РАДІОЕЛЕКТРОННІ ЗАСОБИ МОНІТОРИНГУ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Шабетя Сергій Анатолійович [1]

Опубліковано	Секція	УДК
30.06.2025	Економіка	355.01+327.8

DOI: https://doi.org/10.5281/zenodo.17151367

Анотація. У статті розглядається важлива та актуальна проблема застосування радіоелектронних засобів моніторингу (РЗМ) в умовах інформаційної війни. Наголошується, що стрімкий розвиток цифрових технологій, зокрема систем зв'язку та передачі даних, спричинив суттєві зміни у веденні сучасних бойових дій, де домінуючим чинником стає інформаційна перевага. Особливої актуальності набуває використання радіоелектронних засобів для виявлення, аналізу та протидії інформаційним загрозам, зокрема у формі радіоелектронного придушення, дезінформації та кібератак.

У статті систематизовано сучасні підходи до організації радіоелектронного моніторингу в межах концепції мережецентричної війни, що активно впроваджується провідними державами світу. Автори аналізують структуру та принципи дії систем РЕБ (радіоелектронної боротьби), визначають ключові етапи їх функціонування — від збору та обробки сигналів до інтерпретації результатів і реалізації заходів протидії. Окрему увагу приділено технічним засобам, таким як комплекси RQ-4 Global Hawk і українська система «Кольчуга», а також перспективним технологіям, серед яких штучний інтелект, нейронні мережі, адаптивні фільтри та квантові методи обробки сигналів.

Стаття пропонує алгоритм застосування РЗМ у шість етапів: підготовка, збір інформації, обробка сигналів, аналіз загроз, реагування та протидія, а також підсумкова оцінка ефективності. Також представлено класифікацію РЗМ за функціональністю, типом сигналу, способом застосування та призначенням, що дозволяє системно підійти до побудови комплексів інформаційного захисту.

Автори обґрунтовують необхідність удосконалення існуючих засобів моніторингу та впровадження новітніх методів, здатних вчасно реагувати на складні і динамічні загрози в інформаційному просторі. Підкреслюється роль РЗМ не лише у військовій, а й у цивільній сфері для забезпечення стабільного функціонування критичної інфраструктури.

У висновках зроблено наголос на важливості інтеграції РЗМ з іншими елементами систем безпеки, а також на потребі в подальших дослідженнях у галузі застосування інтелектуальних алгоритмів в умовах гібридних загроз. Таким чином, стаття сприяє поглибленню наукового розуміння інформаційної безпеки та окреслює практичні

[1] Науковий співробітник
Український науково-дослідний інститут
спеціальної техніки та судових експертиз
Служби безпеки України
https://orcid.org/0000-0002-9459-6102

шляхи підвищення ефективності використання радіоелектронних засобів у сучасних умовах.

Ключові слова: радіоелектронні засоби моніторингу; інформаційна війна; радіоелектронна боротьба; радіочастотний спектр; аналіз сигналів; кібербезпека; інтелектуальні технології.

RADIO-ELECTRONIC MONITORING MEANS IN INFORMATION WARFARE CONDITIONS

Abstract. The article considers the important and urgent problem of the use of electronic means of monitoring (EWM) in the conditions of information warfare. It is emphasized that the rapid development of digital technologies, in particular communication and data transmission systems, has caused significant changes in the conduct of modern combat operations, where the dominant factor is information advantage. The use of electronic means to detect, analyze and counter information threats, in particular in the form of electronic suppression, disinformation and cyberattacks, is of particular relevance. The article systematizes modern approaches to the organization of electronic monitoring within the framework of the concept of network-centric warfare, which is actively implemented by leading countries in the world. The authors analyze the structure and principles of operation of electronic warfare (EW) systems, determine the key stages of their functioning - from the collection and processing of signals to the interpretation of results and the implementation of countermeasures. Special attention is paid to technical means, such as the RQ-4 Global Hawk complexes and the Ukrainian Kolchuga system, as well as promising technologies, including artificial intelligence, neural networks, adaptive filters and quantum signal processing methods.

