DOI: 10.18372/2225-5036.29.17873

ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ РЕБ ТА МЕТОДІВ І ЗАСОБІВ ЇЇ ПРОТИДІЇ

Іван Опірський, Роман Бибик

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 190 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
Orcid ID: 0000-0002-8461-8996.

БИБИК Роман Тарасович, асистент
Рік та місце народження: 1995 рік, м. Стрий, Львівська обл., Україна.
Освіта: Національний університет «Львівська Політехніка», 2018 рік.
Посада: асистент кафедри захисту інформації, з 2020 року.
Наукові інтереси: засоби захисту інформації.
E-mail: romanbub3@gmail.com.
Orcid ID: 0000-0002-9506-014X.

Анотація. *Радіоелектронна боротьба (РЕБ) - це процес захисту від радіоелектронних засобів противника, які можуть використовуватись для перешкоджання комунікацій, контролю та розвідки. В умовах сучасного ведення війни радіоелектронна боротьба має вирішальне значення для обох сторін конфлікту. Основними завданнями РЕБ є: дезорганізація управління військами противника; зниження ефективності ведення розвідки і застосування зброї і бойової техніки противника; забезпечення надійної роботи систем і засобів управління своїми військами і зброєю. У цій статті оглянуто сучасні методи РЕБ, їх технічні характеристики та ефективність. Досліджено різні типи засобів РЕБ, включаючи активні та пасивні системи, які використовуються для захисту від радіолокації. Розглянуто проблеми, пов'язані з використанням РЕБ військовими та цивільними організаціями. Наведено приклади сучасних методів та технологій РЕБ. Розглянуто способи, які застосовують для приховування об'єктів від виявлення радіолокаційних засобів противника. Також наведено приклади, що сучасних умовах РЕБ є важливою складовою частиною військової діяльності, оскільки забезпечує збереження власних життів та здоров'я воїнів, збереження та знищення техніки противника, а також виконання бойових завдань. Розглянуто основні методи та засоби протидії РЕБ. Для забезпечення функціонування електронних систем та інших пристроїв в умовах впливу радіосигналів використовуються різноманітні методи та засоби, такі як комплексний технічний контроль та маскування, захист від кібератак, системи захисту від електромагнітного імпульсу та використання резервних систем зв'язку та комунікації. Одним із важливих аспектів боротьби з РЕБ є комплексний технічний контроль та маскування, що передбачає використання екранів, що захищають від радіосигналів, та інших заходів для забезпечення безпеки електронних систем. Також важливою є протидія за допомогою спеціальних систем розвідки та контррозвідки для виявлення ворожих елементів електронної боротьби та їх локалізації. Ця стаття має на меті допомогти читачам зрозуміти складність та важливість РЕБ в сучасному світі та висвітлити найефективніші методи боротьби з радіоелектронними загрозами. Для підтримки дослідження була проведена широка аналіз літератури та статей, які надають інформацію про сучасні методи та засоби РЕБ та їх застосування.*

Ключові слова: *радіоелектронна боротьба (РЕБ), радіоелектронне забезпечення, радіоелектронне придушення, радіоелектронний захист, перешкоди, кібернетичні загрози, радіолокатор.*

Постановка проблеми

Розвиток систем радіоелектронної боротьби стає найбільш ефективним, швидкореалізовуваним, економічно вигідним, а часом і єдино можливим засобом, що нейтралізує технічну перевагу протилежної сторони в інформаційній і технологічній сферах. Основний приріст бойових потенціалів в найближчій перспективі буде можливий за рахунок використання інтелектуальних систем управління військами та зброєю, а також застосування засобів збройної боротьби, які використовують нетрадиційні способи впливу на супротивника. Авторами дослідження встановлено, що оснащення озброєння засобами і комплексами радіоелектронної боротьби здатне багаторазово підвищити їхній бойовий потенціал і знизити можливі втрати. При цьому вартість техніки радіоелектронної боротьби становить одиниці відсотків по відношенню до вартості основних видів озброєння. В ході дослідження авторами були використані основні положення теорії радіоелектронної боротьби, теорії зв'язку, теорії сигналів та загальнонаукові методи аналізу та синтезу.

Авторами встановлено, що найважливішими напрямками досліджень для розвитку систем радіоелектронної боротьби є: інтеграція сил і засобів радіоелектронної боротьби із засобами розвідки і вогневого ураження в єдиному інформаційно-комунікаційному просторі всіх видів збройних сил; створення систем радіотехнічної розвідки (пасивної локації) для достовірного розкриття радіоелектронного обладнання і високоточного визначення місця розташування об'єктів; удосконалення системи моніторингу сигналів в різних фізичних полях. Принциповими особливостями побудови перспективних засобів і комплексів радіоелектронної боротьби є: надширокосмугові радіотехнічної частини апаратури (більше 3 октав); необхідність реалізації паралельної сигнальної обробки прийнятих радіотехнічних сигналів в миттєвій смузі частот, яка дорівнює кільком гігагерц; максимальне збільшення функціональної щільності виконання апаратури для зниження її масогабаритних показників і забезпечення можливості її системної інтеграції; гранична уніфікація базових цифрових елементів апаратури, що дозволяє знизити собівартість, полегшити процеси модифікації і модернізації апаратури. Враховуючи зазначене, напрямком подальших досліджень слід вважати розробку методів підвищення ефективності радіоелектронного подавлення.

