

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ
ІМЕНІ С. П. КОРОЛЬОВА

Інноваційні підходи Щодо форм та способів застосування високотехнологічних зразків озброєння та військової техніки Силами оборони України

Тези доповідей Міжнародної науково-практичної конференції. Частина 1

29 жовтня 2026

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

ІННОВАЦІЙНІ ПІДХОДИ ЩОДО ФОРМ ТА СПОСОБІВ ЗАСТОСУВАННЯ ВИСОКОТЕХНОЛОГІЧНИХ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ СИЛАМИ ОБОРОНИ УКРАЇНИ

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

29 жовтня 2026 року

Т Е З И Д О П О В І Д Е Й

Частина 1

Житомир
2026

УДК 623:355.48 (470+571:477)
І-67

Інноваційні підходи щодо форм та способів застосування
І-67 високотехнологічних зразків озброєння та військової техніки Силами оборони України : Наук. конф., 29 жовтня 2026 р. : тези доп. Ч. 1 / М-во оборони України, Житомир. військ. ін-т імені С. П. Корольова ; відп. за випуск С. А. Середюк. – Житомир : ЖВІ, 2026. – 708 с.

УДК 623:355.48 (470+571:477)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова організаційного комітету – доктор історичних наук, професор СЛЮСАРЕНКО Андрій Віталійович.

Заступник голови організаційного комітету – кандидат технічних наук, старший дослідник ФЕДОРЧУК Д. Л.

Члени організаційного комітету:
кандидат технічних наук, доцент КАНЕВСЬКИЙ Л. Б.;
кандидат технічних наук, доцент КУБРАК О. М.;
кандидат технічних наук, доцент, БОВСУНОВСЬКИЙ В. Ю;
кандидат технічних наук, старший дослідник, САМЧИШИН О. В.;
кандидат технічних наук БОНДАРЕНКО Ю. Л.;
кандидат технічних наук ОСАДЧУК Р.М.;
кандидат технічних наук ТИМЧУК С. В.;
кандидат військових наук СЕРЕДЮК С. А.;
ЗАЄЦЬ Ю. О.;
ТРОХІМЕНКО О. В.;
КУЛІНІЧ Ю. М.;
ЖУРАВСЬКИЙ С. В.;
ГОРБАЧ Т. П.;
ЗУБЕЛЕВИЧ Д. І.

За правильність і достовірність наданого матеріалу, фактів, цитат та інших відомостей відповідальність несуть автори.

Адреса:
Житомирський військовий інститут імені С. П. Корольова,
просп. Миру, 22, м. Житомир, 10004

Тел. (0412) 48-30-19

© Житомирський військовий інститут імені С. П. Корольова, 2026

Вітальне слово начальника Житомирського військового інституту імені С. П. Корольова з нагоди відкриття Міжнародної науково-практичної конференції

Шановні колеги, учасники конференції, читачі!

Збірник тез, який ви тримаєте в руках, – це не просто підсумок наукових доповідей, це зріз практичного досвіду, здобутого Силами оборони України в ході широкомасштабної війни, і системна спроба осмислити його. Темп технологічних змін на фронті невпинно зростає. Рої ударних безпілотних апаратів, оптоволоконне наведення, нові покоління засобів радіоелектронної боротьби, інтеграція штучного інтелекту в контури прийняття рішень на тактичному рівні – усе те, що донедавна належало до категорії перспективних розробок, стрімко переходить у категорію щоденної бойової практики. Війна чітко довела: технологічне рішення сьогодні має життєвий цикл, що вимірюється тижнями, а не роками.

Саме тому тематика цієї конференції набула особливої актуальності. Йдеться вже не лише про те, як створити ефективний зразок, а про те, як побудувати систему, здатну його створити, швидко модернізувати, інтегрувати в бойові порядки та замінити наступним поколінням ще до того, як противник адаптується до попереднього.

Для Житомирського військового інституту імені С. П. Корольова ця проблематика є сферою щоденної наукової та освітньої діяльності. Безпілотні системи, технічні види розвідки та протидії їм, радіоелектронна боротьба, кібербезпека, космічні системи та засоби спеціального призначення – напрями, за якими інститут готує фахівців і провадить дослідження, оскільки вони формують технологічний каркас сучасного поля бою.

Переконаний, жодна інституція поодинці не здатна відповісти на виклики цієї війни. Наша сила – у поєднанні військової науки, бойового досвіду, інженерної думки оборонно-промислового комплексу та міжнародної експертизи. Матеріали збірника відображають саме таку синергію. Завдяки співпраці наукові дослідження спрямовані на реальні потреби бойових підрозділів, а розробки оборонно-промислового комплексу вдосконалюються на основі досвіду їх застосування.

Сподіваюся, що це видання стане джерелом для конкретних технічних рішень, тактичних прийомів і навчальних методик, які підсилять спроможності Сил оборони України.

Бажаю плідної наукової роботи, швидкого впровадження напрацювань і нашої спільної Перемоги!

Слава Україні! Героям Слава!

СЕКЦІЯ 1
Застосування безпілотних систем Силами оборони України

Зубелевич Д. І.
Охріменко Д. В.
Житомирський військовий інститут імені С. П. Корольова

СТІЙКІСТЬ МОДЕЛЕЙ КОМП'ЮТЕРНОГО ЗОРУ АВТОНОМНИХ БЕЗПІЛОТНИХ СИСТЕМ ДО ЦІЛЕСПРЯМОВАНИХ ЗБУРЕНЬ ЗОБРАЖЕНЬ ТА ФІЗИЧНИХ МАСКУВАЛЬНИХ ВІЗЕРУНКІВ

Широкомасштабна збройна агресія Російської Федерації проти України супроводжується масовим застосуванням безпілотних систем (БПС). Одним із чинників, що ускладнюють їх використання, є вплив засобів радіоелектронної боротьби противника на канали управління та передачі відеоданих. За таких умов зростає значення бортових моделей комп’ютерного зору, здатних автономно виявляти, класифікувати та супроводжувати об’єкти. У роботі систематизовано загрози для таких моделей за етапами життєвого циклу та запропоновано підхід до оцінювання їх стійкості.

Окремий клас загроз для моделей машинного навчання становлять атаки на основі спеціально сформованих вхідних даних (англ. adversarial attacks). За таких атак змінене зображення спричиняє помилковий результат моделі під час роботи. Ще Сегеді та співавтори (2014), а згодом Гудфеллоу та співавтори (2015) показали, що навіть візуально малопомітне збурення зображення здатне змінити результат класифікації. Для БПС особливе значення мають фізичні атаки. Ефективність таких атак не є сталою. Вона змінюється залежно від ракурсу спостереження, дальності до об’єкта, освітлення, погодних умов і розмиття внаслідок руху, тому оцінювати її потрібно в межах прийнятої моделі загроз.

Браун та співавтори (2017) запропонували спеціально сформовані локальні візерунки, які дістали назву патчів (англ. adversarial patch, буквально «латка», «нашивка»). Це збурення, обмежені невеликою ділянкою зображення й придатні для друку та розміщення в реальній сцені. Їх оптимізують під конкретну модель або клас моделей, і цим вони відрізняються від традиційного камуфляжу, розрахованого на людське зорове сприйняття. Зворотне твердження хибне: не кожен незвичний маскувальний візерунок є патчем.

Тіс та співавтори (2019) показали друкований патч, який у їхніх експериментах знижував виявлення людей детектором на основі YOLOv2. У роботі Ду та співавторів (2022) патчі розміщували на автомобілях або поруч із ними, знижуючи ефективність детектора YOLOv3 на знімках, отриманих зверху. Тепловізійний канал теж уразливий: Чжу та співавтори (2021, 2022) ввели в оману детектор людей спершу малими джерелами тепла на тілі, а потім одягом із теплоізоляційного матеріалу.

Наведені результати отримано в цивільних сценаріях. Безпосередньо переносити їх на військові системи не можна, бо відрізняються сенсори, дальності, типи цілей і вимоги до надійності. Тому вони доводять принципову можливість атаки, а не вразливість конкретного зразка техніки. Разом із тим ці результати вказують на можливість появи маскувальних засобів, параметри яких підбиратимуть з урахуванням не лише особливостей людського зору, а й характеристик алгоритмів розпізнавання. Виготовлення таких засобів коштує небагато порівняно з вартістю об’єкта, який вони приховують, а ефект полягає в тому, що техніку, яку оператор упізнає без труднощів, модуль комп’ютерного зору не виявляє взагалі або класифікує хибно.

Гіпотетичний сценарій застосування такого маскувального візерунка виглядає так. FPV-дрон (англ. first person view, керування за зображенням із бортової камери) з автономним наведенням на кінцевій ділянці захоплює ціль за командою оператора. Після втрати відеоканалу під впливом засобів радіоелектронної боротьби супроводження переходить до бортових алгоритмів. Нанесений на техніку спеціально сформований візерунок здатний призвести до втрати цілі чи перенаправлення засобу ураження на інший об’єкт саме тоді, коли оператор уже не може втрутитися.

Розглянуті типи загроз можна впорядкувати за етапами життєвого циклу моделі комп’ютерного зору (табл. 1). Це авторська робоча класифікація, яка поєднує об’єкт впливу, етап і припущення про можливості атакувальника; вона співвідноситься з NIST AI 100-2e2025 і MITRE ATLAS. Отруєння даних полягає у внесенні до навчальної вибірки прикладів, які змінюють поведінку навченої моделі. Бекдор (англ. backdoor) є різновидом такого впливу: модель працює звичайно, але за появи заданої ознаки (тригера) видає наперед визначений хибний результат.

Таблиця 1

Класифікація загроз для моделей комп'ютерного зору та пов'язаних компонентів автономних БПС

Клас атаки	Об'єкт впливу	Етап	Припущення щодо доступу	Методи протидії
Отруєння даних (data poisoning)	Дані, модель	Навчання	Навчальні дані або готова модель	Аудит вибірок, контроль походження, реєстр компонентів, виявлення бекдорів
Цифрові збурення зображення	Вхідне зображення	Експлуатація	Вхідний відеопотік	Навчання на спеціально сформованих прикладах, сертифіковані методи
Фізичні патчі та візерунки	Об'єкт, сцена	Експлуатація	Фізичний доступ до об'єкта чи місцевості	Навчання з патчами, кілька спектральних каналів, узгодженість між кадрами
Маніпуляція відеоканалом	Канал, програмне забезпечення	Експлуатація	Канал передачі або програмне забезпечення	Контроль цілісності програмного забезпечення і каналів
Отримання параметрів моделі	Ваги, конфігурація	Розгортання	Фізичний доступ до обладнання	Шифрування ваг, довірене завантаження, ротація моделей

Останній рядок таблиці у військовому застосуванні має особливе значення. Втрата або захоплення апарата відкриває противнику фізичний доступ до бортового обчислювача, а з ним до архітектури й ваг моделі. Якщо параметри не захищені, атаки в режимі «білого ящика» слід вважати базовим

сценарієм моделі загроз. Шифрування ваг і довірене завантаження підвищують вартість такого вилучення. До цього додається залежність від сторонніх компонентів: попередньо навчені моделі, відкриті набори даних і бібліотеки переносять ризики ланцюга постачання в систему наведення.

Ці ризики не є гіпотетичними. У відкритих репозиторіях, тобто мережевих сховищах моделей і наборів даних, фіксували файли, завантаження яких запускає сторонній код. Причина в тому, що відновлення об’єкта з файла у форматі pickle допускає виконання вбудованого в нього коду. Звідси вимога зберігати параметри у форматах без виконання коду та перевіряти походження й цілісність файлів. Другою відомою проблемою є бекдор-атаки на кшталт BadNets (Гу та співавтори, 2017), де роль тригера виконувала невелика наклейка на дорожньому знаку. Окремої уваги потребують навчальні вибірки з відкритих джерел, куди противник може вносити підготовлені матеріали.

Стійкість не досягається жодним окремим заходом, тому їх доводиться поєднувати щонайменше в чотирьох групах. На етапі навчання застосовують спеціально сформовані приклади (англ. adversarial training), зокрема за методом проєктованого градієнтного спуску, який запропонували Мадрі та співавтори (2018). Дієвість цього емпіричного підходу залежить від типу атак і бюджету збурень, а платою є зростання витрат на навчання та можливе зниження точності на неспотворених даних.

До цієї ж групи належать сертифіковані методи. Формальні гарантії дає рандомізоване згладжування (Коен та співавтори, 2019). Універсальними ці гарантії не є: вони прив’язані до метрики, бюджету збурення й архітектури і не поширюються на фізичні патчі. Спеціальні методи протидії патчам поки що надто обчислювально складні для бортового застосування.

Окрему групу становлять архітектурні рішення, зокрема злиття даних оптичного й тепловізійного каналів, перевірка узгодженості рішень між кадрами та ансамблі моделей. Оптимізувати збурення одночасно для кількох спектральних діапазонів і ракурсів складніше, хоча дієвість такого поєднання ще потребує перевірки. Надійність підвищує вимога стабільного виявлення протягом кількох кадрів. Платою є затримка та зниження доступності за несприятливих умов. Якщо виявлення раптово зникає, супроводження триває за рухом об’єкта до повторного підтвердження, а різке перемикання на інший об’єкт на кінцевій ділянці вважають ознакою можливої атаки.

Окремого контролю потребують компоненти, з яких складається програмно-апаратний комплекс. Ідеться про реєстр моделей, наборів даних і бібліотек із версіями та формати збереження ваг без виконання коду під час десеріалізації (зокрема формат safetensors). Сюди ж належать перевірка підписів перед встановленням, шифрування ваг із ключем у захищеному апаратному елементі та можливість відкликати скомпрометовану версію. Принципово важливо зберегти належний рівень людського контролю під час ухвалення рішення про ураження цілі, що узгоджується зі Стратегією НАТО щодо штучного інтелекту (ШІ) редакції 2024 року.

Остання група заходів стосується оцінювання стійкості під час випробувань самої БПС. Орієнтовна програма перевірки силами умовного противника (англ. red teaming) охоплює 1) цифрові атаки методами швидкого градієнтного знака та проєктованого спуску за кількох бюджетів збурення; 2) польові випробування з патчами та маскувальними покриттями за різних висот і часу доби; 3) окрему перевірку тепловізійного каналу; 4) перевірку на бекдори та аудит походження навчальних даних.

Для кількісного оцінювання пропонуємо коефіцієнт невдалих випадків K = N / M, де M позначає кількість епізодів у серії, а N кількість невдалих епізодів. Успішним вважається епізод, у якому ціль утримувалася до заданої дальності без перерв, довших за поріг, і без перемикання на інший об’єкт. Показник обчислюють для контрольної серії та для серії з атакою, а вплив оцінюють за зміною $\Delta K = K(\text{атака}) - K(\text{контроль})$. Епізоди мають бути незалежними, а виділені з одного відеозапису зазвичай такими не є. Позитивне ΔK означає лише більшу частку невдач у серії з атакою і не доводить причинного впливу без зіставності умов. Втрату супроводження, хибну класифікацію та перемикання на інший об’єкт реєструють нарізно.

Загрози для моделей комп’ютерного зору в автономних БПС виникають на різних етапах життєвого циклу, від формування навчальної вибірки до експлуатації та захисту параметрів самої моделі. Особливе місце серед них посідають фізичні збурення. Їх вплив проявляється на кінцевій ділянці й не виявляється під час звичайних перевірок, бо для людського ока ціль лишається розпізнаваною. Найбільша вразливість виникає тоді, коли бортова модель успадкована з відкритих джерел, а апарат може потрапити до рук противника: атаки в режимі «білого ящика» стають базовим припущенням моделі загроз.

Робоча класифікація пов’язує клас атаки з об’єктом впливу, етапом життєвого циклу та припущеннями щодо можливостей атакувальника. Для кількісного оцінювання стійкості запропоновано частку невдалих епізодів і її різницю між контрольною серією та серією з атакою. Втрату супроводження, хибну класифікацію та перемикання на інший об’єкт при цьому враховують окремо.

Перевіряти стійкість потрібно на тій версії моделі, яка фактично встановлюється на бортовий обчислювач, з урахуванням наслідків квантування та умов експлуатації. Перевірка має охоплювати походження навчальних даних, сторонні компоненти й захист параметрів моделі від вилучення в разі захоплення апарата. Результати мають враховуватися під час допуску програмного забезпечення з елементами ШІ до експлуатації.

Раєвський О. В., курсант
Вигівська О. В., канд. іст. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

РОБОТИЗАЦІЯ БРОНЕТЕХНІКИ РАДЯНСЬКОГО ПОХОДЖЕННЯ ЯК НАПРЯМ ЗБЕРЕЖЕННЯ ОСОБОВОГО СКЛАДУ (НА ПРИКЛАДІ МОДЕРНІЗАЦІЇ БРДМ-2)

Масове застосування розвідувальних та ударних безпілотних систем змінило структуру загроз на полі бою: суцільна зона спостереження і ураження поширилася на всю тактичну, а подекуди й на оперативну глибину, а сам факт руху техніки став достатньою підставою для її ураження протягом кількох хвилин. У цих умовах класична логіка захисту бронетехніки, сформована у другій половині ХХ ст., вичерпує свій ресурс. Вона виходила з того, що екіпаж перебуває всередині машини, а його виживання забезпечують бронезахист, рухливість і вогонь. Проте дешевий і масовий засіб ураження впевнено долає захист легкоброньованої техніки, тоді як нарощування бронювання збільшує масу, вартість і навантаження на ходову частину, не даючи пропорційного приросту захищеності. Постає потреба шукати розв’язання не у властивостях броні, а у просторовому рознесенні військовослужбовця і бойової платформи.

Проблематику наземних роботизованих комплексів (НРК) висвітлено переважно у прикладному ключі, насамперед щодо логістичного забезпечення

та евакуації поранених. Водночас переобладнання наявних зразків бронетехніки радянського походження у дистанційно керовані платформи розглядається здебільшого в галузевих та інформаційних джерелах і поки що не дістало узагальненої оцінки з позицій теорії захисту особового складу. Мета цих тез полягає в тому, щоб на прикладі проєкту роботизації БРДМ-2 показати зміну концептуального підходу до збереження особового складу та окреслити обмеження, які супроводжують такий перехід.

БРДМ-2 прийнято на озброєння у 1962 р. як броньовану розвідувально-дозорну машину з екіпажем із чотирьох осіб, озброєнням у складі кулеметів КПВТ калібру 14,5 мм та ПКТ калібру 7,62 мм і бензиновим двигуном ГАЗ-41 потужністю 140 к. с. Бронезахист машини від початку розраховувався на кулі стрілецької зброї та осколки і не перевищує 14 мм сталевої броні у лобовій проєкції корпусу. За критеріями сучасного поля бою цього недостатньо: кумулятивна бойова частина навіть легкого FPV-дрона впевнено долає такий рівень захисту, а помітність і обмежена динаміка колісної машини роблять її зручною ціллю. Разом з тим значна кількість таких машин на складах зберігання формує ресурсну базу для модернізації, за якої Сили оборони отримують бойову платформу без витрат на створення нового шасі.

Саме цим шляхом рухається один із проєктів Центрального управління інноваційної діяльності Збройних Сил України. За інформацією начальника відділу управління полковника В. Волошина, БРДМ-2 переобладнують у дистанційно керовану роботизовану платформу: машина отримує денні та нічні відеокамери для ситуаційної обізнаності, системи дистанційного керування основними функціями, контролю роботи вузлів і агрегатів, визначення місцезнаходження, навігації та орієнтації, а також дистанційно керований бойовий модуль зі зброєю калібру не менше ніж 12,7 мм із застосуванням захищених каналів передавання даних. Опрацьовується можливість керування платформою на відстані до 1000 км. Передбачено заміну бензинового двигуна на дизельний двигун іноземного виробництва, автоматичну коробку перемикання передач, додатковий протимінний захист днища, протиуламковий захист, безкамерні шини підвищеної прохідності та дублюючу систему керування всередині корпусу.

Технічний перелік сам собою не розкриває суті зміни. Принципове значення має поєднання дистанційного керування з дублюючою системою керування зсередини корпусу: платформа стає опційно керованою і

застосовується у двох режимах залежно від рівня ризику на конкретній ділянці. Тим самим у межах одного зразка поєднано різні способи збереження особового складу. Якщо узагальнити, таких способів три: пасивний захист, тобто нарощування бронювання; активний захист, тобто ураження або відхилення засобу нападу на підльоті; просторове рознесення, за якого людина фізично виводиться за межі об'єкта ураження. Перші два залишають військовослужбовця всередині зони ураження і лише знижують імовірність його ураження. Третій змінює саму постановку задачі: ціною вогневого впливу противника стає відновний ресурс, тобто техніка, а не непоправний, тобто життя та підготовлений фахівець.

Такий підхід узгоджується із загальним курсом Сил оборони на масштабування НРК. Станом на початок вересня 2026 р. у бойовій системі DELTA зафіксовано близько 112 тисяч логістичних та евакуаційних місій наземних роботизованих комплексів, виконаних від початку року. Міністерство оборони України визначило метою переведення фронтової логістики на роботизовані рішення та планує законтрактувати десятки тисяч таких комплексів, а для їх застосування запроваджено окрему військово-облікову спеціальність оператора логістично-евакуаційних наземних роботизованих комплексів. Роботизація БРДМ-2 розширює цей ряд: платформа переходить від допоміжних завдань до розвідувальних та вогневих. Показово, що власні варіанти переобладнання БРДМ-2 незалежно пропонують і приватні розробники, а отже, йдеться про формування усталеного напряму, а не про поодинокий зразок.

Об'єктивна оцінка потребує врахування й обмежень такого підходу. По-перше, працездатність платформи прив'язана до каналу керування, а заявлена дальність досяжна лише через ретрансляцію засобами мобільного та супутникового зв'язку, тому машина вразлива до радіоелектронного подавлення і потребує паралельної архітектури каналів та алгоритмів поведінки у разі втрати зв'язку. По-друге, спостереження через камери звужує поле зору і погіршує оцінювання відстаней, що знижує якість водіння та точність вогню порівняно з екіпажем на борту. По-третє, втрачена платформа з бойовим модулем стає для противника трофеєм і джерелом технічних рішень, що потребує процедур блокування та знищення апаратури. По-четверте, корпус і ходова частина зразка 1960-х років обмежують запас для нарощування маси

захисту та енергоспоживання нових систем. По-п’яте, роботизація має організаційну ціну: потрібні пункти керування, посади операторів, ремонтно-евакуаційне забезпечення самих платформ, а також відповідні зміни у штатах і програмах підготовки. Наведені обмеження не заперечують доцільності напряму, але показують, що роботизована платформа не є прямою заміною екіпажної машини і потребує окремої тактики застосування.

Таким чином, переобладнання БРДМ-2 у дистанційно керовану платформу доцільно розглядати не як чергову модернізацію застарілого зразка, а як практичне втілення зміни базового принципу захисту: від нарощування броні навколо людини до виведення людини за межі бойової платформи. Опційно керована схема застосування дає змогу здійснювати цей перехід поступово, без втрати можливості традиційного використання машини. Практична результативність напряму залежить уже не стільки від товщини броні, скільки від стійкості каналів керування, якості каналу спостереження та підготовленості операторів. Перспективним напрямом подальших досліджень є обґрунтування показників оцінювання бойової ефективності роботизованих платформ, створених на базі наявних зразків бронетехніки, та розроблення методики підготовки їх операторів у закладах вищої військової освіти.

Зиков В. Г.
Черняхівський І. В.
Житомирський військовий інститут імені С. П. Корольова

РОЗВИТОК І ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ СИСТЕМ У СУЧАСНОМУ ВІЙСЬКОВОМУ МИСТЕЦТВІ

Сучасні збройні конфлікти демонструють докорінну зміну парадигми ведення війни, де ключовим чинником домінування на полі бою стає масове та системне використання безпілотних систем (БпС). Перехід від поодиноких розвідувальних місій до комплексних мережецентричних операцій перетворив авіаційні (БпЛА) та наземні (НБК) безпілотні комплекси на самостійний і вирішальний інструмент збройної боротьби. Водночас інтеграція штучного інтелекту (ШІ) та автономних функцій відкриває нові можливості, але й створює низку технологічних і правових викликів, що безпосередньо впливає на трансформацію підходів до підготовки військових фахівців.

1. Еволюція форм і способів бойового застосування БпС

Форми застосування безпілотної авіації пройшли шлях від допоміжних засобів забезпечення до самостійних ударних і стратегічних операцій:

• Еволюція функцій: Початкова роль БпЛА обмежувалася веденням тактичної розвідки та коригуванням артилерійського вогню в реальному часі. Сьогодні вони виконують завдання з радіоелектронної боротьби (РЕБ), ретрансляції зв'язку, дистанційного мінування та безпосереднього ураження цілей.

• Ударні та FPV-комплекси: Поява та масове впровадження FPV-дронів (First Person View) змінили архітектуру тактичної оборони й наступу, дозволяючи високоточно знищувати бронетехніку та живу силу супротивника за мінімальної вартості порівняно зі звичайними боєприпасами.

• Тактика «рою» (Swarm intelligence): Сучасним етапом розвитку є перехід від індивідуального керування до скоординованого групового застосування, де десятки дронів взаємодіють між собою для перевантаження систем протиповітряної оборони (ППО) ворога.

Наземні безпілотні системи (НБС):

Розвиток наземних роботизованих комплексів тривалий час стримувався складністю рельєфу та перешкодами на полі бою, проте наразі сформувалися чіткі способи їх застосування:

• Логістичні та евакуаційні місії: Доставка боєприпасів, провізії та медикаментів на передові позиції («остання миля»), а також безпечна евакуація поранених з-під вогню.

• Інженерне забезпечення: Дистанційне мінування території та розмінування (проходи в мінно-вибухових загородженнях).

• Вогнева підтримка: Застосування бойових турелей та рухомих платформ, оснащених кулеметами чи протитанковими керованими ракетами (ПТКР), для утримання позицій без безпосередньої присутності особового складу.

2. Автономність та технології штучного інтелекту (ШІ): можливості, перспективи, обмеження

Нові можливості та переваги ШІ:

• Стійкість до засобів РЕБ: Традиційні дрони залежать від каналів зв'язку з оператором та сигналів GPS. Інтеграція штучного інтелекту дозволяє реалізувати технологію машинного зору (кінетичного захоплення цілі). Після фіксації об'єкта дрон атакує його в повністю автономному режимі, навіть за умов повної втрати зв'язку.

• Навігація без GPS: Використання оптичної навігації (на основі зіставлення рельєфу місцевості з цифровими картами — DSM/TERCOM) дозволяє апаратам орієнтуватися в просторі за умов відсутності супутникових сигналів.

• Автоматизація аналізу даних: ШІ здатний у режимі реального часу обробляти гігабайти відеопотоку, автоматично виявляти замасковану техніку, класифікувати її та передавати координати артилерії швидше, ніж це зробить людина.

Перспективи розвитку:

Майбутнє БпС пов'язане з переходом до повністю автономних екосистем. Це включає автоматизовані платформи базування (дрони-носії, «дрони-матки»), які самостійно випускають менші безпілотники, координують їхні дії через нейромережі та повертають їх для дозарядки без залучення людського ресурсу.

3. Обмеження та виклики

• Проблема ідентифікації («свій-чужий»): ШІ все ще вразливий до засобів маскування, макетів (хибних цілей) та складних погодних умов, що підвищує ризик помилкового удару.

• Обчислювальні потужності: Сучасні алгоритми ШІ вимагають значних енергоресурсів та компактних, але потужних мікропроцесорів, що збільшує вартість і вагу кінцевого виробу.

• Етичний та правовий аспекти: Повна автономія ухвалення рішення на знищення людини суперечить нормам міжнародного гуманітарного права. Постає дилема: хто несе відповідальність за помилки алгоритму — програміст, виробник чи військовий командир?

4. Сучасний досвід підготовки фахівців БпС

Трансформація методів ведення війни вимагає переосмислення підходів до навчання персоналу. Військова освіта зміщується в бік високотехнологічних дисциплін.

Ключові компоненти навчання:

• Симуляційна підготовка: Використання спеціалізованого програмного забезпечення та VR-тренажерів є базовим етапом. Це дозволяє майбутнім операторам напрацювати м'язову пам'ять (особливо для FPV-дронів) без ризику втрати дорогого обладнання.

• Інженерна та технічна грамотність: Сучасний оператор повинен не лише вміти керувати апаратом, а й розуміти основи радіофізики, вміти змінювати робочі частоти для обходу РЕБ, паяти, програмувати плати та налаштовувати антени безпосередньо в польових умовах.

• Тактична адаптивність: Навчання включає роботу в умовах постійного радіоелектронного придушення, маскування позицій розрахунку (оскільки оператори є першочерговою ціллю для ворога) та взаємодію з іншими родами військ (артилерія, піхота).

Проблеми та шляхи їх вирішення:

Головним викликом є швидкість застарівання знань. Технологічний цикл БпС на фронті триває від кількох тижнів до кількох місяців — тактика, що була ефективною місяць тому, сьогодні може не працювати через оновлення засобів РЕБ ворога. Тому підготовка фахівців вимагає децентралізації, залучення цивільних інженерних шкіл та створення гнучких навчальних програм, які оновлюються на основі реального бойового досвіду в режимі – «сьогодні на сьогодні».

Висновки

Розвиток безпілотних систем довів, що майбутнє Збройних Сил залежить від рівня їхньої цифровізації та роботизації. Перехід до автономності на базі штучного інтелекту є безальтернативним шляхом розвитку БпС через щільне насичення поля бою засобами РЕБ. Водночас ефективність цих технологій визначається не лише технічними характеристиками, а й гнучкістю системи підготовки кадрів, здатної оперативно адаптуватися до технологічних змін.

Вінник В. В.
Москалик С. В.
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ КОМПЛЕКСНОГО ЗАСТОСУВАННЯ БЕЗПЛОТНИХ СИСТЕМ

Застосування безпілотних систем (БпС) Силами оборони України (СОУ) на сучасному етапі війни виявило комплекс проблем. Метою дослідження є системний аналіз перешкод по впровадженню і застосуванню БпС та визначення перспективних векторів розвитку для підвищення ефективності міжвидового застосування БпС.

У ході аналізу було виявлено наступні ключові групи проблем що призводить до зниження ефективності застосування або втрати БпС:

а) координації та ситуаційної обізнаності:

- хаос у повітряному просторі через велику щільність БпС різних підрозділів, видів ЗС та родів військ, відомств в одному секторі без єдиного диспетчерського центру створює ризики втрати;

- дублювання цілей через відсутність миттєвого обміну даними кілька підрозділів одночасно витрачають боєприпаси на одну й ту саму ціль;
- різноманіття систем через використання різних протоколів передачі команд управління чи відео сповільнює цикл «виявлення — знищення»;

б) організаційні:

- підпорядкування різним відомствам які діють за власними статутами, що ускладнює їх комплексне застосування на ділянці фронту в єдиній системі;
- організаційна невідповідність через застарілі процедури списання, які обліковуються як дорого вартісне майно, а не розхідний боєприпас;
- організаційна відсутність зворотного зв'язку з виробниками, не дозволяє вчасно змінювати БпС відповідно до реальних бойових умов;
- багато інноваційних рішень залишаються на рівні окремих екземплярів (підрозділів), оскільки винахідники не мають доступних можливостей оперативного впровадження;

в) технічні та виробничі аспекти:

- застосування стандартів які не відповідають сучасним вимогам призводить до використання застарілих або вже не актуальних компонентів;
- хаос у технічному обслуговуванні що виник через повільну реакцію виробників та необхідність адаптації БпС до реальних умов;
- короткий життєвий цикл через швидкий «реверс-інжиніринг» з боку ворога нова технологія залишається ефективною лише 2–3 місяці;
- виробництво критично залежить від іноземних компонентів (особливо з Китаю), що створює ризики припинення поставок;

г) у радіоелектронному просторі:

- відсутність розподілу частот;
- вплив власних засобів РЕБ;
- відсутність ефективної системи розпізнавання «свій-чужий»;

д) логістичні:

- корупційна складова через що на фронт поставляються БпС які або непридатні до застосування або доводиться переробляти самим;
- логістичний розрив через державні закупівлі часто не встигають за технологічним розвитком, через що дрони застарівають ще до потрапляння на фронт.

Ключові пропозиції:

1. Уніфікація управління: Широке впровадження системи Delta як єдиного вікна ситуаційної обізнаності та розвиток Сил безпілотних систем (СБС) для централізації управління.

2. Впровадження ШІ та машинного зору: Перехід на термінальне автонаведення дозволить дронам вражати цілі в умовах повної відсутності зв'язку через РЕБ.

3. Технологічна диверсифікація: Використання альтернативних каналів зв'язку, зокрема оптоволокна, яке є абсолютно несприйнятливим до РЕБ.

4. Спрощення бюрократії: Реформування правової бази для швидкого списання засобів ураження та спрощення передачі майна між різними родами військ.

5. Розвиток нових концепцій: Впровадження «дронів-маток» для ретрансляції сигналу та систем «рою дронів» для перевантаження ППО противника.

Висновок.

Ефективність подальшого застосування БпАС залежить від швидкості переходу до повністю автономних систем та їх інтеграції в єдині контури мережецентричної війни.

Добровінський В. П.
Приймачук О. В.
Житомирський військовий інститут імені С. П. Корольова

ПРОБЛЕМИ МОТИВАЦІЇ ТА ДОБОРУ СТУДЕНТІВ ДО НАВЧАННЯ ЗА ПРОГРАМОЮ ПІДГОТОВКИ ОФІЦЕРІВ ЗАПАСУ ВИСОКОТЕХНОЛОГІЧНИХ СПЕЦІАЛЬНОСТЕЙ

Досвід відсічі широкомасштабній збройній агресії рф проти України засвідчив гостру потребу Збройних Сил України (ЗСУ) в офіцерах, здатних експлуатувати й бойово застосовувати високотехнологічні зразки озброєння та військової техніки (ОВТ), насамперед безпілотні системи, засоби радіоелектронної боротьби та зв'язку. Природним джерелом поповнення офіцерського резерву таких фахівців є студенти інженерних і технічних спеціальностей закладів вищої освіти (ЗВО), які паралельно проходять військову підготовку за програмою підготовки офіцерів запасу.

З 1 січня 2026 року діє нова редакція Порядку проведення військової підготовки громадян України за програмою підготовки офіцерів запасу (постанова КМУ від 5 грудня 2025 р. № 1612), якою загальний обсяг навчального часу збільшено до 44 кредитів ЄКТС і оновлено процедуру конкурсного відбору. Однак більший обсяг годин сам по собі результату не

гарантує: не менше важить те, хто і з якими намірами вступає на навчання. Публікації останніх років здебільшого розглядають нормативні та організаційні засади підготовки офіцерів запасу; емпіричних даних про мотивацію вступників в умовах воєнного стану в доступних нам джерелах майже немає.

Мета дослідження: визначити структуру мотивів вступу студентів на навчання за програмою підготовки офіцерів запасу, проаналізувати причини їх відрахування та обґрунтувати напрями вдосконалення добору кандидатів.

Анкетне опитування проведено на кафедрі військової підготовки офіцерів запасу Житомирського військового інституту імені С. П. Корольова серед випускників 2026 року (близько 100 осіб). Кожен респондент обирав один, основний для себе мотив вступу. Відповіді розподілилися так: усвідомлення невідворотності військової служби та переконання, що краще служити офіцером, ніж солдатом, 30 %; патріотичне покликання, 20 %; намір проходити службу в інших силових структурах, 20 %; порада батьків, 15 %; плани щодо подальшої державної служби, 15 %. Опитано лише випускників, тож ця картина не охоплює весь набір.