The article proposes an algorithm for the use of REM in six stages: preparation, information collection, signal processing, threat analysis, response and counteraction, as well as a final assessment of effectiveness. The classification of REM by functionality, signal type, method of application and purpose is also presented, which allows a systematic approach to the construction of information protection complexes.

The authors justify the need to improve existing monitoring tools and implement the latest methods capable of responding in a timely manner to complex and dynamic threats in the information space. The role of REM not only in the military, but also in the civilian sphere to ensure the stable functioning of critical infrastructure is emphasized.

The conclusions emphasize the importance of integrating REM with other elements of security systems, as well as the need for further research in the field of applying intelligent algorithms in the context of hybrid threats. Thus, the article contributes to a deeper scientific understanding of information security and outlines practical ways to increase the effectiveness of the use of radio-electronic means in modern conditions.

Keywords: radio-electronic monitoring means; information warfare; radio-electronic warfare; radio-frequency spectrum; signal analysis; cybersecurity; intelligent technologies.

Вступ

Постановка проблеми. В умовах сучасного світу, коли інформаційні технології активно впливають на всі сфери життя, особливого значення набувають радіоелектронні засоби моніторингу (РЗМ). Інформаційна війна, що характеризується активним використанням дезінформації, кібератак, радіоелектронного придушення та моніторингу, вимагає нових підходів до захисту інформації та забезпечення національної безпеки.

Радіоелектронні засоби моніторингу є важливим елементом інформаційної безпеки, оскільки вони дозволяють виявляти, аналізувати та попереджувати загрози з боку противника. Завдяки розвитку технологій, сучасні РЗМ можуть перехоплювати

радіосигнали, проводити спектральний аналіз, здійснювати радіолокаційне зондування та виявляти різноманітні джерела випромінювання.

При цьому, концепція мережецентричної війни (МЦВ) відкриває нові можливості для ведення військової протидії, зокрема в інформаційному просторі, який стає новим середовищем бойових дій. Одночасно з цим з'являється новий вид озброєння — інформаційна зброя, основним компонентом якої виступають засоби радіоелектронної боротьби (РЕБ).

Системи РЕБ здатні забезпечити суттєву перевагу в майбутніх військових конфліктах, нейтралізуючи противника, навіть якщо він володіє більш розвиненими технологіями [1].

У зв'язку з цим, виникає проблема забезпечення ефективного моніторингу радіоелектронного середовища в умовах інформаційної війни. Основними викликами є захист власних радіоелектронних систем від ворожого придушення, а також забезпечення точності та оперативності збору даних про потенційні загрози.

Актуальність даного дослідження зумовлена необхідністю розробки нових технологій та методів моніторингу, що враховують нові виклики в умовах сучасних інформаційних загроз.

Аналіз останніх досліджень і публікацій. Проблематика радіоелектронного моніторингу в умовах інформаційної війни активно досліджується як в українській, так і в зарубіжній науковій літературі. Сучасні дослідження здебільшого спрямовані на створення нових систем моніторингу, здатних ефективно протистояти інформаційним загрозам в умовах зростаючого обсягу радіоелектронних атак [2].

Значний внесок у розвиток цієї тематики зробили науковці з України, зокрема Молодцов В.А., Писарєв А.В., Радченко І.О, які у своїх роботах розглядають проблему захисту радіоелектронних систем від придушення та перехоплення сигналів [3]. Наукові публікації Українського державного центру радіочастот присвячені створенню автоматизованих комплексів для моніторингу радіочастотного спектра, що забезпечують високу точність та швидкість обробки даних.

Зарубіжні вчені також приділяють значну увагу розробці новітніх технологій радіоелектронного моніторингу та вказують на необхідність використання штучного інтелекту для покращення розпізнавання радіосигналів в умовах перешкод. Роботи Мюллера Х. зосереджені на інтеграції багатофункціональних сенсорних систем для забезпечення багатоканального збору даних [4].