Аналіз останніх досліджень і публікацій

Проте як і будь яка технологія WPA2 також є Радіоелектронна боротьба (РЕБ) є одним з ключових елементів сучасних бойових дій, який має цілями захист своїх військ від впливу засобів радіоелектронної розвідки та радіоелектронного придушення противника; радіоелектронну розвідку радіозасобів противника та їх радіоелектронне придушення. За своєю суттю РЕБ являє собою постійне протиборство між активними «атакуючими» системами та захисними системами, які «обороняються». До засобів РЕБ відноситься, крім іншого, широка мережа станцій радіоелектронної розвідки, що діють у багатьох країнах. Вони базуються на суші, на морі і в повітрі, та використовуються не тільки для моніторингу електромагнітного спектру, але й для придушення активних засобів противника різними способами. Основними завданнями РЕБ є: дезорганізація управління військами противника; зниження ефективності ведення розвідки і застосування зброї і бойової техніки противника; забезпечення надійної роботи систем і засобів управління своїми військами і зброєю.

Складовими частинами РЕБ є: розвідка РЕЗ противника; ураження, виведення зі строю пунктів управління та інших радіоелектронних об'єктів; радіоелектронне подавлення систем і засобів управління та розвідки; радіоелектронний захист засобів розвідки і систем управління своїми військами та зброєю; протидія технічним засобам розвідки противника. Сучасний етап розвитку збройних сил передових держав світу характеризується пріоритетним розвитком як засобів зв'язку та передачі інформації (ЗЗПІ), так й засобів радіоелектронної боротьби (РЕБ) як одного з найважливіших компонентів забезпечення інформаційної переваги в ході ведення бойових дій з'єднаннями і частинами сухопутних військ. Накопичений збройними силами розвинутих країн досвід і досягнутий технологічний рівень дозволяють їм найближчим часом перейти до оснащення військ передовими інформаційними системами і засобами передачі інформації, що якісно змінюють рівень інформаційного забезпечення бойових дій за рахунок додаткового збільшення обсягів і оперативності одержуваної інформації при реалізації мережного доступу на всіх рівнях управління. При цьому найбільша увага приділяється розвитку багатоканальних ЗЗПІ, щоб максимально скоротити цикл безпосереднього управління в умовах швидкої зміни оперативної і радіоелектронної обстановки.

Методи протидії РЕБ, з свого боку, мають за мету зменшення впливу РЕБ на роботу радіоелектронного обладнання, яке використовується у різних галузях, включаючи військову техніку, літаки, кораблі, транспортні засоби, електронні системи безпеки, телекомунікаційні мережі та багато іншого. Останні дослідження в цій галузі показують, що для ефективної протидії РЕБ необхідно використовувати інноваційні технології, такі як штучний інтелект, машинне навчання, квантові технології та інші. Крім того, з'являються нові методики тестування та валідації електронних систем для забезпечення їх захисту від РЕБ.

Важливою тенденцією останніх досліджень є також розробка і впровадження мультидисциплінарного підходу до розв'язання проблем РЕБ та захисту від нього. Це означає, що науковці з різних галузей співпрацюють для розробки комплексних рішень, які

включають в себе як технічні, так і організаційні заходи. Наприклад, з'явилися нові методи аналізу сигналів, які дозволяють більш точно виявляти електронні загрози та шпигунську діяльність.

До цього ж, з'являється все більше нових пристроїв та технологій, які можуть бути використані для РЕБ та протидії РЕБ. Наприклад, з'явилися нові програми для виявлення та блокування електронних загроз, нові радіоелектронні системи, що дозволяють розробляти більш ефективні методи протидії РЕБ, а також нові методи кодування та шифрування інформації. Усі ці розробки є дуже важливими для забезпечення безпеки та захисту від електронних загроз у сучасному світі, де електронні технології стають все більш поширеними та важливими у різних галузях життя.

Отже, можна зробити висновок, що РЕБ та методи протидії РЕБ є дуже важливими та невід'ємними частинами електронної безпеки. Постійне розвиток та вдосконалення цих методів є необхідним для забезпечення ефективного захисту від електронних загроз та шпигунської діяльності в сучасному світі.

Мета та постановка завдання

Постановка завдання полягає в аналізі сучасних методів радіоелектронної боротьби та методів її протидії. Основною метою є визначення переваг та недоліків цих методів та засобів та їх ефективності у боротьбі з радіоелектронними загрозами. Для досягнення поставленої мети потрібно вивчити теоретичні засади РЕБ, визначити основні методи і засоби, що використовуються в радіоелектронній боротьбі та методи її протидії, а також провести аналіз останніх досліджень та публікацій на цю тему. Отримані результати мають бути використані для розробки пропозицій щодо вдосконалення методів та засобів радіоелектронної боротьби та методів її протидії.

Виклад основного матеріалу дослідження

Радіоелектронна боротьба(РЕБ)

Розрізняють три складові частини радіоелектронної боротьби (рис. 1):

- пасивне радіоелектронне забезпечення;
- активне радіоелектронне придушення (РЕП)
- протидія радіоелектронному придушенню – радіоелектронний захист (РЕЗ).

Рис. 1. Складові частини радіоелектронної боротьби

Особливістю останніх двох складових частин є те, що розробка обладнання, що застосовується для їх ведення, супроводжується постійним змаганням одного з другим. Ця особливість, в цілому, відповідає глобальній тенденції розвитку зброї та протизброї – від давніх часів (щит проти меча) і до сучасності (літак проти зенітної установки і тому подібне). В той час як спеціаліст в області радіоелектронного придушення розробляє системи, які генерують різного роду перешкоди та хибні випромінення, інженер з радіоелектронного захисту розробляє засоби, призначені для зниження негативного впливу таких систем [1].

Типовий сценарій радіоелектронної боротьби – це протистояння між силами і засобами всіх трьох складових, радіоелектронного забезпечення, радіоелектронного придушення та радіоелектронного захисту. При цьому таке протистояння супроводжується постійним розвитком технічних засобів кожної з складових частин і тактики їх бойового застосування. Складність сучасних систем озброєння і обмеженість часу на ухвалення рішення підштовхують до висновку про те, що слабкою ланкою цих систем є людина-оператор через свої обмежені можливості з аналізу бойової обстановки та з прогнозування варіантів її розвитку. Однак це не завжди так і в деяких ситуаціях людина виявляється більш ефективною, ніж автоматичний обчислювач. Під час аналізу обстановки людина може враховувати свій попередній досвід, а

також легко змінювати значення показників своїх критеріїв прийняття рішень, таких, наприклад, як рішення про виявлення корисного сигналу на тлі перешкод. На відміну від цього, машина функціонує в межах заздалегідь запрограмованого простору можливих варіантів таких показників [2].