Переважають прагматичні мотиви, пов’язані зі статусом і кар’єрою: разом їх обрали 65 % респондентів. Найбільша група сприймає військову підготовку як можливість у разі призову служити на офіцерській посаді. Засуджувати такий вибір немає підстав. Він відображає тверезу оцінку безпекової ситуації і дає стійку зацікавленість довести навчання до кінця. Натомість ціннісний мотив, патріотичне покликання, провідний лише для кожного п’ятого опитаного.

Тривожніший сигнал дає група, орієнтована на службу в інших силових структурах (20 %). Частина офіцерів запасу, підготовлених на навчально-матеріальній базі військового навчального закладу, найімовірніше, поповнить не резерв ЗСУ, а інші складові сектору безпеки і оборони. Схожа картина з тими, хто планує державну службу: офіцерське звання для них насамперед перевага в кар’єрі, а не крок до військової служби.

Ще 15 % вступили за порадою батьків, тобто рішення частини кандидатів було не до кінця самостійним. Зовнішня мотивація такого типу нестійка: щойно змінюються життєві обставини, вона поступається іншим пріоритетам, і ризик відсіву зростає.

Серед причин відрахування в процесі навчання перше місце посідає виїзд здобувачів на навчання за кордон. Імовірність таких випадків зросла, відколи з 28 серпня 2025 року чоловікам віком від 18 до 22 років включно дозволено

перетинати державний кордон в умовах воєнного стану (постанова КМУ № 1031). Це означає втрату вкладених у підготовку ресурсів і недобір випускників за відповідними військово-обліковими спеціальностями (ВОС). Конкурсний відбір ґрунтується на результатах вступних випробувань (зокрема оцінювання успішності навчання в ЗВО та засвоєння програми допризовної підготовки), професійного психологічного відбору та медичного огляду військово-лікарською комісією. Психологічний відбір дає загальне уявлення про військово-професійну спрямованість кандидата, проте його планів на період навчання не з'ясовує, тож ризик відсіву на вступі не виявляється.

Для технічних ВОС не менш важлива базова підготовка за цивільною спеціальністю: від неї залежить, чи зможе майбутній офіцер опанувати складні зразки ОВТ. Порядок вимагає відповідності спеціальності здобувача ВОС, проте формальна відповідність ще не свідчить про глибину фахових знань.

З огляду на отримані результати пропонуємо такі напрями вдосконалення добору та мотиваційного супроводу студентів:

1) доповнення конкурсного відбору структурованою співбесідою, під час якої оцінюються мотивація кандидата та його плани на період навчання, зокрема щодо можливого виїзду за кордон;

2) проведення вхідного анкетування вступників і повторного на випускному курсі, щоб відстежувати зміну мотивації;

3) залучення батьків до профорієнтаційної роботи, оскільки їхня думка помітно впливає на рішення кандидатів;

4) адресна профорієнтаційна робота на інженерних і технічних факультетах ЗВО з наочною демонстрацією змісту підготовки за високотехнологічними ВОС;

5) посилення практичної спрямованості навчання: тренажери та симулятори, заняття з інструкторами, які мають бойовий досвід, що формує професійну мотивацію;

6) своєчасне інформування студентів про перспективи служби на офіцерських посадах у ЗСУ.

Отже, у структурі мотивації вступників на навчання за програмою підготовки офіцерів запасу переважають прагматичні мотиви, а ціннісні становлять лише п'яту частину. Чинна система конкурсного відбору майже не враховує мотиваційного компонента і намірів кандидатів, тому не дає змоги ще на етапі вступу виявити ризик відсіву, передусім через виїзд за кордон.

Запропоновані заходи дадуть змогу підвищити якість добору, зменшити відрахування і збільшити частку випускників, які реально поповнюють офіцерський резерв ЗСУ, зокрема за високотехнологічними спеціальностями.

Бондаренко О. О.
Чередніченко Є. В.
Давлетов А. Р.
Військова академія (м. Одеса)

ВПЛИВ ЯКОСТІ ВІДНОВЛЕННЯ ЗОБРАЖЕННЯ В УМОВАХ АКТИВНИХ ШУМОВИХ ЗАВАД НА ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ УДАРНИХ І РОЗВІДУВАЛЬНИХ БЕЗПІЛОТНИХ КОМПЛЕКСІВ

Ефективність застосування ударних і розвідувальних безпілотних комплексів (далі – БпК) значною мірою визначається якістю відеосигналу, на підставі якої оператор виявляє, розпізнає та захоплює ціль. Активні шумові завади, що діють на радіоканал передачі відеосигналу, знижують відношення сигнал-(завада + шум) (далі – ВСЗШ) на вході приймача. В аналогових відеоканалах це спричиняє шумові погіршення якості зображення, а в цифрових втрати даних і погіршення якості кадрів. Як наслідок, скорочується дальність, на якій оператор здатен упевнено виявити та розпізнати ціль.

Досвід бойових дій в Україні показує, що противник масово застосовує засоби радіоелектронної боротьби для придушення радіоканалів керування БпК і передачі відеосигналу. Зокрема, на техніці противник встановлює станції радіоелектронного подавлення, заявлений діапазон робочих частот однієї з яких становить 0,3–6 ГГц. У відповідь розробники та підрозділи змінюють частотні діапазони, удосконалюють антени й тактику заходу на ціль, а також застосовують БпК з керуванням на оптоволокі та автоматичним наведенням на кінцевій ділянці польоту. Проте БпК з оптоволоконним керуванням мають обмеження щодо дальності й маневру, а також ризик обриву кабелю, тому не замінюють повністю БпК з радіоканалами. Відтак підвищення якості зображення, отриманого радіоканалом в умовах активних шумових завад, зберігає практичне значення.

Одним зі способів зменшення впливу активних шумових завад є адаптивна просторово-часова обробка сигналів в антенній решітці приймальної

сторони. Адаптивне формування діаграми спрямованості створює провал у напрямку на джерело завади і тим самим підвищує ВСЗШ, а часова складова обробки забезпечує придушення широкосмугових завад. Разом з тим можливості такої обробки обмежені. Кількість завад, які можна придушити, не перевищує N – 1, де N – кількість елементів антенної решітки. Крім того, ефективність придушення знижується, якщо джерело завади розташоване в напрямку, близькому до напрямку на БпК. Така ситуація можлива, зокрема, на кінцевій ділянці польоту ударного БпК до цілі, оснащеної власним засобом радіоелектронного подавлення. У цьому разі кут між напрямками з пункту керування на БпК і на джерело завади зменшується в міру наближення БпК до цілі. Залишкові погіршення якості зображення, що зберігаються після такої обробки, можуть бути додатково зменшені методами відновлення зображень, зокрема міжкадровою фільтрацією.

Водночас результативність методів протидії завадам та відновлення зображень зазвичай оцінюють за показниками якості сигналу чи якості зображення, як-от ВСЗШ, піковим відношенням сигнал-шум та індексом структурної подібності. Ці показники зручні для порівняння алгоритмів, однак не дають прямої відповіді на питання, наскільки зміниться результат виконання бойового завдання. З огляду на це метою роботи є обґрунтування підходу до оцінювання впливу якості відновлення зображень в умовах активних шумових завад на ефективність застосування ударних і розвідувальних БпК.

Запропонований підхід ґрунтується на послідовному переході від параметрів завадової обстановки до показників ефективності застосування БпК. Вихідними даними є параметри завади (потужність, ширина спектра, кутове положення джерела відносно напрямку на БпК), параметри корисного сигналу, відстань між БпК і пунктом керування, а також параметри антенної решітки та відеокамери БпК. На їх основі визначається ВСЗШ на виході адаптивної просторово-часової обробки, а далі показники якості відновленого зображення. Крім пікового відношення сигнал-шум та індексу структурної подібності, слід визначати кількість розрізнюваних елементів зображення, що припадають на критичний розмір цілі. Цей показник залежить як від роздільної здатності відеокамери та відстані до цілі, так і від рівня залишкового погіршення якості, тому саме він пов’язує якість зображення з можливостями оператора.

Перейти до ймовірностей виявлення та розпізнавання цілі можна за допомогою критерію Джонсона, згідно з яким імовірність виконання завдання зорового

сприйняття визначається кількістю розрізнюваних пар ліній на критичному розмірі цілі. Застосування цього критерію до зображень, погіршує радіоелектронний вплив, потребує визначення ефективної кількості розрізнюваних елементів з урахуванням погіршення якості зображення. На цій основі оцінюють дальності виявлення та розпізнавання цілі в заданій завадовій обстановці.

Як показники ефективності застосування БпК пропонується використовувати дальність захоплення цілі, імовірність виконання завдання за один виліт і середню кількість вильотів на одне виконане завдання. Для ударних БпК з функцією автоматичного супроводження цілі перший із цих показників є особливо важливим, адже оператор повинен захопити ціль до можливої втрати радіозв’язку на кінцевій ділянці польоту. Відповідно, більша дальність розпізнавання збільшує запас часу на захоплення. Наприклад, для системи донаведення “ЗІР” дальність автоматичного розпізнавання цілі становить від 150 до 800 м залежно від типу цілі, а дальність автоматичного наведення на ціль до 1000 м. За іншим джерелом, дальність автоматичного розпізнавання цілі становить 150–400 м, дальність захоплення цілі в автоматичному режимі 300 м, а в ручному режимі 700 м. Система має власну камеру і підключається до польотного контролера та штатного відеопередавача БпК. Отже, автоматичне розпізнавання цілі виконується за зображенням бортової камери, тоді як ручний вибір цілі пілот здійснює за відеоінформацією, отриманою радіоканалом. Саме на етапі ручного вибору цілі якості відновленого зображення безпосередньо впливає на дальність захоплення. Для розвідувальних БпК більша дальність розпізнавання дає змогу вести розвідку з більшої відстані до об’єкта, що може зменшити ризик ураження самого БпК.

Перевірити запропонований підхід можна за допомогою імітаційного моделювання, яке охоплює модель радіоканалу передачі відеоінформації з джерелом активної шумової завади, модель адаптивної просторово-часової обробки сигналів в антенній решітці приймальної сторони та модель відновлення зображення. Порівняння показників якості зображення та дальності розпізнавання цілі за наявності й за відсутності кожного етапу обробки дасть змогу кількісно оцінити внесок цього етапу в ефективність застосування БпК.

Отже, якість відновлення зображень в умовах активних шумових завад доцільно оцінювати не лише за показниками якості сигналу та зображення, а й

через її вплив на дальність захоплення цілі та ймовірність виконання завдання. За запропонованим підходом методи адаптивної обробки сигналів і відновлення зображень можна порівнювати за показниками, які безпосередньо пов'язані з бойовим застосуванням БпК. Подальші дослідження будуть спрямовані на проведення імітаційного моделювання за запропонованою схемою та експериментальну перевірку його результатів в умовах, наближених до реальної завадової обстановки.

Омельчук О. В.
Житомирський військовий інститут імені С. П. Корольова

ШЛЯХИ ВИРІШЕННЯ ПИТАННЯ ЗБІЛЬШЕННЯ ЗАПАСУ ХОДУ БЕЗПІЛОТНИХ НАЗЕМНИХ КОМПЛЕКСІВ

Активне впровадження роботизованих технологій у військовій галузі зумовлене потребою мінімізувати ризики для особового складу та підвищити ефективність бойових і логістичних операцій. Безпілотні наземні комплекси (БпНК) – один із найбільш динамічних напрямів сучасного розвитку оборонних технологій.

Отриманий досвід під час повномасштабного вторгнення збройних сил російської федерації (зс рф) на територію України свідчить про те, що БпНК набувають стрімкого розвитку з обох сторін. Станом на вересень 2026 року, безпілотні підрозділи Збройних Сил (ЗС) України використовують БпНК для: виконання бойових завдань в якості ударних засобів для знищення легко та важко броньованої техніки, укріплень та фортифікаційних споруд противника; вогневої підтримки дій військ; виконання розвідувальних, логістичних, евакуаційних, інженерних, завдань; виконання завдань з риття окопів та бліндажів (землерийні). Останнім часом БпНК використовують в якості БпНК-ретрансляторів для збільшення дальності зв'язку, для ведення радіоелектронної боротьби (РЕБ), гасіння пожеж (пожежні). Відносно новим напрямком застосування БпНК є їх використання в якості зенітних засобів за рахунок встановлення на їх борту засобів протиповітряної оборони для виявлення та ураження повітряних цілей.

Як можна побачити з вище зазначеного, спектр завдань, які виконуються за допомогою БпНК, постійно розширюється.

ЗС України регулярно впроваджують інноваційні підходи до інтеграції БпНК в бойові порядки підрозділів, перетворивши їх з експериментальних зразків у повноцінну “нову кавалерію” сучасного поля бою, самостійний елемент бойового порядку, здатний докорінно змінити тактику ведення бойових дій. Головна мета інтеграції БпНК в бойові порядки підрозділів – збереження життя особового складу шляхом проведення за допомогою БпНК найбільш ризикованих логістичних, евакуаційних, ударних операцій, операцій з вогневого ураження дистанційного мінування та розмінування. В таких підрозділах, як наприклад 3 армійський корпус, застосування БпНК для виконання логістичних та евакуаційних місій підрозділів становить 80 % та 90 % відповідно. Відсоток ударних операцій, операцій з вогневого ураження дистанційного мінування та розмінування, які проводяться із застосуванням БпНК становить від 70 % до 80 %. А, отже, відсоток втрат серед особового складу підрозділів 3 армійського корпусу є одним із самих низьких у ЗС України. Досягнення таких показників стало можливим завдяки застосуванню БпНК із великим запасом ходу, що є важливою характеристикою при постійному збільшенні розмірів “сірої зони” (так званої “killzone”).

Розглянемо питання збільшення запасу ходу детальніше.

На протязі 2022-2024 рр. БпНК використовувались для виконання логістичних, евакуаційних, ударних операцій, операцій з вогневого ураження дистанційного мінування та розмінування на відстані від декількох сотень метрів до декількох кілометрів від точки їх старту (пункту дистанційного пілотування, позиції операторів засобів керування). З часом ця відстань зросла до 10-15 км, але вона завжди була залежною від запасу ходу БпНК.

В подальшому, у зв’язку з постійним збільшенням розмірів “сірої зони” в період бойових дій з 2025 року по теперішній час, виникла необхідність збільшення запасу ходу БпНК. Цього можна досягти за рахунок:

збільшення ємності та потужності акумуляторної батареї (АКБ);

встановлення на борту БпНК засобів, здатних забезпечувати якісний зв’язок на більших відстанях.

Для збільшення ємності та потужності АКБ на БпНК окрім стандартних АКБ з літій-іонними (Li-ion) елементами зараз почали встановлювати АКБ з літій-нікель-марганець-кадмій (Li-NMC) та літій-залізо-фосфатними (LiFePO4) елементами, забезпечуючи їм максимальний захист від вологи, пилу, багнюки.

Відсіки для встановлення АКБ роблять герметичними, утеплюють їх задля збереження заряду АКБ в холодну пору року.

Для забезпечення якісного зв'язку на БпНК активно застосовують супутникові термінали Starlink.

В результаті вжитих заходів, з кінця 2025 року на озброєнні безпілотних підрозділів ЗС України з'явились кодифіковані БпНК ("БІЗОН-Л", "ВОЖАК", "ЄРИХОН", "ГУЛІВЕР", "МУРАХА" та ін.) з запасом ходу від 40 км до 50 км., а деякі, як наприклад, логістичні БпНК "МАУЛ", "BYFALO" та ін. мають запас ходу до від 80 км до 100 км.

Отже, вжиття запропонованих заходів для збільшення запасу ходу БпНК дозволить: підвищити відсоток успішних місій по ураженню особового складу, небронюваної, легкобронюваної техніки, фортифікаційних споруд противника; підвищити відсоток успішно виконаних логістичних та розвідувальних місій та місій з евакуації поранених та полеглих військовослужбовців ЗС України; зменшити відсоток втрат серед особового складу підрозділів та частин ЗС України.

Так як в сучасних бойових умовах буде постійно спостерігатись збільшення розмірів "сірої зони", то концепція використання БпНК для виконання ризикованих логістичних, евакуаційних, ударних операцій, операцій з вогневого ураження дистанційного мінування та розмінування є перспективною та ефективною при виконанні завдань безпілотними підрозділами ЗС України та потребує подальшого розвитку. Доцільним є масштабування необхідної інформації щодо зразків БпНК із збільшеним запасом ходу та можливостей їх закупівлі та поставки у безпілотними підрозділами ЗС України.

Колодницький В. В.
Михайловський В. П.
Житомирський військовий інститут імені С. П. Корольова

ОБҐРУНТУВАННЯ ПРАКТИЧНОЇ ТА ТЕОРЕТИЧНОЇ СКЛАДОВИХ ПІДГОТОВКИ ФАХІВЦІВ БЕЗПІЛОТНИХ СИСТЕМ

Стрімкий розвиток безпілотних систем та розширення сфер їх застосування у Збройних Силах України під час повномасштабного вторгнення рф зумовлюють необхідність підготовки висококваліфікованих фахівців, здатних ефективно працювати із сучасними безпілотними комплексами. Безпілотні системи охоплюють широкий спектр технічних засобів, програмного забезпечення, систем управління, обробки даних та керування що потребує комплексного підходу до професійної підготовки особового складу.

Досвід підготовки спеціалістів безпілотних систем свідчить, що ефективність навчального та освітнього процесу значною мірою залежить від оптимального поєднання теоретичних знань, практичних навичок, управління, технічного обслуговування й застосування. Теоретична та практична складова повинна забезпечувати сприймання принципів функціонування безпілотних систем, їх конструктивних особливостей, систем управління, навігації, зв’язку, технічного обслуговування, програмного забезпечення, роботи з обладнанням, а також здатності ефективно діяти в умовах швидких змін обстановки.

Водночас найголовніше значення має набуття практичного досвіду. Застосування тренажерів та симуляторів дає можливість сформувати базові навички роботи з безпілотними системами, відпрацювати типові алгоритми дій та підвищити якість підготовки особового складу. За допомогою тренажерів та симуляторів зменшується подальша втрата БпЛА під час навчання та у подальшому при виконанні бойових (спеціальних) завдань. Після проходження етапу з симуляторами доцільним є виконання практичних завдань із реальним обладнанням та в подальшому удосконалення своїх навичок.

Важливим напрямом є формування у фахівців здатності аналізувати технічну інформацію, виявляти несправності, оцінювати умови експлуатації системи та приймати обґрунтовані рішення відповідно до поставленого завдання. Не менш важливими є навички взаємодії у складі екіпажу та дотримання встановлених процедур безпечної експлуатації, маскування.

Особливістю підготовки фахівців БпС є необхідність постійного оновлення професійних знань та практичних навичок. Технології розвиваються дуже швидкими темпами, тому освітні програми, навчально-методичні матеріали та практичні завдання та навички мають регулярно переглядатися та оновлюватися. До освітнього процесу доцільно залучати фахівців-практиків, які виконували бойові (спеціальні) завдання та можуть передавати актуальний досвід експлуатації сучасних комплексів (систем).

З постійною модернізацією та оновленням безпілотних систем з'являються нові типи та засоби безпілотних систем, наприклад, реактивні перехоплювачі, які найближчим часом зможуть перехоплювати реактивні дрони противника, а можливо й крилаті ракети. Тому на безпілотних системах акцентують велику увагу на рівні керівництва держави та Збройних Сил України.

Таким чином, підготовка фахівців безпілотних систем має ґрунтуватися на здатності застосовувати знання, уміння та навички в реальних бойових та повсякденних ситуаціях. Оптимальним є поєднання аудиторного навчання, технологій симуляторів і тренажерів, практичних занять та оцінювання сформованих умінь та практичних навичок.

Сучасний досвід підготовки фахівців безпілотних систем підтверджує необхідність інтегрованого підходу до організації освітнього процесу. Основними умовами ефективної підготовки є відповідність змісту навчання сучасним технологіям, достатній обсяг практичних занять, використання симуляторів, тренажерів, залучення досвідчених фахівців та постійне вдосконалення навчально-матеріальної бази.

Подальший розвиток системи підготовки варто спрямовувати на формування універсальних професійних компетентностей, здатності працювати з різними типами безпілотних систем при виконанні бойових (спеціальних) завдань та готовності до постійного професійного вдосконалення у сфері застосування та експлуатації безпілотних систем.

Лиходєєв О. С., канд. техн. наук, доц.
Георгієв Ю. В.
Василенко Р. В.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

РОЗВИТОК БОРТОВОГО КОМПЛЕКСУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ ТА ПЕРСПЕКТИВНІ ВИМОГИ ДО НЬОГО

Російсько-українська війна стала визначальним фактором розвитку безпілотних авіаційних комплексів військового призначення. Досвід їх бойового застосування засвідчив, що ефективність виконання бойових завдань визначається не лише льотно-технічними характеристиками безпілотного літального апарата, а й можливостями його бортового комплексу. Саме він забезпечує автоматичне керування польотом, навігацію, зв'язок, оброблення інформації та взаємодію із наземною станцією керування. Постійне вдосконалення засобів радіоелектронної боротьби (РЕБ) та зміна характеру бойових дій спричинили швидку еволюцію архітектури бортових комплексів, аналіз якої дозволяє визначити перспективні напрями їх розвитку.

У 2022 році БПЛА оснащувалася відносно простими бортовими комплексами, до складу яких входили автопілот, інерціальна навігаційна система, приймач супутникової навігації, телеметричний канал та система передачі відеосигналу. Основними функціями були стабілізація польоту, виконання елементарних автоматичних режимів і передача інформації оператору. Робота комплексу значною мірою залежала від стійкості сигналів глобальних навігаційних супутникових систем (GNSS) та постійного керування оператором.

У 2023 році розвиток бортових комплексів був спрямований на підвищення їх живучості. Удосконалювалися алгоритми автоматичного повернення, резервувалися окремі датчики, розширювалися можливості автономного польоту за визначеним маршрутом, впроваджувалися цифрові канали зв'язку та функції контролю технічного стану.

Протягом 2024 року визначальним фактором стала активна протидія засобів РЕБ. Це обумовило інтеграцію декількох навігаційних джерел,

удосконалення алгоритмів визначення координат при втраті сигналів супутникової навігації, підвищення завадозахищеності каналів зв'язку та розширення можливостей автономного виконання завдань.

У 2025-2026 роках розвиток перейшов до етапу інтелектуалізації. Бортові комплекси оснащуються високопродуктивними процесорами, що забезпечують реалізацію алгоритмів комп'ютерного зору, автоматичного розпізнавання об'єктів, аналізу обстановки та підтримки прийняття рішень. Одночасно активно впроваджується модульна архітектура авіоніки, яка дозволяє швидко інтегрувати нові датчики, засоби зв'язку та функціональні модулі.

Аналіз розвитку свідчить, що перспективний бортовий комплекс повинен забезпечувати автономну навігацію шляхом комплексування супутникових, інерціальних, візуальних та інших навігаційних систем, що дозволить виконувати політ навіть за відсутності сигналів GNSS. Важливого значення набуває використання високопродуктивних обчислювальних платформ, здатних реалізовувати алгоритми штучного інтелекту без залучення зовнішніх ресурсів.

Перспективні комплекси повинні підтримувати автоматичне розпізнавання цілей, аналіз обстановки, вибір оптимального маршруту та підтримку прийняття рішень. Системи зв'язку мають використовувати декілька незалежних каналів передачі інформації, забезпечувати їх автоматичне перемикання, криптографічний захист даних та високу стійкість до впливу засобів РЕБ.

Однією з ключових вимог є підвищення живучості бортового комплексу шляхом збереження працездатності при втраті зв'язку, відмові окремих датчиків або впливі зовнішніх завад. Водночас архітектура комплексу повинна бути модульною та відкритою, що забезпечить швидку модернізацію, інтеграцію нового обладнання та адаптацію до різних типів безпілотних платформ.

Особливої актуальності набувають питання інформаційної безпеки, які передбачають захист програмного забезпечення, контроль його цілісності та безпечне оновлення. До складу перспективного бортового комплексу доцільно включити систему самодіагностики, здатну виявляти несправності, прогнозувати можливі відмови та інформувати оператора про технічний стан обладнання. Подальший розвиток алгоритмів автоматичного керування має бути спрямований на інтелектуальне керування польотом із можливістю адаптації до змін тактичної обстановки та автоматичного обходження небезпечних зон.

Проведений аналіз дозволяє зробити висновок, що розвиток бортових комплексів БПЛА військового призначення відбувається у напрямі переходу від спеціалізованих систем автоматичного керування до інтегрованих інтелектуальних комплексів авіоніки, які поєднують функції навігації, керування, зв'язку, оброблення інформації, самодіагностики та підтримки прийняття рішень. Реалізація зазначених вимог сприятиме підвищенню автономності, живучості та ефективності застосування перспективних безпілотних авіаційних комплексів в умовах сучасних воєнних конфліктів.

Мошаренков В. В., канд. техн. наук., доц.
Мошаренкова Т. В.
Рогуля О. В., Ph.D.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ СИСТЕМ: АНАЛІЗ ДОСВІДУ ТА ОРГАНІЗАЦІЙНІ ВИКЛИКИ

Сучасні виклики російсько-української війни та різкі зміни в оперативній обстановці, а також необхідність адаптації структури Сил оборони України (СОУ) до актуальних геополітичних і безпекових задач підтверджують пріоритетність державного розвитку військової справи та воєнної науки в Україні. Аналіз бойового досвіду переконливо доводить, що здобуття домінування на полі бою здебільшого залежить від адаптивності, гнучкості оборонних стратегій та інноваційної переваги, аніж від кількісного співвідношення сил і засобів. Саме тому ключовим вектором модернізації є нарощування спроможностей СОУ, що досягається впровадженням новітніх технічних розробок, переглядом загальнотехнічних вимог до зразків озброєння та військової техніки (ОВТ), а також проведенням фундаментальних та прикладних наукових досліджень, зокрема у сфері випробувань та метрологічного супроводження.

У цьому контексті масове та інтегроване застосування безпілотних систем (БпС) і комплексів різного базування (повітряного, наземного, морського) є ключовим фактором, який визначає характер сучасних збройних конфліктів.

БпС докорінно змінюють тактику ведення бойових дій, виступаючи критичним елементом операційного циклу “розвідка – зв’язок – навігація – ураження”.

Забезпечення інституційної стійкості та технологічного лідерства СОУ вимагає комплексного вирішення накопичених організаційних, доктринальних та техніко-технологічних викликів за трьома основними напрямами.

По-перше, розвиток форм і способів бойового застосування авіаційних та наземних БпС, що передбачає:

– створення єдиного командно-інформаційного простору – моделювання та впровадження актуальних форм застосування БпС, спрямованих на формування цілісного цифрового простору управління міжвидовими угрупованнями військ у реальному часі;

– нормативно-доктринальне забезпечення – оперативне розроблення та затвердження єдиних доктринальних документів, які регламентують тактичні прийоми застосування, порядок взаємодії та координації підрозділів БпС із підрозділами ракетних військ і артилерії, бронетехніки, піхоти та засобів радіоелектронної боротьби (РЕБ);

– інтегроване застосування та конструктивне вдосконалення – скоординоване задіяння БпС по всій глибині оперативної побудови противника у поєднанні з модернізацією аеродинаміки, матеріалознавчих рішень та джерел енергії, що є критичним чинником здобуття тактичної та оперативної ініціативи.

По-друге, автономність та технології штучного інтелекту (ШІ) в БпС: (можливості, перспективи, обмеження): в умовах високої насиченості операційного простору засобами РЕБ підвищення автономності БпС постає критичним пріоритетом, що реалізується через системну інтеграцію математичного моделювання, алгоритмів ШІ та прискорених методик випробувань бортового радіоелектронного обладнання (БРЕО)**.**

По-третє, розвиток системи підготовки фахівців БпС та роботизованих комплексів, оскільки системна ефективність, надійність та боєздатність підрозділів безпосередньо залежать від рівня фахової підготовки особового складу, формалізації накопиченого бойового досвіду та гнучкості освітніх програм, як то:

– трансформації системи комплектування та фахової підготовки – оптимізація процесів добору, первинного навчання, перепідготовки та підвищення кваліфікації персоналу за напрямами оперативного застосування, технічного обслуговування, випробування, діагностики, ремонту й метрологічного супроводження БпС;

– інтеграції в контур вищої військової освіти – впровадження в освітні програми вищих військових навчальних закладів спеціалізованих дисциплін щодо тактики міжвидової взаємодії підрозділів БпС, а також методологій випробувань і оцінювання завадозахищеності БРЕО;

– формування адаптивного оперативно-тактичного мислення – орієнтація навчального процесу на розвиток навичок експрес-ухвалення рішень в умовах невизначеності, ефективного адміністрування складних роботизованих систем і глибокого розуміння алгоритмів функціонування роботизованих систем контролю технічного стану.

Отже, взаємозалежність між розвитком воєнної науки, науково-технічним прогресом та практичним застосуванням БпС у СОУ вимагає високої синергії доктринальних рішень, новітніх технологій (зокрема ШІ, автономних роботизованих систем контролю технічного стану, прискорених методик випробувань БРЕО та сучасного метрологічного забезпечення) і високопрофесійної підготовки кадрів. Комплексна реалізація окреслених напрямів забезпечить тривале інноваційно-технологічне домінування над противником у ході ведення бойових дій та створить підґрунтя для надійного забезпечення обороноздатності держави.

Коваленко І. О.
Заіченко А. В.
Мошаренков В. В., канд. техн. наук., доц.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ЗАСТОСУВАННЯ ГІБРИДНОЇ МОДЕЛІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ВІДЕОПОТОКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У РЕАЛЬНОМУ ЧАСІ

В умовах повномасштабної війни в Україні безпілотні літальні апарати (БпЛА) стали одним із найважливіших інструментів спостереження та отримання інформації про обстановку. Використання малогабаритних БпЛА, зокрема апаратів із оптико-електронними системами, дозволяє проводити тривалий моніторинг місцевості та отримувати значні обсяги відеоданих у

режимі реального часу. Водночас ефективність такого спостереження значною мірою залежить від здатності оператора своєчасно виявляти й правильно інтерпретувати зміни в обстановці, що відображається у відеопотоці.

Особливої актуальності ця проблема набуває в умовах бойової обстановки, коли оператор працює під впливом психоемоційного стресу, тривалого фізичного та морального виснаження, дефіциту часу й високого інформаційного навантаження. Тривале спостереження за відеопотоком призводить до зниження концентрації уваги та швидкості обробки інформації. Додатковим фактором є зорове навантаження, яке може проявлятися втомою очей, зниженням гостроти та контрастності сприйняття, що ускладнює своєчасне виявлення малопомітних об’єктів на складному фоні.

Складність завдання додатково зростає під час спостереження за місцевістю з великою кількістю природних і штучних об’єктів, які можуть бути помилково сприйняті як потенційні цілі. Рух гілок та листя під впливом вітру, зміна освітлення, туман, дощ, сніг, тіні та інші фактори створюють значну кількість візуальних змін, серед яких оператору необхідно своєчасно розпізнати дійсно важливий об’єкт.

У зв’язку з цим перспективним напрямом є застосування технологій штучного інтелекту (ШІ) для автоматизованого аналізу відеопотоку безпосередньо під час польоту БпЛА. Така система може виконувати первинну обробку зображення, автоматично виявляти зміни у сцені, класифікувати виявлені об’єкти та передавати оператору структуровану інформацію, зменшуючи обсяг рутинного візуального аналізу.

З урахуванням окреслених умов до моделі ШІ, що інтегрується в систему аналізу відеопотоку БпЛА, висувається низка базових функціональних вимог:

– детектування виявлених об’єктів – забезпечення локалізації об’єктів у площині відеокадру шляхом визначення їхніх координат у межах цифрового зображення;

– класифікація виявлених об’єктів – ідентифікація локалізованих об’єктів відповідно до заданих системних категорій (зокрема: “військовослужбовець”, “цивільна особа”, “транспортний засіб”, “БпЛА”, тощо);

– геопозиціонування виявлених об’єктів – обчислення просторових характеристик об’єкта, що передбачає визначення його координат відносно платформи спостереження БпЛА та земної поверхні шляхом комплексування даних оптичного датчика, навігаційного комплексу та телеметричних параметрів польоту.

Для реалізації функцій виявлення та класифікації об’єктів доцільно застосовувати моделі глибокого навчання – підходу машинного навчання, що використовує багатошарові нейронні мережі для автоматичного виявлення складних закономірностей у великих масивах даних, та комп'ютерного зору – галузі ШІ, спрямованої на отримання, обробку та інтерпретацію інформації з цифрових зображень і відео. Серед сучасних підходів, придатних для обробки відеопотоку в режимі, близькому до реального часу, є моделі сімейства YOLO (You Only Look Once), SSD (Single Shot Detector) та RT-DETR (Real-Time Detection Transformer). Зазначені архітектури дають змогу одночасно визначати наявність об'єкта у кадрі, його положення та належність до певного класу.

Для запропонованої системи доцільно розглянути YOLO як основну модель, оскільки її архітектура орієнтована на швидке виявлення об’єктів без необхідності послідовного виконання окремих етапів пошуку та класифікації. Під час роботи моделі кожному виявленому об’єкту також присвоюється оцінка достовірності класифікації об’єкта, яка характеризує ступінь упевненості моделі у правильності його виявлення та класифікації.

Для полегшення сприйняття результатів оператором пропонується використовувати кольорове маркування оцінки достовірності:

– зелений колір – 80÷100 %;

– жовтий – 50÷79 %;

– червоний – 0÷49 %.

Встановлені порогові значення є початковими та можуть коригуватися за результатами експериментального тестування системи.

Модель може бути донавчена на спеціалізованому наборі даних, сформованому з відеоматеріалів, отриманих з БпЛА, зокрема зважуючи на бойовий досвід підрозділів, отриманий під час виконання завдань розвідки. До такого набору доцільно включити зображення різних типів місцевості, природних об'єктів, будівель та інших елементів фону, а також об’єктів визначених класів за різних погодних умов, освітлення, висоти та ракурсу спостереження. Навчальні дані мають охоплювати як загальні класи об’єктів (людина, тварина, транспортний засіб, БпЛА), так і додаткові ознаки, які можливо визначити за достатньої якості зображення. Зокрема, для людини такими ознаками можуть бути наявність спорядження або зброї, а за відповідної деталізації зображення – її тип (“автомат”, “гранатомет”, “кулемет” тощо);

окремо доцільно передбачити приклади поранених, тварин, розпізнавальних знаків, нанесених на броньовану техніку, для автоматизованого визначення її належності до дружнього або ворожого підрозділу, та інших об’єктив за характерними візуальними ознаками. Такий принцип формування вибірки дозволить системі поступово переходити від загального виявлення об’єкта до його більш детальної класифікації залежно від якості отриманого зображення.

Порівняно з розглянутими моделями SSD та RT-DETR, перевагою YOLO для запропонованої системи є поєднання високої швидкості обробки, достатньої точності виявлення та можливості відносно простого донавчання на спеціалізованих наборах даних, що є важливим для аналізу відеопотоку в режимі, близькому до реального часу.

Для забезпечення просторового геопозиціонування запропоновано поєднати результати роботи моделі YOLO з даними навігаційної та бортової системи БпЛА. Після виявлення об’єкта модель визначає його положення у відеокадрі, після чого програмний модуль використовує інформацію про поточне положення БпЛА, висоту польоту, орієнтацію платформи, напрямок оптичної системи та її параметри. Комплексне опрацювання цих даних дає змогу оцінити напрямок на виявлений об’єкт, його відносне положення та орієнтовну відстань до нього. Для підвищення достовірності результатів можуть враховуватися дані кількох послідовних кадрів, що дозволяє зменшити вплив похибок окремого вимірювання. Отримана інформація може передаватися до програмного інтерфейсу оператора разом із результатом класифікації об'єкта.