Важливим напрямом наукових досліджень є вивчення впливу радіоелектронних перешкод на роботу критичних інфраструктур. Так, праці Томпсона Р. демонструють вплив електромагнітних імпульсів на телекомунікаційні системи та пропонують методи зменшення їх впливу на роботу засобів зв'язку.

Таким чином, аналіз літератури показує, що основними науковими напрямами є створення нових технологій моніторингу, адаптація методів обробки даних до умов інформаційної війни та розробка систем захисту від перешкод.

Мета статті – дослідження сучасних радіоелектронних засобів моніторингу в умовах інформаційної війни та розробка рекомендацій щодо їх ефективного застосування з урахуванням новітніх технологій та методів боротьби з інформаційними загрозами.

Результати

Проблематика радіоелектронної боротьби в умовах інформаційної війни є однією з основних елементів інформаційних операцій мережецентричної війни серед стандартів держав – членів НАТО. РЕБ є ключовим елементом нової концепції під назвою «Боротьба з системами бойового управління», яка активно впроваджується Збройними силами США [4]. Основна ідея цієї концепції полягає у застосуванні комплексних заходів,

що включають проведення спеціальних операцій з військової дезінформації, радіоелектронного подавлення та фізичного знищення на основі ретельно зібраних розвідувальних даних. Метою є позбавлення противника можливості отримувати інформацію та керувати своїми силами, а також захистити власні системи управління від аналогічних дій супротивника.

У рамках визначення операцій нового типу основними завданнями РЕБ, окрім дезорганізації систем бойового управління противника, стають недопущення використання ним інформації про власні сили та дії супротивної сторони, забезпечення випередження ворога у прийнятті оперативних рішень, підвищення ефективності бойових дій, мінімізація втрат особового складу та техніки, а також якнайшвидше досягнення успіху операції.

На основі вище сказаного, можна констатувати, що, на даний час, ведення радіоелектронної боротьби в рамках інформаційних операцій базується на кількох ключових принципах. Перш за все, це суворе узгодження дій РЕБ із загальною стратегією інформаційної операції з урахуванням місця, часу та поставлених завдань. Далі — масоване та комплексне використання сил і засобів РЕБ для подавлення всіх радіоканалів зв'язку між об'єктами противника. Важливими аспектами також є раптовість застосування РЕБ та нестандартний підхід до використання наявних засобів.

До основних способів впливу на системи бойового управління противника належить масоване застосування засобів ураження, захоплення командних пунктів та вузлів зв'язку, а також дезінформація через канали розвідки та радіоелектронної протидії, включаючи організацію витоку фальшивих даних. Під час інформаційних операцій тиск на противника здійснюється завдяки використанню сил і засобів, що спрямовані на порушення систем державного та військового управління, зокрема із залученням підрозділів РЕБ.

Таким чином, радіоелектронні засоби моніторингу в умовах інформаційної війни є важливим елементом забезпечення національної безпеки. Вони дозволяють здійснювати безперервний контроль за радіочастотним спектром, виявляти потенційні загрози та оперативно реагувати на інформаційні атаки. З огляду на зростаючу складність інформаційного середовища, РЗМ постійно вдосконалюються як у технічному, так і в програмному аспекті.

Одним із прикладів успішного застосування радіоелектронних засобів моніторингу є система RQ-4 Global Hawk, що використовується Збройними силами США для моніторингу радіочастотного середовища на великих відстанях [4]. Завдяки можливостям радіолокаційного зондування, цей безпілотник може виявляти активність противника на значній території. Інший приклад – система «Кольчуга» українського виробництва, яка здійснює пасивний моніторинг і дозволяє виявляти цілі на великих відстанях без випромінювання власного сигналу.