Змагання між машиною і людиною для такої сфери ведеться в напрямку розвитку штучного інтелекту. І хоча в цьому напрямку вже досягнуті значні успіхи, доведеться пройти ще довгий шлях до того моменту, коли настане ера повної автоматизації. Об'єм необроблених («сирих») даних, що поступають від датчиків різного типу, вже зараз настільки великий, що для його обробки необхідні все сучасніші обчислювальні засоби та складні алгоритми обробки. Це, в свою чергу, тягне за собою підвищення вимог до кваліфікації операторів, тому останнім часом ринок освітніх послуг по системам радіоелектронної боротьби, а також засобів їх моделювання суттєво зріс. Однак мають місце ситуації, коли навіть це не може допомогти, як, наприклад, для пілота одномісного винищувача, якому надходить велика кількість різноманітної інформації, а час на прийняття рішення обчислюється секундами, коли необхідно реагувати на ракетну атаку. В такому випадку кращою є автоматична система протидії (викидання перешкод, виконання протиракетного маневру) з передбаченим пріоритетом ручного керування в якості заходу безпеки [1].

Другим важливим аспектом є те, щоби програмне забезпечення могло бути модифікованим, тобто мало, так звану відкриту архітектуру. Прикладом, що підтверджує доцільність такого підходу, може служити війна в Персидській затоці, коли системи РЕБ, розроблені для протидії радянським радіолокаційним та зенітним засобам, застосовувались проти подібних засобів західного виробництва. З цієї причини сучасні радіолокаційні приймачі та генератори перешкод працюють під управлінням програмного забезпечення, яке може бути гнучко адаптовано відповідно до актуальних загроз.

Радіоелектронне забезпечення

Радіоелектронне забезпечення має два основних види [5]:

- *Радіотехнічна розвідка, РТР* - радіотехнічна розвідка ведеться, головним чином, шляхом перехоплення та аналізу сигналів, випромінюваних радіолокаторами виявлення, управління вогнем та наведення ракет. Часто отримані дані передаються на засоби радіоелектронного придушення.
- *Радіорозвідка, РР* - радіорозвідка ведеться шляхом перехоплення повідомлень, що передаються як голосовими каналами зв'язку, так і каналами передачі даних.

Якість функціонування систем РТР та РР багато в чому визначається їхніми обчислювальними системами, за допомогою яких реалізуються функції аналізу прийнятих сигналів. Програмне забезпечення таких систем виконує аналіз безлічі сигналів. База даних типової обчислювальної системи містить параметри 2000 і більше різноманітних радіо- та радіолокаційних систем. Крім цього, програмне забезпечення може бути налаштоване оператором для зберігання невпізнаних сигналів з метою їх аналізу в подальшому. Процес обробки прийнятих сигналів складається з трьох послідовних етапів:

- сортування сигналів по мірі їх надходження;
- розподіл їх по класам, групам;
- ідентифікація джерел сигналів.

Об'єднання систем радіотехнічної розвідки та радіорозвідки називають системою радіоелектронної розвідки (РЕР) (рис. 2).

Рис. 2. EL/L-8300 SIGnals INTelligence System, що охоплює діапазон частот від 0,03 до 40 ГГц

Радіоелектронне придушення

Радіоелектронне придушення (РЕП) являє собою активну складову частину радіоелектронної боротьби. Воно проводиться з метою порушення функціонування систем розвідки противника, його радіолокаційних систем та систем зв'язку, а також протидії будь-яким його системам озброєння, які використовують радіоелектронні або оптико-електронні (інфрачервоні або лазерні) системи для наведення або прицілювання. Для досягнення цієї мети використовуються два методи: постановка перешкод та генерування хибних сигналів. При правильному використання обидва методи достатньо ефективні. У багатьох сучасних зразках техніки радіоелектронного придушення, особливо у військово-морських силах, обидва методи використовуються в єдиній інтегрованій системі. В якості перешкод можуть формуватися як активні, так і пасивні перешкоди [3-4].

Випромінювання активних шумових перешкод виконується з метою порушення функціонування каналів зв'язку противника або для введення його радіолокаційного обладнання в режим насищення та приховування, тим самим, своїх об'єктів від виявлення. Хоча це і може призводити до втрати противником його інформаційних каналів, але на станціях

активних перешкод вже не може проводиться приймання та аналізування сигналів противника. Крім цього, сучасні системи зв'язку, що використовують швидке переналаштування частоти, вже не так просто ефективно придушити.

Прості шумові перешкоди як і раніше широко застосовуються у наземних бойових діях. При цьому одним з важливих варіантів їх застосування є передавачі перешкод, які закидаються дистанційно. Вони можуть бути встановлені вручну, закинуті за допомогою спеціальних артилерійських боєприпасів, скинуті з літаків або встановлені на безпілотних літальних апаратах. Такі передавачі, як правило, використовуються короткочасно, в рамках конкретної бойової операції (рис. 3).

