УДК 621.396.96:004.056

РАДІОЕЛЕКТРОННА БОРОТЬБА: ЩО ПОТРІБНО ЗНАТИ КОЖНОМУ

Ломака С.Р., Солодов В.Д.
e-mail: sofiia.lomaka@nure.ua
Харківський національний університет радіоелектроніки, каф. МІРЕС
м. Харків, Україна

This work is devoted to the fundamentals of electronic warfare and its significance in modern security systems. It examines the three main components of electronic warfare: electronic attack, electronic protection, and electronic support, analyzing their application in military operations and civil infrastructure security. Additionally, the work highlights the role of electronic warfare in countering modern threats such as unmanned aerial vehicles, guided missile systems, and cyber-electronic attacks.

Радіоелектронна боротьба (РЕБ) є невід'ємною складовою сучасної військової та інформаційної безпеки. Вона охоплює комплекс заходів, спрямованих на контроль над електромагнітним спектром, що дозволяє знижувати бойові можливості противника та забезпечувати ефективний захист власних засобів зв’язку, навігації та управління. Умовно РЕБ поділяється на три основні складові: радіоелектронний напад (РЕН), радіоелектронний захист (РЕЗ) та радіоелектронну підтримку (РЕП), кожна з яких має своє призначення та унікальні методи реалізації.

Радіоелектронний напад є активним компонентом РЕБ, що передбачає створення перешкод для ворожих комунікацій, систем управління військами, навігації та розвідки. Це включає постановку активних і пасивних радіоперешкод, спрямованих на зниження ефективності роботи радіоелектронних засобів противника. Сучасні технології дозволяють реалізовувати високоточне подавлення ворожих радіолокаційних станцій (РЛС) за допомогою потужних засобів радіоелектронного впливу. Наприклад, мобільні комплекси типу AN/ALQ-99, здатні ефективно блокувати роботу радіолокаційного та навігаційного обладнання супротивника, що критично впливає на його можливості ведення бойових дій.

Радіоелектронний захист спрямований на забезпечення стійкості власних комунікаційних і навігаційних систем у присутності ворожих засобів РЕН. Основні методи захисту включають використання адаптивних антенних систем, технологій змінної частоти передачі сигналу, криптографічного захисту даних та заходів із зменшення електромагнітного випромінювання критичних об'єктів. Наприклад, сучасні військові літальні апарати та командні пункти оснащуються пристроями активного радіозахисту, які автоматично коригують частоти зв’язку та здійснюють шифрування переданих даних, що ускладнює їхню ідентифікацію та перехоплення противником.

Радіоелектронна підтримка полягає у зборі, аналізі та використанні даних про електромагнітне середовище для забезпечення ефективної роботи сил РЕБ. Це включає виявлення та класифікацію джерел радіосигналів, оцінку їхнього рівня загрози та забезпечення інформаційної підтримки операцій РЕН і РЕЗ. Наприклад, сучасні комплекси SIGINT (signals intelligence) здатні відстежувати активність ворожих радіозасобів у режимі реального часу, що дозволяє командуванню приймати своєчасні рішення щодо використання засобів електронного впливу.

В останні роки безпілотні літальні апарати (БПЛА) стали важливим інструментом у веденні бойових дій та розвідки. Відповідно, розробка методів протидії дронам набула великого значення. Системи РЕБ здатні нейтралізувати БПЛА шляхом пригнічення каналів зв’язку, блокування сигналів супутникової навігації (GPS, GLONASS) або навіть шляхом дистанційного перехоплення управління. Деякі передові комплекси, такі як "SkyWall" та "DroneShield", забезпечують ефективний захист стратегічних об'єктів від атак дронів, запобігаючи їхньому проникненню в контрольовану зону.

Сучасні тенденції ведення війни демонструють зростаюче поєднання радіоелектронної боротьби з кібероперaціями. Взаємодія засобів РЕБ та кібератак дозволяє не тільки перехоплювати та глушити сигнали противника, але й здійснювати деструктивний вплив на його інформаційні системи, змінюючи або знищуючи важливі дані. Комплексний підхід до РЕБ та кібероперацій дає змогу створювати повноцінні інформаційні атаки, що паралізують системи зв’язку та управління супротивника.

РЕБ є критично важливим компонентом сучасної безпеки та військових операцій. Зростання використання електронних систем у військових конфліктах робить необхідним поглиблене вивчення та розвиток засобів РЕБ для забезпечення інформаційної переваги. Розуміння принципів РЕБ є важливим не лише для військових спеціалістів, а й для фахівців у сфері інформаційних технологій, безпеки та оборони.

Список використаних джерел:

1. Белокурський Ю. П., Іохов О. Ю., Козлов В. Є., Щербина О. О. Принципи побудови системи радіоелектронного захисту підрозділів Національної гвардії України під час виконання завдань за призначенням. Військово-технічний збірник, 2018. С. 73–80.

2. Єрохін В. Ф., Шолохов С. М., Ніколаєнко Б. А. Завадозахист радіоелектронних засобів. Частина 1. Основи завадозахисту систем зв'язку: навчальний посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 210 с.