У цивільній сфері використовуються мобільні системи моніторингу спектра для контролю за роботою радіочастотних пристроїв у мегаполісах. Такі комплекси допомагають виявляти незаконне використання частот та забезпечують оптимізацію використання спектра, що особливо важливо у великих містах з насиченою інфраструктурою зв'язку.

Сучасні розробки, в рамках тематики статті, здебільшого спрямовані на створення нових систем моніторингу, здатних ефективно протистояти інформаційним загрозам в умовах зростаючого обсягу радіоелектронних атак.

Деталізуємо основні етапи алгоритму використання радіоелектронних засобів моніторингу в умовах інформаційної війни. Першим етапом є підготовчий, на якому визначаються основні цілі та завдання моніторингу, що можуть включати виявлення загроз, контроль інформаційного простору або протидію інформаційним атакам. На цьому етапі проводиться аналіз середовища для виявлення потенційних джерел загроз,

а також вибираються радіоелектронні засоби та обладнання відповідно до поставлених завдань, з урахуванням технічних можливостей та вимог до моніторингу.

Другий етап передбачає збір інформації. На цьому етапі організовується робота систем радіоелектронного моніторингу, проводиться налаштування обладнання для виявлення та реєстрації радіосигналів. Особливу увагу приділяють збиранню даних з різних каналів зв'язку та інформаційних потоків, що дозволяє отримати повну картину радіоелектронної обстановки.

Третій етап включає обробку зібраної інформації, яка передбачає первинну обробку сигналів, що включає фільтрацію шумів та декодування отриманих сигналів. Далі проводиться аналіз змісту повідомлень та виявлення аномалій у структурі даних. Також на цьому етапі здійснюється кореляція отриманих даних із зовнішніми факторами та контекстом, що дозволяє підвищити достовірність висновків.

Четвертий етап зосереджений на аналізі та інтерпретації результатів. На основі зібраної та обробленої інформації створюються інформаційні моделі загроз, проводиться оцінка достовірності даних та їх значущості для подальших дій. За підсумками аналізу формуються звіти, які містять рекомендації для прийняття управлінських рішень щодо реагування на виявлені загрози.

П'ятий етап — це реакція та протидія. На цьому етапі розробляються заходи з нейтралізації або зменшення впливу виявлених загроз. До них можуть належати застосування радіоелектронної боротьби, реалізація кіберзахисту або організація інформаційних контратак. Результати та рекомендації доводяться до відома керівництва та зацікавлених сторін для оперативного прийняття рішень.

Завершальний етап включає оцінку ефективності застосованих заходів та корекцію подальших дій. На цьому етапі аналізуються результати впроваджених рішень, виявляються недоліки у методиках або обладнанні та пропонуються шляхи їх усунення. Також здійснюється актуалізація методик та засобів моніторингу з урахуванням отриманого досвіду, що дозволяє підвищити ефективність системи радіоелектронного моніторингу в майбутньому.

Таким чином, алгоритм використання радіоелектронних засобів моніторингу в умовах інформаційної війни забезпечує системний підхід до виявлення, аналізу та нейтралізації загроз, дозволяючи своєчасно реагувати на виклики інформаційної безпеки.

Зазначимо, що представлені етапи алгоритму працюють циклічно, що забезпечує безперервний моніторинг та адаптацію до нових викликів інформаційної війни.

При цьому, основними викликами є захист власних радіоелектронних систем від ворожого придушення, а також забезпечення точності та оперативності збору даних про потенційні загрози.

РЗМ можна класифікувати за декількома критеріями: функціональністю, способом застосування, типом прийому сигналу та призначенням. За функціональністю розрізняють пасивні системи, що здійснюють безконтактне спостереження, та активні системи, що використовують радіолокаційне зондування. За способом застосування – стаціонарні комплекси, мобільні системи та переносні пристрої. За типом прийому сигналу – одноканальні та багатоканальні. За призначенням – розвідувальні та оперативного контролю. Основними технічними рішеннями є впровадження технологій спектрального аналізу на основі штучного інтелекту, що дозволяють здійснювати автоматичне розпізнавання загроз на основі аналізу спектральних характеристик сигналів. Використання нейронних мереж сприяє підвищенню точності виявлення сигналів в умовах перешкод.