У результаті роботи запропонованої системи оператор отримуватиме на екрані автоматично сформоване повідомлення про виявлений об’єкт, синхронізоване з відповідною ділянкою відеопотоку. На відеозображенні об’єкт виділятиметься графічною рамкою, а поруч відображатимуться його визначений клас, оцінка достовірності розпізнавання у відсотках, просторове положення та орієнтовна відстань. Для швидкого сприйняття інформації оцінка достовірності може додатково позначатися кольором: зелений – висока, жовтий – середня, червоний – низька достовірність. Таким чином, оператор отримуватиме не лише первинний відеопотік, а й автоматично сформовану структуровану інформацію про виявлені об'єкти, що дозволить швидше оцінювати отримані дані.

Запропонований підхід може використовуватися під час виконання завдань з розвідки для автоматизованого аналізу відеопотоку БпЛА, виявлення та класифікації об’єктів, оцінювання достовірності їх розпізнавання та визначення просторового положення. Його застосування дозволяє зменшити інформаційне навантаження на оператора, скоротити час первинного опрацювання відеоданих та підвищити оперативність отримання інформації про об’єкти, що спостерігаються. Перспективним є використання результатів роботи системи для формування структурованої інформації про обстановку та підтримки оператора під час аналізу значних обсягів відеоданих. Запропоновані рішення мають перспективи подальшого розвитку шляхом розширення навчальної вибірки, використання додаткових матеріалів бойового досвіду, удосконалення алгоритмів ШІ та оптимізації їх роботи в реальному часі.

Піонтківський П. М. канд. техн. наук, ст. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова

БАГАТОВИМІРНА МОДЕЛЬ ОЦІНЮВАННЯ АВТОНОМНОСТІ БЕЗПІЛОТНИХ СИСТЕМ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Широке поширення безпілотних систем (БпС) у сучасних збройних конфліктах перетворює автономність із суто технічної характеристики окремої платформи на комплексну властивість усієї системи. Досвід російсько-української війни демонструє, що реальна ефективність БпС визначається і здатністю виконувати окремі функції без безпосереднього керування людиною, і здатністю функціонувати із застосуванням засобів штучного інтелекту (БпС з ШІ) за неповних даних, нестабільного зв'язку, змінного середовища та інших форм деградації інформаційного забезпечення. Оцінювання БпС з ШІ лише за шкалою "керована – напівавтономна – автономна" недостатнє.

У зв'язку з цим розробимо модель, у якій автономність БпС з ШІ будемо розглядати як вектор: A=(P, N, D, C, L, R, S), де P – автономність сприйняття; N – автономність навігації; D – автономність прийняття рішень; C – автономність комунікації; L – автономність навчання/адаптації; R – стійкість до деградації середовища; S – рівень нагляду оператора.

P – характеризує здатність БпС з ШІ самостійно отримувати, обробляти та інтерпретувати інформацію про навколишнє середовище. Більш автономна система самостійно виявляє об'єкти, визначає їхні характеристики, зіставляє інформацію від різних джерел і формує узагальнену картину середовища. Оцінювання автономності сприйняття враховує ступінь незалежності системи від оператора під час збору та інтерпретації інформації, здатність автоматично виявляти релевантні об'єкти, класифікувати їх, інтегрувати інформацію від різних сенсорів і працювати з неповними або суперечливими даними. Важливо оцінювати не лише точність розпізнавання, а й здатність системи визначати власну невпевненість. В умовах збройного конфлікту помилкова інтерпретація інформації є наслідком не тільки недосконалості алгоритму, а й принципової відмінності реального середовища від даних, на яких система навчалася. Високий рівень автономності сприйняття передбачає і здатність "бачити", і здатність визначати межі достовірності власного сприйняття.

N – характеризує здатність системи самостійно визначати своє положення, формувати маршрут, підтримувати задану траєкторію та змінювати її відповідно до ситуації. Якщо система лише виконує заздалегідь задану послідовність команд, її навігаційна автономність залишається обмеженою. Вищий рівень автономності передбачає здатність самостійно оцінювати ситуацію, знаходити альтернативний маршрут, обходити перешкоди та адаптувати траєкторію до зміни умов. Особливістю оцінювання є необхідність врахування залежності від зовнішніх навігаційних джерел та якості інформації про положення системи. Оцінювання повинно проводитися не лише в нормальних умовах, а й за сценаріїв, коли частина навігаційної інформації стає недоступною або суперечливою. Важливо визначати не тільки здатність системи рухатися автономно, а й те, наскільки вона здатна зберігати навігаційну функціональність при погіршенні інформаційного забезпечення.

D – є одним із центральних компонентів запропонованої моделі, оскільки саме вона визначає, наскільки система здатна переходити від автоматичного виконання команд до самостійного вибору способу дії. Вищий рівень означає здатність обирати один із декількох варіантів дій відповідно до ситуації. Найвищі рівні передбачають можливість самостійного формування альтернатив, оцінювання їхніх наслідків, вибору найбільш доцільного варіанта та коригування поведінки у разі зміни ситуації. При цьому автономність

прийняття рішень не повинна ототожнюватися з повною незалежністю від людини. Навпаки, важливою характеристикою зрілої автономної системи є здатність визначати ситуації, у яких її власної інформації або впевненості недостатньо для продовження автономної діяльності. Оцінювання цього компонента враховує не лише кількість рішень, які система може приймати без оператора, а й їх складність, здатність адаптувати їх до ситуації, обґрунтовувати власну поведінку та своєчасно передавати контроль людині.

C – характеризує здатність системи самостійно підтримувати необхідний інформаційний обмін із оператором, іншими безпілотними платформами та зовнішніми системами. Для автономних систем розглядатимемо її як окремий вимір автономності, оскільки залежність від постійного зовнішнього зв'язку безпосередньо впливає на здатність системи виконувати поставлені завдання. Оцінювання цього компонента повинно враховувати здатність системи самостійно встановлювати та підтримувати комунікацію, адаптуватися до зміни доступності каналів, відновлювати зв'язок після його втрати та продовжувати виконання критично важливих функцій за відсутності зовнішнього управління. Особливе значення має визначення того, які саме функції система зберігає при частковій або повній втраті зв'язку. Тому автономність комунікації доцільно оцінювати не лише через технічні характеристики каналу, а насамперед через ступінь функціональної незалежності системи від нього.

L – характеризує здатність БпС з ШІ змінювати свою поведінку відповідно до отриманого досвіду, нових даних або зміни умов середовища. Цей компонент є принципово відмінним від попередніх, оскільки характеризує не лише поточну здатність системи діяти автономно, а її здатність змінювати власну поведінку у відповідь на нові обставини. Система може автоматично змінювати окремі параметри відповідно до встановлених правил, не навчаючись у повному сенсі цього поняття. Вищий рівень передбачає здатність узагальнювати попередній досвід і використовувати його для формування нової поведінки. Водночас автономне навчання створює окрему проблему безпеки та надійності: здатність системи змінювати власну поведінку не означає, що ці зміни завжди будуть правильними або безпечними. Тому оцінювання повинно враховувати контрольованість адаптації, стабільність отриманих результатів та можливість повернення системи до перевіреного стану.

R – є особливим компонентом запропонованої моделі, оскільки дозволяє

відокремити формальну автономність від її практичної ефективності. Автономна система може бути здатною самостійно приймати рішення за нормальних умов, але втрачати цю здатність при погіршенні якості сенсорної інформації, навігаційних даних, комунікації або зміні характеристик середовища. Тому сама наявність автономних функцій ще не свідчить про високу автономність системи в реальних умовах. Оцінювання стійкості повинно визначати, наскільки система здатна зберігати свої ключові функції при поступовому погіршенні умов. Важливо встановлювати не лише факт втрати працездатності, а й характер цієї втрати: які функції деградують першими, які зберігаються найдовше, чи здатна система переходити до спрощених режимів функціонування та чи може вона самостійно розпізнати, що умови вже не дозволяють їй продовжувати автономну діяльність. Таким чином, стійкість до деградації характеризує своєрідну "глибину" автономності – тобто здатність системи залишатися функціонально автономною за межами нормального сценарію.

S – характеризує взаємозв'язок між автономною системою та людиною, яка контролює її діяльність. У цьому випадку важливо не розглядати людський контроль як протилежність автономності. Сучасна автономна система може бути високофункціональною саме завдяки раціональному розподілу функцій між оператором та БпС з ШІ. Людина може визначати загальну мету, встановлювати обмеження та здійснювати контроль, тоді як система самостійно виконуватиме значну частину поточних функцій. Оцінювання цього компонента повинно враховувати частоту втручання оператора, характер такого втручання, обсяг повноважень людини, можливість скасувати рішення системи, час, необхідний для перехоплення контролю, а також прозорість поведінки автономної системи для оператора. Особливого значення набуває здатність системи своєчасно повідомляти людину про виникнення ситуації, яку вона не може надійно оцінити самостійно. У цьому сенсі високий рівень автономності не повинен означати усунення людини, а має передбачати оптимальний розподіл функцій між людиною та БпС з ШІ.

Запропонована модель дозволяє розглядати автономність БпС з ШІ не як єдину лінійну шкалу, а як сукупність взаємопов'язаних характеристик. Її ключова особливість полягає у можливості сформувати індивідуальний "профіль автономності" конкретної системи. Наприклад, одна система може мати високий рівень автономності навігації та сприйняття, але залишатися

залежною від оператора у прийнятті рішень. Інша може мати високий рівень автономного прийняття рішень, але бути істотно залежною від комунікаційної інфраструктури. Третя – демонструвати високі показники за всіма основними функціональними параметрами, але суттєво втрачати працездатність при зміні середовища. За традиційної класифікації всі три системи можуть бути віднесені до однієї категорії "автономних", тоді як запропонований підхід дозволяє виявити принципові відмінності між ними.

Запропонована модель не зводить всі компоненти до одного інтегрального показника. Для дослідницьких цілей більш інформативним є саме профіль автономності, оскільки він дозволяє виявляти сильні та слабкі сторони системи за окремими функціональними напрямами. Інтегральна оцінка може приховати принципові відмінності: одна система може компенсувати низьку автономність прийняття рішень високою автономністю навігації, а інша – навпаки. Однак ці системи матимуть принципово різні моделі функціонування та різну залежність від оператора і зовнішньої інфраструктури.

У такому розумінні запропонована модель має не лише класифікаційне, а й методологічне значення. Вона створює основу для переходу від питання "наскільки автономною є БпС з ШІ?" до більш змістовного питання: "у яких саме функціях система здатна діяти автономно, за яких умов зберігає цю здатність та якою є роль людини у відповідному контурі управління?". Саме така постановка питання є особливо актуальною для дослідження БпС з ШІ в умовах збройного конфлікту, де автономність повинна оцінюватися не в лабораторному середовищі, а з урахуванням невизначеності, динамічності, деградації інформаційного забезпечення та необхідності постійної адаптації.

Для моделі дуже важливою є вимога: людина визначає рамки застосування, а система автономно функціонує всередині цих рамок. В умовах деградованого або відсутнього зв’язку автономність БпС з ШІ має компенсувати втрату оперативного людського контролю, але не повинна автоматично означати необмежену автономність прийняття рішень.

У підсумку багатовимірний підхід дає змогу розглядати автономність як комплексну системну властивість, що формується взаємодією сприйняття, навігації, прийняття рішень, комунікації, навчання, стійкості та людського контролю. Його перспективність полягає у можливості визначити для кожного з цих компонентів конкретні критерії та показники (за необхідності з ваговими

коефіцієнтами), а в подальшому – сформувати стандартизовану методику оцінювання і порівняння різних БпС з ШІ. Така методика може стати основою для емпіричного дослідження еволюції автономності БпС з ШІ та визначення того, які саме її компоненти є критичними для функціонування систем у складних умовах сучасного збройного конфлікту.

Дзіковський А. П.
Житомирський військовий інститут імені С. П. Корольова

АВТОНОМНІ ФУНКЦІЇ російських БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Автономність безпілотного літального апарата (БпЛА) — це його здатність виконувати завдання без постійного керування оператором. Вона зменшує залежність БпЛА від каналів керування і передачі даних, що особливо важливо в умовах радіоелектронної протидії. Автономні функції можуть працювати на основі алгоритмів оцінки стану, навігації, планування та керування, а також методів машинного навчання. Варто зазначити, що нейронні мережі є всього лиш одним із доступних інструментів і не повинні бути самоціллю.

Автономність БпЛА доцільно розглядати не як одну окрему функцію, а як сукупність функцій, які можуть бути автоматизовані незалежно одна від одної. На практиці конкретна система може автоматизувати лише одну або декілька з цих функцій, тоді як решту виконує оператор. При цьому, використання нейронних мереж не означає, що вони здійснюють керування апаратом. У багатьох випадках роль нейронної мережі обмежується лише обробкою відеопотоку. Отримані дані передаються традиційним алгоритмам навігації, планування та керування, які формують траєкторію польоту і команди виконавчим механізмам.

Одним із найбільш поширених напрямів є автоматизація аналізу відеозображення для виявлення, класифікації та супроводу об’єктів. Такі можливості реалізовані, зокрема, на ZALA Z-16 і T-16 із системою ИРРА, Альбатрос М5 та Supercam-Нейро і дозволяють частково перенести на борт функції, які традиційно виконував оператор.

Іншим напрямом є автоматизація наведення. У російських FPV-дронах, наприклад Овод та Мікроб-10, застосовуються так звані плати донаведення, які після

вибору цілі оператором забезпечують її супровід та автономне ураження. Ланцет має ширший набір автономних функцій. Окрім автономного ураження він здатний самостійно детектувати і класифікувати об’єкти, а також здійснювати автономний політ вздовж доріг та інших помітних орієнтирів на місцевості.

Для автоматизації наведення зображення з бортової камери обробляється методами машинного зору для отримання інформації про навколишнє середовище — положення цілі або орієнтира відносно БпЛА. Водночас машинний зір може бути використаний зовсім по іншому — для отримання інформації про сам БпЛА. Такий підхід реалізований у СКАТ-350М із модулем візуальної навігації БОНС, який зіставляє зображення з бортової камери з картографічними даними та формує оцінку місцезнаходження БпЛА навіть в умовах подавлення сигналів глобальної навігаційної супутникової системи.

Іщенко Д. А., канд. техн. наук, доц.
Стрінада В. В., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ ОСОБЛИВОСТЕЙ РОБІТ ІЗ ВІЙСЬКОВОЇ СТАНДАРТИЗАЦІЇ В АСПЕКТІ НАУКОВОЇ ПІДТРИМКИ НАБУТТЯ СПРОМОЖНОСТЕЙ У СФЕРІ ВІЙСЬКОВОЇ ТЕХНІКИ З ВИСОКОЮ ДИНАМІКОЮ РОЗВИТКУ

Досвід відбиття широкомасштабної рф дозволяє зробити висновок, що фактор існуючої ресурсної переваги противника, обумовлює потребу технологічної переваги для ефективного застосування військ (сил) Збройних Сил (ЗС) України. Значну місію для досягнення технологічної переваги над противником виконують військові частини (підрозділи), на озброєнні яких знаходяться засоби безпілотних систем (БпС) і радіоелектронної боротьби (РЕБ), які зменшують вплив різниць людського і матеріального ресурсів як безпосередньо на лінії бойового зіткнення, так і в оперативній та стратегічній глибині. Таки засоби, за відмінністю, щодо асиметричної (протиборчої) призначеності, в аспекті загальної проблеми набуття спроможностей військ (сил) за рахунок удосконалення їх озброєння, доктринальної бази застосування, кадрового забезпечення та підготовки доцільно розглядати як засоби військової техніки (ВТ) із “високою динамікою розвитку” (ВДР).

Особливість розвитку носіїв відповідних спроможностей обумовлена специфікою ВТ ВДР – стисліть часових меж стадій (фаз) життєвого циклу (ЖЦ) зразків (комплексів, систем) (швидке моральне старіння, втрата актуальності технологій), яка викликає необхідність перманентної модернізації засобів і доопрацювання їх складових без зняття з експлуатації, що призводить до різних їх модифікацій у військах (силах). Врахування такої необхідності формує потреби: прискорена процедура допуску до експлуатації; інноваційні підходи до уніфікації та сумісності; вдосконалення організаційного забезпечення. Наявність потреб за відсутністю нормативно прийнятих, дієвих інструментів їх вирішення в умовах воєнного стану обумовлює формування загальної проблеми ефективності застосування засобів ВТ ВДР, яка характеризується складовими, що визначають часткові проблеми:

технічні (нерівномірність оснащення підрозділів уніфікованими платформами та цільовим обладнанням, що ускладнюють логістичні обмеження ремонту і модернізації, вразливість своїх каналів управління та зниження ефективності подавлення противника, який оперативно змінює протоколи, частоти, алгоритми та тактику);

організаційні (централізоване управління при одночасному забезпеченні тактичної самостійності і координації дій за єдиної обізнаністю щодо поточної оперативної обстановки за обмеженнями часу на підготовку до застосування носіїв спроможностей ВТ ВДР різної відомчої підпорядкованості);

кадрові (дефіцит персоналу при високому психологічному навантаженні та обмежених можливостях навчання).

Одним з шляхів забезпечення ВДР, стандартизації виробів таких видів ВТ та уніфікації їх складових є нарощування нормативної бази формування технічних вимог до них у роботах з військової стандартизації: адміністративної; оперативної; матеріальної; комплексної системи загальних технічних вимог до озброєння та військової техніки (КСЗТВ ОВТ).

Житомирський військовий інститут імені С. П, Корольова (ЖВІ), згідно Переліку організацій з військової стандартизації (ОВС), затвердженого заступником Міністра оборони (МО) України (№ 225/уд від 27.11.2023), визначено такою ОВС, що здійснює діяльність:

на виконання Положення про організацію наукової і науково-технічної діяльності в системі МО України, затвердженого наказом МО України від

16.07.2024 № 480 (зі змінами), зареєстрованого в Міністерстві юстиції України 30.07.2024 за № 1164/42509;

відповідно Положення про військову стандартизацію, затвердженого наказом МО України від 24.02.2020 № 56, зареєстрованого в Міністерстві юстиції України 05.03.2020 за № 240/34523;

за напрямами Розподілу основних напрямів наукових досліджень між науковими установами (НУ) та вищими навчальними закладами МО України та ЗС України, затвердженого наказом МО України від 26.01.2017 № 53 (зі змінами, внесеними наказом МО України від 15.02.2019 № 65).

Проблематика нарощування спроможностей у сфері ВТ ВДР (РЕБ та засобів безпілотних наземних комплексів (систем) БпНК(С)) ускладняється відсутністю системи загальних технічних вимог (СЗТВ) до ВТ ВДР. Формування такої СЗТВ неможливе без нормативно визначеної термінологічної та класифікаційної. Вказана проблематика є актуальною за такими чинниками.

По-перше, у національної галузі виробництва (та оборонних закупівель) склалася проблемна ситуація, коли органи військового управління, заклади військової освіти, НУ та виробники ВТ ВДР мають різні бачення щодо класифікації засобів, що призводить до плутанини у поняттях. За відсутності визначених СЗТВ до конкретних видів ВТ ВДР фахівці можуть по-різному інтерпретувати технічні характеристики засобів, що ускладнює забезпечення їх призначеності, технологічності, уніфікації та сумісності.

По-друге, у відомчої галузі військової освіти. Ефективність застосування засобів ВТ ВДР залежить не лише від їхніх технічних характеристик, але й від рівня підготовки персоналу. Відсутність уніфікованої термінологічної та класифікаційної бази, СЗТВ ВТ ВДР створює труднощі у навчанні та методичному забезпеченні освітнього процесу.

По-третє, у галузі реалізації Стратегії розвитку ЖВІ. Перспектива створення нового науково-дослідного управління Сертифікації та випробувань (виробів ВТ ВДР), передбачає розвиток спроможностей для розроблення відповідних нормативних документів (НД).

Науково-методичний аспект удосконалення діяльності ЖВІ у сфері стандартизації ВТ ВДР, полягає у розроблення НД, глосаріїв та класифікацій, потрібних для набуття та розвитку спроможностей у відповідних галузях ВТ ВДР. Військовий стандарт (ВСТ) сам по собі не є науковим продуктом, але він

є результатом наукової та науково-технічної діяльності. Згідно із законодавством України, ВСТ — це правовий та нормативно-технічний акт, призначений для встановлення правил, вимог (характеристик), у тому числі шляхом запровадження стандартів НАТО, для багаторазового використання у сфері оборони держави. Наприклад, положення документів НАТО адаптовано та введено ВСТ: ВСТ 700.004:2024(01) Підготовка мінімальні вимоги до зовнішніх пілотів (операторів) безпілотних авіаційних систем (STANAG 4670 Ed. 5 / ATP-3.3.8.1 Ed. B “MINIMUM TRAINING REQUIREMENTS FOR UNMANNED AIRCRAFT SYSTEMS (UAS) OPERATORS AND PILOTS”, MOD); ВСТ 003.001:2024(01) “Лінгвістичне забезпечення. Рівні мовленнєвої компетенції (STANAG 6001 Ed. 5/ ATrainP-5 Ed. A "Language Proficiency Levels", IDT)”.

Національні ВСТ — це інструмент регулювання, а його зв'язок з науковим продуктом виражається у процесі створення ВСТ, на приклад у науково-дослідних роботах (НДР). Перед тим як прийняти ВСТ НУ проводять дослідження та тестування. Звіти про НДР, математичні моделі та методики випробувань є науковими продуктами. Зараз виконуються дві НДР: “КСЗТВ ОВТ. Техніка РЕБ. Терміни та визначення понять, класифікація” (“ТИС”); “Удосконалення СЗТВ ОВТ за напрямом “Безекіпажні наземні комплекси”” (“КРАБ”). Результати НДР будуть використані у проєктах ВСТ КСЗТВ ОВТ, розроблення яких за пропозиціями ЖВІ та замовників, включено Головним управлінням забезпечення супроводження ЖЦ ОВТ в проєкт Програми робіт з військової стандартизації.

Воєнно-науковий та військово-технічний аспекти полягають у впровадженні ОВС, у тому числі ЖВІ, результатів наукових досліджень, що забезпечує адаптацію ВСТ до сучасних досягнень науки і техніки. Тобто нові наукові продукти інтегруються у ВСТ. На приклад, результати досліджень подані у статті “Підхід до вдосконалення термінологічної системи з РЕБ” (Іщенко Д. А., Федорчук Д. Л., Марищук Л. М.), що корелюються з сучасним станом та перспективами розвитку електромагнітної боротьби, адаптовано у ВСТ 602.001:2024(01) “Електромагнітна та кіберборотьба. РЕБ. Терміни та визначення”. Результати досліджень подані у статті “Засади формування термінологічної та класифікаційної бази СЗТВ до військової техніки (Іщенко Д. А., Стрінада В. В., Марищук Л. М.), планується до адаптації у запланованих ВСТ КСЗТВ ОВТ (РЕБ та БнК(С).

Розробленням ВСТ займаються безпосередньо науково-дослідні управління, у тому числі ЖВІ, для них створення проєкту ВСТ є виконанням технічного (науково-технічного) завдання. Результати такої діяльності ЖВІ:

самостійно розробили: ВСТ 01.104.002 (Видання 1) “Боротьба радіоелектронна. Радіоелектронний захист (РЕЗт). Захист радіоелектронних засобів (РЕЗ) від ураження електромагнітною зброєю противника. Захист РЕЗ та радіоелектронних пристроїв військових об’єктів від впливу зброї електромагнітного імпульсу (ЕМІ). Основні організаційні та технічні вимоги”; ВСТ 01.104.002 (Видання 2) “Боротьба радіоелектронна. РЕЗт РЕЗ та електронних пристроїв військових об’єктів від впливу зброї ЕМІ. Основні організаційні та технічні вимоги”; ВСТ 602.001:2024(01) “Електромагнітна та кіберборотьба. РЕБ. Терміни та визначення”; ВСТ 01.048.001 (Видання 1) “Космічна діяльність у сфері оборони Терміни та визначення” (завершують розроблення ВСТ…“Космічна діяльність. Космічна діяльність у сфері оборони. Основні положення”);

у складі робочих груп прийняли участь у розроблені 7 (сім) ВСТ 600.005-(01-07):(2023-2025) “Комунікаційні та інформаційні системи Словник НАТО щодо інформаційних технологій. Частина 1” (STANAG 5625 Ed. 1 / ADatP – 02 Ed. (2005) NATO Information Technology Glossary, MOD);

опрацювали не менш 40 і надалі відгуки аркуші погодження проєктів ВСТ, розроблених іншим ОВС (Державний науково-дослідний інститут випробувань і сертифікації ОВТ; Національний університет оборони України; Науково-дослідний інститут воєнної розвідки тощо).

Освітньо-методичний аспект удосконалення діяльності ЖВІ у сфері стандартизації ВТ ВДР, полягає у впровадженні в освітній процес НД, глосаріїв та класифікацій, потрібних для підготовки фахівців. Це забезпечує єдність термінології, формує системне бачення ВТ ВДР та створює основу для інтеграції українських освітніх програм із міжнародними стандартами та НАТО. Застосування, на приклад термінологічної та класифікаційної бази СЗТВ у сфері ВТ ВДР охоплює основні напрями підготовки та методичного забезпечення освітнього процесу: теоретичну підготовку (вивчення принципів: телеуправління, створення перешкод, захисту власних систем, аналізу сигналів противника тощо); практичну апробацію (підготовку) (тренування на тренажерах і симуляторах та реальних засобах (зразках, комплексах, системах)

моделювання застосування засобів ВТ ВДР у сценаріях бойових дій); методичне забезпечення (створення навчальних посібників, інструкцій, силабусів (нормативних та навчально-методичних матеріалів необхідних для ефективного виконання робочої програми навчальної дисципліни та програм підготовки); міжнародний контекст (гармонізація освітніх програм із стандартами НАТО та ІЕС).

Таким чином, освітньо-методичний аспект у сфері техніки ВТ ВДР охоплює напрями підготовки, групи методичних матеріалів та компоненти практичної апробації, що разом формують цілісну систему, навчання і стандартизації виступає не лише як інструмент навчання, але й як механізм апробації нових термінів та класифікацій.

Отже, удосконалення наукової діяльності за напрямом військової стандартизації щодо створення НД як інструментів освітньої, наукової і науково-технічної діяльності у сфері ВТ ВДР є актуальним завданням, вирішення якого сприятиме розвитку та набуттю нових спроможностей як у галузях видів ВТ ВДР, так і реалізації Стратегії розвитку ЖВІ.

Аналіз особливостей робіт з військової стандартизації щодо наукової підтримки набуття спроможностей у сфері ВТ ВДР дозволив визначити воєнно-науковий, військово-технічний, науково-методичний та освітньо-методичний аспекти реалізації та впровадження результатів наукової та науково-технічної діяльності.

Мірошніченко С. І.
Пількевич І. А., д-р. техн. наук, проф.
Житомирський військовий інститут імені С. П. Корольова

ЗАБЕЗПЕЧЕННЯ ЗАПУСКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ З ВОДНОЇ ПОВЕРХНІ

Сучасний розвиток безпілотних систем передбачає можливість використання безпілотних літальних апаратів (БпЛА) не тільки з наземного базування, але й з підводних носіїв. Даний тип носія забезпечує доставку БпЛА в підводному положенні до точки здійснення його запуску, вихід на водну поверхню за визначеним сигналом або часом та запуск БпЛА для ураження заданої цілі. Запуск БПЛА з поверхні води розширює можливості застосування безпілотних систем для ураження цілі противника. Справа у тому, що час на

прийняття рішення противником значно скорочується, а саме це веде для підвищення ефективності ураження цілі.

Але на відміну від запуску з нерухомої наземної поверхні, запуск з водної поверхні накладає багато додаткових факторів на запуск БпЛА. Носій, який знаходиться на поверхні води постійно змінює своє положення. Наприклад, під впливом хвиль носій здійснює горизонтальні, вертикальні та кутові переміщення. Додатково на носій впливають зовнішні фактори (вітер, течія, температура), стан самого носія та похибки датчиків вимірювання.

Тому запуск БпЛА з носія, який знаходиться на воді, доцільно розглядати як динамічний процес, у якому взаємодіють сам носій, зовнішнє середовище, похибки вимірювання та сам БпЛА (його розміри, вага тощо).

Загальну послідовність процесу запуску БпЛА можна представити наступним чином: з носія, який перебуває на воді під діями зовнішніх факторів, датчики вимірювання знімають параметри поточного стану та намагаються стабілізувати положення носія на водній поверхні. В цей час йде підготовка БпЛА до запуску: визначається момент запуску, оцінюється можливість здійснення запуску БпЛА та якщо досягнута відповідність всіх параметрів заданим здійснюється запуск БпЛА. Перед запуском БпЛА з носія необхідно визначити його поточний стан, основними параметрами якого є: крен φ; тангаж θ; рискання ψ; вертикальна та кутові швидкості тощо.

Особливо важливими параметрами є крен і тангаж. Наприклад, якщо носій має значний кут нахилу в момент запуску під впливом зовнішніх факторів, БпЛА може отримати початкові значення параметрів з датчиків, і вони будуть значно відрізнятися від розрахункових. Тому можуть виникати проблеми під час здійснення запуску.

Таким чином, необхідно не тільки визначити параметри носія в цей час, але й оцінити їх зміну (спрогнозувати) протягом найближчого проміжку часу.

Головними факторами процесу, що буде досліджуватися, є невизначеність параметрів зовнішнього середовища. Під час запуску БпЛА умови водної поверхні постійно змінюються через хвилі (їх висота), вітер (швидкість та напрям), течію (швидкість та напрям) тощо. Тому носій змінює своє положення та нахил. Крім того носій постійно змінює свій крен (нахил вправо-вліво), тангаж (нахил вгору-вниз) та рискання (поворот носія навколо вертикальної осі). Тому, потрібно дослідити багато різних умов для запуску БпЛА з носія. Для цих цілей потрібно використовувати метод Монте-Карло,

коли проводиться багато експериментів, в яких значення різних параметрів випадковим чином змінюються у допустимих межах і є можливість дослідити, як зміна зовнішніх параметрів впливає на запуск БпЛА.

Для досліджень поведінки носія під час запуску БпЛА доцільно використовувати, замість реальних об'єктів, математичні моделі. Це дозволить відійти від використання реального об'єкта та проводити велику кількість експериментів та зробити висновки, як змінюється стан системи з часом під впливом зовнішніх факторів.

Математично роботу системи можна записати у вигляді:

$$\frac{dX}{dt} = F(X, E, \theta, U),$$

де X – поточний стан системи. Наприклад, це можуть бути положення носія, швидкість та кути нахилу тощо;

E – зовнішні впливи. До них можуть належати хвилі, вітер, течія та інші фактори зовнішнього середовища;

Θ – параметри самого носія. Наприклад, маса, розміри, швидкість та інші фізичні параметри;

U – керуючий вплив. Система стабілізації виробляє сигнали, які повинні стабілізувати систему;

$\frac{dX}{dt}$ – каже про те, як швидко відбуваються зміни стану системи.

Наприклад, якщо носій зараз знаходиться в одному стані, а через деякий час його положення змінюється, то математична модель повинна визначити, під впливом яких факторів це відбулося. Тоді керуючий вплив формує потрібні команди та стабілізує положення носія.

Для визначення положення носія використовуються різні датчики. Але дані датчиків самі по собі також є показниками з похибками. На них впливають, як похибки самих датчиків, так і інші фактори, які діють на носій. Для зменшення впливу таких похибок на роботу системи можна використовувати фільтр Калмана. Він постійно порівнює інформацію, яку система очікує отримувати з реальними показниками датчиків, тобто робота повинна поділятися на два кроки: спочатку є прогноз системи, яким буде стан носія через короткий проміжок часу (наприклад, на даний час крен 3°, але носій продовжує нахилятися, тому у наступний момент крен буде 3,5^o). Потім система порівнює цей прогноз з показниками, які отримані від датчиків (наприклад, крен, що прогнозувався 3,5^o, а датчики показали 3,8^o). Якщо датчик має велику похибку,

фільтр Калмана більше довіряє прогнозу, інакше показникам датчика. Наприклад, модель прогнозує крен 4,5º, а датчик показує 5,0º. Фільтр Калмана враховує обидва значення та, залежно від їхньої точності, формує уточнену оцінку. Якщо фільтр Калмана більше довіряє прогнозу (вірогідність 60%), то розрахунок такий:

$$X \approx 0{,}6 \cdot 4{,}5 + 0{,}4 \cdot 5{,}0 = 2{,}7 + 2{,}0 = 4{,}7°.$$

У наведеному прикладі отримано значення приблизно 4,7º. Це значення далі буде використовується системою для оцінювання стану носія та визначення умов запуску БПЛА.

Таким чином, система отримує не просто значення, що надійшли з датчиків, а оцінку стану, яка враховує як прогноз руху моделі носія, так і фактичні дані датчиків.

Для задачі запуску це дозволяє отримувати більш стабільні оцінки крену, тангажу, рискання та кутових швидкостей.

Для компенсації коливань, що виникли, система повинна сформувати керуючий вплив, який зменшить ці коливання. У носії для його стабілізації може використовуватися PID-регулятор. Він може складатися з трьох основних складових, які відповідають на запити:

– пропорційна складова – наскільки велика похибка на даний час?

– інтегральна складова – як довго вона існує?

– диференціальна складова – наскільки швидко вона змінюється?

Для кожної складової необхідно визначити свою похибку та сформувати окремі керуючи сигнали. У реальній системи ці сигнали поступають на виконавчі механізми, наприклад рулі, які змінюють положення носія та отримати його стабілізацію.

Наприклад, бажаний крен повинен бути 0º. Фільтр Калмана після обробки даних датчиків визначив, що він дорівнює 4,7º і це є похибка, яка передається у PID-генератор та формує керуючий сигнал для повороту рулів та зменшення кута нахилу. Система знову знімає показники датчиків і так далі, поки відхилення нахилу носія не вийде у визначений діапазон значень.

Але повністю усунути стабілізацію носія на воді неможливо тому, що зовнішні впливи постійно діють на носій, а для компенсування нахилів потрібен певний час. Тому система не тільки намагається стабілізувати носій, але і визначити час, який найбільш підходить для запуску БпЛА.

Запуск БпЛА з носія на воді не можна виконувати просто через який певний час після підготовки БпЛА до запуску. У цей час носій може мати значний крен або тангаж. Тому перед запуском потрібно перевірити поточний стан носія.

Для цього задаються межі параметрів та здійснюється прогноз. Дійсно, недостатньо знати, що крен на даний час є 4,7°. Необхідно також знати, що у найближчий час він не буде значно збільшений.

Загальна послідовність роботи може бути наступна:

зовнішні впливи → рух носія → датчики → фільтр Калмана → оцінка стану носія → PID-стабілізація →прогноз зміни стану → та перевірка умов запуску (якщо умови дозволяють, то відбувається запуск БпЛА, а якщо ні, то подальша стабілізація та прогноз). Тобто разом фільтр Калмана та PID-регулятор дозволяють підготувати носій до запуску БпЛА. PID-регулятор відповідає за стабілізацію носія, а фільтр Калмана – за отримання більш достовірної інформації про його стан.

Система не чекає поки небезпечний стан виникне. Рішення, крім поточного стану, приймається на основі прогнозу на короткостроковий час. Якщо носій знаходиться у допустимому положенні, а прогноз показує швидке збільшення тангажу, то запуск може бути відкладений.

Отже моментом запуску БпЛА є момент часу, коли крен, тангаж, їхні швидкості зміни та параметри зовнішнього середовища знаходяться в допустимих межах, а прогноз не показує їх швидкого погіршення.

