

складної завадової обстановки, ідентифікуючи специфічні акустичні сигнатури двигунів БПЛА. Розроблений алгоритм комплексування на основі адаптивного фільтра Калмана дозволяє знизити рівень хибних спрацьовувань на 18-22% і забезпечити точне прогнозування точки та часу потенційного удару. Та розробити трирівневу ієрархічну структуру взаємодії елементів, в рамках якої розглядається архітектурний поділ системи на три взаємопов'язані ешелони захисту:

- Пасивний ешелон з Легких гнучких радіопоглинаючих захисних конструкції (LFRAP — Lightweight Flexible Radar Absorbing Protective structures): спеціалізовані радіопоглинаючі та теплоізоляційні покриття, які на постійній основі знижують базову ефективну площу розсіювання станцій РЕБ та нівелюють їх тепловий контраст відносно фону підстильної поверхні.

- Ешелон активного спотворення, що включатиме ІЧ-стробоскопи та лазерні емітери: у разі верифікації загрози сенсорами, система активує імпульсні високоінтенсивні джерела випромінювання. Вони створюють динамічну заваду, яка «засліплює» CMOS-матриці камер БПЛА та вносить критичну похибку в роботу кореляційних трекерів типу SiamRPN, змушуючи алгоритм втратити контур цілі.

- Ешелон активного приховування, що передбачає застосування димів та аерозолів, які виступатимуть як фінальний рубіж захисту. Піротехнічні або пневматичні модулі за сигналом обчислювача вистрілюють мультиспектральні заряди, створюючи непрозорий екран безпосередньо перед об'єктом, повністю ізолюючи його від оптичних систем наведення противника.

Наукова новизна дослідження полягає у формалізації принципів побудови локального мультиспектрального захисту об'єктів РЕБ як інтегрованого компоненту концепції СЕМА, що дозволяє парирувати загрози нового покоління — автономні системи з машинним зором, об'єднанні різнорідних сенсорів (у поєднанні з жорстким лімітом часу на реакцію, що дозволить нівелювати технологічні переваги ШІ-наведення противника на кінцевому етапі траєкторії. Практична цінність архітектури полягає у суттєвому підвищенні коефіцієнта живучості дорогих комплексів РЕБ у зонах високої інтенсивності бойових дій, а перспективи подальших досліджень лежать у площині експериментального оцінювання стійкості нейромереж детекції до комбінованого впливу швидкісних ІЧ-стробоскопів у різних метеорологічних умовах.

Пономаренко Максим Юрійович

викладач кафедри тактики

підполковник

Київський інститут національної гвардії України

Коваль Євген Сергійович
старший викладач кафедри тактики
підполковник

Київський інститут національної гвардії України

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАСОБІВ РЕБ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ ПРИ ВИКОНАННІ СЛУЖБОВО-БОЙОВИХ (БОЙОВИХ) ЗАВДАНЬ

Електронна війна – це сукупність технологій та методів, спрямованих на контроль електромагнітного середовища під час ведення бойових дій. Вона включає в себе виявлення сигналів радіоелектронних засобів (РЕЗ) противника, перехоплення комунікацій, придушення каналів зв'язку та захист власних радіоелектронних систем.

Радіоелектронна боротьба (РЕБ) – це ключова складова електронної війни. Основна задача таких систем полягає у впливі на РЕЗ противника через придушення чи спотворення сигналів. У практичних умовах це може стосуватися каналів управління дронами, передачі відеосигналу або навігаційних систем.

На початку повномасштабних бойових дій в 2022 році засоби РЕБ були поодиноким ситуативним явищем в підрозділах. Їх можна було розглядати як реакцію на застосування противником безпілотних літальних апаратів (БпЛА). Вони швидше закривали прогалини там, де могли, і їх не розглядали як єдину систему.

Станом на 2026 рік засоби радіоелектронної боротьби (РЕБ) та радіоелектронної підтримки (ЕП) стали критичним елементом «електронної війни» в Україні, визначаючи успіх бойових дій. Сектор безпеки та оборони перейшов від використання застарілих радянських зразків до насичення фронту сучасними вітчизняними системами, що адаптуються до нових загроз у режимі реального часу.

Сучасний стан (2026)

1. **«Окопний РЕБ» та мобільність:** основний фокус зроблено на портативних (переносних) та автомобільних «купольних» системах, які захищають бронетехніку, автомобілі, позиції та штурмові групи від FPV-дронів та скидів. Дані засоби мають компактний розмір і використовуються особовим складом на лінії бойового зіткнення. Вони давно вже стали такою ж частиною озброєння взводу, як кулемет чи гранатомет.

2. **Інтеграція ЕП та РЕП:** сучасні системи часто об'єднують функції виявлення (радіоелектронна підтримка/ радіоелектронна розвідка) та придушення (радіоелектронне подавлення), що дозволяє автоматично фіксувати частоту ворожого дрона і генерувати заваду, економлячи енергію та мінімізуючи кількість засобів РЕБ, які використовуються. Такі засоби отримали назву - «засоби радіоелектронної боротьби з дорозвідкою».

