати активні системи перешкод для запобігання виявленню та слідування за ними.
- Космічні застосування – захист супутникових систем у космосі, де супутники навколо Землі взаємодіють із різними електромагнітними джерелами, важливо забезпечити захист від перешкод. Випадки використання електромагнітних засобів для захисту супутникових систем стають важливими в контексті космічних досліджень та комунікацій.
- Електронні перешкоди у життєвих ситуаціях – у певних ситуаціях електромагнітні перешкоди можуть використовуватися для захисту від стеження чи перехоплення приватних комунікацій. Наприклад, у сфері кібербезпеки електромагнітні методи можуть застосовуватися для ускладнення виявлення зловмисниками.

Зазвичай перед використанням засобів РЕБ (розвідки й електронної боротьби) проводиться уважна розвідка, яка охоплює виявлення радіоелектронних засобів противника, визначення їхнього місця розташування та аналіз характеристик сигналів. Збір таких даних відбувається постійно, навіть у мирний час [11, 13, 15].

У військовій сфері терміни "датчик" і "сенсор" застосовуються для отримання інформації та мають різне значення (РЛС, оптика, оптоелектроніка, далекоміри, детектори та інше). Вони можуть бути різного розміру та технічного рівня і встановлюються на зброї, бойовій техніці або інших платформах. Вони поліпшують обізнаність екіпажів, бойових груп та окремих бійців або забезпечують відповідний рівень захисту. Окрім того, є складні сенсорні системи, які використовуються для виявлення, ідентифікації, прицілювання, розвідки або створення перешкод на значні відстані з високою точністю. Роль таких сенсорів постійно зростає: вони є базою більшої частини систем озброєння та підтримки. Згідно з оцінкою польського ресурсу Defence-24, розвиток сенсорів невдовзі змінить обличчя майбутнього поля бою. До 2035 року передбачається виникнення нових сенсорів, що значно прискорять виявлення цілей, аналіз розвідувальної інформації та ухвалення відповідних рішень. Це також скоротить час реакції під час бою та покращить взаємодію всіх елементів армії – від окремих бійців до командувачів вищого рівня.

Сучасну видову (образну) розвідку переважно здійснюють з використанням супутників. Проте безпека цих супутників на орбітах є під загрозою через зусилля у створенні космічних військ, які зростають і які вже мають США та КНР. Усі ці країни експериментують з електромагнітною та лазерною зброєю для виведення з ладу супутників противника. Також розробляються наземні оптичні телескопи й РЛС, які відіграють роль систем попередження та супроводження цілей. Можливості щодо атак супутників також має Індія, та ще кілька інших країн активно працюють у цьому напрямку. Водночас ефективність інших систем розвідки загалом буде зменшуватися через збільшення дальності ведення бойових дій і зростання можливостей маскування. Також зміниться тактика ведення бойових дій: від принципу "знайди та знищуй" до

“перевір та атакуй першим”. У такому разі буде важливо випереджати противника й розкривати його наміри, а роль безпосереднього спостереження, імовірно, зменшиться. Використання ж просунутих сенсорів SIGINT (з генерованими електронними сигналами) надалі дають локалізувати РЛС, окремі системи озброєння й техніки або, наприклад, радіоприймачі чи телефони. Відповідно системи ELINT будуть забезпечувати перехоплення електронних сигналів, ідентифікацію та аналіз характеристик випромінювання, режиму роботи, функцій передавального пристрою або зв’язку з іншими системами озброєння. Нарешті, системи COMINT збиратимуть інформацію про передавання радіо та авдіосигналів, телефонних розмов, текстових повідомлень і комунікацій у режимі онлайн. Перспективні рішення в цьому напрямку мають відповідати цільовим вимогам та забезпечувати ефективне накопичення, аналіз та розподіл результатів сигнальної розвідки. Така система має не лише ідентифікувати окремих емітентів, а й визначати характеристики та можливості останніх у межах цільової системи й навіть об’єднаної комплексної бойової системи [3, 4].