Використання реальних об’єктів для аналізу роботи системи дороге та трудомістке рішення. Для практичного дослідження можливе використання емулятора процесу запуску БпЛА, який повинен задавати параметри зовнішніх збурень, самого носія, похибки датчиків та параметри БпЛА. Результатами можуть бути значення та графіки крену, тангажу та рискання.

Для дослідження впливу невизначеності на носій проводиться велика кількість досліджень. При кожному дослідження випадковим чином формуються параметри зовнішнього середовища та початкові умови роботи системи, а також визначаються показники якості. Це дозволяє оцінити поведінку системи при багатьох невизначених ситуаціях.

За підсумками проведеного аналізу пропонується наступна послідовність забезпечення запуску БПЛА:

1. Вимірювання параметрів зовнішнього середовища за допомогою датчиків.
2. Фільтрація вимірювань за допомогою фільтра Калмана.
3. Визначення поточного стану носія.
4. Прогнозування зміни орієнтації носія.
5. Формування керуючих сигналів стабілізації носія.
6. Визначення меж допустимих умов запуску.
7. Вибір оптимального моменту запуску.
8. Оцінювання результату запуску. За необхідності – перенесення запуску на наступний час.

Наукова новизна запропонованого підходу полягає у комплексному врахуванні динамічного стану носія та невизначеності зовнішнього середовища при визначенні умов запуску БпЛА.

В роботі зроблено висновки, що запуск БпЛА з носія на воді є складним динамічним процесом, оскільки початкові умови польоту формуються з носія, який постійно змінює своє положення під дією хвиль, вітру та інших зовнішніх факторів.

Для підвищення достовірності визначення стану носія доцільно використовувати фільтр Калмана, який дозволяє поєднати дані датчиків з математичною моделлю руху носія. Для стабілізації носія може використовуватися PID-регулятор, а для вибору моменту запуску – прогнозування зміни її просторового стану.

Використання методу Монте-Карло дає можливість дослідити вплив невизначених параметрів на результат запуску та отримати статистичну оцінку його характеристик.

Дзюбчук Р. В., канд. техн. наук, ст. наук. співроб.
Перфілов А. Ю.
Житомирський військовий інститут імені С. П. Корольова

СИСТЕМА ВІДБОРУ Й ПІДГОТОВКИ ОПЕРАТОРІВ БЕЗПІЛОТНИХ СИСТЕМ: ПСИХОЛОГІЧНИЙ АСПЕКТ

Система підготовки операторів безпілотних систем для Збройних Сил України є відносно «молодою». Лише у 2017 році в Житомирському військовому інституті було створено першу в Україні кафедру, яка готувала офіцерські кадри для безпілотних авіаційних комплексів тактичного класу.

Приблизно в той самий час розпочалася підготовка рядового та сержантського складу для експлуатації та обслуговування безпілотних літальних апаратів на базі 190 навчального центру. Проте, як показав досвід відбиття повномасштабної агресії російської федерації проти України, кількість підготовлених кадрів виявилася явно недостатньою. Крім того, з 2022 року суттєво збільшилася кількість типів безпілотних авіаційних комплексів, широко почали використовуватися безпілотні наземні комплекси. Окремо зазначимо, що першу школу підготовки операторів безпілотних наземних роботизованих комплексів було створено на базі одного з навчальних центрів Збройних Сил України лише у 2024 році. Тому розвиток системи підготовки фахівців для безпілотних систем є надзвичайно важливим і актуальним завданням.

Як показує досвід підготовки фахівців для безпілотних систем (як літальних, так і наземних), важливою складовою є система відбору та підготовки операторів, зокрема її складова, яка враховує психологічні аспекти цієї підготовки.

Найповніше психологічні особливості діяльності операторів безпілотних авіаційних комплексів тактичних класів описано в дослідженнях В. І. Пасічника, В. С. Афанасенка, Ю. М. Широбокова. На перші місця експерти поставили такі якості, як стійка й розподілена увага, розвинені пам'ять і просторова уява. Далі йдуть здатність до навчання, прагнення до професійного успіху, емоційна стійкість, точність рухів, саморегуляція, працездатність і вміння спілкуватися в напружених ситуаціях. Ці якості потрібні операторам будь-яких систем. Відмінності, на нашу думку, полягають в акцентах. Для безпілотних авіаційних систем особливо важливі швидка просторова реакція та точність рухів, тоді як для безпілотних наземних систем на перший план виходять відповідальність, уважність до деталей, командна робота, технічне мислення та стресостійкість.

Як правило, відбір операторів безпілотних систем складається з чотирьох етапів: соціально-правового (відповідність кандидата певним соціально-демографічним, правовим і морально-етичним нормам), медичного (зокрема психофізіологічного), освітнього та психологічного. Негативне рішення на будь-якому етапі припиняє процедуру подальшого відбору. До протипоказань належать висока тривожність, нездатність долати страх, низький адаптаційний потенціал, нездатність до взаємодії, імпульсивність і конфліктність.

У цій доповіді розглянемо детальніше лише етап психологічної оцінки провідних якостей. Основними вважаються: стійка й розподілена увага, пам'ять і просторова уява, здатність до навчання й гнучкість мислення, спрямованість на професійний успіх і сумлінність, емоційна стійкість і самовладання, адаптивність і саморегуляція, уміння чітко висловлюватися й спілкуватися в напружених ситуаціях, а також точність рухів і висока працездатність. Останні дві перевіряють переважно шляхом виконання практичних завдань (як правило, на симуляторах), а решту сім – тестами та діагностичною бесідою за визначеними методиками (наприклад, прогресивні матриці Равена для оцінювання уваги й мислення). Доцільним вважаємо введення пробного періоду, під час якого оператор працюватиме на тренажері з наростаючим навантаженням, а інструктор оцінюватиме кандидата за єдиним листом спостереження. Завершальним кроком етапу психологічної оцінки має бути підсумковий висновок за трьома рівнями: придатний, умовно придатний (з рекомендаціями щодо розвитку) і непридатний. Подібні градації придатності вже застосовують у медичному відборі.

Рішення про придатність ухвалюють колегіально. Дослідники радять залучати до психофізіологічного відбору лікарів-психофізіологів, психологів і фахівців з фізичної підготовки. До цього складу пропонується додати командира або інструктора, який спостерігав кандидата на тренажері. Кожен учасник заповнює власний бланк оцінки за визначеними психологічними якостями, а підсумок обговорюють спільно. Окремо слід посилити особисту відповідальність посадових осіб, які готують характеристики й довідки на кандидатів, адже за порівняно короткий період психологічного обстеження не завжди вдається виявити військовослужбовців, які в подальшому будуть непридатними до виконання обов'язків операторів безпілотних комплексів.

Щоб процедура психологічного відбору була надійною, пропонується шість правил. Перше: кожну провідну якість оцінюють щонайменше двома різними способами, наприклад тестом і бесідою чи спостереженням. Друге: наявність протипоказання означає, що кандидат є непридатним незалежно від інших результатів, оскільки негативне рішення на будь-якому етапі припиняє процедуру. Незадовільна оцінка за однією з провідних якостей не є підставою для відмови, але виключає віднесення кандидата до категорії «придатний» і переводить його до категорії «умовно придатний» з рекомендаціями щодо

розвитку цієї якості. Третє: процедура має спільну частину для всіх кандидатів і додатковий модуль залежно від типу системи, для якої відбирається оператор. Для безпілотних авіаційних комплексів у ньому посилюють перевірку реакції та точності рухів, а для наземних – відповідальності, уважності й роботи в команді. Четверте: кожну якість оцінюють за простою шкалою (високий, достатній, недостатній рівень), а підсумковий висновок виводять із цих оцінок. П'яте: умовно придатних кандидатів повторно оцінюють після першого етапу навчання, і лише тоді ухвалюють остаточне рішення, що відповідає ідеї стеження за динамікою якостей. Шосте: результати відбору слід зберігати й використовувати для розвитку операторів, а також як зворотний зв'язок для оцінювання всіх попередніх етапів відбору.

Розвиток операторів безпілотних систем має бути поетапним. Приклад дає рекрутинговий центр Drone Force Сухопутних військ Збройних Сил України: після відбору кандидати проходять оформлення контракту, базову підготовку та фахове навчання, а супровід отримують на кожному етапі. У підготовці вже використовують симулятори, що передають динаміку керування FPV-дроном, і психологічну смугу перешкод із 14 завдань, яка моделює атаки FPV-дронів, шум, вибухи й роботу групи під тиском. Дослідники також пропонують стежити за динамікою професійно важливих якостей під час навчання та готувати старших операторів як наставників і майбутніх командирів розрахунків.

Під час підготовки операторів безпілотних систем необхідно враховувати особливості їхньої майбутньої військової служби, а саме повсякденну діяльність підрозділів. У дослідженні 426 операторів дистанційно пілотованих літальних апаратів Повітряних сил США більшість професійного стресу респонденти пов'язали з організаційними чинниками: змінністю, тривалістю роботи й ергономікою робочого місця. Оператори діючої служби вдвічі частіше повідомляли про емоційне виснаження та цинізм, ніж оператори резерву. Автори дослідження рекомендували скоротити кількість годин і змін та проводити періодичні психологічні обстеження операторів.

Для оцінювання самої системи відбору та підготовки операторів безпілотних систем пропонуються прості показники: частка відсіву на етапах навчання, динаміка показників стійкості, випадки вигорання та ротація операторів. Їх слід періодично використовувати для перегляду критеріїв відбору.

Отже, для операторів безпілотних авіаційних і наземних систем доцільно виділити спільне ядро психологічних якостей та якості, які більшою мірою притаманні операторам авіаційних або наземних систем. Відбір пропонується проводити з дотриманням зазначених вище шести правил, а підготовку – поетапно, з підтриманням дієвої системи зворотного зв'язку для коригування системи відбору. Напрям подальших досліджень – емпіричне порівняння психологічних профілів операторів безпілотних авіаційних і наземних систем із виділенням ядра спільних психологічних якостей та специфічних для кожної системи модулів.

Осадчук Р. М., канд. техн. наук
Коровайний Є. О.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДОЛОГІЯ ОЦІНЮВАННЯ ЙМОВІРНОСТІ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ ВІЙСЬКОВОЇ ТЕХНІКИ НА ЗНІМКАХ ІЗ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Актуальність дешифрування аерофотознімків не зменшилася з часу їх винайдення, навпаки з поширенням сучасних технологій та зростанням обсягів даних, що генеруються з повітряних засобів, значення дешифрування аерофотознімків збільшується.

Аналіз процесу дешифрування матеріалів повітряної розвідки свідчить, що це складний процес, який вимагає від дешифрувальника високої кваліфікації та досвіду, а саме знання дешифрувальних (розпізнавальних) ознак озброєння та військової техніки (ОВТ).

Постійне зростання насиченості ЗС БпС стимулює противника до розроблення нових способів маскування військової техніки. Це, у свою чергу, актуалізує процес удосконалення структури процесу воєнного дешифрування знімків з БпЛА. Водночас відсутні кількісні показники, які б відображали ефективність розпізнавання ОВТ за допомогою апаратних засобів на основі ШІ.

Чинні методи дешифрування зазвичай базуються на загальних характеристиках техніки, таких як форма, розміри або колір. Але цього недостатньо, коли йдеться про визначення близьких за характеристиками моделей, наприклад, бронетехніки, особливо радянського зразка (Т-64, Т-72, Т-80). Ці моделі мають багато спільних розпізнавальних ознак, але відрізняються

окремими конструктивними елементами. Саме такі деталі, хоч і не завжди очевидні, відіграють вирішальну роль у точній ідентифікації. З огляду на перелічені фактори, виникає необхідність створення детальної, структурованої, логічно узгодженої та гнучкої методики дешифрування. Це дозволить не лише спростити розпізнавання техніки, але й забезпечити достовірність цього процесу в умовах, максимально наближених до реального бойового середовища.

Під час вдосконалення методики були враховані як теоретичні положення зі сфери дешифрування аерофотознімків, так і практичні аспекти, пов'язані з реальними умовами експлуатації БпЛА у польових ситуаціях. Її основна концепція полягає у використанні багаторівневого аналізу візуальних ознак, що дозволяє поступово відсіювати нерелевантні варіанти та зосереджувати увагу на найперспективніших.

Приклад роботи удосконаленого підходу: Зображення танка з додатковим захистом типу "сарай" (рис. 1). На ньому не видно оснащення башти, але наявна вихлопна система з лівого боку та повернута гармата праворуч — що дозволило визначити танк як Т-72.



Рис. 1. – Зображення танка із додатковим захистом типу "сарай"

Цей приклад демонструє, що навіть за умов обмеженої видимості, викликаної перешкодами типу рослинності, тіні чи специфічного ракурсу, набір із трьох-чотирьох характеристик є достатнім для точного дешифрування. Це значно підвищує ефективність роботи операторів БпЛА.

Переваги:

можливість використання навіть при часткових умовах спостереження;

швидкість аналізу вища порівняно з традиційним дешифруванням;

висока адаптивність: методика ефективно працює за різних умов місцевості, часу доби та кутів огляду.

Обмеження:

Непридатність для цивільного застосування;

вимагає мінімальної підготовки дешифрувальника;

деякі ознаки можуть бути недоступними за складних погодних умов.

В доповіді представлено методологічний підхід до ймовірності розпізнавання військової техніки такої як танки на знімках з БпЛА.

Салій Д. В.
Бедрій Н. А.
Житомирський військовий інститут імені С. П. Корольова

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В БЕЗПІЛОТНИХ СИСТЕМАХ

Розвиток безпілотних систем (БпС) пов’язаний із переходом від дистанційно керованих платформ до комплексів, здатних автоматизовано обробляти інформацію та підтримувати прийняття рішень оператором. Важливим чинником цього переходу є застосування технологій штучного інтелекту (ШІ), зокрема машинного навчання та комп’ютерного зору. Метою роботи є узагальнення основних напрямів застосування ШІ у БпС, їх можливостей, перспектив та обмежень.

На початкових етапах автоматизація забезпечувала стабілізацію платформи, підтримання параметрів руху, виконання заданого маршруту та передавання телеметрії. Розвиток обчислювальних засобів і сенсорного обладнання розширив перелік автоматизованих функцій. Водночас виконання наперед заданої програми не слід ототожнювати із застосуванням ШІ: інтелектуальні алгоритми забезпечують аналіз складних даних, розпізнавання закономірностей та формування результатів за змінних умов спостереження.

Одним з основних напрямів є оброблення зображень і відеоданих. Алгоритми комп’ютерного зору можуть здійснювати попередній аналіз матеріалів, виявляти та класифікувати об’єкти, визначати зміни на місцевості й відбирати інформативні фрагменти для перевірки оператором. Це створює передумови для зменшення інформаційного навантаження та скорочення часу опрацювання даних. Результат має містити інформацію про впевненість алгоритму й забезпечувати можливість перевірки за первинним матеріалом.

Важливим напрямом є багатосенсорне об’єднання інформації. Поєднання даних оптико-електронних і тепловізійних засобів, навігаційних систем та інерційних датчиків дозволяє формувати повніше представлення про обстановку. Для цього необхідно враховувати узгодженість даних у часі, їх точність і можливі суперечності. Інтеграція результатів із геоінформаційними системами сприяє просторовому впорядкуванню інформації та підтримці ситуаційної обізнаності.

Перенесення частини оброблення на бортові засоби може зменшувати обсяг передавання даних і затримку отримання результатів. Реалізація такого підходу обмежується обчислювальною продуктивністю, енергоспоживанням, масою обладнання та умовами тепловідведення. Вибір моделі ШІ потребує узгодження точності, швидкодії й доступних ресурсів. Розподіл оброблення між бортом і наземними засобами залежить від ресурсів системи.

Підвищення автономності слід розглядати як перерозподіл функцій між людиною та автоматизованою системою. Алгоритми можуть підтримувати навігаційні функції, оцінювання середовища та виконання рутинних операцій. Однак наявність цих можливостей не означає готовності до повністю автономного застосування. Межі самостійних дій системи мають бути визначені, а критично важливі рішення повинні залишатися під контролем людини. Оператору необхідні зрозуміле подання результатів та можливість втручання у процес управління.

Основним обмеженням машинного навчання є залежність результатів від якості та репрезентативності навчальних даних. Зміна освітлення, погодних умов, ракурсу спостереження й характеристик місцевості може знижувати точність розпізнавання. Тому перевірка моделей має охоплювати різні умови та враховувати помилкові спрацювання і пропуски об’єктів. Важливо забезпечити виявлення невизначених ситуацій та їх передавання на розгляд оператору.

Подальший розвиток ШІ у БпС доцільно пов’язувати з узгодженням отримання даних, інтелектуального оброблення, відображення результатів та їх перевірки людиною. Перспективними є мультимодальні моделі, які поєднують різні види даних, і засоби пояснення машинних висновків. Їх упровадження потребує перевірки сумісності з інформаційними системами та підготовки операторів до критичного оцінювання результатів.

Таким чином, основними напрямами застосування ШІ у БпС є оброблення зображень і відеоданих, багатосенсорне об’єднання інформації, бортовий аналіз та підтримка ситуаційної обізнаності. Практичне значення узагальнення полягає у визначенні умов їх упровадження: відповідності даних умовам використання, достатності обчислювальних ресурсів, перевірки достовірності результатів і збереження контролю людини. Їх урахування визначає передумови розвитку автономних функцій.

Солошенко Ю. В., канд. техн. наук
Куровська Т. Ю.
Центральний науково-дослідний інститут
озброєння та військової техніки Збройних Сил України

АРХІТЕКТУРНІ ПРИНЦИПИ ТА ПЕРСПЕКТИВИ ІНТЕГРАЦІЇ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В БЕЗПІЛОТНІ АВІАЦІЙНІ КОМПЛЕКСИ СИЛ ОБОРОНИ УКРАЇНИ

В умовах сучасного високоінтенсивного збройного протистояння динаміка змін операційної обстановки вимагає миттєвого збирання та аналізу даних. Традиційні методи управління безпілотними авіаційними комплексами (далі - БпАК) за участю оператора вичерпують свій потенціал через надмірне радіоелектронне придушення каналів зв'язку та керування, а також критичне когнітивне перевантаження операторів пунктів керування.

Вирішення цієї проблеми полягає у системній інтеграції технологій штучного інтелекту (далі – ШІ) безпосередньо у бортові обчислювальні комплекси та наземні сегменти керування безпілотними літальними апаратами (далі – БпЛА). Впровадження технологій ШІ дає змогу реалізувати автономну навігацію в умовах відсутності або спотворення сигналів глобальних навігаційних супутникових систем, автоматизувати процеси детекції, класифікації та ідентифікації об'єктів, а також забезпечити алгоритмічне термінальне донаведення на цілі в умовах повного радіоелектронного блокування.

Керування автономними та напівавтономними БпЛА доцільно будувати на основі алгоритмів глибокого навчання з підкріпленням. Це дозволяє бортовому інтелектуальному агенту ШІ формувати адаптивну траєкторію польоту, оминати

зони дії ворожих комплексів протиповітряної оборони та радіоелектронної боротьби (далі – РЕБ) і маневрувати в динамічному повітряному просторі.

Архітектура інтелектуальної системи керування БпАК будується за ієрархічним принципом і включає такі взаємопов'язані рівні:

1. Сенсорний рівень – збирання та первинна фільтрація телеметричних і видових даних від бортових оптико-електронних систем, інфрачервоних сенсорів, LiDAR, інерціальних навігаційних систем та засобів радіотехнічної розвідки.

2. Аналітичний рівень – комплексна обробка та комплексування даних від різнорідних датчиків, придушення завад та розпізнавання об'єктів за допомогою нейромережевих моделей безпосередньо на бортовому прискорювачі.

3. Рівень прийняття рішень та донаведення – оцінка поточного стану виконання польотного завдання, локальна навігація, видача команд на автозахоплення та супровід цілей.

4. Виконавчий рівень – безпосереднє формування керуючих сигналів на польотний контролер, сервоприводи та силову установку.

Прикладними напрямами інтеграції ШІ в БпАК є:

1. Бортові системи комп'ютерного зору – використання оптимізованих нейромережевих архітектур (MobileNet, DETR, Vision Transformers) на базі малогабаритних обчислювальних прискорювачів (NVIDIA Jetson, Coral TPU) забезпечує високу точність детекції, класифікації цілей та автономне автозахоплення/донаведення ударних БпЛА навіть в умовах повної втрати зв'язку з оператором.

2. Автономна навігація – застосування алгоритмів зіставлення поточного оптичного або інфрачервоного зображення підстильної поверхні з еталонними матрицями висот та супутниковими знімками забезпечує коригування дрейфу інерціальної системи навігації в умовах роботи засобів РЕБ.

3. Бортова радіотехнічна розвідка та адаптивна РЕБ – застосування методів машинного навчання для автоматизованого спектрального аналізу сигналів, класифікації джерел радіовипромінювання та динамічної адаптації робочих частот.

4. Розподілений ройовий ШІ – алгоритми децентралізованого прийняття рішень для координації групи БпЛА, що забезпечують самоорганізацію, децентралізований розподіл розвідувальних і ударних функцій між апаратами без участі наземного пункту керування.

Аналіз бойового застосування БпЛА Силами оборони України демонструє стрімку інтеграцію вітчизняних програмно-апаратних розробок. Модулі ШІ активно впроваджуються у розвідувальні БпАК (типу SHARK, “Лелека-100”, “Фурія”), а також побудовані на FPV-платформах ударні системи із бортовими контролерами автозахоплення цілей. Зазначені комплекси інтегруються до національних систем ситуаційної обізнаності, утворюючи єдину цифрову мережу поля бою.

Водночас масове масштабування технологій ШІ в безпілотній авіації супроводжується низкою проблемних питань:

1. Уразливість ML-моделей до завадових впливів – ризики викривлення даних та алгоритмічного введення в оману нейромереж через засоби маскування цілей та оптичні завади.

2. Апаратні обмеження – необхідність глибокої оптимізації та стиснення важких моделей (шляхом квантування, стиснення та дистиляції знань) для забезпечення високої частоти обробки кадрів на малогабаритних платформних обчислювачах з обмеженим енергоспоживанням.

3. Нормативно-правові та етичні аспекти. Відсутність стандартизованих процедур верифікації та валідації автономних алгоритмів прийняття рішень, а також визначення меж автономії під час застосування летального озброєння.

Зважаючи на викладене, інтеграція технологій ШІ в БпАК Сил оборони України є визначальним чинником досягнення тактичної та технологічної переваги над противником. Перехід від дистанційного керування до високого рівня автономності дозволяє подолати критичну залежність БпЛА від наявності радіочастотного каналу зв'язку та супутникової навігації.

Впровадження концепції оброблення та комплексування даних на основі ієрархічної чотирирівневої архітектури забезпечує мінімізацію затримок під час оброблення видової інформації та дає змогу реалізувати високоточне термінальне донаведення в умовах щільної дії засобів РЕБ.

Системне вирішення викликів, пов'язаних із навчанням нейромереж, апаратною оптимізацією обчислювачів та розробкою стандартизованих методик верифікації, є пріоритетним напрямом подальших наукових і дослідно-конструкторських робіт у сфері розбудови оборонного потенціалу України.

Чуканов А. І., Ph. D.
Щерблюк В. А.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ АВТОНОМНОСТІ БЕЗПІЛОТНИХ СИСТЕМ СИЛ ОБОРОНИ УКРАЇНИ

Сучасний розвиток безпілотних систем характеризується переходом від дистанційно керованих платформ до комплексів із підвищеним рівнем автономності, здатних самостійно виконувати окремі функції оцінювання навколишньої обстановки, навігації, планування руху, контролю технічного стану та інформаційної взаємодії. Для Сил оборони України цей напрям має особливе значення через необхідність діяти в умовах динамічної обстановки, обмеженого радіозв'язку, дефіциту часу на прийняття рішень та постійної зміни характеристик середовища застосування. Штучний інтелект (ШІ) у такому контексті доцільно розглядати не як заміну оператора, а як сукупність методів, що зменшують навантаження на людину, підвищують ефективність виконання завдання та забезпечують безперервність функціонування безпілотної системи за часткової втрати зовнішнього керування.

Обґрунтовано перспективні напрями застосування технологій ШІ для підвищення функціональної автономності безпілотних систем (БпС) із одночасним забезпеченням контрольованості, прогнозованості та безпечності їх функціонування. Під автономністю пропонується розуміти здатність системи підтримувати визначений рівень функціонування в межах заданої місії за мінімальної кількості команд оператора, використовуючи бортові сенсори, локальні обчислювальні ресурси та наперед визначені правила переходу між режимами. Такий підхід дозволяє розділити технічну автономність платформи і право людини на прийняття критичних рішень, що є принципово важливим для застосування ШІ у військових системах.

Найбільш доцільною сферою впровадження ШІ є інтелектуальне оцінювання навколишньої обстановки. Поєднання даних від оптичних, тепловізійних, інерціальних, радіотехнічних та інших бортових сенсорів може використовуватися для розпізнавання типових об'єктів місцевості, виявлення

перешкод, оцінювання прохідності маршруту й контролю зміни умов руху. На відміну від алгоритмів, орієнтованих на один тип сигналу, комплексна обробка даних від різних сенсорів дає змогу зберігати працездатність за погіршення якості окремого каналу спостереження. Перспективним є застосування моделей, які не лише формують результат класифікації, а й оцінюють власну невизначеність. Це створює підстави для переходу системи до консервативного режиму або передачі рішення оператору, коли достовірність автоматичної оцінки є недостатньою.

Другим напрямом є інтелектуальна навігація та планування руху. ШІ може забезпечувати адаптивний вибір маршруту з урахуванням стану платформи, геометрії місцевості, доступності орієнтирів, енергетичних обмежень та ймовірності втрати окремих джерел навігаційної інформації. Для повітряних, наземних і морських БпС функціональне значення має не максимально складний алгоритм, а гарантована здатність своєчасно перейти до резервного способу орієнтування, безпечного завершення маршруту або повернення до контрольної точки. Тому перспективна архітектура автономності повинна бути багаторівневою: базові стабілізаційні функції мають залишатися незалежними від високорівневих моделей ШІ, а інтелектуальний модуль повинен працювати в межах чітко визначених обмежень.

Окремої уваги потребує застосування ШІ для керування групами безпілотних платформ. Практична цінність такого підходу полягає насамперед у розподілі задач, узгодженні маршрутів, запобіганні взаємним конфліктам та підтриманні працездатності групи за вибуття окремих елементів. Централізована модель керування є вразливою до втрати каналу зв’язку й перевантаження пункту управління, тому доцільним є розвиток розподілених механізмів координації, у яких кожна платформа має обмежений набір локальних правил, а оператор контролює цілі, пріоритети та допустимі межі поведінки. Для Сил оборони України такий підхід може бути корисним у логістиці, інженерному забезпеченні, спостереженні, ретрансляції зв’язку, пошуково-рятувальних завданнях та інших функціях, де зменшення участі людини безпосередньо знижує ризик для особового складу.

Важливим компонентом автономності є інтелектуальний контроль технічного стану. Обробка телеметрії засобами машинного навчання може застосовуватися для виявлення нетипових режимів роботи приводів, енергетичної

системи, сенсорів і каналів зв’язку до моменту виникнення критичної відмови. На цій основі можливо формувати прогностичну оцінку ресурсу, рекомендувати зміну режиму експлуатації або завчасне технічне обслуговування. У масштабі парку БпС така функція має подвійний ефект: підвищує надійність окремої платформи та створює структуровані дані для коригування вимог до нових зразків, планування запасних частин і підготовки персоналу.

Ефективність ШІ безпосередньо залежить від якості даних. Дані, отримані в реальних умовах експлуатації, є неоднорідними, можуть містити пропуски, зміщення та помилки розмітки. Тому підготовка наборів даних має включати контроль походження, контроль версій програмного забезпечення та моделей ШІ, опис умов отримання та процедури виявлення аномалій. Доцільно розділяти дані для навчання, валідації та незалежних випробувань, а оцінювання моделей проводити не лише за середньою точністю, але й за стабільністю роботи в граничних умовах. Перспективним є застосування цифрових моделей середовища та симуляторів для відтворення рідкісних ситуацій, однак результати, отримані у віртуальному середовищі, повинні підтверджуватися реальними випробуваннями на різних типах платформ.

Для військових БпС критичною вимогою є кіберстійкість ШІ-компонентів. Моделі та програмні модулі повинні бути захищені від несанкціонованої заміни, втручання у параметри, підміни вхідних даних і неконтрольованого оновлення. Доцільною є модульна побудова програмного забезпечення, за якої функції ШІ ізольовані від базових контурів безпеки, а кожна нова версія проходить повторну перевірку на репрезентативному наборі сценаріїв. Важливим показником має бути не лише продуктивність алгоритму, а й можливість пояснити причину переходу системи до певного режиму, відтворити журнал подій та встановити, які вхідні дані вплинули на результат.

Підготовка операторів і технічного персоналу повинна змінюватися разом із розвитком автономності. Якщо в традиційній моделі основна увага приділяється ручному керуванню, то для інтелектуальних БпС зростає значення навичок постановки задач, контролю обмежень, інтерпретації рівня довіри до автоматичного рішення та коректного втручання в нестандартній ситуації. Навчальні програми доцільно доповнювати сценаріями відмови сенсорів, деградації навігації, втрати зв’язку, помилкової класифікації та переходу між ручним і автономним режимами. Це дозволить оцінювати не окремо оператора або алгоритм, а ефективність взаємодії оператора з безпілотною системою в цілому.

Для оцінювання результативності технологій ШІ пропонується використовувати сукупність показників: тривалість автономного виконання функцій без втручання оператора; частку коректно завершених завдань за погіршення зовнішніх умов; кількість переходів до безпечного режиму; навантаження на оператора; відтворюваність результатів; стійкість до відмов окремих сенсорів; обчислювальну та енергетичну вартість алгоритмів. Така система показників дозволяє уникнути ситуації, коли висока точність окремої моделі не приводить до реального підвищення ефективності БпС через надмірну ресурсомісткість або недостатню прогнозованість.

Отже, перспективи застосування ШІ для підвищення автономності БпС Сил оборони України пов’язані з переходом від окремих інтелектуальних функцій до керованої модульної архітектури, у якій сприйняття, навігація, планування, контроль технічного стану та координація платформ взаємодіють через стандартизовані інтерфейси. Пріоритетними принципами мають бути стійкість до деградації даних, локальна працездатність за обмеженого зв’язку, контроль невизначеності, можливість безпечного втручання людини та систематична перевірка в умовах, максимально наближених до реальної експлуатації. Реалізація цих принципів створює передумови для зменшення навантаження на операторів, підвищення живучості безпілотних комплексів і скорочення.

Казєв О. В.
Курилін Я. В.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

НАЗЕМНІ РОБОТИЗОВАНІ КОМПЛЕКСИ ЯК ЗАСІБ ЗНИЖЕННЯ РИЗИКІВ ДЛЯ ОСОБОВОГО СКЛАДУ ПІД ЧАС ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ТА ЕВАКУАЦІЇ

Сучасні умови ведення бойових дій істотно підвищують ризики для особового складу під час підвезення матеріальних засобів, переміщення майна та евакуації поранених із небезпечних районів. Вогневий вплив, мінна небезпека, складний рельєф, обмежена видимість і нестабільність каналів зв’язку ускладнюють виконання навіть типових логістичних завдань. За

офіційними повідомленнями Міністерства оборони України, у 2026 році застосування наземних роботизованих комплексів (НРК) у логістичних та евакуаційних місіях продовжує масштабуватися. Це свідчить про перехід НРК від окремих експериментальних зразків до повноцінного елемента системи забезпечення підрозділів.

Основна увага зосереджена на визначенні умов, за яких НРК здатні реально зменшувати перебування військовослужбовців у небезпечних зонах без погіршення надійності логістичного забезпечення та евакуації. НРК у цьому контексті доцільно розглядати не лише як дистанційно керовану транспортну платформу, а як складову організаційно-технічної системи, що включає сам комплекс, оператора, засоби зв'язку, навігації, технічного обслуговування та процедури застосування. Ключовим показником результативності має бути не кількість залучених роботизованих платформ сама по собі, а частка небезпечних операцій, виконаних без безпосередньої присутності людини.

Найбільш очевидною сферою застосування НРК є доставка вантажів до підрозділів, які перебувають у районах з підвищеним ризиком. Роботизована платформа може виконувати перевезення боєприпасів, води, продовольства, засобів зв'язку, інженерного майна, елементів енергозабезпечення та інших вантажів, зменшуючи потребу у використанні транспортних засобів із екіпажем або піших груп забезпечення. Особливе значення має повторюваність таких місій: якщо маршрут і процедура завантаження стандартизовані, НРК може систематично виконувати однотипні перевезення, звільняючи особовий склад для інших завдань і знижуючи сумарний час його перебування у небезпечній зоні.

Ефективність логістичного НРК визначається сукупністю взаємопов'язаних характеристик. До них належать вантажопідйомність, прохідність, запас енергії, стійкість руху, можливість подолання типових перешкод, точність маневрування, час підготовки до роботи та зручність технічного обслуговування. Надмірна орієнтація лише на одну характеристику, наприклад максимальну вантажопідйомність, може погіршити мобільність або збільшити складність обслуговування. Тому доцільним є функціональний підхід, за якого параметри платформи визначаються типовими сценаріями застосування та умовами місцевості, а не прагненням до універсальності одного зразка.

Для евакуаційних завдань вимоги до НРК мають додаткові особливості. Платформа повинна забезпечувати надійне розміщення евакуйованої особи,

мінімізувати небажані переміщення під час руху та мати конструкцію, яка спрощує завантаження і розвантаження. Важливими є плавність руху, стійкість на нерівній поверхні, можливість оперативної зупинки та прогнозована поведінка при втраті зовнішнього керування. Евакуаційний НРК не замінює медичну допомогу, але дозволяє скоротити ділянку маршруту, на якій для переміщення пораненого необхідна безпосередня присутність декількох військовослужбовців.

Перспективним є модульний принцип побудови НРК, коли одна базова платформа може оснащуватися змінними функціональними модулями для перевезення вантажів або евакуації. Такий підхід спрощує постачання, ремонт і підготовку операторів, оскільки основні вузли ходової частини, енергоживлення та керування залишаються уніфікованими. Стандартизовані механічні та електричні інтерфейси дозволяють швидше адаптувати платформу до конкретного завдання без створення повністю нового комплексу. Для масштабного застосування це важливіше, ніж збільшення кількості вузькоспеціалізованих зразків із несумісними комплектуючими.

Окремим напрямом є підвищення автономності руху без втрати контролю з боку оператора. Доцільними функціями є утримання заданого маршруту, обхід очевидних перешкод, автоматична зупинка при виникненні небезпечної ситуації та повернення до контрольної точки за наперед визначеними умовами. Автоматизація таких операцій зменшує навантаження на оператора і дозволяє йому контролювати завдання на рівні маршруту та стану платформи, а не безперервно коригувати кожен рух. При цьому критичні рішення щодо продовження місії, зміни маршруту або завершення евакуації повинні залишатися контрольованими та передбачуваними.

Стійкість керування НРК необхідно забезпечувати з урахуванням можливих переривань зв’язку. Функціонування комплексу не повинно залежати від безперервного надходження команд у кожний момент часу. За тимчасової втрати каналу доцільним є перехід до безпечного режиму: зупинка, утримання положення або виконання заздалегідь визначеної дії відповідно до типу місії. Такий підхід зменшує ризик неконтрольованого руху та спрощує роботу оператора у складній обстановці. Відновлення керування має відбуватися прогнозовано, без різкої зміни режиму або втрати накопичених даних про стан платформи.