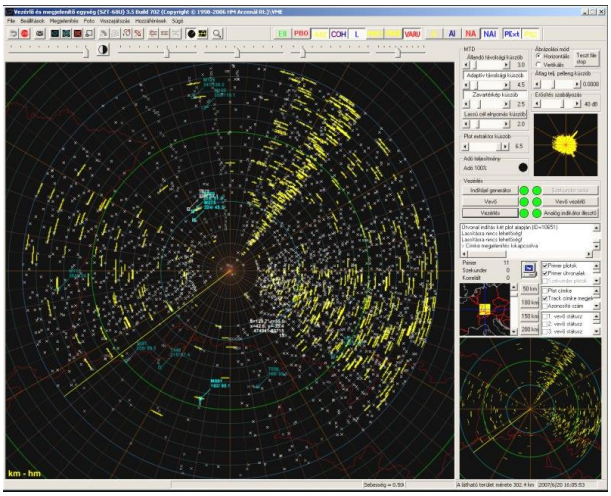

Рис. 3. На індикаторі радіолокатора — інтенсивні несинхронні імпульсні перешкоди з напрямку 30° (S-діапазон), пристрій виявлення відміток перевантажений

В рамках другого методу радіоелектронного придушення використовуються штучні відбивачі (частіше за все — дипольні відбивачі) для протидії радіолокаційним засобам або різноманітні джерела випромінення в оптичному діапазоні (наприклад, патрони з факелами) для протидії оптико-електронним засобам. Перші застосування дипольних відбивачів відносяться до періоду Другої світової війни та з тих пір самі відбивачі мало змінилися. При цьому суттєво змінилися засоби їх доставки та викидання. Патрони з факелами, використовувані проти оптико-електронних систем, викидаються з контейнерів. Більшість таких контейнерів пристосовані для доставки як дипольних відбивачів, так і патронів з факелами.

Радіоелектронний захист

Радіоелектронний захист (РЕЗ) є заходом у відповідь в умовах, коли противник проводить радіоелектронне придушення. Радіоелектронний захист охоплює всі методи та засоби, які має радіоелектроніка, включно із заходами щодо забезпечення скритності дій радіо- та радіолокаційних систем, методи комплексування та дублювання, спеціальні методи перешкодостійкої обробки сигналів. Це надзвичайно чутлива сфера, оскільки розкриття заходів радіоелектронного захисту, реалізованих в конкретній системі, дає противнику інформацію про вразливості даної системи до радіоелектронного придушення. Якість радіоелектронного захисту характеризується показниками перешкодозахищеності, які відносяться до найважливіших тактико-технічних характеристик радіоелектронної системи. Перешкодозахищеність системи характеризує її здатність забезпечувати потрібні точність визначення інформативних параметрів сигналів та пропускну спроможність (швидкодію) з урахуванням впливу можливих перешкод. У загальному випадку перешкодозахищеність системи забезпечується перешкодостійкістю та скритністю її дії. Скритність дії утруднює можливому противнику виявлення факту функціонування системи та визначення характеристик випромінюваних нею радіосигналів з метою створення ефективних навмисних радіоперешкод. Перешкодостійкість забезпечує нормальне функціонування системи в умовах дії певної сукупності ненавмисних та навмисних (організованих) перешкод[9].

Розрізняють три основні групи методів захисту від перешкод: захист приймача від перевантажень, селекція від перешкод, компенсація перешкод.

Для захисту від перевантажень, які призводять до нелінійних ефектів, застосовують лінеаризацію широкосмугового високочастотного тракту приймача. Один з самих розповсюджених способів боротьби з перевантаженнями — автоматичне регулювання підсилення (АРП).

Селекція передбачає відділення сигналу від перешкод за рахунок використання відмінностей в їхніх властивостях та параметрах. Розділяють просторово-часову селекцію, частотну селекцію, функціональну селекцію та адаптацію. Найбільш часто використовуються частотна селекція та переналаштування робочої частоти. Частотна селекція ґрунтується на відмінностях спектрів сигналів та перешкод по несівним частотам та ширині смуги частот, на основі чого в тракт прийому вводяться фільтри, узгоджені зі спектром сигналу. Переналаштування частоти (як правило, стрибкоподібне) призводить до необхідності противнику генерувати перешкоду в широкій смузі частот, що викликає «розмазування» потужності перешкоди по всій цій смузі, або до необхідності безперервно визначати робочу частоту кожного імпульсу та миттєво переналаштовувати частоту постановника перешкод. Компенсацію перешкод здійснюють спеціальні схеми придушення сигналів, прийнятих по бічним пелюсткам діаграми направленості антени. Реалізація цих методів потребує наявності спеціальних компенсаційних антен та додаткових приймальних каналів.

Крім цього, в рамках радіоелектронного захисту виконуються заходи, спрямовані на захист радіолокаторів від протирадіолокаційних ракет (снарядів, са-

монавідних на випромінення). Основними заходами, в даному випадку, є: зниження рівня випромінення по бічним пелюсткам, переналаштування по частоті та використання хибних передавачів, які імітують роботу радіолокатора. При цьому, імітуючий передавач має знаходитися достатньо близько до радіолокатора, який ним захищається. Цим забезпечується перенацілювання ракети на нього. Проте він не має розташовуватися занадто близько, щоби уникнути пошкодження радіолокатора при попаданні ракети в хибний передавач.

Радіоелектронні перешкоди

Багато складних радіоелектронних систем встановлені в аеропортах, на літаках або на кораблях. Здатність цих систем одночасно одна з одною виконувати свої функції в умовах ненавмисних перешкод та не створювати, при цьому, перешкод іншим радіоелектронним засобам називають електромагнітною сумісністю (EMC). Перешкодами називають сторонні електромагнітні випромінювання, які погіршують характеристики приймачів радіоелектронних систем (рис. 4). Загалом радіоелектронні перешкоди можливо розбити на такі категорії [9].