Особливо актуальним є захист від радіоелектронного придушення. Впровадження адаптивних фільтрів, систем автоматичного налаштування частоти та методів фазового придушення завад дозволяє забезпечити стійкість роботи РЗМ в умовах

дезінформаційних атак. Крім того, застосування квантових технологій у поєднанні з інтелектуальними системами управління сприяє підвищенню швидкості розпізнавання радіосигналів.

В умовах гібридної війни, коли разом із традиційними методами використовуються інформаційні атаки, радіоелектронні засоби моніторингу є ключовим елементом захисту. Наприклад, під час військових протистоянь ЗСУ активно задіюють засоби радіоелектронної боротьби для придушення комунікацій противника. Зокрема, робота комплексів «Буковель-АД» дозволяє блокувати сигнали безпілотників та інших радіокерованих об'єктів.

Загалом, використання радіоелектронних засобів моніторингу в інформаційній війні дозволяє не лише виявляти загрози, а й ефективно боротися з ними за допомогою сучасних технологій.

Подальший розвиток технологій дозволить підвищити ефективність цих засобів у складних умовах інформаційної війни, забезпечуючи надійний захист критичних інфраструктур та інформаційних ресурсів.

Висновки

Радіоелектронні засоби моніторингу є невід'ємною складовою системи інформаційної безпеки в умовах інформаційної війни. З огляду на зростаючі загрози радіоелектронного впливу, моніторинг радіочастотного спектра стає важливим інструментом забезпечення національної безпеки та захисту критичних інфраструктур.

На основі аналізу останніх досліджень та практичних застосувань РЗМ можна стверджувати, що подальший розвиток даної галузі має бути спрямований на вдосконалення технологій розпізнавання сигналів, підвищення стійкості до перешкод та інтеграцію з іншими системами безпеки. Впровадження новітніх методів, таких як штучний інтелект та квантові обчислення, дозволить створити більш точні та швидкі системи моніторингу.

Важливою складовою ефективного застосування РЗМ є їх адаптація до умов сучасної інформаційної війни. Це включає розробку автоматизованих комплексів, що дозволяють проводити моніторинг у реальному часі та зменшують вплив людського фактору. Підвищення точності виявлення джерел загроз дозволить знизити ризик успішних атак на інформаційні системи та забезпечити надійний захист даних.

Загалом, застосування радіоелектронних засобів моніторингу в інформаційній війні є ключовим елементом сучасної стратегії забезпечення безпеки. Подальші дослідження в цьому напрямі сприятимуть створенню нових технологій, що дозволять ефективніше захищати інформаційні ресурси та знижувати вплив радіоелектронних загроз.

Література:

1. Антонович П.І., Макаренко С.І., Михайлов Р.Л., Ушань К.В. Перспективні методи деструктивного впливу на системи військового управління у єдиному інформаційному просторі. Вісник Академії військових наук. 2014. № 3(48). С. 93–101.

2. Доктрина ЗС США JP 3-85. Спільні електромагнітні операції зі спектром. 2020. 163 с.

3. Молодцов В.А., Писарєв А.В., Радченко І.О. Необхідність реформування воєнного управління відповідно до концепції мережецентричної війни. Актуальні проблеми будівництва та службово-бойової діяльності сил охорони правопорядку : Збірник тез доповідей Всеукраїнської науково-практичної конференції. Харків : НАНГУ, 2021. С. 31–32.

4. Польовий статут сухопутних військ ЗС США: FM 3-12. Ведення електронної війни та бойових дій у кіберпросторі. Департамент армії. 2017. 108 с.