Навігаційна підсистема НРК повинна поєднувати дані від кількох доступних датчиків і оцінювати достовірність поточного положення. Супутникова навігація може бути важливим, але не єдиним джерелом інформації. Для підтримання руху можуть використовуватися інерціальні датчики, одометрія, камери, цифрові карти та інші засоби оцінювання навколишньої обстановки. Практичне значення має не максимальна точність одного датчика, а здатність комплексу своєчасно виявити погіршення навігаційної інформації та перейти до режиму, який не створює додаткової небезпеки для людей і техніки.

Взаємодія оператора з комплексом повинна бути максимально простою та однозначною. На робочому місці доцільно відображати стан зв'язку, рівень заряду, активний режим керування, орієнтовне положення, наявність попереджень і можливість продовження місії. Надлишок другорядної інформації може підвищувати когнітивне навантаження і сповільнювати реакцію. Тому інтерфейс має підтримувати швидке розуміння ситуації та чітко виділяти події, що потребують втручання оператора. Для евакуаційних місій особливо важливими є підтвердження готовності платформи до руху та зрозумілий контроль зупинки.

Важливою умовою масштабування НРК є ремонтопридатність. Комплекси, які працюють у складних дорожніх та погодних умовах, потребують швидкої заміни коліс, гусениць, елементів підвіски, акумуляторів, приводів і сенсорних модулів. Конструкція має забезпечувати доступ до типових вузлів без складного спеціалізованого обладнання. Доцільно передбачати уніфіковані змінні блоки та мінімізувати кількість унікальних компонентів. Це скорочує час повернення комплексу до роботи та спрощує формування запасу комплектуючих у підрозділі.

Підготовка операторів повинна охоплювати не лише навички дистанційного керування. Необхідно формувати вміння оцінювати технічний стан платформи, планувати безпечний маршрут, контролювати заряд і вантаж, діяти при втраті зв'язку, правильно переходити між ручним та автоматизованим режимами, а також виконувати базове технічне обслуговування. Ефективність НРК значною мірою залежить від того, наскільки його застосування інтегроване у звичайні процедури логістики та евакуації. Якщо роботизований комплекс потребує надмірно складної окремої організації, його переваги можуть бути частково втрачені.

Для оцінювання результативності НРК доцільно використовувати систему показників, що відображає не лише технічні можливості, а й практичний ефект. До таких показників можна віднести частку успішно завершених місій, масу доставленого вантажу, тривалість циклу перевезення, кількість втручань оператора, частоту технічних відмов, час відновлення працездатності, споживання енергії та кількість операцій, під час яких вдалося уникнути безпосереднього залучення особового складу до небезпечної ділянки маршруту. Для евакуаційних комплексів додатково важливими є стабільність руху, час підготовки до евакуації та зручність завантаження.

Економічну ефективність роботизації слід оцінювати з урахуванням повного життєвого циклу. Низька початкова вартість окремої платформи не є перевагою, якщо вона має малий ресурс, складно ремонтується або потребує унікальних комплектуючих. Водночас більш дорогий комплекс може бути виправданим за умови високої повторюваності місій, швидкого відновлення та значного скорочення потреби у залученні людей до ризикованих операцій. Для порівняння різних рішень доцільно використовувати вартість успішно виконаної місії та середню готовність комплексу до застосування.

Водночас НРК не слід розглядати як універсальну заміну традиційним засобам логістики. Їх можливості обмежуються рельєфом, станом ґрунту, погодою, запасом енергії, якістю зв’язку, масою вантажу та доступністю технічного обслуговування. Окремою проблемою є повернення пошкодженого комплексу. Тому роботизовані платформи доцільно включати до багаторівневої системи забезпечення, у якій для кожного типу маршруту й завдання визначається оптимальний транспортний засіб, а НРК використовуються насамперед там, де зниження ризику для особового складу має найбільшу цінність.

Таким чином, наземні роботизовані комплекси є перспективним інструментом зниження ризиків для особового складу під час логістичного забезпечення та евакуації. Найбільший ефект досягається не за рахунок окремої технічної характеристики, а завдяки поєднанню достатньої прохідності, вантажопідйомності, надійного керування, безпечних режимів при втраті зв’язку, модульної конструкції, ремонтопридатності та підготовленого персоналу. Подальше масштабування НРК доцільно орієнтувати на стандартизацію платформ і змінних модулів, уніфікацію інтерфейсів, сценарне випробування та оцінювання за показником реально усунутого ризику для людини. Такий підхід дозволяє перетворити роботизовані комплекси з окремого технічного засобу на стійкий елемент.

Петров В. М., канд. військ. наук
Афанасьєв В. В., канд. техн. наук, доц.
Крук Б. М. канд. техн. наук, ст. наук. співроб.
Кудрявцев А. Ф.
Марченко О. М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ТРАНСФОРМАЦІЯ ФОРМ ТА СПОСОБІВ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ НА ОСНОВІ ВПРОВАДЖЕННЯ БОЙОВОГО ДОСВІДУ

Російсько-українська війна стала найбільш масштабним прикладом застосування безпілотних авіаційних систем (БпАС) у збройних конфліктах світу. За роки війни відбулася суттєва трансформація їх ролі: від переважно розвідувального засобу до багатофункціонального елемента системи розвідки, ураження, протидії повітряним загрозам та інформаційного забезпечення бойових дій. За таких умов ефективність застосування БпАС визначається вже не стільки характеристиками окремого безпілотного літального апарата (БпЛА), скільки організацією їх комплексного застосування, взаємодією з іншими силами і засобами та здатністю адаптуватися до динамічної обстановки.

Досвід російсько-української війни показує широке застосування безпілотних систем у різних сферах бойових дій, а також впровадження, адаптації та масштабування нових технологій. В Україні поступово розвиваються розвідувальні, ударні, FPV, далекобійні та БпАС-перехоплювачі. Це зумовлює необхідність удосконалення не лише технічних характеристик БпАС, а насамперед форм і способів їх застосування.

Метою доповіді є узагальнення досвіду застосування БпАС у російсько-української війні та визначення основних напрямів розвитку форм і способів їх застосування.

Аналіз бойового досвіду свідчить про поступову трансформацію від одиночного застосування БпЛА до системного використання спеціалізованих підрозділів та груп БпАС. На початковому етапі БпАС здебільшого використовувалися для повітряної розвідки, спостереження та коригування вогню. Надалі сформувалася концепція їх функціонального об’єднання в

розвідувально-ударні контури, у яких інформація про повітряну або наземну ціль практично безперервно передається від засобу розвідки до засобу ураження. Таким чином, відбувається зміна підходу: БпАС розглядається не як окремий літальний апарат, а як елемент інформаційно-вогневої системи. Основною характеристикою такої системи стає скорочення часу між виявленням цілі, її ідентифікацією, прийняттям рішення, ураженням та оцінюванням результату.

За досвідом бойових дій можна виділити такі основні форми застосування БпАС: одиночне, групове та масоване застосування угруповання безпілотних систем. Одиночне застосування зберігає значення для виконання локальних завдань, проте його ефективність істотно залежить від можливостей конкретного екіпажу та стійкості окремого каналу управління. Групове застосування передбачає одночасне або послідовне використання декількох платформ для виконання спільних завдань. Воно забезпечує розподіл функцій між системами, взаємне резервування та можливість одночасного виконання розвідувальних і ударних завдань.

Найбільш перспективною є форма масованого застосування угруповання БпАС, до складу якого можуть входити розвідувальні, ударні, ретрансляційні, БпАС-перехоплювачі та інші безпілотні системи, а також наземні пункти управління, засоби зв’язку, навігації та інформаційно-аналітичного забезпечення. Такий підхід створює умови для переходу від застосування окремих платформ до формування інтегрованої безпілотної спроможності. При цьому масоване застосування доцільно розуміти не лише як одночасне використання значної кількості БпЛА, а як можливість постійного та розподіленого застосування великої кількості відносно дешевих платформ. Це дає змогу забезпечувати безперервність розвідки, створювати необхідну щільність впливу, компенсувати втрати окремих апаратів та ускладнювати функціонування систем протидії. Вказана форма застосування БпАС потребує подальшого удосконалення та розвитку.

Наступним напрямом трансформації форм застосування БпАС є інтеграція БпАС з іншими силами та засобами. Досвід бойових дій показав, що найбільший ефект досягається при взаємодії БпАС з артилерією, засобами протиповітряної оборони (ППО), радіоелектронної боротьби, розвідки, авіацією та наземними роботизованими комплексами. Тому перспективною формою є міжвидове застосування БпАС у єдиному інформаційному полі.

Суттєвий вплив на способи застосування БпАС чинить радіоелектронна боротьба. Протидія каналам управління та навігації стимулює розвиток захищених і альтернативних способів керування, резервування каналів зв'язку, автономної навігації та підвищення стійкості безпілотних систем. Показовим напрямом розвитку способів застосування є поширення БпАС із волоконно-оптичним каналом управління, які дають змогу зменшити залежність від радіоканалів у відповідних умовах.

Ще одним напрямом трансформації способів застосування є автономізація та інтелектуалізація БпАС. Вже сьогодні автоматизуються окремі функції навігації, стабілізації, виявлення та супроводження об'єктів. У перспективі передбачається збільшення ролі алгоритмів штучного інтелекту в аналізі інформації, розподілі завдань між платформами та оптимізації їх застосування. При цьому доцільним є поетапний розвиток людино-машинних систем, у яких автоматизованим засобам передаються окремі функції, а критичні рішення залишаються під відповідним рівнем людського контролю.

Окремого значення набуває використання БпАС для протидії іншим безпілотним системам. Розвиток БпАС-перехоплювачів свідчить про формування нового напряму їх застосування у складі багаторівневої системи ППО. Такі системи можуть доповнювати традиційні засоби ППО та використовуватися для боротьби з малорозмірними повітряними цілями.

Узагальнення досвіду бойових дій дозволяє сформувати перспективну послідовність застосування БпАС: використання єдиного інформаційного поля, оцінка обстановки, виявлення та ідентифікація цілей, оцінювання загроз, визначення пріоритетів, вибір засобів впливу, застосування БпАС (угруповань БпАС), контроль результатів впливу (у тому числі вогневих), коригування подальших дій.

В доповіді підкреслено, що основними напрямами розвитку форм і способів застосування БпАС доцільно визначити:

- перехід від платформоцентричного до системоцентричного підходу;
- створення спеціалізованих підрозділів та угруповань БпАС;
- інтеграцію розвідки та ураження в єдиний розвідувально-ударний контур;
- масоване і розподілене застосування;
- підвищення стійкості до радіоелектронного впливу;
- розвиток автономних функцій;
- удосконалення БпАС-перехоплювачів;

- інтеграцію безпілотних систем у загальну систему управління у єдиному інформаційному полі Сил оборони.

Зроблені висновки, що досвід російсько-української війни свідчить, що розвиток БпАС відбувається одночасно за технічним, організаційним та тактичним напрямами. Головною тенденцією є перехід від застосування окремих БпЛА до системного використання угруповань безпілотних систем, інтегрованих із засобами розвідки, управління, ураження, РЕБ та ППО. Перспективна модель застосування БпАС повинна базуватися на принципах системності, масовості, розподіленості, адаптивності та мережевої взаємодії. Вирішальним фактором стає не окрема технологія, а здатність системи швидко адаптуватися до змін тактики противника, електромагнітної обстановки та характеру бойових завдань.

Таким чином, подальший розвиток БпАС доцільно спрямовувати на формування інтегрованої безпілотної спроможності, у якій окремі платформи функціонують як елементи єдиного інформаційно-вогневого контуру. Саме такий підхід створює передумови для підвищення ефективності застосування безпілотних систем та їх адаптації до вимог сучасної війни.

Лазакович М. С.
Лех А. І.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТАТІВ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ХІМІЧНОГО, БІОЛОГІЧНОГО, РАДІОЛОГІЧНОГО ТА ЯДЕРНОГО ЗАХИСТУ

Використання безпілотних літальних апаратів (БпЛА) є одним із засобів новітнього озброєння, використовувались у воєнних конфліктах кінця ХХ – початку ХХІ ст., стали безпілотні літальні апарати, які довели свою здатність значно ефективніше вести повітряну розвідку, а ніж пілотовані літаки, та виконувати інші завдання бойового забезпечення, завдаючи ударів по противнику. Сучасну армію неможливо уявити без безпілотних летальних апаратів, адже вони вказують на ціль, наводять артилерію, коригують вогонь, передають розвіддані прямо до штабу військової частини або підрозділу, якій виконує бойове

завдання, а головне – бережуть життя бійців. В умовах ведення швидкоплинних бойових дій та різкої зміни обстановки застосування безпілотних літальних апаратів являється одним з чинників забезпечення розвідувальною інформацією відповідних командирів (начальників) в масштабі реального часу і можливості здійснити вогневий вплив на особовий склад та об'єкти противника.

Застосування безпілотних літальних апаратів (БПЛА) під час виконання завдань хімічного, біологічного, радіологічного та ядерного захисту (ХБРЯ) є одним із найперспективніших напрямків сучасних військових та цивільних технологій.

Використання дронів дозволяє виявляти загрози, не наражаючи на небезпеку особовий склад, і забезпечує швидкий збір даних у реальному часі.

Основні напрямки застосування БПЛА у сфері ХБРЯ захисту включають:

Радіологічна та ядерна розвідка

Дистанційне виявлення: Дрони, оснащені спектрометрами та детекторами гамма-випромінювання (наприклад, Geiger-Mueller dose rate detectors), дозволяють проводити радіаційний моніторинг місцевості.

Картографування забруднення: БПЛА автоматично створюють карти радіоактивного зараження, визначаючи осередки високої радіації ("гарячі точки") у реальному часі.

Моніторинг критичної інфраструктури: Використання БПЛА (AARM Kromek) навколо АЕС або місць зберігання радіоактивних матеріалів.

Хімічна розвідка

Виявлення токсичних агентів: БПЛА використовують для виявлення бойових отруйних речовин (БОР) та токсичних промислових хімікатів (ТПХ) за допомогою датчиків іонної рухливості (IMS).

Дистанційний аналіз: Прилади дозволяють ідентифікувати хімічні сполуки на відстані, що безпечно для оператора.

Біологічна розвідка

Відбір проб повітря: БПЛА оснащуються системами для забору проб повітря в підозрілих зонах для подальшого лабораторного аналізу на наявність біологічних загроз.

Моніторинг біоаерозолів: Спеціалізовані датчики (UV particle fluorometer) здатні фіксувати аномально високі рівні біологічних частинок у повітрі.

Додаткові завдання ХБРЯ захисту

Ретрансляція сигналу: БПЛА можуть використовуватися для ретрансляції сигналів зв'язку між оператором та наземними робототехнічними комплексами.

Оцінка збитків: Повітряна розвідка місця ХБРЯ-інциденту для планування заходів з ліквідації.

Переваги використання БПЛА

Безпека персоналу: Виключення присутності людей у зонах високого ризику.

Висока мобільність та швидкість: Здатність оперативно обстежити важкодоступні території.

Точність даних: Автоматизоване нанесення загроз на цифрові карти.

Висновок

Впровадження безпілотних систем дозволяє досягти **нульового ризику для життя** особового складу на етапі первинної розвідки. Сучасні сенсори забезпечують точність вимірювань, порівняну зі стаціонарними лабораторіями, а швидкість картографування заражених зон скорочується з годин до хвилин. БПЛА стають критичною ланкою, що поєднує виявлення загрози та прийняття рішень у реальному часі.

Рекомендації:

Технічне оснащення:

Пріоритет слід надавати модульним платформам, які дозволяють швидко змінювати датчики (наприклад, з радіаційного на хімічний) залежно від ситуації.

Використовувати дрони з захистом не нижче IP65/67, щоб забезпечити можливість їх подальшої дезактивації (миття) після контакту з небезпечними речовинами.

Операційна діяльність:

Впроваджувати автоматизовані польотні завдання для регулярного моніторингу потенційно небезпечних об'єктів (АЕС, хімзаводи), щоб мінімізувати вплив людського фактора.

Інтегрувати дані з БПЛА безпосередньо в системи управління військами/службами порятунку для створення єдиної цифрової карти загроз.

Підготовка персоналу:

Проводити спільні навчання пілотів БПЛА та фахівців ХБРЯ захисту для відпрацювання алгоритмів дій у разі виявлення аномальних показників.

Аналіз даних:

Використовувати програмне забезпечення з елементами штучного інтелекту для прогнозування поширення хмари зараження на основі метеоданих у реальному часі.

Рибчинський Д. А.
Житомирський військовий інститут імені С. П. Корольова

МЕТОД БАГАТОКРОКОВОЇ ОПТИМІЗАЦІЇ МАРШРУТУ РОЗВІДУВАЛЬНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ ПРОСТОРОВО-ЧАСОВИХ ЗАГРОЗ

В умовах російсько-української війни зменшення ймовірності ураження безпілотних літальних апаратів (БпЛА) є особливо актуальним при плануванні польотного завдання. Досвід ведення бойових дій свідчить про те, що противник активно застосовує засоби протидії БпЛА Сил оборони України (СО України).

Ефективність виконання БпЛА бойових завдань в сучасних умовах залежить не лише від побудови оптимального маршруту польоту, але й його здатністю обходити ешелоновані зони протидії противника. Врахування просторових загроз дозволяє мінімізувати ймовірність ураження (подавлення), тим самим забезпечуючи необхідний рівень його живучості. Вирішення задачі комплексного планування маршруту польоту БпЛА в умовах інтенсивних радіоелектронних завад та кінетичної загрози вимагає мінімізації інтегральних ризиків на основі системного підходу. Таке завдання реалізується в межах багатокрокової оптимізації маршруту.

На першому кроці здійснюється побудова оптимального маршруту польоту БпЛА за допомогою генетичного алгоритму за відстанню (протяжністю). Подальша оптимізація маршруту здійснюється шляхом кластеризації за метрикою зони охоплення БпЛА із урахуванням висоти його польоту та кута огляду.

На наступному кроці проводиться оцінювання ризику ураження (подавлення) БпЛА. Для цього запропоновано ймовірнісну модель, яка враховує як просторово-геометричні параметри та ТТХ засобів протидії противника:

$$P(r,t) = P_1(r) + P_2(t) - P_1(r) \cdot P_2(t) \quad (1)$$

Аналіз отриманих складових інтегральної ймовірності $P(r,t)$ дозволяє сформувати багатокритеріальний підхід до прийняття рішень щодо підвищення живучості літального апарату.

На третьому кроці здійснюється пошук обходу виявлених зон протидії противника. Він реалізується шляхом алгоритму Белмана-Форда, з урахуванням

інших вихідних даних засобів протидії противника та їх ТТХ, критерій оптимізації якого формалізується у вигляді цільової функції:

$$d[t] = \min_{p \in P(s,t)} \sum_{(i,j) \in p} w(e_{ij}) \quad (2)$$

Вибір алгоритму Белмана-Форда обумовлений його стійкістю до динамічних змін у структурі графа та можливістю врахування інтегральних показників "компенсації ризику". У бойових умовах вага ребра може інтерпретуватися як сумарний вектор загроз та переваг. Негативні значення ваг у даній моделі відповідають ділянкам, де застосування власних некінетичних засобів або активне придушення засобів ворога забезпечує "чистий приріст" живучості БпЛА. Коректне моделювання таких умов функціонування є неможливим за умови застосування типового алгоритму Дейкстри через його математичне обмеження на роботу з від’ємними вагами ребер.

На четвертому кроці багатокрокової оптимізації виконується розрахунок інтегральної ймовірності ураження (подавлення) БпЛА. Зазначений етап реалізується за аналогією до другого кроку дослідження із застосуванням раніше визначеної ймовірнісної моделі сумісних випадкових подій, яка інтегрує просторову та часову компоненти ризику. Водночас як аргументи функцій математичного очікування загрози використовуються скориговані геометричні координати нових сегментів маршруту та перерахований час знаходження апарату в зонах потенційного впливу засобів протидії противника.

Таким чином, даний підхід забезпечує отримання об'єктивних кількісних показників ризику для подальшої верифікації ефективності побудованого маршруту.

Краснодубець А. І.
Житомирський військовий інститут імені С. П. Корольова

УДОСКОНАЛЕННЯ СПОСОБІВ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ СИСТЕМ НА ОСНОВІ ІНТЕГРАЦІЇ БОЙОВОГО ДОСВІДУ, ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА АДАПТИВНОГО ЗАХИСТУ ВІД БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Сучасний етап ведення війни характеризується інтенсивним впровадженням високотехнологічних зразків озброєння та військової техніки. Особливе місце посідають безпілотні авіаційні комплекси, наземні роботизовані комплекси, засоби радіоелектронної боротьби (РЕБ) та автоматизовані системи управління. Їх застосування змінює підходи до ведення розвідки, забезпечення підрозділів, ураження цілей і захисту особового складу.

Ефективність безпілотних систем визначається не лише тактико-технічними характеристиками окремого зразку, а й здатністю системи адаптуватися до зміни бойової обстановки, протидії противнику та умов виконання завдань. Розвиток засобів РЕБ, зміна способів використання безпілотних систем і поширення автоматизованих технологій зумовлюють потребу в постійному вдосконаленні способів їх застосування.

Тому визначення організаційно-технологічних підходів до підвищення ефективності застосування безпілотних систем Силами оборони України на основі інтеграції бойового досвіду, інтелектуальних технологій та комплексного захисту є перспективним напрямом.

Одним із ключових чинників удосконалення є системне вивчення, узагальнення та впровадження бойового досвіду. Доцільно розглядати цей процес як безперервний цикл: збір інформації про застосування озброєння; її перевірка й аналіз; визначення причин успішних дій і недоліків; формування рекомендацій; перевірка рекомендацій у підготовці та на практиці; оцінювання результатів і подальше оновлення відповідних матеріалів.

Перспективним напрямом є інтеграція різнотипних безпілотних платформ і засобів інформаційного забезпечення. Узгоджене використання повітряних та наземних роботизованих комплексів, розвідувальних засобів і систем управління може підвищити ситуаційну обізнаність, забезпечити обмін

даними та зменшити ризики для особового складу. Водночас така інтеграція потребує сумісності інформаційних форматів, визначених процедур обміну та належного захисту інформації.

Застосування технологій штучного інтелекту й машинного навчання доцільно спрямовувати на автоматизовану обробку інформації, розпізнавання та класифікацію об’єктів, виявлення закономірностей і підтримку прийняття рішень. Використання таких засобів має супроводжуватися перевіркою достовірності результатів, оцінюванням ризиків помилкової класифікації та збереженням належного контролю з боку уповноваженого особового складу.

Також одним із завдань для Сил оборони є захист від БпЛА противника, тому організацію протидії БпЛА доцільно організовувати як комплекс заходів, що поєднує своєчасне виявлення загроз, оповіщення, маскування, інженерний і пасивний захист, застосовуючи засоби РЕБ та інші сили та засоби протидії. Склад і порядок застосування відповідних засобів мають визначатися з урахуванням конкретної обстановки, сумісності систем і вимог безпеки.

Для практичної реалізації зазначених підходів пропонується: запровадити єдиний порядок документування та аналізу досвіду застосування безпілотних систем; розробити критерії оцінювання результативності, стійкості та ресурсної ефективності; регулярно актуалізувати навчальні програми операторів; використовувати тренажерні комплекси й документовані бойові епізоди; забезпечити зворотний зв’язок між бойовими підрозділами, військовими навчальними закладами та розробниками.

Підвищення ефективності застосування безпілотних систем потребує поєднання технологічних інновацій, організаційних змін і системного впровадження бойового досвіду. Інтеграція різнотипних платформ, обґрунтоване використання інтелектуальних технологій та комплексний підхід до захисту від БпЛА створюють передумови для підвищення адаптованості й результативності застосування високотехнологічного озброєння. Подальші дослідження доцільно спрямувати на розроблення методики оцінювання запропонованих підходів та механізму їх впровадження в систему підготовки Сил оборони України.

Гаєвський С. О.
Піонтківський П. М., канд. техн. наук, старш. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова

НОВІ ПІДХОДИ ДО ОБ'ЄДНАНОЇ ПІДГОТОВКИ ФАХІВЦІВ БЕЗПІЛОТНИХ СИСТЕМ НА ОСНОВІ БОЙОВОГО ДОСВІДУ

Сучасний характер збройного протистояння зумовлює трансформацію підходів до підготовки військовослужбовців, здатних ефективно діяти в умовах динамічного безпекового середовища. Особливого значення набуває підготовка фахівців безпілотних систем (БпС), застосування яких стало невід'ємною складовою розвідувального, вогневого, інформаційного та ударного контурів військ. Досвід російсько-української війни засвідчує, що результативність застосування БпС визначається не лише технічними характеристиками платформ, а й рівнем професійної компетентності особового складу, злагодженістю розрахунків, якістю управління, спроможністю адаптувати тактику застосування до змін обстановки та швидкістю впровадження бойового досвіду в систему підготовки. Дослідження сучасних тенденцій розвитку БпС також вказують на необхідність одночасного вдосконалення технологічної, доктринальної, організаційної та освітньої складових їх застосування.

У цих умовах об'єднана система підготовки фахівців БпС має розглядатися як цілісна багаторівнева система формування, розвитку та підтримання необхідних військово-професійних компетентностей особового складу, органів військового управління та підрозділів. Її функціонування доцільно будувати за принципом безперервності підготовки – від базової загальновійськової та фахової підготовки до підготовки операторів, командирів, інструкторів, штабних фахівців і колективів підрозділів БпС. Такий підхід має забезпечувати не ізольоване формування навичок окремого оператора, а набуття підрозділом спроможності виконувати визначені завдання у складі єдиного розвідувально-ударного, інформаційного та управлінського контуру.

Важливою передумовою удосконалення системи підготовки є перехід від переважно нормативно визначеної моделі навчання до моделі, орієнтованої на набуття конкретних спроможностей. Зміст підготовки фахівців БпС має визначатися не тільки переліком навчальних дисциплін та технічних операцій, а передусім характером завдань, які підрозділ повинен виконувати в реальних

умовах застосування. Відповідно, кваліфікаційні вимоги до фахівців доцільно формувати з урахуванням функціонального призначення конкретних категорій персоналу, типу БпС, рівня управління, особливостей району виконання завдань та характеру протидії противника.

Бойовий досвід України свідчить про високу швидкість еволюції тактики та технологій застосування БпС. Постійна зміна технічних рішень, засобів радіоелектронної боротьби, способів маскування, розвідки, навігації та управління призводить до швидкого морального старіння окремих елементів підготовки. У зв’язку з цим система підготовки має функціонувати за замкненим циклом "бойове застосування – виявлення проблеми – узагальнення досвіду – розроблення навчального матеріалу – підготовка – оцінювання – повторне коригування". Саме такий механізм дозволяє перетворювати окремі спостереження та ідентифіковані бойові приклади на системно впроваджені вивчені уроки. Дослідження трансформації військової освіти України в умовах війни також акцентують увагу на необхідності скорочення часу між виникненням нового бойового досвіду та його інтеграцією у навчальний процес.

Принципово важливим напрямом є формування уніфікованого ядра професійної підготовки фахівців БпС із подальшою спеціалізацією за функціональними напрямами. Базовий рівень має передбачати формування загальновійськових компетентностей, розуміння принципів застосування БпС у структурі підрозділу, основ тактики, управління, зв’язку, навігації, інформаційної безпеки та протидії засобам противника. Фахова підготовка повинна забезпечувати опанування конкретних типів і класів БпС, засобів їх наземного забезпечення та програмно-апаратних комплексів. Наступним рівнем має бути підготовка операторів і командирів розрахунків, здатних не лише технічно експлуатувати систему, а й приймати обґрунтовані рішення відповідно до тактичної обстановки.

Окреме місце в системі має посідати підготовка інструкторського складу. Динаміка розвитку безпілотних технологій не дає змоги забезпечити актуальність підготовки виключно шляхом централізованого оновлення навчальних програм. Необхідне формування розгалуженої мережі підготовлених інструкторів безпосередньо у військах, здатних оперативно адаптувати навчальні матеріали до нових способів застосування БпС, аналізувати результати виконання завдань та передавати передовий досвід

особовому складу. Таким чином, інструктор має виконувати не лише функцію викладача, а й роль носія та транслятора бойового досвіду.

Особливістю сучасної підготовки має стати інтеграція індивідуальної та колективної складових. Ефективність БпС залежить від взаємодії оператора, зовнішніх розрахунків, командирів, засобів розвідки, вогневих засобів, органів управління та інших елементів бойової системи. Тому підготовка повинна переходити від відпрацювання ізольованих навичок до моделювання повного циклу виконання завдання. Колективна підготовка має злагоджувати розрахунки БпС із підрозділами розвідки, управління, вогневого ураження, зв'язку, радіоелектронної боротьби та забезпечення.

Перспективним напрямом є широке застосування технологій імітаційного моделювання, віртуальних тренажерів та цифрових навчальних середовищ. Вони дозволяють відпрацьовувати прийняття рішень у змінній тактичній обстановці, моделювати втрату навігації або зв'язку, вплив засобів радіоелектронної боротьби, обмеження розвідувальної інформації та інші чинники, які складно або небезпечно відтворити під час натурної підготовки. Водночас симуляційні технології мають доповнювати, а не замінювати польову підготовку, оскільки практична експлуатація БпС в умовах реального середовища залишається критично важливою для формування стійких професійних навичок.

Окремої уваги потребує удосконалення системи оцінювання підготовленості фахівців. Пропонуємо оцінювати не лише засвоєння теоретичного матеріалу або виконання окремих технічних нормативів, а комплекс показників, що характеризують здатність військовослужбовця та розрахунку виконувати визначене завдання за призначенням. Така система враховуватиме якість планування та підготовки до виконання завдання, правильність прийняття рішень, стійкість управління, взаємодію з іншими елементами підрозділу, здатність діяти за умов зміни обстановки та ефективність застосування наявних засобів.

Об'єднана підготовка фахівців БпС також передбачатиме регулярне проведення командно-штабних, тактичних і міжвидових навчань із широким залученням БпС до єдиного контуру управління військами. Це забезпечить формування у командного складу практичного розуміння можливостей та обмежень БпС і водночас сприятиме переходу від сприйняття їх як окремого виду технічного забезпечення до розуміння як повноцінного елемента бойової системи.

Важливою складовою розвитку системи підготовки є забезпечення її сумісності з підходами держав-партнерів та стандартами НАТО. Міжнародна взаємодія має охоплювати не лише передачу зразків техніки та проведення окремих навчальних заходів, а й обмін методиками підготовки, підходами до оцінювання спроможностей, досвідом застосування тренажерних комплексів та організації підготовки інструкторів. Водночас імплементація зарубіжного досвіду має здійснюватися з урахуванням національного бойового досвіду та специфіки застосування БпС у російсько-українській війні.

Запропонований підхід до об’єднаної підготовки фахівців БпС доцільно будувати на поєднанні стандартизації базових вимог із гнучкістю змісту підготовки, орієнтації на набуття спроможностей, безперервному врахуванні бойового досвіду, розвитку інструкторського корпусу, інтеграції індивідуальної та колективної підготовки, широкому використанні тренажерних та цифрових технологій і системному оцінюванні готовності до виконання завдань за призначенням. Реалізація такого підходу дозволить сформувати адаптивну систему підготовки, здатну оперативно реагувати на зміни характеру збройного протистояння, технологічний розвиток БпС та трансформацію способів їх бойового застосування.

Перспективним напрямом подальших досліджень вважаємо розроблення моделі компетентностей фахівців БпС та відповідних кваліфікаційних вимог для різних категорій особового складу, а також механізму оперативного трансферу бойового досвіду до освітніх і навчальних програм профільних навчальних центів та вищих військових навчальних закладів. Така модель забезпечуватиме узгодження вимог до підготовки оператора, командира розрахунку, інструктора, командира підрозділу БпС, фахівця з планування та штабного персоналу в єдиній системі підготовки, що зрештою формуватиме спроможність підрозділів БпС діяти як інтегрована складова сил оборони України в багатодоменному операційному середовищі.

Гаврилюк В. В.
Селезенєв А. П.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ СПІЛЬНО ІЗ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ ДЛЯ ЕВАКУАЦІЇ ПОРАНЕНИХ В УМОВАХ ВОГНЕВОГО ВПЛИВУ ПРОТИВНИКА

Повномасштабне вторгнення російської федерації (рф) до України є наймасштабнішим із часів Другої Світової війни. Збройні сили рф (зс рф) почали наступ відразу з кількох напрямів та в перші дні йшли колонами техніки, а також застосовували ракети по мирним містам України. Проаналізувавши 2022-2026 роки видно, що від початку повномасштабної війни й до сьогодення вона пройшла шлях від класичної маневреної та артилерійської війни до високотехнологічного конфлікту на виснаження. Технології вийшли на перший план та зазнають стрімкого розвитку. Сучасне поле бою стрімко насичується новими технологіями, які слугують для більш безпечного та якісного виконання завдань у найбільш небезпечних та недоступних місцях, а також допомагають зберегти життя особового складу.

Одним із ключових напрямів розвитку технологій є наземні роботизовані комплекси (НРК). НРК – це безпілотні платформи, які здатні виконувати різнопланові завдання (бойові, логістичні та евакуаційні), зменшуючи ризик втрат особового складу, особливо в умовах вогневого впливу противника. Проблемою нинішнього етапу війни на багатьох напрямках фронту є ускладнена евакуація поранених з “нуля” або “kill zone” (“зона смерті”), вона є однією із найскладніших задач у військових операціях. Якщо у 2022-2023 роках медична евакуація могла підходити на сотні метрів до бойових позицій, то зараз такі виїзди часто неможливі. “Зона смерті” (kill zone), яка сягає близько 20 кілометрів, перебуває під цілодобовим повітряним наглядом противника, тут зосереджується масований вогонь із засідки або активне ураження за допомогою артилерії, авіації та дронів. Й в цих умовах використання НРК стає найбільш вірогідним способом для вивезення поранених, так як здійснюється без прямого залучення особового складу у зоні підвищеного ризику та дозволяє уникнути додаткових втрат. Керування роботою НРК здійснюється оператором

дистанційно: контроль відбувається через радіоканал або автономні датчики навігації. Для більш успішного виконання завдання, зазвичай НРК працюють в парі з безпілотними літальними апаратами (БпЛА). Перед початком проведення евакуації оператор БпЛА проводить розвідку місцевості, виявляє мінні загородження та позиції противника. Також, БпЛА стають “очима” оператора НРК, оскільки можуть рухатись над ним на висоті 100-300 м, та дозволяють спостерігати за маршрутом переміщення НРК у реальному часі, виконувати дорозвідку та виявляти FPV противника. Це є надзвичайно важливо, оскільки під час застосування вогню противником, на заздалегідь прокладеному маршруті для евакуації пораненого можуть утворюватись вирви, завали дерев й т.п. А це призводить до того, що необхідно переузгоджувати маршрут тут і зараз.

Для евакуації пораненого НРК мають бути обладнані однією із систем фіксації та захисту пораненого:

спеціальні кріплення для нош;

евакуаційні стропи та ремені фіксації;

броньовані евакуаційні капсули.



Рис. 1. Український НРК “Мауль” (Maul)

З урахуванням того, що під час проведення операцій з евакуації пораненого, НРК часто стають ціллю, яка наражається на сильне вогневе ураження противником, – НРК, оснащені броньованими евакуаційними капсулами, стають пріорітетними для масштабування в Збройних Силах України. Вони здатні витримати удари FPV-дронів, забезпечують протикульний захист від стандартних калібрів автоматичної зброї, а також захищають від уламків снарядів під час щільного артилерійського чи мінометного обстрілу. На рис. 1 представлений український НРК “Мауль” (Maul), розроблений компанією DevDroid спільно з Першим окремим медичним батальоном.