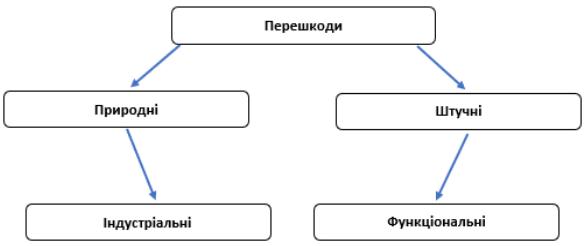

Рис. 4. Можливі типи радіоелектронних перешкод

Перешкоди бувають:

1. Індустріальні - індустріальними або промисловими перешкодами називають випромінення різноманітних засобів, не призначених спеціально для випромінення електромагнітних хвиль. До них відносяться лінії електропередачі, електродвигуни та перемикачі;

2. Функціональні - перешкоди, джерелами яких є засоби, нормальною частиною роботи яких є випромінення електромагнітних хвиль (рис. 5). Такі перешкоди можуть бути ненавмисними (випромінення інших бортових засобів крім того, що розглядається) або навмисними (радіоелектронне придушення);

3. Природні - електромагнітні перешкоди, що спричинені природними явищами, такими як гроза, електромагнітне випромінення сонця та зірок.

Приймальні системи мають в своєму складі захисні пристрої та кола, призначені для відділення корисних сигналів від перешкод. Таке розділення здійснюється на основі відмінностей в характеристиках сигналів та перешкод, наприклад, спектральних (частотних) відмінностей.

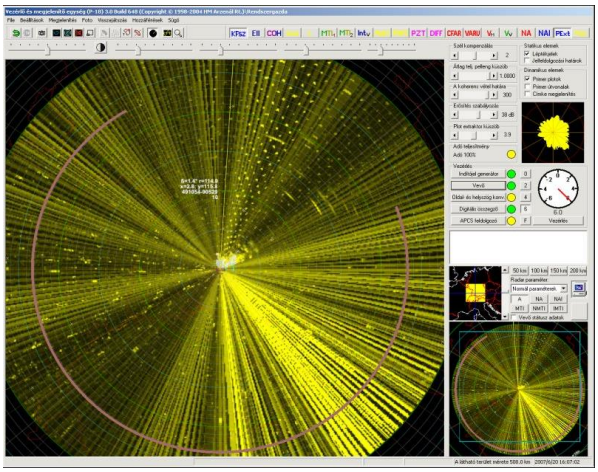

Рис. 5. Індикатор огляду радіолокатора метрового (VHF) діапазону у випадку впливу активних шумових перешкод (постановник перешкод знаходиться на азимуті 150°)

До таких пристроїв відносяться преселектори, обмежувачі, фільтри і т. п. Слід розуміти, що всі ці пристрої не забезпечують повного придушення перешкод, а лише зменшують їх вплив. Поряд з цим застосовують й просторове рознесення, коли антени різних випромінюючих пристроїв розміщують на певних відстанях одна від одної, що забезпечують прийнятний рівень ненавмисних перешкод. Крім цього, виконуються заходи з контролю рівня небажаного випромінення активних радіоелектронних засобів. До них відносяться використання фільтрів, які обмежують позасмугове випромінення, а також металевих екранів [7-9].

Комплексний технічний контроль та маскування

Одним з способів, що застосовують для приховування своїх об'єктів від виявлення радіолокаційними засобами противника, є постановка перешкод. Оскільки їх основним призначенням є маскування корисного сигналу, такі перешкоди відносяться до класу маскувальних перешкод. Маскувальні перешкоди можуть бути активними та пасивними [4].

У випадку активних шумових перешкод до внутрішніх шумів приймача радіолокатора додається шум у вигляді перешкоди. Таким чином, відношення «сигнал-шум» погіршується. Це, в свою чергу, призводить до зниження імовірності виявлення та до збільшення імовірності хибної тривоги. У випадку застосування потужних активних перешкод може відбуватися повне маскування цілі, тобто має місце ситуація, коли ціль радіолокатором не виявляється. В практиці радіоелектронної боротьби застосовують шумові перешкоди різних видів. Найбільш розповсюдженими є загороджувальні перешкоди (по часу, по частоті, по куту) та прицільні перешкоди. Загороджувальні шумові перешкоди мають достатньо велику ширину спектру та застосовуються у випадках, коли параметри радіолокатора, який потрібно придушити, не відомі. Прицільні перешкоди, навпаки, мають спектр, узго-

джений із спектром сигналів радіолокатора, який придушується.

Активні перешкоди можуть бути настільки інтенсивними, що повністю закривають радіолокаційний приймач (рис. 6). Тоді на виході приймача вже не буде імпульсних сигналів, а замість цього буде мати місце певна постійна напруга. В таких випадках зашумлена область на екрані індикатору радіолокатора не стає яскравішою, а навпаки, згасає [11].

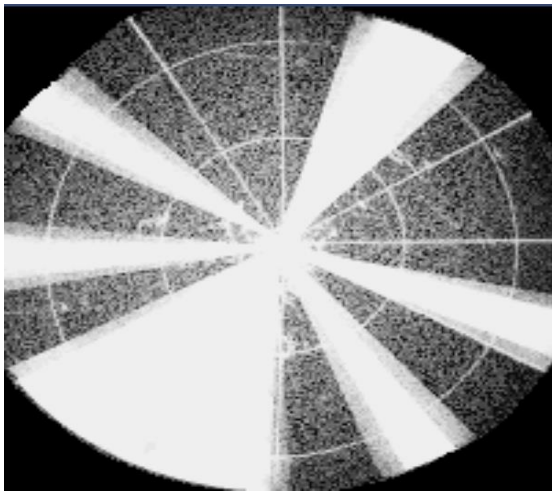

Рис. 6. Вигляд індикатора радіолокатора при дії активної шумової перешкоди. Постановник перешкод на азимуті 210°

До *пасивних маскувальних перешкод* відносяться перешкоди, спричинені відбиттями зондувальних сигналів радіолокатора від хмар дипольних відбивачів (рис. 7). Історично дипольні перешкоди (станіолієві стрічки) — найперші засоби, що почали використовуватися для радіоелектронного маскування ще з часів Другої світової війни. Проте їх з успіхом застосовують дотепер. Маючи малу вагу та будучи викинутими з літака, дипольні відбивачі утворюють хмару, яка повільно переміщується в просторі під дією вітру. Задля збільшення маскувального ефекту довжину дипольних відбивачів підбирають під довжину хвилі радіолокаторів противника. Відбиті від хмар дипольних відбивачів сигнали спричиняють засвічення значних областей на індикаторі радіолокатора, погіршуючи або унеможливлюючи виявлення сигналів, відбитих справжніми цілями.