3. **Ширококутовість:** через постійну зміну частот ворожими БПЛА, засоби РЕБ переходять від вузькокутового (прицільного) до ширококутового (загороджувального) подавлення (охоплення діапазонів (700–1050) МГц, (2.4) ГГц, (5.8) ГГц тощо). Цей процес постійний та ґрунтується на співпраці військовослужбовців з розробниками засобів РЕБ, надаючи об'єктивну інформацію для подальшого врахування в розробці нових та модернізації вже існуючих ефективних засобів РЕБ.

4. **Вплив на супутникову навігацію:** активно застосовуються засоби для придушення сигналів GPS/GLONASS, що дезорієнтує ворожі дрони та крилаті ракети. Як правило, дані засоби застосовуються в сукупності із засобами, призначеними для підміни сигналу GPS/GLONASS («спуфери») з метою зриву польотного завдання шляхом відхилення ударних БПЛА від цілі ураження. Спугер імітує супутниковий сигнал, змушуючи GPS-приймач показувати неправильне місцезнаходження. Роботу даного обладнання можна віднести до інтелектуальних завад.

5. **«BRAVE1» та приватні ініціативи:** на даний час Україна лідирує у розробці засобів РЕБ завдяки швидкій взаємодії військових з інженерами, що дозволяє випускати нові зразки та модернізувати вже існуючі за лічені тижні.

Перспективи розвитку (2026–2027)

1. **Штучний інтелект (ШІ):** Інтеграція ШІ для автоматичного розпізнавання цілей та адаптивного впливу на них, що зменшує навантаження на оператора та швидкість реакції на загрозу.

2. **Розвиток та застосування інтелектуальних завад:** перехід від стратегії «енергетичного подавлення» до «інформаційного маніпулювання» є критично необхідним для захисту об'єктів критичної інфраструктури та урбанізованої місцевості, оскільки це дозволяє нейтралізувати загрозу з мінімальним впливом на навколишню інфраструктуру. Адаптивний цифровий спугінг, інтегрований у комплексну систему автоматичного захисту, перетворює статичну оборону на гнучкий інструмент, здатний не просто зупиняти атаку, а буквально керувати засобами ворога у повітрі. Це відкриває перспективи для створення повністю автономних куполів безпеки, які здатні в реальному часі «переписувати» координати для будь-якого несанкціонованого об'єкта, змушуючи його приземлитися у безпечних для об'єкта прикриття місцях, що значно підвищує рівень захищеності об'єктів критичної інфраструктури та урбанізованої місцевості від сучасних засобів повітряного нападу.

3. **Протидія «розумним» дронам:** Розвиток систем, здатних боротися з дронами, які використовують машинний зір та наводяться без GPS-сигналу (функція захоплення цілі для донаведення для удару). Сучасний етап розвитку безпілотних технологій характеризується відмовою від простих каналів управління на користь повної автономності, через що традиційні засоби РЕБ, які орієнтовані на розрив зв'язку між оператором і дроном, дедалі частіше виявляються неефективними. Оскільки новітні зразки БПЛА використовують багаточастотні приймачі та

інерціальні системи доведення, звичайне «зашумлення» ефіру лише змушує дрон переходити на автономний режим польоту за інерцією, що в умовах щільної міської забудови не знімає загрозу, а лише робить її непередбачуваною.

4. **РЕБ проти волоконно-оптичних дронів:** пошук технічних рішень для протидії дронам, керування якими здійснюється через фізичний (оптоволоконний) кабель, що робить їх нечутливими до класичного РЕБ.

5. **Автономні системи РЕБ:** створення мережецентричних систем, де РЕБ-платформи працюють узгоджено, автоматично перекриваючи частоти залежно від обстановки.

6. **Експортний потенціал:** у 2026 році Україна починає офіційний експорт деяких зразків оборонних технологій, що підтверджує високу якість вітчизняних розробок.

Проблемні питання, які потребують постійного вирішення в ході ведення електронної війни:

1. **Постійна гонка частот:** Противник адаптується, змінюючи робочі частоти БпЛА, що вимагає постійної модернізації та адаптації вже існуючих систем та розробки нових.

2. **Дефіцит кадрів:** Висока потреба у кваліфікованих інженерах засобів РЕБ/ЕП, здатних працювати з цифровими протоколами.

3. **Енергозалежність:** Сучасне поле бою потребує великої кількості енергії для постійної роботи засобів РЕБ/ЕП, що вимагає потужних джерел живлення.

Савранський Валерій Петрович

старший викладач кафедри тактики – начальник служби РЕБ

полковник

Київський інститут Національної гвардії України

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРотьБИ ПІД ЧАС ВИКОНАННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ

У тезі розглянуто ключові особливості застосування засобів радіоелектронної боротьби (РЕБ) під час виконання службово-бойових завдань у сучасних умовах ведення бойових дій. Проаналізовано фактори, що впливають на ефективність РЕБ, а також визначено основні напрями підвищення її результативності.

Сучасні збройні конфлікти характеризуються високим рівнем насиченості радіоелектронними засобами, що зумовлює зростання ролі радіоелектронної боротьби як важливого елементу забезпечення бойових дій. Засоби РЕБ застосовуються з метою порушення функціонування систем управління, зв'язку, навігації та розвідки противника, а також для захисту власних інформаційних систем.

Однією з ключових особливостей застосування РЕБ під час виконання службово-бойових завдань є необхідність її інтеграції в загальну систему управління військами. Ефективність РЕБ значною мірою залежить від своєчасного отримання