Не дивлячись на ряд переваг щодо застосування НРК спільно із БпЛА, є й певні недоліки в роботі, які потребують покращення. Враховуючи досвід бойових дій, можна визначити наступні напрями вдосконалення застосування НРК спільно із БпЛА:

використання адаптивних ходових систем, гібридних силових установок та спеціалізованих підвісок дозволить ефективніше долати складні ділянки місцевості та зменшить ризик втрати мобільності під час евакуації;

використання штучного інтелекту – алгоритми дозволять НРК орієнтуватись без GPS (надзвичайно актуально в тих випадках, коли сигнал може глушитися ворогом). Завдяки поєднанню даних від камер, датчика Lidar, інерційних датчиків та використанню машинного зору – будується маршрут на місцевості без потреби постійного зв'язку з оператором;

інтеграція НРК із БпЛА в єдину систему управління дозволить проводити складні маневри на полі бою, здійснювати обмін розвідувальними даними між операторами БпЛА та НРК у режимі реального часу та поліпшить планування маршруту;

створення стійких каналів управління та передачі даних, яке потребує використання багатоканальних систем зв'зяку, захищених цифрових протоколів та ретрансліторів на баз БпЛА для забезпечення безперервного контролю над НРК на великих дистанціях.

Отже, для НРК головним критерієм є факт успішного вивезення людини із небезпечної ділянки та її перевезення до місця, де знаходиться медична команда. Використання НРК спільно із БпЛА дозволяє скоротити час евакуації пораненого, підвищити ефективність рятувальних операцій та зменшити ризик для військових медиків. Роботизовані платформи стають важливим інструментом у системі евакуації поранених із поля бою.

Павленко В. О.
Сокальський І. М., канд. вет. наук, доц.
Поліський національний університет

СУЧАСНІ ТЕХНОЛОГІЇ У ФОРМУВАННІ КОМПЕТЕНТНОСТЕЙ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ З ОСНОВ НАЦІОНАЛЬНОГО СПРОТИВУ

Сучасна війна стрімко трансформується під впливом новітніх технологій, серед яких особливе місце посідають безпілотні літальні апарати, роботизовані системи, цифрові засоби зв’язку, навігації, спостереження та передавання інформації. Особливо виразно ця тенденція проявилася під час повномасштабної російсько-української війни, у якій безпілотні системи набули широкого застосування на різних рівнях виконання завдань – від тактичного до оперативного. Їх використання для розвідки, спостереження, коригування дій, передавання інформації, ураження цілей та виконання інших завдань за призначенням суттєво впливає на характер сучасних бойових дій і зумовлює подальше технологічне переосмислення безпекового середовища.

Поширення безпілотних та інших дистанційно керованих систем має значення не лише для військової сфери. Технології, що використовуються під час сучасних воєнних конфліктів, безпосередньо впливають на умови перебування цивільного населення та потребують відповідного рівня обізнаності щодо їх можливостей, потенційних загроз і правил безпечної поведінки. У зв’язку з цим технологічна складова підготовки здобувачів вищої освіти набуває особливого значення. Водночас її зміст не повинен ототожнюватися з професійною військовою підготовкою або підготовкою операторів безпілотних систем. Для здобувачів цивільних спеціальностей доцільним є формування базового розуміння призначення, можливостей та обмежень сучасних технологічних систем, а також алгоритмів безпечної поведінки у разі їх використання або виявлення.

Відповідно до програми навчальної дисципліни «Основи національного спротиву», затвердженої наказом Міністерства освіти і науки України від 30 червня 2026 р. № 1002, підготовка здобувачів вищої освіти передбачає формування загальної компетентності «здатність до національного спротиву» та набуття комплексу теоретичних знань і практичних навичок, пов’язаних із

діями в умовах сучасного безпекового середовища. З огляду на технологічну трансформацію сучасних воєнних конфліктів, важливою складовою такої підготовки є формування базової технологічної обізнаності здобувачів щодо сучасних безпілотних і роботизованих систем, засобів зв'язку, навігації, спостереження та передаванні інформації.

У межах проведеного нами аналізу змісту освітньої компоненти «Основи національного спротиву» встановлено, що технологічна підготовка здобувачів доцільно реалізовувати не в межах однієї ізольованої теми, а через взаємопов'язане вивчення декількох напрямів.

Зокрема, тема «Зв'язок та передача інформації» передбачає ознайомлення здобувачів з основними способами зв'язку, правилами радіообміну, використанням радіостанцій малої потужності, засобів супутникового зв'язку, принципами безпечної роботи з цифровими пристроями та захистом інформації. Тема «Сучасні військові технології, роботизація та безпілотні літальні апарати» доповнює цей зміст відомостями про види та призначення безпілотних систем, їх основні конструктивні елементи, канали управління та відеопередавання, навігацію, засоби спостереження, а також базові принципи радіоелектронної розвідки та боротьби.

Такий зміст дає підстави розглядати технологічну підготовку як цілісну систему, у якій окремі технології пов'язані між собою. Для прикладу, функціонування безпілотної системи передбачає використання каналів зв'язку, навігації, передавання даних та засобів спостереження. Тому розуміння здобувачем лише конструкції або призначення БпЛА без усвідомлення ролі зв'язку, навігації та інформаційного обміну не забезпечує цілісного уявлення про сучасне технологічне середовище.

На нашу думку, саме такий системний підхід має бути покладений в основу підготовки здобувачів закладів вищої освіти. Його сутність полягає у формуванні не окремих фрагментарних знань про технічні засоби, а здатності розуміти взаємозв'язок між людиною, технологічною системою та інформаційним середовищем.

На основі аналізу змісту навчальної дисципліни «Основи національного спротиву» обґрунтовано доцільність поєднання теоретичного пояснення технологій із їх візуальною демонстрацією, аналізом ситуацій та виконанням навчально-практичних завдань.

Окремого значення набуває розуміння здобувачами взаємозв’язку між безпілотними системами (БпС) та засобами зв’язку. Радіозв’язок у цьому випадку розглядається не лише як самостійний елемент підготовки, а як складова функціонування сучасних технологічних систем. Здобувач має отримати загальне уявлення про канали управління, передавання інформації та відеоданих, роль навігаційних систем, а також можливість виникнення перешкод або втрати зв’язку.

Важливою складовою є також формування базового розуміння засобів радіоелектронної розвідки та радіоелектронної боротьби. Для здобувача це не передбачає оволодіння професійними методиками їх застосування, а передусім розуміння принципів їх впливу на сучасні технологічні системи. Зокрема, передавання та приймання радіосигналів забезпечує функціонування багатьох таких систем, а їх виявлення, перешкоджання або придушення може впливати на роботу відповідного обладнання. Такі знання необхідні для розуміння можливостей та обмежень сучасних технологій.

Узагальнення результатів аналізу змісту навчальних тем дає змогу визначити чотири взаємопов’язані складові технологічної обізнаності здобувачів: безпілотні та роботизовані системи; зв’язок і передача інформації; навігація та спостереження; технологічна безпека. Взаємопов’язаний розгляд цих складових дає змогу сформувати у здобувачів системне уявлення про сучасні технологічні системи, особливості їх функціонування, можливості та потенційні загрози.

Петраш С. В., канд. техн. наук, доц.
Зелінський О. В.
Коваль М. В.
Житомирський військовий інститут імені С. П. Корольова

ПРОПОЗИЦІЇ ЩОДО УСУНЕННЯ НЕОДНОЗНАЧНОСТІ ВИМІРУ КООРДИНАТ НАЗЕМНИХ ОБ’ЄКТІВ У БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТАХ

У сучасних безпілотних авіаційних комплексах для підвищення роздільної здатності бортових радіолокаційних станцій (РЛС) огляду земної поверхні активно застосовують технологію радіолокації з синтезованою апертурою (РСА).

Перенесення цих результатів з космічних апаратів та літаків до малогабаритних безпілотних літальних апаратів (БпЛА) викликає проблему: виникає неоднозначність вимірювання координат наземних об’єктів.

До причин виникнення неоднозначності можна віднести: малі розміри бортових антенних систем; низьку швидкість польоту БпЛА; наявність збурень маршруту руху за рахунок природних факторів.

Однозначний вимір координат наземних об’єктів спряжений із високою роздільною здатністю. Двовимірна часово-частотна функція розузгодження за когерентного накопичення відбитих від наземних об’єктів сигналах має багатопіковий характер. Це призводить до виникнення просторових накладання зображень різних ділянок місцевості одна на одну, що критично знижує ймовірність виявлення малорозмірних наземних цілей. Проведений аналіз показав, що для усунення цієї невизначеності застосовуються: зміна кутової орієнтації антени; звуження смуги розвідки за дальністю.

Перший підхід передбачає зміну кутової орієнтації антени, що наближує зону спостереження до лінії шляху БпЛА і дозволяє збільшити дистанцію між хибними піками та винести їх за межі інтервалу синтезування. Недоліком є погіршення роздільної здатності за горизонтальною дальністю через малий кут проекції променю на поверхню. Другий підхід полягає у штучному звуженні смуги розвідки за дальністю, що забезпечує повну математичну однозначність виміру. Недоліком є зменшення площі зони розвідки за один прохід, що зменшує інформативність ведення розвідки. Реалізація такого підходу вимагає зниження висоти польоту БпЛА або збільшення розміру антенної системи. Перший варіант реалізації збільшує ризик вогневого ураження БпЛА, другий – погіршує його масо-габаритні показники.

Пропонується змінювати період випромінювання імпульсів в залежності від висоти польоту БпЛА. Знаючи розміри зони опромінення поверхні, можливо визначити період слідування імпульсів для однозначного виміру координат за горизонтальною та шляховою дальністю. Проведені розрахунки дозволять застосовувати їх як апріорні дані для управління періодом формування зондувальних імпульсів радіопередавального пристрою БпЛА.

У процесі польоту в атмосфері Землі БпЛА підлягає збуренням за рахунок переміщення повітряних мас та турбулентності повітря. Пропонується враховувати такі фактори шляхом використання в РСА малогабаритної бортової

інерціальної та супутникової систем навігації. За допомогою навігаційних систем в реальному часі з високою точністю фіксуються просторові мікропереміщення фазового центру антени під дією атмосферних переміщень. На основі цих даних та рельєфу бортовий обчислювач БпЛА може динамічно вносити корективи у визначення періоду слідування імпульсів. Це дозволить забезпечити однозначність та точність виміру координат без звуження робочої смуги огляду БпЛА. Таким чином, проведений аналіз перерізів тіла невизначеності показує, що вона має у межах інтервалу однозначності багатопіковий характер за шляховою дальністю.

Наближення зони спостереження до лінії шляху не усуває неоднозначність вимірювання шляхової дальності і значно погіршує роздільну здатність за горизонтальною дальністю.

Зменшення розмірів зони спостереження забезпечує однозначність вимірювання координат, як за шляховою, так і за горизонтальною дальністю, але при цьому значно обмежується зона спостереження за горизонтальною дальністю. Пропонується використовувати апріорні дані щодо періоду слідування зондувальних імпульсів для однозначного виміру координат на різних висотах польоту БпЛА. Поточну корекцію пропонується проводити врахуванням атмосферних змін від систем навігації та цифрової карти місцевості.

Горбач В. Я., Ph. D.
Горбач Т. П.
Житомирський військовий інститут імені С. П. Корольова

ВПЛИВ ГЕОМЕТРИЧНИХ ХАРАКТЕРИСТИК ОБ’ЄКТА НА ВИБІР ОПТИМАЛЬНОГО КУТА СПОСТЕРЕЖЕННЯ З БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Досвід застосування безпілотних літальних апаратів (БпЛА) підтвердив їх важливу роль у веденні повітряної розвідки. Ефективність розпізнавання об’єктів залежить не лише від технічних характеристик оптико-електронної системи, а й від ракурсу спостереження за об’єктами. Зміна напрямку польоту БпЛА впливає на видиму проєкцію об’єкта та кількість розвідувальних ознак. За наявності попередньої інформації про район виконання завдання, ймовірний

тип і характеристики об’єкта розвідки існує можливість обґрунтувати оптимальний кут його повторного спостереження. Це особливо важливо після першого виявлення, коли маршрут БпЛА у подальшому може бути скоригований для отримання зображення з іншого ракурсу.

Для формалізації завдання в математичному вигляді горизонтальну проєкцію об’єкта доцільно представити у вигляді прямокутника із відомими довжиною та шириною. Його геометрична проєкція буде змінюватись в залежності від напрямку спостереження відносно поздовжньої осі. Таким чином об’єкти із різним співвідношенням сторін по-різному змінюють видиму проєкцію за однакового кута спостереження з БпЛА. Тому геометричні характеристики доцільно розглядати, як вихідні дані для визначення оптимального кута повторного спостереження об’єкта після першого. Інтегральна ймовірність розпізнавання об’єкта враховуватиме кут між двома спостереженнями та матиме більше значення через взаємодоповнюваність двох спостережень одного об’єкта. Проте збільшення кута між напрямками спостережень не завжди забезпечує підвищення ймовірності розпізнавання, оскільки ефективність кожного спостереження залежить від геометрії об’єкта.

Результати розрахунків свідчать, що значення інтегральної ймовірності розпізнавання залежить від співвідношення геометричних розмірів цілі. Наприклад, для об’єкта із розмірами 3×6 м розрахунковий оптимальний кут повторного спостереження становить близько 26°, а максимальна інтегральна ймовірність розпізнавання – близько 0,879 а для об’єкта – 4×9 м оптимальний кут повторного спостереження збільшується приблизно до 29,8°, а максимальна ймовірність – до 0,883.

Практичне застосування запропонованого підходу передбачає використання попередньої інформації про район виконання завдання та ймовірний тип об’єкта за критерієм максимізації інтегральної ймовірності розпізнавання. Після першого виявлення об’єкта оцінюються його геометричні характеристики та визначається оптимальний кут повторного спостереження. Отримане значення може бути використане, як вихідний параметр для коригування маршруту БпЛА. Таким чином, урахування геометричних характеристик об’єкта дозволяє обґрунтовано визначати кут для його повторного спостереження з БпЛА з метою підвищення ефективності планування повітряної розвідки з БпЛА.

Оверчук С. П.
Пількевич І. А., д-р техн. наук, проф.
Житомирський військовий інститут імені С. П. Корольова

ПІДВИЩЕННЯ ТОЧНОСТІ НАВІГАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ ШЛЯХОМ НЕЙРОМЕРЕЖЕВОЇ КОМПЕНСАЦІЇ ПОХИБОК

Сучасні умови застосування розвідувальних безпілотних літальних апаратів (БпЛА) характеризуються активним використанням противником засобів радіоелектронної боротьби (РЕБ), спрямованих, зокрема, на порушення функціонування навігаційних систем. Особливу проблему становить подавлення або втрата сигналів глобальних навігаційних супутникових систем (GNSS), які використовуються для періодичної корекції інерціального навігаційного розв’язку.

У разі втрати GNSS навігаційна система переходить до автономної роботи на основі інформації від інерціальних вимірювальних пристроїв. При цьому похибки визначення параметрів руху накопичуються внаслідок похибок акселерометрів і гіроскопів, їх зміщень та дрейфів, похибок початкових умов і впливу динаміки руху БпЛА. За тривалої відсутності зовнішніх навігаційних вимірювань це призводить до поступового зростання навігаційної похибки.

Для оцінювання навігаційного стану доцільно використовувати фільтр помилок на основі розширеного фільтра Калмана (Error-State Extended Kalman Filter, ESKF). Він забезпечує оцінювання похибок навігаційного розв’язку та параметрів похибок інерціальних датчиків. Проте можливості ESKF щодо компенсації накопичуваних похибок обмежені за тривалої відсутності зовнішніх навігаційних вимірювань.

Перспективним напрямом підвищення точності автономної навігації є використання методів машинного навчання для прогнозування накопичення навігаційних похибок. Нейромережеві моделі дають змогу враховувати нелінійні залежності між параметрами руху та часовою історією їх зміни.

Для розв’язання цієї задачі запропоновано гібридну архітектуру ESKF – NARX – ELM, яка поєднує ESKF, нелінійну авторегресійну модель із зовнішніми входами (Nonlinear Autoregressive with Exogenous Inputs, NARX) та

нейромережу з екстремальним навчанням (Extreme Learning Machine, ELM). ESKF залишається базовим алгоритмом оцінювання навігаційного стану, а NARX – ELM виконує функцію зовнішнього модуля прогнозування накопичуваних похибок.

В основі запропонованої архітектури лежить послідовне використання часової інформації навігаційного процесу. Інформація від інерціальних вимірювальних пристроїв надходить до інерціальної навігаційної системи (ІНС), де формується первинний навігаційний розв'язок. ESKF здійснює оцінювання стану та похибок системи, після чого поточні й попередні навігаційні параметри формують часову вибірку для нейромережевого модуля.

NARX враховує часову залежність навігаційної інформації та попередню історію зміни параметрів руху і похибок. На основі сформованої часової вибірки ELM забезпечує нелінійну апроксимацію залежності між навігаційними параметрами та похибками ІНС. У результаті формується прогноз окремих складових похибки, насамперед похибок координат і швидкості, який використовується для додаткової компенсації навігаційного розв'язку.

Функціонування запропонованої архітектури передбачає два режими. За наявності GNSS супутникова інформація використовується для корекції інерціального розв'язку та оцінювання похибок за допомогою ESKF. На цій основі формується інформація для навчання та налаштування NARX – ELM. Після втрати або деградації GNSS система переходить до автономного режиму, у якому ESKF продовжує формувати навігаційний розв'язок, а NARX – ELM прогнозує накопичувані похибки за доступною часовою інформацією.

Принципово важливо, що прогноз NARX – ELM не використовується як псевдовимірювання для ESKF. Нейромережевий модуль не замінює процедуру оцінювання стану та не формує альтернативний навігаційний фільтр. Його призначення полягає у прогнозуванні окремих складових накопичуваних похибок і подальшій компенсації навігаційного розв'язку.

Запропонована архітектура орієнтована на програмно-математичне вдосконалення навігаційного забезпечення БпЛА І класу. Її особливістю є можливість доповнення існуючого алгоритму ESKF без принципової зміни його базової структури, що створює передумови для подальшої реалізації нейромережевого модуля на бортовій обчислювальній платформі БпЛА.

Подальші дослідження будуть спрямовані на оптимізацію кількості часових затримок NARX, визначення оптимальної архітектури ELM,

формування навчальних і тестових вибірок на основі реальних польотних даних, а також математичне моделювання та експериментальне оцінювання точності прогнозування і ефективності запропонованої архітектури.

Соломатін Д. О., канд. військ. наук, ст. наук. співроб.
Седляр А. А., канд. військ. наук, ст наук. співроб.
Центральний науково-дослідний інститут
Збройних Сил України

АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ ТА МОЖЛИВОСТЕЙ УДАРНИХ FPV-ДРОНІВ І МУЛЬТИКОПТЕРІВ ЗІ СКИДАМИ

Узагальнений аналіз особливостей застосування ударних fpv-дронів та мультикоптерів зі скидами показує, що до переліку основних факторів, які впливають на характер загроз зразкам ОВТ на полі бою від цих БпЛА, слід віднести:

політ на гранично малих висотах на фоні складно пересіченого рельєфу місцевості. Цей фактор зазвичай негативно впливає на своєчасність виявлення та ураження повітряних цілей і зумовлює необхідність формування загроз, спрямованих на перевірку спроможностей засобів виявлення КАЗ (КГАЗ) щодо селекції та ідентифікації цілей з надмалою ефективною площею розсіювання на фоні місцевих перешкод;

використання у складі цільового навантаження оптико-електронного обладнання, що дозволяє виявляти зразки ОВТ на значних віддаленнях. Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку спроможностей КАЗ (КГАЗ) щодо виявлення та знищення цих БпЛА на максимальних дальностях;

зависання (для мультироторних БпЛА) над об’єктом удару. Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку спроможностей радіолокаційних засобів КАЗ (КГАЗ) виявляти як рухомі повітряні цілі, так і тих, що зависають;

швидке змінювання траєкторії польоту (як за напрямком, так і висотою). Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку якості програмного забезпечення КАЗ (КГАЗ) (відсутності зривів автосупроводження цілей, відсутності суттєвих затримок у формуванні трас та

їх переплутування під час маневру цілей, виключення можливості формування та видачі неправильних цілевказань тощо);

нанесення ударів як по настильній траєкторії із різних напрямків, так і з пікірування. Ці фактори зумовлюють необхідність формування загроз, спрямованих на перевірку спроможностей КАЗ (КГАЗ) щодо створення суцільної зони захисту з усіх ракурсів як у горизонтальній проекції, так і у верхній напівсфері;

здатність уражати як стаціонарні, так і рухомі цілі. Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку спроможностей КАЗ (КГАЗ) щодо виявлення та ураження цілей за умов, коли зразок ОВТ, що захищається, перебуває як у стаціонарному положенні так і у русі;

автономність застосування (без втручання оператора, з використанням штучного інтелекту та машинного зору, з можливістю нанесення удару по раніше запам’ятованих координатах цілі за умов її візуальної втрати). Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку доцільності використання у складі КАЗ (КГАЗ) засобів радіоелектронного подавлення і маскування димами (аерозолями) та ефективності застосування засобів кінетичного впливу (вогневих модулів, сіткометів тощо);

застосування із режиму очікування на землі у безпосередній близькості від зразків ОВТ. Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку спроможностей КАЗ (КГАЗ) щодо виявлення та ураження повітряних цілей, що з’являються раптово, у тому числі з нижньої півсфери (з напрямків, які за висотою нижче опорної поверхні), перевірку достатності часу реакції комплексу, відсутності “сліпих” ділянок у його ближніх зонах виявлення та ураження тощо;

здатність діяти групами (у складі 2–3 апаратів з короткими дистанціями між ними). Цей фактор зумовлює необхідність формування загроз, спрямованих на перевірку спроможностей КАЗ (КГАЗ) щодо протидії груповим ударам (як з одного, так і з різних напрямків);

можливість комплексного вогневого впливу по зразку ОВТ БпЛА різного типу (наприклад, fpv-дронів та баражуючих боєприпасів). Цей фактор зумовлює необхідність формування загроз, спрямованих переважно на ураження зразків ОВТ, що оснащені захисними екранами, або тих, що перебувають в укритті. Окрім того, аналіз можливостей fpv-дронів та мультикоптерів зі скидами

показав, що до переліку основних факторів, які впливають на характер загроз зразкам ОВТ на полі бою від цих БпЛА, належать:

дальність польоту – до 30 км (для деяких зразків – до 100 км), швидкість польоту – на рівні 60–200 км/год (16–56 м/с), висота польоту – до 5000 м (для деяких зразків – до 7000 м), тривалість польоту – до 30 хв. (у більшості випадків);

особливості польоту: на основному етапі – висота 70 м (в середньому) зі швидкістю 80–100 км/год (22–28 м/с); на кінцевому етапі (під час підльоту до цілі) – зниження висоти та зменшення швидкості залежно від радіогоризонту та характеру цілі;

дальність виявлення цілей: для fpv-дронів – 250–600 м (з висоти 150–200 м); для мультикоптерів зі скидами – до 2 км (для деяких зразків – до 5 км);

дальність ідентифікації цілей: для fpv-дронів – 100–400 м; для мультикоптерів зі скидами – 400–700 м;

вага боєприпасів (БЧ) – від 0,5 до 5 кг;

максимальна зона суцільного ураження (для осколкових, осколково-фугасних, термобаричних БЧ) – до 15 м; бронепробиття – до 600 мм (для кумулятивних БЧ);

кількість ударних fpv-дронів із зарядом кумулятивної дії для нанесення ураження зразку ОВТ – від 5 і більше (залежно від типу броні і додаткового захисту);

середня кількість атак по зразку ОВТ, що призводить до його ураження: для броньованої техніки, що обладнана додатковим антидроновим захистом – 5–10; небронювана автомобільна техніка – 1–2;

необхідність завчасного надходження цілевказань від розвідувальних БпЛА для точного виходу на ціль, що зумовлено обмеженими можливостями відеокамер більшості БпЛА щодо виявлення та ідентифікації зразків ОВТ;

незначні габаритні розміри, що значно ускладнює їх виявлення та ураження.

На основі аналізу даних щодо досвіду застосування противником малорозмірних ударних БпЛА, що надані підрозділами СВ ЗС України, встановлено наступні особливості їх польоту:

для ударних fpv-дронів мультикопторного типу: на основному етапі – політ на висотах 150–300 м із крейсерською швидкістю 65–75 км/год під кутом нахилу близько 15°; на етапі атаки – перехід у динамічне пікірування зі зниженням висоти до 50–100 м і підвищенням швидкості до 75–90 км/год. Кут атаки становить до 20–35°, що дозволяє уражати техніку у верхні, менш захищені проекції;

для багаторазових мультикоптерів зі скидами: на основному етапі – політ на висотах 50–300 м зі швидкістю 20–70 км/год; на етапі атаки –зниження швидкості до нуля та скидання боєприпасів під кутом 90° із положення зависання над ціллю (вертикальний удар). Це дозволяє уражати статичні цілі через відкриті люки або вразливий дах корпусу.

Основні особливості застосування fpv-дронів і мультикоптерів зі скидами, визначені за досвідом підрозділів Сил безпілотних систем ЗС України, наведені у табл. 1.1.

Проведений аналіз дозволив також визначити певні специфічні особливості застосування противником fpv-дронів мультикоптерного типу з різним типом керування (радіокерованих та з управлінням на оптоволокні), а саме:

для радіокерованих fpv-дронів: на основному етапі – політ на висотах

150–300 м при швидкості до 120 км/год; на кінцевому етапі – нанесення удару з висот 100–150 м при швидкості 200 км/год та кутах атаки 30–90о. Загальна протяжність маршруту зазвичай становить 20–40 км. Застосування радіокерованих fpv-дронів вимагає прокладати маршрут в обхід зон дії радіотехнічних засобів, комплексів радіоелектронної боротьби (РЕБ) та дотримуватись висот польоту для забезпечення видимості в межах радіогоризонту.

для fpv-дронів на оптоволокні – наднизький політ на гранично малих висотах (до 70 метрів) при швидкості 40–90 км/год; на кінцевому етапі – нанесення удару з висот 1–15 метрів (фактично на рівні контуру техніки) при збільшенні швидкості до 100–160 км/год. Загальна протяжність маршруту зазвичай становить 15–20 км, що зумовлено довжиною оптоволоконного кабелю та і більш обережним маневруванням. Застосування БпЛА на оптоволокні дозволяє не зважати на радіогоризонт, здійснювати політ з огинанням рельєфу місцевості на значно нижчих висотах та більш вибірково атакувати зразків ОВТ у найбільш уразливі та (або) ключові зони.

Таким чином, з огляду на можливості застосування fpv-дронів і мультикоптерів зі скидами, загрози зразкам ОВТ від них формуються на основі таких параметрів:

для зразків ОВТ, що захищаються КГАЗ на основному етапі польоту, – поодинокі та групові дії БпЛА, що здійснюють горизонтальний політ з незначним маневруванням за курсом та висотою на гранично малих висотах (100–600 м) та на дальностях, з яких ці БпЛА спроможні самостійно виявляти

цілі, починають перетинати дальню межу зони виявлення (6 км) і перебувають в її середині (на віддаленнях 1,5–6 км від зразка ОВТ) здійснюючи політ на середніх швидкостях (80–100 км/год (22–28 м/с));

для зразків ОВТ, що захищаються КГАЗ та КАЗ на кінцевому етапі польоту, – поодинокі та групові дії БпЛА, що здійснюють горизонтальний політ з різким (для мультикоптерів) маневруванням на гранично малих (100–300 м і нижче) висотах та з дальностей, з яких вони починають ідентифікувати ціль (400–700 м), атакувати її з настильних траєкторій, з верхньої півсфери (під кутами 100–870) та (або) з нижньої півсфери (з висот, нижчих за опорну поверхню), підлітаючи до цілі на малих швидкостях 60–70 км/год (16–20 м/с), зависати над ціллю з нульовою швидкістю і здійснювати скиди з висот до 60 м (для мультикоптерів).

З огляду на практичний досвід застосування fpv-дронів і мультикоптерів зі скидами, загрози зразкам ОВТ доцільно скоригувати з урахуванням таких параметрів:

для ударних fpv-дронів мультикопторного типу: на основному етапі – політ на висотах 150–300 м із крейсерською швидкістю 65–75 км/год (18–21 м/с); на кінцевому етапі – перехід у динамічне пікірування зі зниженням висоти до 50–100 м і підвищенням швидкості до 75–90 км/год при кутах атаки 20–35°;

для багаторазових мультикоптерів зі скидами: на основному етапі – політ на висотах 50–300 м зі швидкістю 20–70 км/год; на кінцевому етапі – зниження швидкості до нуля та скидання боєприпасів під кутом 90° із положення зависання над ціллю (вертикальний удар).

Слід також зазначити, що важливим фактором, який слід обов’язково враховувати під час формування параметрів (сценаріїв) загроз зразкам ОВТ від разових fpv-дронів (мультикоптерного та літакового типу), є те, що їх швидкість на кінцевому етапі польоту може як знижуватися (для ураження нерухомих цілей) так і підвищуватися (для ураження рухомих цілей).

Луцевят О. І.
Попков С. Б.
Центральний науково-дослідний інститут
Збройних Сил України

ТРАНСФОРМАЦІЯ ФОРМ І СПОСОБІВ БОЙОВОГО ЗАСТОСУВАННЯ УДАРНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ВІДПОВІДНО ДО ЕВОЛЮЦІЇ ЇХ ЕЛЕМЕНТНОЇ БАЗИ

Аналіз застосування ударних безпілотних апаратів (БпЛА), а також їх еволюція свідчить, одним із ключових чинників, який впливає на форми і способи бойового застосування ударних БпЛА є технічні обмеження їх конструкції та складу, що зумовлені використаною елементною базою.

Безпрецедентне використання значного переліку елементів цивільного призначення, які маючи високі технічні та експлуатаційні показники, а також суттєву апаратну та програмну сумісність дозволяють створювати високо адаптивні сучасні зразки озброєння та військової техніки (ОВТ). Тому, саме завдяки сучасним технічним рішенням, існує можливість розширювати (змінювати) цільове призначення БпЛА та перелік завдань до яких вони залучаються, а також забезпечувати вищий рівень ефективності.

Так, до прикладу, стійкість БпЛА до засобів радіоелектронної боротьби (РЕБ) та навігація, що забезпечуються використанням сучасної елементної бази, дозволяють застосовувати БпЛА методом глибоких автономних ударів в умовах повного придушення супутникового зв'язку та навігації. Натомість, спрощена елементна база змушує обмежувати радіус дії, використовувати апарати лише як “хибні цілі” або засоби виснаження системи протиповітряної оборони.

Також, способи застосування БпЛА суттєво відрізняються залежно від того, чи здійснює БпЛА політ автономно, чи під постійним або частковим управлінням оператора. Елементна база з підтримкою обчислень на борту БпЛА дозволяє реалізувати спосіб його застосування “вистрілив та забув”, за якого апарат самостійно виконує політ в район цілі, виявляє (ідентифікує) та уражає її. Зазначене, нівелює потребу в постійному каналі зв'язку, захищає розрахунок БпЛА від виявлення засобами радіоелектронної розвідки, а також дозволяє здійснювати синхронізовані за часом та місцем удари цілі.

Вплив технічних рішень (елементної бази) БпЛА на форми та способи їх

застосування доцільно розглянути на прикладі двох найбільш революційних засобів сучасної війни – ударних fpv-БпЛА (fpv strike drones) та баражуючих боєприпасів великої дальності (One-Way Attack UAVs). Саме цивільна елементна база, зокрема китайського виробництва, змінила архітектуру БпЛА та перетворила поодинокі технологічні рішення на засіб масового терору в оперативній (оперативно-стратегічній) глибині та високоточного ураження широкого переліку цілей в тактичній (оперативно-тактичні) глибині.

Елементна база є технологічним фундаментом, який обмежує або розширює тактичні можливості зразка ОВТ. Вона визначає, чи буде ударний БпЛА простим дистанційно керованим снарядом (протитанковим засобом) із радіусом дії кілька кілометрів, чи перетвориться на автономну інтелектуальну зброю стратегічного значення, здатну діяти в умовах щільної протидії сучасних систем протиповітряної оборони та РЕБ.

Відтак, еволюція елементної бази прямо пропорційно трансформує форми (поодинокі, групові, системні, мережецентричні) та способи (пряме керування, автономне полювання, інтеграція в розвідувально-вогневі контури тощо) застосування БпЛА.

Засядько А. А., д-р техн. наук, проф.
Стригун В. В.
Барвінок Р. Д.
Швець С. І.
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки

ТЕСТУВАННЯ АНТЕН ІЗ КЕРОВАНОЮ ДІАГРАМОЮ СПРЯМОВАНОСТІ ЗА ДОПОМОГОЮ ЛАБОРАТОРНИХ ВИПРОБУВАЛЬНИХ СТЕНДІВ

Особливе місце в дослідженнях займають антени з керованою діаграмою спрямованості прийому (CRPA). Корекція діаграмою спрямованості у напрямку джерел завад дозволяє суттєво підвищити співвідношення сигнал/шум на вході приймача.

Для систем геодезичної прив’язки, куди інтегрується CRPA як елемент завадостійкого позиціонування, CRPA слід оцінювати у категорії збереження фазових або часових настройок певної точності. Тому засоби протидії завадам CRPA не мають спотворювати засоби отримання навігаційних даних.

Належне тестування CRPA є складним і дороговартісним процесом завдяки перехресним перешкодам у трактах і залежними від напрямку на джерело навігаційного сигналу амплітудно-фазовими похибками. Багатоантенне отримання сигналів та динамічне коригування обробки сигналів в режимі реального часу змінюють не тільки завадостійкість, а й поведінку самого приймача. Тому системи тестування CRPA повинні бути функціональними, простими у використанні і дозволяти проводити повторювані тести з імітацією загроз, які важко відтворити навіть у польових умовах.

Для конкретної задачі перевірки CRPA обирається оптимальний тип тестування: якщо перевіряється лише електроніка антенної системи, моделювання хвильового фронту справді часто виграє у швидкості й повторюваності; якщо потрібно оцінити просторове розташування та взаємний зв’язок елементів (архітектуру антени), фазові центри та інтегровану систему — обирається тестування в безлунній камері; якщо потрібна зовнішня валідація в реальній динаміці — обираються польові випробування.

Лабораторні випробувальні стенди дозволяють випробовувати алгоритми в керованому середовищі. Система моделювання хвильового фронту є найдешевшим варіантом, якщо врахувати усі змінні, проте лабораторне тестування не можна замінити іншими видами тестування, що підтверджується науковими дослідженнями.

Протокол випробувань має містити не тільки сценарії протидій заглушенню, а й серію фазово-орієнтованих перевірок: статичне позиціонування – визначення курсу до ввімкнення просторової обробки; статичне позиціонування під вузькосмуговими, широкосмуговими завадами та імітуючимими вплив спуфінгу; порівняння похибки геоприв’язки цілі до та після включення CRPA; оцінювання відхилення курсу рухомого об‘єкта під дією РЕБ; перевірку часу фіксації після короткочасної втрати сигналу; аналіз залишкової похибки, пов’язуючи антенно-алгоритмічний рівень із похибкою навігаційних даних.

Наведемо мінімальний перелік контрольних експериментів:

еталонний сигнал без завади, у якому визначають власний шум, міжканальну когерентність і стабільність фази системи.

серія дослідів з однією завадою (single-jammer sweep), коли послідовно змінюється її кут приходу, потужність і тип модуляції.

серія дослідів з вимкненою та увімкненою адаптивною обробкою (weight on/off comparison) для відокремлення ефекту решітки від ефекту алгоритму.