Для протидії негативному впливу маскувальних перешкод проводять заходи радіоелектронного захисту. Так, наприклад, для придушення пасивних маскувальних перешкод використовують відмінності їхніх спектральних характеристик від спектральних характеристик сигналів відбитих від реальних цілей. Останні, як правило, рухаються у просторі набагато швидше, а значить мають більші значення допплерівського зсуву несівної частоти. Здатність радіолокатора виявляти цілі на фоні пасивних маскувальних перешкод називають під завадовою видимістю [10].

Рисунок 7. Дипольні відбивачі RR-129 та RR-144, а також їх контейнери

Імітаційні перешкоди застосовують для створення хибної інформації. За структурою такі перешкоди подібні до сигналів, що використовуються в радіолокаторі, і тому створюють на його індикаторі відмітки хибних цілей, подібні до реальних. Цей ефект призводить до перевантаження обчислювача великою кількістю хибних сигналів, до втрати частини (або всіх) корисних сигналів, до збільшення імовірності хибної тривоги, що, в підсумку, призводить до ухвалення помилкових рішень. Якщо йдеться про радіолокатори керування зброєю, то застосування противником імітуючих перешкод може призводити до зриву автоматичного супроводження цілі по одній або декільком координатах (напрямку, дальності, швидкості) та до перенацілювання слідкуючих систем на хибні цілі. Частота повторення імітаційних перешкод може не співпадати або співпадати з частотою повторення зондувальних імпульсів радіолокатора, який намагаються придушити. Відповідно до цього розрізняють:

1. Асинхронні перешкоди, коли частота слідування сигналів перешкоди не співпадає з частотою слідування сигналів радіолокатора. Вплив асинхронної перешкоди проявляється у вигляді спіральних ліній на індикаторі радіолокатора (рис. 8);

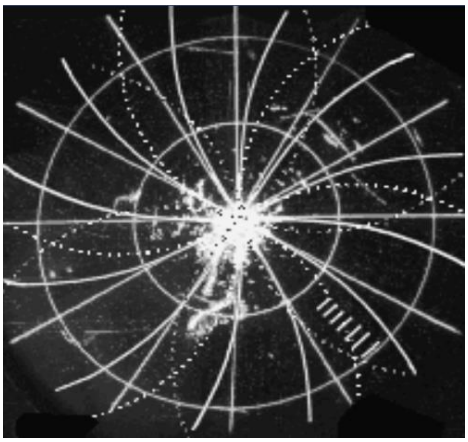

Рисунок 8. Вигляд індикатора радіолокатору при впливі імітаційних перешкод

2. Синхронні перешкоди, коли частота слідування сигналів перешкоди співпадає з частотою слідування сигналів радіолокатора. Одним з способів отримання такої перешкоди є приймання зондувальних сигналів радіолокатора з подальшим їх спотворенням та перевипромінюванням. Такі перешкоди називають імітаційними у відповідь. Параметри сигналу імітаційної перешкоди у відповідь підбираються таким чином, щоби спричинити в радіолокаторі формування відміток цілей з координатами (кутовий напрямок, дальність) та параметрами руху (швидкість), які відрізняються від реальних цілей.

На рис. 8 показаний приклад впливу імітаційної синхронної перешкоди: в напрямку азимута 135° спостерігається сім відміток цілей, розташованих одна за одною. Очевидно, що це хибні відмітки хоча б тому, що їхня ширина не відповідає ширині діаграми направленості антени: із збільшенням дальності від радіолокатора лінійний розмір відеовідмітки має збільшуватися, тоді як в даному випадку він лишається постійним. Для захисту радіолокатора від таких перешкод використовують навмисне змінення частоти слідування імпульсів за певним законом.

Для радіолокаторів, в яких реалізоване автоматичне виявлення цілей, застосування проти них імітаційних перешкод небезпечне ризиком перевантаження обчислювальної системи хибними відмітками. Наприклад, радіолокатор СТ-68У забезпечує обробку лише 128-ми відміток цілей, з яких тільки 32 цілі в режимі автоматичного супроводження. Якщо на вхід пристрою обробки (обчислювальної системи) поступить більша кількість відміток цілей, то відмітки деяких реальних цілей будуть втрачені, а їхні траєкторії, як наслідок, скинуті з автоматичного супроводження [8-9]. Якщо апаратні та програмні засоби радіолокатора дають змогу виділяти імітаційні перешкоди, то на індикаторі кругового огляду (ІКО) формуються спеціальні «строби» у вигляді засвіченої смуги шириною в декілька кілометрів на краю екрану (рис. 9). За азимутом «строби» відповідають напрямку, з якого надходять сигнали перешкоди.

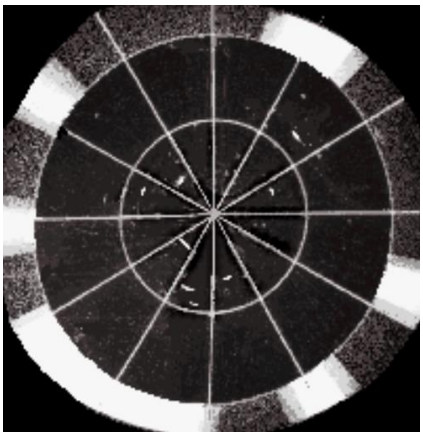

Рис. 9. Вигляд індикатора радіолокатору з ввімкненою системою захисту від перешкод

Методи та засоби протидії РЕБ

В сучасних умовах РЕБ є важливою складовою частиною військової діяльності, оскільки забезпечує збереження власних життів та здоров'я воїнів, збереження та знищення техніки противника, а також виконання бойових завдань. Нижче наведені основні методи та засоби протидії РЕБ, що включають в себе [9]:

1. Використання захисту від електронної боротьби. Це можуть бути різноманітні екрани, що захищають від радіосигналів.