7. Результати дослідження

Під час дослідження було виявлено, що електромагнітні перешкоди можуть значно впливати на ефективність і надійність функціонування систем зв’язку та радіолокації. Аналіз різних видів електромагнітних перешкод показав, що їхнім джерелом можуть бути різноманітні електронні та електричні пристрої, радіоелектронне обладнання, а також зовнішні електромагнітні поля. Взаємодія електромагнітних перешкод із системами зв’язку та радіолокації демонструє їхній великий вплив на точність та надійність цих систем. Зокрема, виявлено, що електромагнітні перешкоди можуть спричиняти втрату сигналу, спотворення інформації, а також перешкоджати нормальному функціонуванню радіолокаційних систем.

Дослідження також показало, що є різноманітні технічні рішення та інновації для захисту систем зв’язку і радіолокації від електромагнітних перешкод. Зокрема, використання екранів, фільтрів та розроблення спеціальних алгоритмів для компенсації електромагнітних перешкод може допомогти підвищити стійкість цих систем.

Отже, результати досліджень підтверджують потребу подальших розроблень та впровадження заходів захисту для забезпечення стійкості і надійності систем зв’язку та радіолокації в умовах електромагнітного впливу.

Висновки

Внаслідок вивчення впливу електромагнітних перешкод на системи зв’язку та радіолокації, а також заходів захисту можна зробити кілька основних висновків:

- Вплив електромагнітних перешкод: електромагнітні перешкоди становлять значний ризик для нормального функціонування систем зв’язку та радіолокації. Вони можуть викликати втрату зв’язку, спотворювати сигнали та створювати загрози для безпеки і конфіденційності.
- Заходи захисту: технічні засоби захисту, такі як фільтри, екрани та електромагнітно сумісні компоненти, відіграють важливу роль у зменшенні впливу електромагнітних перешкод. Сучасні стратегії захисту охоплюють інтеграцію штучного інтелекту та комплексних систем моніторингу.
- Ризики та специфічні виклики: ризики варіюють залежно від контексту використання систем. У військовому середовищі електромагнітні перешкоди можуть бути використані з метою обману та приховання, тоді як у цивільних системах вони можуть викликати втрату зв’язку або завадити роботі критичних інфраструктурних об’єктів.
- Подальші дослідження: підсумки вивчення вказують на продовженні подальших досліджень у цій ділянці. Перспективи розвитку містять розроблення ефективніших технічних рішень, а також вдосконалення стратегій захисту на основі аналізу нових методів атак.

Із проведених досліджень можна виділити такі позитивні кількісні показники:

- Зменшення часу реакції систем зв’язку та радіолокації на електромагнітні перешкоди.

- Підвищення ефективності передання даних через системи зв'язку під впливом електромагнітних перешкод.
- Зниження кількості помилок та переривань у роботі систем зв'язку і радіолокації під час дії електромагнітних перешкод.
- Поліпшення точності та стабільності роботи радіолокаційних систем під час управління електромагнітними перешкодами.
- Збільшення дальності зв'язку та зменшення втрат сигналу під впливом електромагнітних перешкод.

Загалом вплив електромагнітних перешкод на системи зв'язку та радіолокації визначається великою кількістю факторів, таких як технічні характеристики систем, контекст використання та можливі сценарії атак. Загальна оцінка ризиків вказує на те, що це дуже важлива проблема, яка потребує постійного вдосконалення заходів захисту.

Список літератури

1. Sokolov V. Yu. (2015). The latest technologies of electronic warfare. Weapons and military equipment, 2(14), p. 48–50. https://nbuv.gov.ua/UJRN/ovt_2015_2_13

2. Shohat R. (2019). Cyber Electronic Warfare. Cyber Defense Review, 4(2), pp. 5–11. https://doi.org/10.18462/cdr.2019.0402.02

3. Schleher D. C. (2019). Electronic warfare in the 21st century: challenges, threats and opportunities. IET Radar, Sonar & Navigation, 13(3), pp. 328–333. https://link.springer.com/chapter/10.1007/978-94-011-6985-1_6