серія дослідів з перестановкою каналів та заміною кабелів (channel permutation / cable swap test), яка допомагає виявити приховану несиметрію тракту, що утворює нев’язки несучої фази – різницю між фактично виміряною фазою сигналу від супутника та розрахованою (теоретичною) фазою, обчисленою на основі передбаченого положення приймача.

Ієрархія тестування повинна охоплювати такі рівні: компонентний рівень для перевірки роботи елементів антени; рівень тракту для перевірки передавачів і приймачів антени;системний рівень для дослідження діаграми спрямованості; експлуатаційний рівень (вплив CRPA в реальному середовищі з урахуванням завад)

Висновки: перевірка на різних етапах – від окремого каналу (наприклад, радіометричного) до всієї системи в цілому під впливом різних температур або сигнальних навантажень та зонування контролю для ідентичного калібрування кожного каналу антени відповідно до конкретних зон контролю, забезпечуватиме високу точність технічних характеристик антени з керованою діаграмою спрямованості.

Винту А. О.
Волощук Т. Ю.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ОПТИМІЗАЦІЯ СТРУКТУРИ ТА ТЕХНОЛОГІЧНОГО ОСНАЩЕННЯ РУХОМОГО КОМПЛЕКСУ ОБСЛУГОВУВАННЯ ТА РЕМОНТУ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

Інтенсивне бойове застосування безпілотних авіаційних комплексів супроводжується накопиченням механічних пошкоджень безпілотних повітряних суден, відмовами електроніки під дією засобів радіоелектронної боротьби та деградацією елементів живлення. Традиційна система технічного забезпечення передбачає евакуацію пошкоджених апаратів на стаціонарні підприємства тилу, що призводить до тривалого простою техніки та зниження бойової готовності підрозділів. Наявні рухомі майстерні автомобільного чи бронетанкового типу розроблялися для важких слюсарних робіт і позбавлені обладнання для точної пайки поверхнево-змонтованих елементів, тривимірного

друку або захисту від статичної електрики. Виникає науково-технічна суперечність між високими вимогами до відновлення складних безпілотних авіаційних систем та реальними можливостями польових засобів технічного обслуговування.

Метою дослідження є наукове обґрунтування тактико-технічних вимог, компонувальної організації та технологічного оснащення рухомого комплексу технічного обслуговування і ремонту для оперативного відновлення безпілотних авіаційних комплексів у польових умовах.

Ефективне застосування рухомого комплексу обслуговування та ремонту БпАК визначається нормативними критеріями готовності до роботи, тривалої автономності, високої мобільності та живучості. Його граничний радіус дії розраховується на основі балансу часу робочого циклу з урахуванням швидкості руху, тривалості відновлювальних робіт та оперативності розгортання. Для підвищення захищеності обслуги та обладнання використовується повнопривідне автомобільне шасі з каркасно-панельним бронюванням, протимінними сидіннями та засобами радіоелектронного й світлового маскування. Інтеграція вантажно-розвантажувального гакового механізму дає змогу відокремлювати робочий модуль від шасі, що знижує помітність комплексу на місцевості та розширює його функціональну гнучкість.

Просторову оптимізацію розміщення технологічного обладнання всередині тришарового ізотермічного кузова-контейнера реалізовано за допомогою багатокритеріального математичного алгоритму на основі генетичних методів. Цільова функція мінімізує сумарний час виконання ремонтних операцій та відхилення центра мас від центра шасі при жорсткому дотриманні обмежень на взаємне неперетинання елементів. Це дає змогу зменшити внутрішні переміщення обслуги на чверть та забезпечити стабільність транспортного засобу під час руху бездоріжжям.

Технологічне оснащення комплексу містить чотири ключові субсистеми. Інженерний сегмент містить бортовий дизельний генератор потужністю тридцять кіловат, літій-залізо-фосфатний накопичувач енергії, прецизійний кондиціонер, автономний обігрівач та триступеневу систему фільтровентиляції, яка створює надлишковий тиск у приміщенні. Адитивний та металообробний сегмент оснащено принтерами пошарового наплавлення та фотополімеризації, оптичним тривимірним сканером високої точності, компактним фрезерним верстатом із програмним керуванням для обробки карбону й алюмінію, а також прецизійним токарним верстатом. Лабораторію мікроелектроніки організовано

з дотриманням вимог антистатичного захисту, вона включає індукційну паяльну станцію, стереоскопічний мікроскоп, чотириканальний цифровий осцилограф, аналізатор спектра радіочастот та універсальні програматори. Акумуляторний сегмент забезпечує діагностику та збирання елементів за допомогою багатоканальних зарядних станцій й апарата точкового контактного зварювання із дотриманням суворих заходів пожежної безпеки.

Оцінка ефективності свідчить, що впровадження комплексу підвищує коефіцієнт технічної готовності парку безпілотної авіації до рівня вісімдесяти п’яти – дев’яноста відсотків, скорочуючи цикл повернення пошкодженої техніки у стрій до кількох годин. Забезпечується відновлення щонайменше трьох чвертей пошкоджених апаратів безпосередньо у зоні виконання завдань, а очікуваний термін окупності капітальних витрат становить менше одного року активної експлуатації.

Майборода Ю. М.
Науково-дослідний центр ракетних військ і артилерії

ТРАНСФОРМАЦІЯ БЕЗПІЛОТНИХ СИСТЕМ СИЛ ОБОРОНИ УКРАЇНИ: ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ПЕРЕХІД ДО АВТОНОМНОСТІ

Сучасне операційне середовище зазнало фундаментальних трансформацій, перетворивши повномасштабну технологічну війну на унікальне протистояння робототехніки, алгоритмів та інженерної думки. Сили оборони України (СОУ) першими у світовій історії сформували окремий рід сил - Сили безпілотних систем, вивівши застосування дронів на стратегічний рівень. У ситуації, коли традиційні супутникові навігаційні системи (GPS) та радіоканали зв’язку перебувають під постійним тиском засобів радіоелектронної боротьби (РЕБ) противника, критичного значення набуває інтеграція штучного інтелекту (ШІ) та перехід до автономності безпілотних систем.

Впровадження технологій ШІ в безпілотні літальні апарати (БпС) - це не просто модернізація, а єдиний дієвий спосіб зберегти життя особового складу, подолати ворожий РЕБ та забезпечити асиметричну перевагу над чисельно переважаючим противником.

Станом на 2026 рік використання дронів Силами оборони досягло безпрецедентних масштабів: лише за один місяць підрозділи виконують понад 440 тисяч бойових та логістичних завдань. Застосування охоплює три ключові середовища:

1. Повітряне: від мікро- та FPV-дронів тактичного рівня до важких бомбардувальників і далекобійних БпЛА стратегічного радіуса дії. Особливого розвитку набули інноваційні дрони-перехоплювачі (на кшталт комплексів типу Skyfall P1), призначені для дешевого знищення ворожих розвідників та ударних БпЛА.
2. Морське: безекіпажні морські надводні та підводні човни повністю змінили архітектуру безпеки в Чорному морі, ізолювавши флот противника.
3. Наземне: масово впроваджуються наземні роботизовані комплекси (НРК), які щомісяця виконують десятки тисяч місій із мінування, вогневого ураження, підвезення провізії та евакуації поранених із зони безпосереднього вогневого контакту.

Можливості та переваги технологій ШІ та автономності у БпС. Впровадження елементів ШІ та машинного зору на борту дронів відкриває перед СОУ принципово нові тактичні можливості:

- Стійкість до РЕБ (Термінальне наведення): ШІ-модуль автоматичного донаведення дозволяє оператору лише вказати ціль на екрані. На фінальній ділянці польоту (останні 500–2000 метрів) дрон повністю розриває зв’язок із пультом керування та автономно супроводжує і вражає об'єкт, ігноруючи будь-яке радіоелектронне придушення.
- Автоматичне розпізнавання цілей (ATR): інтегровані нейромережі здатні самостійно ідентифікувати та класифікувати замасковані об’єкти (танки, артилерію, ППО) в режимі реального часу, знижуючи когнітивне навантаження на людину.
- Навігація без GPS: використання оптичної навігації за рельєфом місцевості (співставлення відеопотоку з бортової камери з цифровою картою), що дозволяє далекобійним БпЛА точно виходити на цілі в глибині території ворога за повної відсутності супутникових сигналів.

Перспективи розвитку:

1. Еволюція концепції «Рою дронів»: перехід від індивідуального керування до скоординованих груп автономних систем. Один дрон-розвідник із ШІ наводить групу ударних БпЛА, які самостійно розподіляють між собою цілі та одночасно атакують позиції з різних напрямків.
2. Роботизована контрбатарейна боротьба та перехоплення: створення повністю автономних повітряних заслонів, де ШІ-перехоплювачі патрулюють

зони у режимі «вільного полювання», самостійно виявляючи та таранячи ворожі розвідувальні крила.

3. Повна автоматизація логістичного ланцюжка: інтеграція наземних та повітряних безпілотних платформ у єдині цикли без участі людини (наприклад, автономна доставка боєприпасів роботом на передову за запитом з інформаційної системи).

Обмеження та виклики:

- Попри колосальний потенціал, масове розгортання автономного ШІ на фронті стикається з низкою суворих технологічних та експлуатаційних бар’єрів:
- Обчислювальні потужності та вартість: повна автономність вимагає встановлення на борт потужних мікропроцесорів для обробки відеопотоку нейромережами. Це здорожує конструкцію дрон-систем, які за своєю суттю мають залишатися дешевим розхідним матеріалом. Україна вирішує це розробкою малих оптимізованих ШІ-моделей, здатних працювати на мікрочіпах вартістю до кількох десятків доларів.
- Етично-правовий бар’єр та втрата контролю: Передача права на відкриття вогню та ліквідацію об’єктів повністю автономній машині (без фінального підтвердження людиною в контурі управління — Human-in-the-loop) викликає жорсткі міжнародні дискусії та несе ризики неконтрольованої ескалації чи ураження цивільних об’єктів. Наразі СОУ переважно використовують напіввідкриту модель, де ШІ допомагає утримувати ціль, але рішення про атаку приймає людина.

Досвід Сил оборони України у застосуванні безпілотних систем довів, що майбутнє глобального воєнного мистецтва належить алгоритмам та автономності. Штучний інтелект у БпС успішно долає обмеження, пов’язані з радіоелектронним придушенням, перетворюючи кожну одиницю зброї на високоефективний інструмент. Разом із тим, технологічні обмеження мікрочіпів та етичні виклики автономного вогню утримують людину як головного арбітра на полі бою. Стратегічна перспектива України полягає в масштабуванні виробництва гнучких, модульних ШІ-платформ, які здатні безперервно навчатися на реальних бойових даних та випереджати адаптаційні цикли противника.

Стрінада В. В., канд. техн. наук, доц.
Іщенко Д. А., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ БОЙОВОГО ЗАСТОСУВАННЯ ПІДРОЗДІЛІВ БЕЗПІЛОТНИХ НАЗЕМНИХ КОМПЛЕКСІВ

Аналіз досвіду бойового застосування підрозділів безпілотних наземних комплексів (БпНК) військових частин свідчить, що на сучасному етапі розвитку бойових дій ці комплекси стали важливим елементом системи забезпечення та підтримки дій військ. Якщо на початковому етапі їх використання мало переважно експериментальний характер, то сьогодні БпНК широко застосовуються у практичній діяльності військових частин для виконання широкого спектра бойових (спеціальних) завдань. Насамперед вони використовуються для логістичного забезпечення підрозділів, евакуації поранених і загиблих військовослужбовців, виконання інженерних робіт, вогневого ураження противника, ведення розвідки, а також виконання інших спеціальних завдань у районах, де перебування особового складу пов'язане з високим ризиком ураження.

Проведений аналіз показав, що ефективність бойового застосування БпНК значною мірою залежить не лише від технічних характеристик самих платформ, а насамперед від якості організації їх застосування. Найбільший вплив на успішне виконання бойових (спеціальних) завдань мають правильний вибір і планування маршруту руху, організація взаємодії з підрозділами радіоелектронної боротьби, безпілотних систем та загальновійськовими підрозділами, а також організація прикриття БпНК від ударних безпілотних літальних апаратів противника. Саме ці чинники визначають можливість своєчасного виконання завдань (місій) та збереження роботизованої платформи.

Водночас виникає проблема відсутності єдиного уніфікованого науково-методичного апарату, який дозволив би об'єктивно оцінювати ефективність застосування таких підрозділів для обґрунтування управлінських рішень щодо їх розгортання та комплектування. Питанням оцінки ефективності зразків озброєння та військової техніки (ОВТ) присвячено праці багатьох вітчизняних та закордонних науковців. У більшості з них критерії оцінки базуються на класичних теоріях ефективності стрільби та моделювання бойових дій. Проте

специфіка безпілотних систем вимагає корегування існуючих підходів та введення нових вагових коефіцієнтів.

Чинна система оцінювання через е-бали має певні обмеження. Вона недостатньо враховує внесок логістичних завдання (місій), не повною мірою стимулює евакуацію загиблих і пошкоджених БпНА, а також не відображає технічну складність завдань, рівень ризику для комплексу та ефективність використання ресурсу платформи. Існуюча система оцінювання, заснована переважно на кількості е-балів, не повною мірою відображає реальну ефективність бойового застосування.

Оцінювання ефективності бойового застосування підрозділів БпНК доцільно здійснювати на основі системи часткових показників, які характеризують інтенсивність застосування, результативність виконання завдань (місій), кількість виконаних логістичних завдань, евакуаційні спроможності та рівень бойового навантаження на екіпажі.

Основними вихідними показниками для оцінювання є кількість екіпажів БпНК, кількість застосувань, кількість завдань (місій) зі звітами, частка успішних місій, кількість евакуаційних місій, загальна маса перевезеного вантажу, середня маса вантажу за одне застосування та кількість е-балів, нарахованих за виконані завдання.

Прийняті значення вагових коефіцієнтів повинні відповідати сучасним особливостям бойового застосування підрозділів БпНК, у яких основним показником є досягнення поставленої мети бойового застосування, а допоміжними інтенсивність роботи, обсяг виконаних логістичних завдань, евакуаційні спроможності та повнота документального супроводження результатів діяльності.

Оцінювання ефективності бойового застосування підрозділів БпНК запропоновано проводити виконанням п’яті етапів.

На першому етапі оцінювання ефективності бойового застосування підрозділів наземних комплексів визначається інтенсивність бойового застосування БпНК, яка характеризує середню кількість виконаних завдань одним екіпажем протягом звітного періоду. Використання цього показника дозволяє усунути вплив різної чисельності екіпажів у військових частинах та забезпечує можливість коректного порівняння ефективності їх діяльності. Інтенсивність застосування розраховується як відношення загальної кількості застосувань до кількості екіпажів БпНК.

На другому етапі оцінювання ефективності бойового застосування підрозділів БпНК проводиться аналіз структури виконаних бойових (спеціальних) завдань. Такий аналіз дає змогу визначити функціональне навантаження підрозділів, встановити співвідношення між основними видами місій та оцінити фактичні напрями використання БпНК у сучасних бойових умовах. Для цього визначаються частки логістичних, евакуаційних та ударних місій у загальній кількості застосувань. Отримані результати дозволяють оцінити рівень спеціалізації підрозділів, виявити тенденції розвитку бойового застосування БпНК та визначити перспективні напрями їх подальшого вдосконалення.

На третьому етапі проводимо аналіз виконаних логістичних завдань БпНК. Для цього визначаються обсяги перевезених вантажів за окремими категоріями, середня маса вантажу за одне застосування та частка успішно виконаних завдань (місій). Такий підхід дає змогу встановити, які види матеріальних засобів становлять основне логістичне навантаження на підрозділи БпНК, а також оцінити ефективність використання їх вантажопідйомності.

Оскільки часткові показники ефективності бойового застосування БпНК мають різну розмірність та діапазони значень, їх безпосереднє порівняння є некоректним.

Тому на четвертому етапі проводиться комплексне оцінювання підрозділів БпНК, шляхом нормування показників, що дозволяє привести їх до єдиної безрозмірної шкали в інтервалі від 0 до 1. За еталонне значення приймається максимальне значення відповідного показника серед досліджуваних підрозділів. Такий підхід забезпечує об'єктивне порівняння результатів діяльності підрозділів незалежно від абсолютних значень окремих показників та створює основу для подальшого розрахунку інтегрального показника ефективності.

На п’ятому етапі проводиться розрахунок інтегрального показника ефективності застосування БпНК. Такий показник формується шляхом агрегування нормованих часткових показників із урахуванням їх вагових коефіцієнтів, що відображають ступінь впливу кожного з них на загальну ефективність виконання бойових (спеціальних) завдань.

Запропонований підхід дозволяє комплексно оцінити результати діяльності підрозділів, враховуючи успішність виконання місій, інтенсивність застосування екіпажів, структуру виконуваних завдань та рівень документального підтвердження їх виконання.

Застосування багатокритеріального підходу дає змогу оцінювати підрозділи БпНК за сукупністю показників, а не лише за кількістю е-балів. Це дозволить більш об'єктивно визначати реальний внесок підрозділів у виконання бойових завдань, удосконалити систему мотивації та сформувати прозорий механізм їх матеріального й організаційного стимулювання.

Наумчак Л. М.
Житомирський військовий інститут імені С. П. Корольова

ВИЗНАЧЕННЯ КООРДИНАТ НАЗЕМНИХ ОБ’ЄКТІВ ЗА ДАНИМИ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА І КЛАСУ В УМОВАХ ПОДАВЛЕННЯ GNSS

Активне застосування противником засобів радіоелектронної боротьби (РЕБ) призводить до часткової або повної втрати сигналів глобальних навігаційних супутникових систем (GNSS) безпілотними літальними апаратами (БпЛА). Це безпосередньо впливає на можливість визначення координат наземних об’єктів, від точності яких зокрема залежить виконання завдань корегування вогню артилерії та цілевказання.

Класичний променевий метод геоприв’язки ґрунтується на побудові променя візування за координатами платформи та кутами орієнтації камери й вимагає двох достовірних інформаційних потоків – від GNSS та від бортових датчиків орієнтації. У бойових умовах принаймні один із них недоступний або недостовірний, що унеможливлює визначення координат. За результатами моделювання з похибками GNSS від 3 до 100 м і похибками орієнтації від 0,1° до 0,5° на похилій дальності ≈1550 м сумарна похибка класичного методу становить від ≈7,5 м до ≈188 м, що неприпустимо для вирішення зазначених завдань. Ручне визначення координат за електронною картою потребує значного часу й збільшує навантаження на оператора.

Сучасні дослідження за цією тематикою можна умовно поділити на три напрями: геолокалізація БпЛА за різноракурсними зображеннями із використанням технології нейронних мереж; зіставлення зображень із побудовою точкових відповідностей; визначення координат цілі за кутами повороту підвісу камери та навігаційними даними. Перші два розв’язують

задачу локалізації носія, а не наземної цілі, третій зберігає залежність від сигналів навігації. Тому актуальною лишається задача визначення координат наземних об'єктів за відеопотоком БпЛА в режимі, наближеному до реального часу, за повної або часткової відсутності GNSS, з опорою лише на канал відеоданих і заздалегідь завантажене еталонне зображення.

Одним із підходів до розв'язання цієї задачі є використання геоприв'язаного еталонного зображення місцевості, завантаженого в наземну станцію заздалегідь. Оператор позначає чотири опорні точки (репери) на поточному кадрі та на еталоні, за якими обчислюється проєктивне перетворення (гомографія) площини кадру в площину еталона:

$$\lambda \mathrm{p}' = \mathrm{H}\mathrm{p}, \qquad (1)$$

де p і p' – однорідні координати точки на кадрі та на еталоні; H – матриця гомографії розміром 3×3 з вісьмома незалежними параметрами; λ – масштабний множник.

Чотирьох пар точок достатньо за умови, що жодні три репери не лежать на одній прямій. Координати позначеного оператором об'єкта $\mathbf{p}_o$ визначаються за тим самим перетворенням з подальшим переходом до системи координат еталона:

$$\mathrm{p}'_o \propto \mathrm{H}\,\mathrm{p}_o. \qquad (2)$$

Такий підхід не залежить ні від GNSS, ні від кутів орієнтації камери. Головна умова – об'єкт має перебувати всередині чотирикутника, утвореного реперами.

Недоліком цього підходу є те, що він працює лише доти, доки всі репери одночасно перебувають у кадрі. Під час маневрування платформи, зміни висоти польоту чи повороту підвісу частина реперів виходить за межі поля зору камери, і геоприв'язка втрачається. Для її збереження передбачено автоматичне переприв'язування реперів засобами візуальної одночасної локалізації та картографування (SLAM): положення репера $\mathbf{X}_i$ у локальній карті допроєктується на поточний кадр k за моделлю камери:

$$\hat{\mathrm{p}}_i^{(k)} = \pi\big(\mathrm{K}(\mathrm{R}_k \mathrm{X}_i + \mathrm{t}_k)\big), \qquad (3)$$

де K – матриця калібрування камери; R_k, t_k – оцінка орієнтації та положення камери на кроці k; $\pi(\cdot)$ – перехід від однорідних до декартових координат. Допроєктовані репери разом із видимими формують повний набір для обчислення H; стан кожного репера контролюється скінченним автоматом із верифікацією.

Як показник точності використано середньоквадратичне відхилення (СКВ) за n вимірами:

$$\text{СКВ} = \sqrt{\frac{1}{n}\sum_{j=1}^{n}\Delta_j^2}, \qquad (4)$$

де Δ_j – відстань між визначеним та істинним положенням об’єкта в j-му вимірі. Імітаційне моделювання методом Монте-Карло (10 серій по 1000 реалізацій) показало, що методична складова похибки визначається просторовою роздільною здатністю на місцевості g (розміром пікселя кадру на місцевості):

$$g = \frac{2H\tan(\varphi/2)}{N}, \qquad (5)$$

де H – висота польоту; φ – горизонтальне поле зору камери; N – кількість пікселів у рядку кадру. Відповідно, СКВ зростає з висотою приблизно лінійно: для штатної камери Full HD вона становить від 0,49 м на висоті 600 м до 0,83 м на висоті 1000 м, а відхилення рельєфу від площини на ±10 м збільшує її на 34…78 % (табл. 1).

Таблиця 1 – СКП за результатами моделювання, м

H, м	g, м/піксель	Площинна місцевість	Перепад рельєфу ±5 м	Перепад рельєфу ±10 м
600	0,291	0,49	0,62	0,88
700	0,340	0,58	0,69	0,93
800	0,389	0,66	0,76	0,99
900	0,437	0,75	0,84	1,05
1000	0,486	0,83	0,91	1,11

Окремо проведено моделювання втрати реперів під час маневрування: за виходу з кадру одного та двох реперів середня похибка зростає лише від 0,66 м до 0,85 м і 0,99 м відповідно за збереження геоприв’язки в усіх реалізаціях, тоді як базовий метод втрачає її повністю.

Польові випробування проведено на висоті близько 600 м за участі 3х БпЛА з камерами одного типу; отримано 500 вимірів усередині чотирикутника реперів (табл. 2). Середня похибка становить 2,25 м за максимального значення 4,00 м; за нормальних умов спостереження середня похибка дорівнює 2,17 м, а за несприятливих атмосферних умов (хмарність, термічна конвекція) вона зростає до 3,41 м.

Таблиця 2 – Похибка за результатами польових випробувань, м

Умови спостереження	n	Середня	Медіана	Максимум
Нормальні	468	2,17	2,17	3,10
Хмарність і конвекція	32	3,41	3,44	4,00
Усі умови	500	2,25	2,47	4,00

Розбіжність між результатами моделювання та польових випробувань пояснюється складовими похибки, які не пов'язані з математикою алгоритму. Незалежні складові сумарної похибки узагальнено за правилом додавання дисперсій:

$$\sigma_\Sigma = \sqrt{\sigma_m^2 + \sigma_e^2 + \sigma_r^2}, \qquad (6)$$

де σ_m – методична складова алгоритму, що узгоджується з даними моделювання; σ_e – похибка еталонних вимірювань; σ_r – складова, зумовлена способом вибору реперів. Аналіз показав, що домінує саме остання складова, тобто основний резерв підвищення точності пов'язаний не з алгоритмом, а з методикою вибору реперів і точністю еталонних вимірювань; за попередньою оцінкою їх удосконалення дозволяє наблизити похибку до 1 м без зміни алгоритму.

Висновки:

1. Чотириточкова гомографічна прив'язка відеокадру до геоприв'язаного еталонного зображення забезпечує визначення координат наземних об'єктів без залучення GNSS і даних про орієнтацію платформи.

2. За результатами моделювання методична СКП становить 0,49…0,83 м на висотах 600…1000 м і зростає на 34…78 % за перепаду рельєфу ±10 м; механізм переприв'язування реперів зберігає геоприв'язку за виходу з кадру одного-двох реперів із приростом похибки до 0,99 м.

3. Польові випробування підтвердили працездатність підходу: середня похибка 2,17 м за нормальних умов і 2,25 м у сукупності.

4. Подальші дослідження спрямовано на натурну перевірку механізму переприв'язування реперів, урахування цифрової моделі рельєфу та вдосконалення методики вибору реперів.

Демидюк М. О., курсант
Кухарчук І. В.
Житомирський військовий інститут імені С. П. Корольова

РЕАКТИВНІ БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ-ПЕРЕХОПЛЮВАЧІ ЯК ЗАСІБ ПРОТИДІЇ ВОРОЖИМ РЕАКТИВНИМ ПОВІТРЯНИМ ЦІЛЯМ

У зв'язку з масовим застосуванням російською федерацією реактивних ударних безпілотних літальних апаратів (далі — БпЛА) та крилатих ракет, зокрема «Герань-5» і С-8000 «Бандероль», актуалізувалося питання підвищення

ефективності перехоплення швидкісних повітряних цілей. Традиційні БпЛА-перехоплювачі типу FPV, як правило, мають обмежені можливості щодо протидії таким об’єктам, швидкість польоту яких може перевищувати 500 км/год, а висота польоту — сягати 10 км.

Одним із перспективних напрямків розв’язання цієї проблеми без залучення пілотованої авіації та застосування дороговартісного зенітно-ракетного озброєння є використання реактивних БпЛА-перехоплювачів. На сьогодні офіційно підтвердженим прикладом такого засобу є БпЛА «Alexa Spatium», призначений для протидії швидкісним повітряним цілям, що характеризуються значною швидкістю польоту та висотою застосування.

Порівняно з традиційними БпЛА-перехоплювачами, використання реактивної силової установки зумовлює низку конструктивних та експлуатаційних особливостей. Зокрема, необхідність розміщення запасу палива, що впливає на масу апарата, а наявність бойової частини додатково визначає його масогабаритні характеристики. Висока швидкість польоту висуває підвищені вимоги до міцності конструкції, аеродинамічної стійкості та ефективності системи керування. Під час виконання маневрів зростають аеродинамічні навантаження на органи керування та інші елементи конструкції. Одним із перспективних напрямів підвищення ефективності реактивних БпЛА-перехоплювачів є інтеграція алгоритмів штучного інтелекту для автоматизованого виявлення та супроводження повітряних цілей і підтримки процесів наведення. За наявними оцінками, противник також активно працює над розробленням і впровадженням подібних технологічних рішень.

Подальший розвиток реактивних БпЛА-перехоплювачів створює передумови для розширення переліку повітряних об’єктів, проти яких вони здатні застосовуватися. Застосування реактивних БпЛА-перехоплювачів може розширити можливості наявних засобів протиповітряної оборони та сприяти зменшенню потреби у використанні дороговартісного зенітного- ракетного озброєння.

Мукосій Д. В.
Лях І. Ю.
Новічков В. О.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

КЛЮЧОВА РОЛЬ ЗАСОБІВ АВТОМАТИЗАЦІЇ В СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТАХ

Особливістю сучасних збройних конфліктів є динамічна зміна бойової обстановки, що вимагає від командирів ухвалення рішень у мінімальні терміни. Саме тому провідне місце посідають засоби автоматизації, які забезпечують оперативне отримання, опрацювання та доведення інформації, злагоджену взаємодію підрозділів і високу точність селекції цілей для першочергового ураження.

Основу засобів автоматизації становлять сучасні надшвидкі системи обміну даними та їх обробки, комплекси керування безпілотними літальними апаратами, автоматизовані системи управління вогнем і системи підтримки прийняття рішень. Завдяки їм значно скорочується цикл «виявлення – ухвалення рішення – ураження», тривалість якого в сучасному бою часто визначає його результат.

Наочно ефективність автоматизації підтверджує війна Росії проти України. Застосування БпЛА для розвідки, корекції артилерійського вогню та миттєвого передавання координат цілей істотно підвищує точність ураження й оперативність дій підрозділів. У 2026 році українські дрони-перехоплювачі завдяки використанню технологій штучного інтелекту та нейронних мереж уже здатні самостійно, в автономному режимі, знищувати ударні БпЛА типу «Шахед».

Схожі тенденції простежуються і в конфлікті США–Іран. У ході операції, що розпочалася наприкінці лютого 2026 року, автоматизовані засоби аналізу розвідувальних даних і цифрового управління – C4ISR – забезпечили швидке виявлення загроз, планування ударів та координацію сил. Таким чином, в обох випадках технологічна перевага сторін безпосередньо пов’язана з рівнем автоматизації.

Отже, засоби автоматизації відіграють ключову роль в ефективному веденні сучасних бойових дій, оскільки динаміка сучасних бойових дій немислима без використання потужних комплексів засобів автоматизації для підвищення оперативності управління військами, точності застосування зброї та результативності бойових дій загалом.

Trokhymenko V. O.
Malakhov O. V., Dr. Sc., Prof.
Research Center of the Armed Forces of Ukraine "Derzhavnyi Okeanarium"
Naval Institute of National University "Odessa Maritime Academy"

SPECIFIC OF CONFINED FLOW DEPARTURE FROM THE BODY WITH CONTOUR BREAK

The process of body outflowing by an unrestricted flow with subsequent fluid separation is a classical fluid dynamics problem described in numerous scientific papers. A completely different picture takes place in flows confined by rigid walls. Due to the influence of rigid boundaries, flow conditions in this case differ significantly, and studies that thoroughly examine specific of non-compressible flow around bodies with flow separation at a surface contour break in confined spaces are practically absent. The influence of rigid walls onto the flow pattern near a break in a body's surface contour is rarely considered in detail.

To study the characteristic behavior of a bounded flow near a body with a sharp break in its surface contour, a large series of numerical experiments was conducted. The problem of flow around disks and rectangles in confined flow was calculated using a finite-difference method based on the solution of 3D unsteady Navier-Stokes equations with two types of initial conditions. In the first case, the flow was assumed to be stationary at the beginning of the calculation, and the pressure was specified in the first computational cross-section only. In the second variant, positive velocity and pressure gradients were formulated for the entire flow along the longitudinal axis of liquid motion.

The boundary conditions in the calculations corresponded to the leakproof condition on the rigid surfaces of the computational volume. At the entrance to the computational volume, velocity and pressure were defined at each computational point, while at the exit from the computational volume, only pressure was defined at all time moments.

In both cases, the initial conditions were specified with a calculation error that did not exceed the value of 10^{-6} at each computational point. The final results were almost identical. These results are very unusual, because in opposition to the results of the flow separation theory in unbounded flow, the position of the flow separation

line on the disk surface shown in Figure 1 never coincided with the break line of its surface contour. Separation always occurred either before or after the break line of the surface contour. In the range of Reynolds parameter from 400 to 50000, flow separation from the break line of the body's surface contour never occurred.

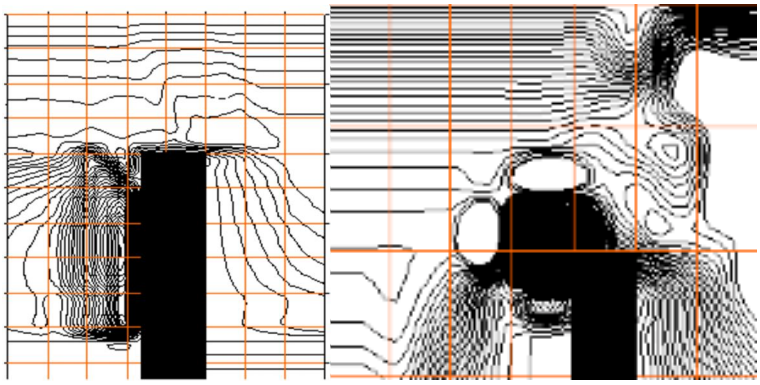


Fig. 1. Flow streamlines near a disk 20 mm thick. Re=5000

The value of critical pressure on the surface of an outflowing body was determined in two ways: either by the inflection point of the pressure diagram or by the maximum on the pressure curve.

The resulting displacement of the separation line is the main reason of the unstable spatial position of outflowing bodies in the flow. Because of this reason near fairings in a confined flow a low-amplitude and high-frequency vibrations occur always.

Finally, for all confined flows it could be stated that positionof a separation line from the body's surface in the region of the break line of its surface contour is not a fixed value in space. It can be stated that, in a restricted flow in the studied Reynolds parameter diapason of 400 to 50,000, unlike an unconfined flow around a body with a sharp break in the surface contour, a constant jump in the separation line from the frontal surface to the lateral surface will be observed.

The importance of this result is clearly demonstrated by two practical examples. The first example is medical fluid dynamics, where standard designs of disc heart valves are used. In the region of the break in the disc surface contour, the constant spatial jump in the flow separation line will lead to the destruction of blood cells in the blood flow through the valve. The cause of this destruction will be the high values of the pulsating pressure components and the high rotational speeds of the resulting small-scale vortices.

The second example is hydraulic throttle devices. Inside of them, during flow regulation, vibration from the constant shift in the flow separation line on the disc

valves will lead to earlier seal wear and subsequent depressurization of the device. In both examples, smoothing of the disk's surface contour from a sharp break in the surface contour to a plain hemispherical transition can lead to a fixed separation line position for each specific range of flow Reynolds parameters. In this case, the overall flow field of the confined flow near the outflowing body will always stabilize.

Зуєв Т. Є., курсант
Котвицький М. М.
Житомирський військовий інститут імені С. П. Корольова

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В БЕЗПІЛОТНИХ СИСТЕМАХ

Сучасний характер ведення бойових дій характеризується стрімким впровадженням цифрових технологій та роботизованих комплексів. Особливе місце серед них займають безпілотні системи, які використовуються для розвідки, спостереження, коригування вогню, логістичного забезпечення та ураження цілей. Досвід російсько-української війни продемонстрував, що безпілотні системии стали одним із ключових елементів сучасного поля бою. У зв’язку з цим особливої актуальності набуває використання технологій штучного інтелекту (ШІ), які дозволяють підвищити рівень автономності безпілотних платформ та ефективність виконання ними бойових завдань.

На сьогодні автономні безпілотні системи розглядаються як важливий елемент перспективних концепцій ведення бойових дій. Їх використання дозволяє виконувати широкий спектр завдань без безпосередньої участі людини в небезпечних умовах, що сприяє зменшенню втрат особового складу та підвищенню ефективності ведення бойових дій. Впровадження алгоритмів штучного інтелекту забезпечує якісно новий рівень функціонування безпілотних систем, дозволяючи їм не лише виконувати команди оператора, а й самостійно аналізувати обстановку та адаптувати власну поведінку відповідно до поставлених завдань.