Екрани - це матеріали, які використовуються для зменшення або блокування проходження радіосигналів. Їх також можна називати екрануючими матеріалами або екранами РЧ-сигналу. Екрани використовуються для захисту електронних пристроїв та обладнання від шуму, перешкод та звуження смуги пропускання.

Є кілька типів екранів, які використовуються для захисту від радіосигналів, зокрема:

- металеві екрани: це екрани, зроблені з металу, такого як мідь, алюміній або сталь. Металеві екрани можуть бути у вигляді металевої фольги або сітки, що захищає електронне обладнання від небажаних радіосигналів;
- провідні екрани: це екрани, що складаються з провідного матеріалу, такого як мідна сітка або плетінка, яка може захищати електронні пристрої від електромагнітних перешкод;
- композитні екрани: це екрани, що складаються з композитних матеріалів, таких як вуглецеві волокна, кевлар або фіберглас. Вони можуть бути більш ефективними для блокування електромагнітних хвиль, ніж металеві екрани;
- ферромагнітні екрани: це екрани, зроблені з матеріалів, які вміщують феромагнітні властивості, такі як залізо, нікель або кобальт. Ці екрани можуть блокувати електромагнітні хвилі;
- акустичні екрани: це екрани, що захищають від радіосигналів, які працюють на принципі зменшення шуму, що створюється небаж;
- використання засобів та методів маскування, що знижують електромагнітну зону видимості техніки та об'єктів. Це можуть бути різноманітні засоби розсіювання радіосигналів, розведення антен, використання діелектричних покриттів тощо.

2. Використання спеціальних систем розвідки та контррозвідки для виявлення ворожих елементів електронної боротьби та їх локалізації.

Ці системи дозволяють виявляти та локалізувати ворожі елементи РЕБ та вживати заходів для їх нейтралізації. Один із способів розвідки ворожих елементів РЕБ полягає в використанні радіотехнічних засобів, таких як спектральні аналізатори, радіолокаційні системи та приймачі сигналів. Ці засоби дозволяють виявляти сигнали, які випромінюються від ворожих елементів РЕБ, і встановлювати їхнє місцезнахо-

дження. Контррозвідка полягає у заходах для виявлення та нейтралізації ворожих елементів РЕБ, які можуть бути розташовані на території або в електронних системах власної армії. Для цього використовуються різноманітні засоби, такі як спеціальні радіотехнічні комплекси, які дозволяють виявляти інформаційні потоки ворога, системи виявлення забезпечують надійний захист від вторгнень у системи управління та зв'язку. Крім того, контррозвідка включає в себе інші заходи, такі як відлов сигналів, зміна параметрів зв'язку, розробка нових антен і систем захисту від РЕБ [6-9].

3. Використання систем захисту від кібератак та інших видів кібернетичних загроз, що можуть бути використані для атак на електронні системи.

Кібератаки можуть бути спрямовані на різні види електронних систем, включаючи системи зв'язку, електронні системи керування, комп'ютерні мережі та інші. Для захисту від кібератак, необхідно використовувати комплексні підходи та застосовувати різноманітні технології захисту. Однією з ключових технологій є застосування криптографічних методів захисту, таких як шифрування трафіку та ідентифікація користувачів. Інші технології захисту включають застосування брандмауерів, систем виявлення вторгнень, антивірусного програмного забезпечення та інших заходів.

4. Використання резервних систем зв'язку та комунікації для забезпечення продовження ведення операцій в разі порушення роботи основних систем.

Резервні системи зв'язку та комунікації можуть бути забезпечені через використання резервних каналів зв'язку, забезпечення альтернативних джерел живлення, використання резервних засобів збереження даних та інші методи. Одним з найпоширеніших методів забезпечення резервних систем зв'язку є використання супутникового зв'язку. Цей метод забезпечує можливість зв'язку в будь-якому місці, де є пряма видимість на супутник, та не потребує будь-яких інфраструктурних засобів зв'язку на місці. Також можуть бути використані мобільні системи зв'язку, такі як мобільні телефони, радіостанції та інші засоби зв'язку, що не потребують певних інфраструктурних засобів для функціонування [9].

5. Використання спеціальних систем захисту від електромагнітного імпульсу (ЕМР), що можуть виникнути внаслідок ядерного вибуху або іншого джерела.

Системи захисту від ЕМР можуть бути різного типу і мати різні рівні захисту, в залежності від вимог і потреб користувача. Одним зі способів захисту від ЕМР є використання спеціальних екранів, які забезпечують електромагнітну ізоляцію електронних систем. Ці екрани забезпечують захист від електромагнітних полів інших систем та пристроїв, що можуть викликати ЕМР. Іншими методами захисту від ЕМР є використання захисних оболонок, які зменшують електромагнітну енергію, що входить до системи, або використання систем, що автоматично вимикають або відключають електронні системи, щоб запобігти їх пошкодженню. Також можна використовувати бекап-системи, які дозволяють відновлювати роботу систем після ЕМР.

6. Заборона використання певних електронних систем та протоколів зв'язку, що можуть бути особливо вразливими до ворожої електронної боротьби.

Це може включати заборону використання застарілих або вразливих систем, які можуть бути підвергнуті атакам. Також може включати заборону використання певних типів бездротових зв'язків, які можуть бути залучені до інтерференції з ворожими сигналами.