4. Choi Seungcheol, Kwon Oh-Jin. Method for Effectiveness Assessment of Electronic Warfare Systems in Cyberspace. https://doi.org/10.3390/sym12122107

5. Opirskyy I., Bybyk R. Research on modern methods of Electronic Warfare (EW) and methods and means of its counteraction // Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 2, pp. 88–97. https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/17873

6. Montrose M. Introduction to EMI/EMC Design for Printed Circuit Boards. https://6146am.com.br/wp-content/uploads/2022/04/Intro_EMC_Printed_Circuit_Board_Montrose.pdf

7. Williams Arthur B., Taylor Fred J. Electronic Filter Design Handbook. https://d1.amobbs.com/bbs_upload782111/files_32/ourdev_573166.pdf

8. Poisel R. (2013). Electronic Warfare Target Location Methods. https://ezproxy.villanova.edu/login?URL=https://library.books24x7.com/library.asp?villanova&bookid=65241

9. Richards M. A., Scheer J. A., & Holm W. A. (2014). Principles of Modern Radar: Basic Principles. SciTech Publishing.

https://ftp.idu.ac.id/wpcontent/uploads/ebook/tdg/MILITARY%20PLATFORM%20DESIGN/Richards_M._Scheer_J._Holm_W._Principles_of_mo.pdf

10. Rihaczek A. W. (1996). Principles of High-Resolution Radar. McGraw-Hill Education. https://www.scirp.org/reference/referencespapers?referenceid=634903

11. Lozynskyi V. V. (2018). Electronic combat in the system of preparation and conduct of combat operations of the Armed Forces of Ukraine. Armament and military equipment, 2(14), pp. 48–57. https://journal.utm.md/index.php/ctve/article/view/10770

12. Pozar D. M. (2011). Microwave Engineering Wiley. http://mwl.diet.uniroma1.it/people/pisa/RFELSYS/MATERIALE%20INTEGRATIVO/BOOKS/Pozar_Microwave%20Engineering(2012).pdf

13. Budge Mervin C., Shawn Jr., German R. Basic Radar Analysis https://dokumen.tips/document/basic-radar-analysispdf.html?page=1

14. McPeak W. M., et al. Design of nanostructured metamaterials for optical magnetometry. Nature materials 14.4 (2015). pp. 395–400. https://www.nature.com/articles/nmat4221

15. Foundations of Electromagnetic Compatibility: with Practical Applications (pp. 439–452) by Bogdan Adamczyk (2017). https://doi.org/10.1002/9781119120810.ch15

RESEARCH ON THE IMPACT OF ELECTROMAGNETIC INTERFERENCE ON THE FUNCTIONING OF COMMUNICATION AND RADAR SYSTEMS

R. Bybyk, Y. Nakonechnyi

Lviv Polytechnic National University,
Department of Cybersecurity
E-mail: roman.t.bybyk@lpnu.ua, yurii.m.nakonechnyi@lpnu.ua

The impact of electromagnetic interference on the operation of communication and radar systems is discussed. In modern military conflicts, the effectiveness of communication and reconnaissance is crucial for success. Through precise research and experiments conducted in this article, the fundamental aspects of how electromagnetic interference affects the ability of communication and radar systems to operate in combat conditions are revealed. Various types of interference, their effects, and interaction with communication systems, as well as methods of management and mitigation of interference effects, are also examined. The results obtained serve as a valuable addition to understanding the issues of the radio frequency spectrum and ensuring the reliability of communication and radar systems in the electromagnetic environment of contemporary theaters of war. The article aims to investigate and systematize knowledge regarding the impact of electromagnetic interference on communication and radar systems and provide readers with information that can serve as a basis for further research and development in this area. A wide range of literature and articles providing information on the impact of electromagnetic interference on radar systems were analyzed to support the research.

Keywords: Electromagnetic Interference (EMI), Electronic Warfare (EW), Electronic Support (ES), Electronic Suppression (ES), Electronic Protection (EP), Jamming, Radar.