УДК 621.396.96

СИСТЕМИ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ І РАДІОПРОТИДІЇ

Костров Є.О.
Науковий керівник – ст. викладач Бобнєв Р.О
Харківський національний університет радіоелектроніки, каф. МІРЕС
м. Харків, Україна, e-mail: yevhenii.kostrov@nure.ua

This work explores the field of Radio Electronic Intelligence (REI) and Radio Countermeasures (RCM), examining their applications and advancements. REI systems play a crucial role in modern warfare, gathering vital information on enemy communications and electronic systems. RCM, on the other hand, focuses on disrupting and deceiving those same systems to achieve battlefield superiority. We'll delve into the historical development of these technologies, tracking their evolution from rudimentary techniques to the sophisticated systems in use today.

Радіоелектронна розвідка (РЕР), (абр. РЕР; англ. Electronic signals intelligence (ELINT)) – це система збору розвідувальної інформації про противника шляхом перехоплення та аналізу його радіоелектронних сигналів. РЕР відіграє важливу роль у сучасній війні.

Перші напрацювання для військових цілей у цьому напрямку почали вести ще у 1898 році Системи РЕР використовують широкий спектр методів, включаючи радіоелектронну розвідку (SIGINT), розвідку зв'язку (COMINT) та електронну розвідку (ELINT), щоб створити цілісну картину переміщень, можливостей та намірів противника.

РЕР може визначити місцезнаходження ворожих підрозділів, виявити закономірності в їхньому зв'язку та отримати важливі деталі щодо їхніх систем озброєння та тактики.

РЕР може бути поділена на радіорозвідку, радіотехнічну розвідку, радіолокаційну розвідку, теплову та інфрачервону розвідку, лазерну розвідку, телевізійну розвідку, звукову розвідку, гідроакустичну розвідку.

РЕР відіграла ключову роль у багатьох війнах. Наприклад, під час Другої світової війни РЕР допомогла союзникам розшифрувати код німецької шифрувальної машини Enigma, що дало їм значну перевагу.

Проте ефективність РЕР нейтралізується її взаємною протилежністю – системами захисту від радіоелектронних засобів (ЗРЕЗ). ЗРЕЗ представляють собою комплекс технологій та тактик, призначених для захисту власних комунікацій та електронних систем від ворожого порушення та експлуатації.

Наприклад, радіочастотний обман передбачає передачу оманливих сигналів для того, щоб заплутати або обдурити ворожі системи РЕР, приховуючи справжні переміщення військ та їхні наміри. Таким чином, наприклад, на радарах для станцій протиповітряної оборони можуть бути

хибні цілі, які будуть відволікати війська ППО та давати змогу справжнім ракетам, БПЛА чи літакам досягти своїх цілей.

Дуже важливим прикладом використання ЗРЕЗ є радіоелектронна рушниця – це пристрій, який використовує радіочастотні хвилі для виведення з ладу або пошкодження електронних пристроїв. Завдяки ньому перший час у російсько-українській війні багато розвідувальних БПЛА не мали змоги працювати на полі бою.

Існують різні платформи, які використовуються для експлуатації систем РЕР та ЗРЕЗ:

1. Літаки – використовуються для перевезення систем РЕБ на великі відстані. Вони можуть бути оснащені різними системами РЕБ, включаючи РЕБ-передавачі, РЕБ-приймачі та РЕБ-засоби постановки перешкод.

2. Супутники – використовуються для перевезення систем РЕБ на орбіту. Вони можуть бути оснащені різними системами РЕБ, включаючи РЕБ-передавачі, РЕБ-приймачі та РЕБ-засоби постановки перешкод.

3. Бронетранспортери – використовуються для перевезення систем РЕБ на поле бою. Вони забезпечують захист систем РЕБ від вогню противника.

4. Кораблі – використовуються для перевезення систем РЕБ у море. Вони можуть бути оснащені різними системами РЕБ, включаючи РЕБ-передавачі, РЕБ-приймачі та РЕБ-засоби постановки перешкод.

РЕР використовується не лише у військових, але й у цивільних сферах, таких як боротьба з тероризмом, контроль кордонів, моніторинг навколишнього середовища тощо.

Так, наприклад, теракти 11 вересня 2001 року стимулюють розвиток РЕР для боротьби з тероризмом.

Симбіотичний зв'язок між РЕР та ЗРЕЗ проявляється в їхньому постійному розвитку. Вдосконалення РЕР потребує розробки більш складних методів ЗРЕЗ для підтримки безпечного електронного середовища. І навпаки, посилення ЗРЕЗ змушує системи РЕР підвищувати свою чутливість та можливості обробки сигналів, щоб залишатися на крок попереду в цій технологічній гонці озброєнь.

Підбиваючи підсумки, на основі аналізу сучасних тенденцій у розвитку систем радіоелектронної розвідки та радіопротидії, варто звернути увагу на інтеграцію штучного інтелекту із засобами збору та аналізу даних. Розробка алгоритмів машинного навчання для автоматизації процесів розпізнавання, класифікації та аналізу сигналів дозволить підвищити ефективність роботи систем, забезпечуючи оперативне реагування на загрози та забезпечуючи високий рівень захисту від радіоелектронних загроз. Під час боротьби української нації за життя, вважаю цю тему актуальною.

Список використаних джерел:

1. Радіоелектронна розвідка Збройних Сил України. Режим доступу до ресурсу: https://mil.in.ua/uk/articles/137316/ (дата звернення: 04.03.2024).

2. Левченко О.В. Розвідка та іноземні армії. Інформаційна робота. 2022. – 124 с.

3. Базавляк О. С. Огляд існуючих РЛС та перспективи їх розвитку // Радіоелектроніка та молодь у XXI столітті : матеріали 23 Міжнар. молодіж. форуму, 16–18 квітня 2019 р. – Харків : ХНУРЕ, 2019. – Т. 3. – С. 38–39.

4. Средства функционального подавления радиоэлектронных средств малоразмерных беспилотных летательных аппаратов с фокусировкой электромагнитного излучения / А. В. Гомозов, Д. В. Грецких, А. В. Демченко, Н. М. Цикаловский // Космическая техника. Ракетное вооружение. - 2018. - Вып. 1. - С. 13-19. – URL: http://nbuv.gov.ua/UJRN/Ktrv_2018_1_5

5. Гомозов А.В., Грецких Д.В., Шарапова Е.В., Цикаловский Н.М. Фокусировка электромагнитного излучения в средствах функционального поражения беспилотных летательных аппаратов средней и большой дальности / Технология приборостроения, науч.-технич. журнал, Гос. предпр. науч.-иссл. технологич. ин-т. – Вып. 1′ 2017 г – Х., 2017. – с. 3 – 8