Однак, заборона використання певних електронних систем та протоколів зв'язку може мати свої недоліки, такі як обмеження можливостей комунікації та обмеження можливостей використання новітніх технологій. Таким чином, цей метод повинен використовуватись з обережністю та відповідним чином збалансовуватись з іншими методами протидії ворожій електронній боротьбі [9-11].

Висновки. Загальною метою радіоелектронної боротьби є забезпечення функціонування електронних систем та інших пристроїв в умовах впливу радіосигналів, що може бути використано для розвідки, перешкоджання та навіть знищення. Для досягнення цієї мети використовуються різноманітні методи та засоби, такі як комплексний технічний контроль та маскування, захист від кібератак, системи захисту від електромагнітного імпульсу та використання резервних систем зв'язку та комунікації. Одним із важливих аспектів боротьби з РЕБ є комплексний технічний контроль та маскування, що передбачає використання екранів, що захищають від радіосигналів, та інших заходів для забезпечення безпеки електронних систем. Також важливою є протидія за допомогою спеціальних систем розвідки та контррозвідки для виявлення ворожих елементів електронної боротьби та їх локалізації.

Нарешті, одним зі способів протидії РЕБ є використання систем захисту від кібератак та інших видів кібернетичних загроз, що можуть бути використані для атак на електронні системи. Загальною метою всіх цих заходів є забезпечення безпеки електронних систем та забезпечення продовження їх роботи в умовах впливу радіосигналів та інших видів електронної боротьби.

Список літератури

[1]. Соколов, В. Ю. (2015). Новітні технології радіоелектронної боротьби.Озброєння та військова техніка, 2(14), С. 48-50. http: // nbuv.gov.ua / UJRN /ovt_ 2015_ 2_13.

[2]. 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.

[3]. Smith, J. (2018). Electronic Warfare in the New Threat Environment. Military Electronics, 12(2). pp. 32-37.

[4]. Martinez, M. A., & Ratti, R. (2020). Radar Electronic Warfare (EW) Techniques in the Modern Battlefield. Journal of Military and Strategic Studies, 22(2), pp. 1-20.

[5]. Schleher, D. C. (2019). Electronic warfare in the 21st century: challenges, threats and opportunities. IET Radar, Sonar & Navigation, 13(3), pp. 328-333. DOI: 10. 1049/iet-rsn.2018.5344.

[6]. Satori, K. (2020). Electronic Warfare: A Brief Overview of the Current State of Technology and Its Impact on the Battlefield. Journal of Cybersecurity and Information Management.

[7]. Gromov, A., Stogniy, A., & Chechin, A. (2021). The Use of Artificial Intelligence for Electronic Warfare Tasks. International Journal of Advanced Computer Science and Applications, 12(4), pp. 152-158.

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

[9]. Лозинський, В. В. (2018). Електронна боротьба у системі підготовки та проведення бойових дій Збройних Сил України. Озброєння та військова техніка, 2(14), pp. 48-57. http: // journal.utm.md / index. php/ctve/article/view/10770.

[10]. Коваленко, М. В., Гаєвський, І. М., & Матюшенко, В. Ю. (2019). Методи та засоби радіоелектронної боротьби на сучасному етапі. Вісник Національного технічного університету України "КПІ". Серія: Радіотехніка, радіоапаратобуду.

[11]. Артюх В. М., Купріянов І. Л., Левенець В. О. Аналіз ефективності систем радіоелектронної боротьби за методикою множинного вибору. Вісник Національного університету "Львівська політехніка". 2017. № 881. С. 95-101.

УДК 629.735.05:621.396.6(043.2)

Opirskyy I., Bybyk R. Research on modern methods of Electronic Warfare (EW) and methods and means of its counteraction

Abstract. *Electronic warfare (EW) is the process of protecting against enemy electronic devices that can be used to interfere with communications, control, and reconnaissance. In modern warfare, electronic warfare is crucial for both sides of the conflict. The main objectives of EW are to disrupt enemy troop management, reduce the effectiveness of reconnaissance and enemy weapons and equipment, and ensure the reliable operation of systems and equipment for managing one's troops and weapons. This article reviews modern methods of electronic warfare, their technical characteristics, and effectiveness. Different types of EW tools are explored, including active and passive systems used for protection against radar. Issues related to the use of EW by military and civilian organizations are discussed, and examples of modern EW methods and technologies are provided. Methods for hiding objects from detection by enemy radar devices are also examined. In modern conditions, EW is an important component of military operations, as it ensures the preservation of soldiers' lives and health, the preservation and destruction of enemy equipment, and the accomplishment of combat tasks. The article also discusses the main methods and means of countering EW. To ensure the functioning of electronic systems and other devices under the influence of radio signals, various methods and means are used, such as complex technical control and masking, protection against cyber-attacks, protection systems against electromagnetic impulses and the use of backup communication and communication systems. One of the important aspects of the fight against EW is complex technical control and masking, which involves the use of shields that protect against radio signals and other measures to ensure the security of electronic systems. It is also important to counteract with the help of special intelligence and counter-intelligence systems to detect enemy elements of electronic warfare and their localization. The aim of this article is to help readers understand the complexity and importance of EW in the modern world and to highlight the most effective methods of combating electronic threats. To support the research, a wide analysis of literature and articles providing information on modern EW methods and tools and their application was conducted.*

Key words*: Electronic Warfare (EW), Electronic Protection, Electronic Suppression, Electronic Defense, Interference, Cyber Threats, Radar.*

Опірський Іван Романович, доктор технічних наук, професор, кафедра захисту інформації, Національного університету «Львівська політехніка».
Ivan Opirskyy, doctor of Technical Sciences, professor, Department of Information Security, Lviv Polytechnic National University.

Бибик Роман Тарасович, асистент, кафедра захисту інформації, Національного університету «Львівська політехніка».
Roman Bybyk, assistant, Department of Information Security, Lviv Polytechnic National University.

Отримано *7 серпня 2023 року,* затверджено редколегією *28 серпня 2023 року*