Одним із головних напрямів застосування штучного інтелекту у військовій сфері є автономна навігація безпілотних платформ. Традиційні системи навігації переважно базуються на використанні сигналів глобальних супутникових навігаційних систем, таких як GPS, Galileo або GLONASS. Однак

у сучасних умовах бойових дій противник активно застосовує засоби радіоелектронної боротьби для подавлення або спотворення навігаційних сигналів. У таких умовах особливого значення набувають технології автономної навігації, що базуються на алгоритмах комп'ютерного зору, нейронних мережах та методах одночасної локалізації й побудови карти місцевості (SLAM). Сучасні системи штучного інтелекту здатні аналізувати інформацію, отриману від камер, лідарів, радарів, інерціальних навігаційних систем та інших сенсорів. На основі цих даних формується цифрова модель навколишнього середовища, що дозволяє безпілотному апарату визначати власне місцезнаходження, виявляти перешкоди та будувати оптимальний маршрут руху. Не менш важливим напрямом є автоматичне розпізнавання та класифікація об'єктів. Сучасні системи штучного інтелекту забезпечують високоточне виявлення різноманітних об'єктів за допомогою алгоритмів глибокого навчання. Використання згорткових нейронних мереж (CNN) та інших сучасних архітектур дозволяє автоматично розпізнавати бронетехніку, автомобілі, артилерійські системи, фортифікаційні споруди, живу силу противника та інші потенційні цілі. Особливої актуальності набуває інтеграція даних від різнорідних сенсорів. Поєднання інформації від відеокамер видимого спектра, тепловізійних систем, радарів та акустичних датчиків дозволяє значно підвищити достовірність розпізнавання об'єктів навіть у складних погодних умовах або за обмеженої видимості. У результаті суттєво скорочується час обробки розвідувальної інформації та зменшується навантаження на операторів безпілотних комплексів.

Перспективним напрямом розвитку автономних безпілотних систем є застосування технологій колективної взаємодії, відомих як ройові технології (swarm technologies). Основна ідея такого підходу полягає в організації взаємодії великої кількості безпілотних платформ, які функціонують як єдина система. Кожен окремий апарат виконує відносно прості функції, однак завдяки обміну інформацією між елементами рою формується складна колективна поведінка. Використання ройових алгоритмів дозволяє ефективно вирішувати завдання пошуку, розвідки, спостереження та ураження цілей на значних територіях. При втраті окремих апаратів система зберігає працездатність завдяки перерозподілу функцій між іншими елементами рою. Такий підхід підвищує живучість безпілотних систем і значно ускладнює протидію з боку

противника. Очікується, що в найближчі роки ройові технології стануть одним із ключових напрямів розвитку військових роботизованих комплексів.

Окремої уваги заслуговує використання штучного інтелекту для підтримки прийняття рішень командирами різних рівнів управління. Сучасне поле бою характеризується надзвичайно великим обсягом інформації, що надходить від різноманітних джерел: безпілотних систем, супутникової розвідки, радіолокаційних станцій, засобів радіоелектронної розвідки та інформаційних мереж. Людина не завжди здатна оперативно обробити такі обсяги даних та своєчасно прийняти оптимальне рішення. Інтелектуальні системи підтримки прийняття рішень здатні автоматично аналізувати отриману інформацію, виявляти приховані закономірності, прогнозувати розвиток бойової обстановки та формувати рекомендації для командирів. Застосування таких систем дозволяє скоротити час проходження циклу спостереження–орієнтування–рішення – дія OODA (Observe–Orient–Decide–Act), що є одним із вирішальних факторів досягнення переваги над противником.

Важливим напрямом розвитку є також використання штучного інтелекту для автономного управління наземними роботизованими комплексами та морськими безекіпажними платформами. Такі системи можуть виконувати завдання логістичного забезпечення, розвідки, розмінування, охорони об'єктів та нанесення вогневого ураження. Інтеграція технологій штучного інтелекту дозволяє забезпечити автономне пересування, уникнення перешкод та координацію дій між різними роботизованими платформами. На сьогодні провідні держави світу та країни-члени НАТО активно впроваджують технології штучного інтелекту у військову сферу. Розробляються спеціалізовані програми розвитку автономних систем, здійснюються масштабні інвестиції у створення перспективних алгоритмів машинного навчання та формуються міжнародні стандарти їх застосування.

Разом із численними перевагами застосування автономних безпілотних систем виникає низка технічних, правових та етичних проблем. Однією з головних загроз залишається кібербезпека. У разі компрометації каналів зв'язку або втручання у програмне забезпечення противник може отримати можливість впливати на функціонування автономних платформ. Тому важливим завданням є розроблення захищених архітектур управління та використання сучасних криптографічних засобів захисту інформації.

Крім того, значна увага приділяється проблемам надійності функціонування алгоритмів штучного інтелекту в реальних бойових умовах. Помилки розпізнавання об'єктів або неправильна інтерпретація ситуації можуть призвести до прийняття некоректних рішень та виникнення небажаних наслідків. Саме тому більшість сучасних концепцій розвитку військового штучного інтелекту передбачає реалізацію принципу “людина в контурі прийняття рішення” (Human-in-the-Loop), який забезпечує можливість контролю людиною критично важливих дій автономної системи.

Інтеграція штучного інтелекту перетворює БпС із простих дистанційно керованих інструментів на повноцінні суб'єкти виконання тактичних завдань. Технологічний стек для автономного польоту та розпізнавання цілей уже сформовано, проте його масштабування стримується фізичними обмеженнями мікроелектроніки та ризиками “хибних спрацьовувань” ШІ.

Найбільш раціональним вектором на найближчі роки залишається концепція Human-on-the-loop (людина як супервізор): ШІ бере на себе рутинне пілотування, аналіз гігабайтів відеопотоку та наведення в умовах РЕБ, тоді як фінальне право на відкриття вогню чи зміну стратегічного завдання залишається за людиною.

Сисоєнко С. В., канд. техн. наук, доц.
Аркушенко П. Л., канд. техн. наук, ст. досл.
Кузьміч О. Є.
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки

ПІДВИЩЕННЯ НАДІЙНОСТІ НАВІГАЦІЙНО-КЕРУЮЧОЇ СИСТЕМИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ШЛЯХОМ КОМПЛЕКСНОГО КОНТРОЛЮ СЕНСОРНИХ ДАНИХ

Сучасне застосування безпілотних літальних апаратів (БпЛА) потребує забезпечення стабільної роботи навігаційно-керуючої системи за умов впливу широкого спектра експлуатаційних факторів. Надійність виконання польотного завдання значною мірою визначається не лише характеристиками апаратної частини, а й достовірності інформації, що надходить від інерціальних,

барометричних, магнітометричних та супутникових навігаційних датчиків до автопілота. Практика експлуатації БпЛА свідчить, що помилки калібрування, некоректне встановлення сенсорів, механічні вібрації, електромагнітні завади та особливості компонування літального апарату можуть призводити до спотворення вимірювальної інформації. У результаті виникають помилки оцінювання просторового положення, висоти та навігаційних параметрів, що безпосередньо впливають на якість автоматичного керування. Особливого значення ця проблема набуває для автопілотів типу (ArduPilot, PX4 Autopilot, INAV та ін.). В ArduPilot стабілізація та керування формуються на основі комплексного використання інформації від декількох сенсорів. Тому контроль працездатності та узгодженості сенсорної інформації доцільно розглядати як окремий елемент забезпечення надійності БпЛА.

Метою дослідження є обгрунтування комплексного підходу до контролю достовірності сенсорної інформації навігаційно-керуючої системи БпЛА на етапах підготовки та виконання польоту.

У системі керування БпЛА використовується сукупність сенсорів, серед яких ключову роль відіграють акселерометри, гіроскопи, магнітометри, барометр та GPS-приймач. Кожен із цих каналів забезпечує отримання інформації про окремі параметри руху або просторового положення, однак похибки одного датчика можуть вплинути на результат комплексної оцінки стану літального апарату. Одним із важливих етапів підготовки БпЛА до польоту є калібрування сенсорів. При цьому недостатньо лише виконати передбачену програмним забезпеченням процедуру калібрування. Необхідно забезпечити правильне просторове встановлення датчиків, відповідність їх орієнтації заданій конфігурації, відсутність надмірних вібрацій та впливу сторонніх електромагнітних полів. Особливу увагу необхідно приділяти акселерометрам та гіроскопам. За результатами калібрування формуються поправки, які використовуються автопілотом для визначення параметрів руху. Водночас механічне зміщення контролера або зміна його положення після калібрування може призвести до виникнення систематичної похибки. Калібрування необхідно розглядати не як одноразову операцію, а як складову процедури контролю технічного стану навігаційно-керуючої системи.

Окремою проблемою є функціонування магнітометра. Його показання можуть спотворюватися силовими кабелями, електродвигунами, регуляторами

обертів та іншими елементами бортового обладнання. Тому результати калібрування компасанеобхідно оцінювати з урахуванням фактичного компонування конкретного БпЛА.

Важливим елементом комплексного контролю є Extended Kalman Filter (EKF) – алгоритм оцінювання стану системи, який використовує інформацію від різних джерел для формування узгодженої оцінки параметрів руху. Поява розбіжностей між даними сенсорів може бути індикатором проблеми як окремого вимірювального каналу, так і умов експлуатації літального апарату.

Практично важливим є використання механізму Pre-Arm (режим підготовки), за допомогою якого система здійснює перевірку деяких умов перед дозволом на запуск двигунів та виконання польоту. Такий підхід дає змогу виявити частину несправностей або невідповідностей ще до початку польоту.

Доцільним є формування послідовності контролю: калібрування; перевірка орієнтації сенсорів; контроль вібрації; перевірка GPS; контроль компаса; оцінювання EKF; перевірка Pre-Arm; контроль параметрів у польоті; аналіз журналу польоту. Важливим результатом такого підходу є перехід від контролю окремих датчиків до комплексної оцінки інформаційного стану навігаційно-керуючої системи. При цьому необхідно врахувати, що характер проблем може залежати від типу апарата. Зокрема, для мультикоптерів та БпЛА літакового типу можуть виникати різні умови формування похибок. Навіть силові установки можуть створювати локальні аеродинамічні умови, здатні впливати на роботу барометричного каналу.

Не менш важливим є контроль функціонування GPS та магнітометра за наявності зовнішніх перешкод. Дослідження комплексного підходу до контролю інформаційної працездатності навігаційно-керуючої системи БпЛА, який передбачає оцінювання не тільки параметрів окремих сенсорів, а й узгодженості інформації між ними та її впливу на оцінку стану літального апарату є досить актуальним. Даний підхід полягає у можливості його використання під час підготовки БпЛА до польоту, технічного обслуговування та аналізу результатів польотних завдань. Застосування послідовного контролю калібрування, орієнтація сенсорів, GPS, компаса, EKF; Pre-Arm та параметрів польоту дозволяє своєчасно виявляти причини нестабільної роботи системи та зменшувати ризики втрати керованості.

Підвищення надійності навігаційно-керуючої системи БпЛА потребує переходу від окремого контролю працездатності сенсорів до комплексної оцінки достовірності інформації, що використовується автопілотом.

Основним елементом такого контролю є правильне калібрування сенсорів, перевірка їх просторової орієнтації, контроль вібрацій та електромагнітних впливів, оцінювання стану GPS і магнітометра, аналіз EKF, виконання Pre-Arm перевірок та аналіз даних польоту. Такий підхід створює основу для підвищення надійності автоматичного керування БпЛА та зниження ймовірності відмов, обумовлених недостатністю навігаційної інформації.

Кузнецов В. О.
Засядько А. А., д-р техн. наук, проф.
Орлов С. В., канд. техн. наук
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

ПОРІВНЯННЯ НОВИХ ВІЙСЬКОВИХ СТАНДАРТІВ ЛАБОРАТОРНИХ ВИПРОБУВАНЬ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ ЩОДО ВПЛИВУ МЕХАНІЧНИХ ФАКТОРІВ

Одним з обов’язкових циклів випробувань, яким піддається безпілотний авіаційний комплекс (БпАК) під час надходження на випробування, є лабораторні механічні випробування. Під час таких випробувань штучно імітуються механічні навантаження, максимально наближені до умов експлуатації. Зазвичай беруться до уваги навантаження на елементи БпАК під час застосування за призначенням, транспортування та зберігання.

Лабораторні механічні випробування дозволяють виявити приховані дефекти складових частин БпАК, перевірити їх функціонування та здатність зберігати свої параметри в межах установлених норм під час дії механічних навантажень (випробування на стійкість), а також дослідити властивості зберігати працездатність і задані характеристики після тривалого впливу (випробування на витривалість). Такі випробування можуть проводитися як для всього комплексу, так і для окремих його елементів, що дозволяє скоротити витрати часу і ресурсів порівняно з повномасштабними польовими випробуваннями.

Авторами було розглянуто зміст і методологію застосування стандарту ВСТ 01.055.011 – 2021 (01) Озброєння та військова техніка. Випробування. Методи та порядок проведення механічних випробувань (STANAG 4370 Edition

7 / AECTP-400 Edition D, Mechanical Environmental Tests, IDT) для виконання задачі проведення механічних лабораторних випробувань БпАК.

У результаті структурного узагальнення положень документа визначено групи найбільш критичних методів для випробувань окремих складових БпАК (корпус, електроніка, оптика, засоби зв'язку, пульт керування), а також запропоновано типові параметри навантажень для реалізації відповідних процедур у лабораторних умовах. Це дозволяє адаптувати підходи STANAG 4370 до специфіки національної системи оцінювання надійності та забезпечити ресурсозберігаюче тестування зразків озброєння й військової техніки на ранніх етапах життєвого циклу.

Проведений аналіз методів лабораторних механічних випробувань безпілотних авіаційних комплексів відповідно до положень стандарту STANAG 4370 Ed.6 / AECTP-400 Ed.3 підтверджує доцільність та ефективність їх застосування для визначення надійності, стійкості та функціональної збереженості основних елементів БпАК у реальних умовах експлуатації, транспортування і зберігання. Встановлено, що методи AECTP-400 охоплюють увесь спектр механічних впливів, зокрема вібрацію, удари, падіння, акустичне навантаження, фіксоване прискорення, комбіновані впливи та умови транспортування.

Наведені найважливіші методи та їх параметри є об'єктивною основою для формування програми проведення лабораторних випробувань безпілотних авіаційних комплексів щодо впливу механічних факторів. Ці дані гармонізовані зі stanag 4370, але адаптовані до реальних умов бойового застосування, що знижує надмірність випробувань і одночасно забезпечує їх надійність.

Впровадження згаданого стандарту в національну випробувальну практику дозволяє уніфікувати підходи до дослідження механічної витривалості зразків, гармонізувати нормативну базу з вимогами НАТО, забезпечити технічну сумісність і підвищити рівень науково-технічної обґрунтованості сертифікаційних процедур. У перспективі це створює умови для серійного виробництва БпАК, сертифікованих за міжнародними вимогами, з підвищеними показниками бойової живучості, експлуатаційної безпеки та довговічності.

Засядько А. А., д-р техн. наук, проф.
Юла О. В.
Рижков О. В.
Братко В. В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

АНАЛІЗ МЕТОДІВ ТЕСТУВАННЯ АНТЕН ІЗ КЕРОВАНОЮ ДІАГРАМОЮ СПРЯМОВАНОСТІ

Методи тестування CRPA поділяються на п’ять основних видів: відтворення записів сигналів середовища, симулятори GNSS-сигналів, моделювання хвильового фронту, випробування в безлунній камері та польові випробування.

Метод відтворення запису відтворює реалістичні (а не штучно змодельовані чи згенеровані умови експлуатації з прогнозованими перешкодами. Цей метод корисний для регресійних тестів, повторюваного відтворення окремих сценаріїв і перевірки алгоритмів на відкритих наборах даних, але він не гнучкий для до варіативного сценарного аналізу загроз та не замінює кероване моделювання. Тому недоліки полягають в неможливості зміни існуючого запису і складністю запису реальних перешкод, оскільки такий запис вимагає знаходження в бойовій обстановці.

Метод симуляції GNSS є найдешевшим, що наразі стрімко розвивається завдяки новим технологічним рішенням. Раніше для імітаційного тестування CRPA використовувалося дороговартісне і складне фазово-матричне обладнання. Таке моделювання забезпечує високу відтворюваність, гнучкість для швидкого охоплення кількох тестових випадків, швидкі ітерації, зручність для програмної відладки та сприяє високій швидкості реалізації, проте не охоплює повністю реальну антену з її архітектурою і просторовий канал.

Моделювання хвильового фронту отримує високу повторюваність, точний контроль фазових співвідношень між каналами та швидку ітерацію сценаріїв, однак напряму не перевіряє фізичну антену, фазові центри та взаємний просторовий зв’язок елементів.

Моделювання у безлунній камері, навпаки, дозволяє оцінювати антену, антенну електроніку та інтегровану систему як єдине ціле, але потребує значно жорсткіших процедур калібрування випромінювачів, затримок, втрат і

поляризаційного відтворення хвильового поля. Передбачає наявність повної системи безлунної камери, що складається з дороговартісних фізичної камери та обладнання для моделювання, складних в калібруванні та геометрично чутливих. Під час монтажу безлунної камери також необхідно врахувати або компенсувати вплив зовнішнього середовища.

Польове тестування відтворює реальні умови до реального (бойового) застосування, моделюючи як середовище, так і перешкоди або загрози, але різко знижують повторюваність і ускладнюють відокремлення внеску окремих факторів. Захід має бути укомплектований персоналом, і у разі обмеженого доступу до загроз неможливо охопити всі можливі тестові випадки.

До основного переліку методів тестування варто додати OTA-випробування – метод бездротового тестування, який використовується для оцінки характеристик випромінення, прийому та загальної продуктивності бездротових пристроїв у реальних або наближених до них умовах.

Перевага моделювання в безлунній камері полягає в тому, що можна протестувати архітектуру антени: взаємного зв’язку елементів, фазових і амплітудних розкидів, кабельних неузгоджень та інтеграції антени з корпусом виробу. Натомість переваги моделювання хвильового фронту в повторюванні сценаріїв зі складною комбінацією супутників, завад і спуферів, а також в керованому фазовому розподілу по входах решітки. Отже, ці два підходи не є взаємовиключними: безлунна камера потрібна, щоб не втратити фізику реальної антени; моделювання хвильового фронту — щоб не втратити контрольованість експерименту. Польові випробування завершують цикл валідації, але не можуть бути єдиним інструментом розробки через вартість, слабку повторюваність і обмежений контроль над сценарієм.

Висновок. Розглянувши переваги і недоліки основних методів тестування CRPA для її повної валідації доцільно рекомендувати каскадну схему тестування, що містить в собі: чисельне моделювання та перевірка коректності просторової обробки оцифрованого радіосигналу методом відтворення запису та симулятором GNSS; тестування системами хвильвого фронту із контрольованим фазовим узгодженням; тестування в безлунному середовищі з реальною антеною й електронним блоком; польовий експеримент, де перевіряються живучість контуру й збіжність лабораторних метрик із реальною динамікою місії.

Засядько А. А., д-р техн. наук, проф.
Цуря Е. І.
Гусак М. Ю., канд. техн. наук
Кот О. Б.
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки

ОСОБЛИВОСТІ ВИКОРИСТАННЯ АНТЕН ІЗ КЕРОВАНОЮ ДІАГРАМОЮ СПРЯМОВАНОСТІ ДЛЯ ГЕОДЕЗИЧНОЇ ПРИВ’ЯЗКИ РАДІОЛОКАЦІЙНОГО ПОСТА

Уразливість глобальних навігаційних супутникових систем (GNSS) до радіоперешкод і навмисної підміни сигналів давно перестала бути суто теоретичною проблемою. Для безпілотних платформ, рухомих сенсорних систем, засобів спостереження та малогабаритних радіолокаційних станцій (МРЛС) вона вже напряму впливає не тільки на просторову орієнтацію, а й на часову синхронізацію, працездатність контурів супроводу та метрологічну відтворюваність усієї системи. Саме тому в сучасних дослідженнях антени з керованою діаграмою спрямованості прийому (CRPA) розглядають не як додатковий пристрій, а як ключовий радіочастотний компонент, призначений для прийому сигналів GNSS в умовах активної радіоелектронної боротьби, де просторове придушення завад має узгоджуватися з навігаційною цілісністю, визначенням напрямку приходу та фазовими вимірюваннями.

Для геодезичної прив’язки МРЛС використовуються захищені системи позиціювання. Для систем геодезичної прив’язки, куди інтегрується CRPA як елемент завадостійкого позиціонування, CRPA слід оцінювати у категорії збереження фазових або часових настройок певної точності. Тому засоби протидії завадам (такі, як CRPA) не мають спотворювати засоби отримання навігаційних даних.

Для МРЛС GNSS-підсистема виконує щонайменше три функції: задає абсолютну координатну прив’язку пункту, забезпечує часове узгодження та підтримує курс та орієнтацію, від яких залежить коректне перетворення радіолокаційних вимірювань у зовнішню систему координат. Якщо ця підсистема працює в завадовому середовищі, простого одноантенного GNSS уже недостатньо. Тому CRPA зменшує ймовірність втрати навігації на

радіочастотному рівні, а далі її корекція повинна бути придатною для високоточного оцінювання положення, часу й орієнтації, оскільки просторова фільтрація, яка протидіє заглушенню, але псує курс і фазу, вирішує лише половину задачі.

Геодезична прив'язка малогабаритної РЛС або радіолокаційного поста є двокомпонентною задачею, де потрібно визначити координати референтної точки системи та її просторову орієнтацію відносно локальної або глобальної системи координат. Будь-яка деградація координат, курсу, крену, тангажу або узгодження осей безпосередньо переходить у помилку геолокації цілі. Тому контур позиціонування, навігації та синхронізації часу, який забезпечує таку прив'язку, має бути не лише точним, а й достовірним у завадовому середовищі. Саме тут CRPA входить до складу системи як просторовий захисний шар GNSS-модуля позиціювання, орієнтації та синхронізації часу.

У складі МРЛС CRPA доцільно розглядати як елемент завадостійкого GNSS-вузла, який часто інтегрується в один комплекс із МРЛС для забезпечення стабільної часової шкали та підтримання позиціювання МРЛС-поста без втрати працездатності при перешкодах.

Для геодезичної прив'язки МРЛС необхідно визначити:

координати опорної точки платформи, положення фазових центрів GNSS/CRPA-входів відносно цієї точки,

відстань між антенами,

кутові зсуви між корпусом, інерціальним модулем, антеною GPS/GNSS та радаром,

матрицю юстировки прицілювання.

Далі ці параметри повинні коригуватися під час просторової обробки.

Критеріями придатності CRPA стають: ефективність просторового придушення, стабільність фази несучої частоти, коректність оцінок визначення напрямку, сумісність із супутниковими технологіями, що забезпечують сантиметрову точність позиціонування, відтворюваність курсу, якість часової прив'язки та похибка перетворення радарних вимірювань у зовнішню координатну систему

Висновки: у складі малогабаритної РЛС CRPA розглядається як підсистема захищеного високоточного PNT, від якого залежать координатна прив'язка, курс, юстировка прицільної лінії, часове узгодження та достовірність перетворення радарних вимірювань у зовнішню систему координат.

Верголяс О. О., канд. юр. наук
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ВІДЕОКОНТЕНТ ІЗ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ВІДКРИТОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ: КОМУНІКАЦІЙНИЙ ЕФЕКТ, КАНАЛИ ДЕМАСКУВАННЯ ТА ВІДБІР ПЕРЕД ОПРИЛЮДНЕННЯМ

Постановка проблеми. Відео з борту безпілотних літальних апаратів (далі – БпЛА) за роки повномасштабної війни стало головним візуальним жанром її публічного висвітлення і разом з тим основним документом обліку бойової роботи. За повідомленням Міністерства оборони України від 31 липня 2026 року, лише за червень підрозділи внесли до бойової системи DELTA понад 200 тисяч уражень, тобто більше ніж 6 600 на добу, а щодня через систему проходить понад 75 тисяч відеотрансляцій. Ураження в межах програми «Армія дронів. Бонус» у тій самій системі фіксуються і підтверджуються, після чого обмінюються на техніку через Brave1 Market; за 2025 рік таких підтверджених уражень набралося, за даними міністра оборони, майже 820 тисяч. Отже, той самий файл виконує щонайменше три функції: він є матеріалом об'єктивного контролю, підставою для обліку й винагороди підрозділу і, після оприлюднення, продуктом стратегічних комунікацій. Вимоги безпеки до кожної з цих функцій різні, тоді як порядок відбору матеріалу перед оприлюдненням чинними документами не визначений.

Стан дослідження. Комунікаційний бік питання вивчений краще за безпековий. П. Скрейвер (International Journal of Intelligence and CounterIntelligence, 2025) на масиві 2 606 повідомлень офіційного каналу Головного управління розвідки за два роки показав, що близько 46 % дописів працюють на проєкцію інституційної легітимності, передусім через «брендинг успіхів» з бойовим відео, а ще 42 % спрямовані на противника через розкриття інформації. Автор прямо фіксує компроміс, у якому оперативна безпека свідомо приноситься в жертву інформаційному ефекту, адже кожне оприлюднене перехоплення видає противникові скомпрометований канал. М. Барейкіте та М. Махортих (Media, War & Conflict, 2025) описують «цифрово засвідчувану війну» на матеріалі Telegram-спільноти окупованого міста. У вітчизняній

літературі OSINT розглядається як цикл розвідки з методами побудови міжоб'єктних зв'язків (Т. Коробейнікова, І. Симак, 2025), а прийоми приховання й ідентифікації авторства акаунтів – як елемент інформаційного протиборства (О. Курбан, 2016). У той же час слід констатувати, що опубліковане відео з БпЛА як самостійний об'єкт розвідки противника, тобто як носій координат, часу, тактики і техніки, у цих працях не розглядається. Від проблематики агрегації цифрового сліду особового складу з його власних дописів ця тема відрізняється об'єктом. Ідеться про один оприлюднений від імені підрозділу артефакт, чий зміст і службові дані розкривають позицію і спосіб дій, а не про сукупність особистих публікацій.

Виклад основного матеріалу. Розпочинаючи аналіз, передусім слід розвести три канали, якими опубліковане відео демаскує підрозділ, адже захисні заходи для кожного з них різні. Перший канал – службові дані файла. Й. Ульріх (SANS Internet Storm Center, 2024) на прикладі апарата DJI показав, що поряд з основним MP4-файлом, у якому зафіксовано серійний номер і версію прошивки, апарат записує файл субтитрів SRT, де на кожен часовий зріз зазначено широту й довготу, відносну й абсолютну висоту, час і параметри камери. Координати належать апаратові, а не операторові, проте перші й останні секунди запису прив'язують точку зльоту і посадки. Для FPV-апаратів з цифровою системою передачі відео окуляри з відповідним програмним забезпеченням пишуть окремий файл накладання бортової індикації, який при відтворенні або пост-обробці повертає на зображення, серед іншого, GPS-координати (О. Лян, 2023). Соціальні платформи при завантаженні відкидають метадані, проте файл, переданий у месенджері як документ, зберігає їх повністю.

Другий канал – візуальний зміст кадру, і тут методика противника є загальнодоступною, адже її роками відпрацьовували журналісти-розслідувачі. Напрямок і довжина тіні при відомому часі зйомки дають азимут камери і кільце можливих широт (Ю. ван дер Вейде, 2021; інструмент Shadow Finder від Bellingcat, 2024), а два кадри з різних днів звужують це кільце до кількох точок. Показовим є випадок, описаний виданням The Insider у вересні 2024 року: Міноборони РФ розмило частину зображення в ролику, поданому як удар по українських силах на Курщині, однак проєкт EjShahid геолокував зйомку за відбиттями у склі камери літака і встановив, що її зроблено за сотні кілометрів від заявленого місця. Видання зазначає, що російське відомство почало

розмивати місця зйомки лише нещодавно і з обмеженим успіхом. Розмиття впізнаваних об'єктів саме по собі не захищає кадр, у якому лишилися горизонт, рослинність, відбиття і тіні. При цьому поріг кваліфікації для такої роботи падає. Модель PIGEON Стенфордського університету (2024) розміщує понад 40 % вгадувань у межах 25 км від справжнього місця і в сліпому експерименті увійшла до верхніх 0,01 % гравців GeoGuessr. Комерційний сервіс GeoSpy, за публікацією 404 Media від січня 2025 року, визначав місце зйомки за рослинністю, архітектурою та відстанями між будівлями за секунди, і користувалися ним люди без підготовки. Для серії роликів одного підрозділу це означає накопичувальний ефект: кожне наступне відео, навіть геолоковане приблизно, звужує район попереднього.

Третій канал – час і закономірності публікації. Інтервал між ураженням і оприлюдненням, повторюваність ракурсів, висот і маршрутів, впізнавана манера монтажу й озвучення видають сектор відповідальності, час активності та спосіб дій підрозділу не гірше за координати. Цей канал не закривається жодною технічною обробкою, а лише дисципліною відбору. Водночас приклад прийнятної практики дає оприлюднення Службою безпеки України 7 червня 2025 року повного польоту одного FPV-апарата від зльоту до ураження бомбардувальника на аеродромі «Бєлая». Кадри вийшли через шість діб після завершення операції «Павутина», коли оперативна цінність відомостей про маршрут і точку запуску була вичерпана, а комунікаційна сила – збережена.

Нормативний рівень цього питання лишається непослідовним. Стаття 114-2 Кримінального кодексу України, запроваджена Законом від 24 березня 2022 року № 2160-IX, карає поширення інформації про переміщення, рух або розташування Збройних Сил «за можливості їх ідентифікації на місцевості», якщо така інформація не розміщувалася у відкритому доступі Генеральним штабом. Однак ця норма адресована сторонній особі і не дає відповіді на питання, за яких умов сам підрозділ вважається таким, що санкціоновано оприлюднив матеріал. Наказ Головнокомандувача Збройних Сил України від 3 березня 2022 року № 73 з подальшими змінами регулює роботу акредитованих медіа і визначає категорії обмежених відомостей, серед яких результати ракетних ударів, переміщення озброєння, розташування Сил оборони та позиції протиповітряної оборони. Проте власний контент підрозділів лишається поза його предметом, а рекомендації Військової служби правопорядку від грудня

2022 року зводяться до заклику не публікувати в реальному часі. Отже, між кримінальною забороною для сторонніх і загальними рекомендаціями для своїх утворилася прогалина: немає норми, яка б визначала, хто в підрозділі ухвалює рішення про оприлюднення, що саме перевіряється перед ним і яка відстрочка є обов'язковою.

З цією метою пропонується триступеневий відбір відеоматеріалу перед оприлюдненням. Технічний ступінь передбачає перекодування файла з відкиданням метаданих, вилучення файлів телеметрії та накладання бортової індикації, обрізання початку й кінця запису, що прив'язують точку зльоту і посадки, і видалення звукової доріжки, адже голоси, позивні й радіообмін ідентифікують екіпаж краще за зображення. Змістовий ступінь зводиться до самоперевірки на геолокованість: перед публікацією кадр перевіряється тими самими відкритими інструментами, що доступні противникові, і міряється часом, за який аналітик або модель виходить на район зйомки. Часовий ступінь передбачає відстрочку, яку визначає командир залежно від обстановки, а не фіксований строк, з обов'язковим урахуванням серії попередніх публікацій підрозділу. Для закріплення цього порядку пропонується доповнити керівні документи з інформаційної безпеки військових частин положенням такого змісту: «Відео- та фотоматеріали, отримані з безпілотних літальних апаратів, оприлюднюються від імені військової частини лише після технічного очищення від службових даних, перевірки на можливість установлення місця і часу зйомки за відкритими джерелами та після закінчення строку відстрочки, визначеного командиром з урахуванням раніше оприлюднених матеріалів».

Висновки. Відео з БпЛА є одночасно документом обліку, засобом стратегічних комунікацій і джерелом розвідувальних відомостей для противника, і саме третя якість досі не має ні вимірюваного показника, ні процедури. Три канали демаскування – службові дані, візуальний зміст і закономірності публікації – потребують трьох різних заходів, з яких лише перший є суто технічним. Подальше дослідження передбачає експериментальну оцінку часу до геолокації на вибірці вже оприлюднених відкритих відеоматеріалів засобами загальнодоступних моделей, без залучення неоприлюднених даних підрозділів.

Пулеко І. В., канд. техн. наук, доц.
Бородуліна М. В., курсантка
Житомирський військовий інститут імені С. П. Корольова

ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ ПІД ЧАС ВИВЧЕННЯ ЕЛЕМЕНТІВ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ

Для формування кваліфікованого складу операторів та технічного персоналу, що працюють з безпілотними авіаційними системами (БпАС), одного лише вивчення теоретичної бази недостатньо. Необхідно мати чітке уявлення про внутрішню архітектуру безпілотного апарата та механізми взаємодії його елементів. Класичні освітні засоби, такі як технічні схеми чи плакати, не завжди забезпечують належне просторове розуміння розташування вузлів. Окрім того, фізичні зразки часто перебувають у дефіциті, а постійні маніпуляції з розбиранням та збиранням справжнього літального апарата можуть призвести до його поломки або зносу. У доповіді обґрунтовано застосування доповненої реальності (Augmented Reality, AR) як засобу, що робить підготовку спеціалістів БпАС більш безпечною та наочною.

Принцип роботи доповненої реальності полягає у накладанні цифрового контенту на фізичне середовище. Це можуть бути анімації, схеми, підписи або тривимірні моделі, що відображаються в режимі реального часу. Важливою відмінністю від віртуальної реальності є те, що користувач продовжує взаємодіяти з реальним світом. Завдяки використанню таких інструментів, як Vuforia Engine та Unity AR Foundation, можливо створювати ефективні програми для мобільних платформ. Дослідження підтверджують високу перспективність AR для сфер технічного сервісу, оскільки вона спрощує візуалізацію складних процесів і знижує ризик помилок.

Для вивчення конструкції БпАС доцільно інтегрувати цифрову модель із реальним об'єктом або спеціальним маркером. Після ідентифікації об'єкта системою, користувач отримує можливість послідовно вивчати окремі компоненти: від рами, двигунів та гвинтів до регуляторів, польотного контролера, GNSS-модуля, акумулятора, камери та приймача. Можлива реалізація різних режимів, наприклад, покрокове відображення конструкції, демонстрація зв'язків між вузлами або візуалізація правильної послідовності збирання та розбирання з використанням підказок. Такий підхід дозволяє проводити тренування без прямого фізичного контакту з реальним пристроєм.

Наприклад, під час вивчення польотного контролера на екрані можна відобразити назви його роз’ємів, функціональну блок-схему, напрямки передавання даних і послідовність проходження сигналів від датчиків до систем керування.

Основна перевага AR полягає у можливості необмеженого повторення навчальних циклів без загрози пошкодження техніки. Оскільки пояснювальні елементи розміщені безпосередньо на об'єкті, користувачеві легше орієнтуватися в деталях, розуміти їхнє взаємне розташування та швидше переходити від теорії до практичної діяльності. Водночас слід зауважити, що AR не повинна повністю замінювати практичні заняття, а має слугувати ефективним інструментом для візуальної підтримки та попереднього навчання.

Впровадження подібних рішень у систему військової підготовки супроводжується певними викликами. Зокрема, програмне забезпечення має функціонувати автономно, не потребуючи постійного зв'язку з хмарними сервісами чи Інтернетом. Також слід враховувати обмежену потужність та заряд батареї мобільних пристроїв, а також можливе погіршення якості розпізнавання при недостатньому освітленні. Крім того, цифрові моделі потребують регулярного оновлення відповідно до модернізації техніки, щоб забезпечити їхню повну відповідність реальним зразкам.

Для підтвердження ефективності методу розробляється прототип AR-застосунку для конкретного типу БпЛА та проводиться порівняльний аналіз двох груп студентів: тих, хто навчався за традиційною методикою, та тих, хто застосовував AR. Можна проаналізувати швидкість засвоєння матеріалу, точність ідентифікації деталей та кількість помилок під час виконання практичних завдань. Такий експеримент дозволить отримати конкретні дані та оцінити реальну користь технології.

Таким чином, доповнена реальність є перспективним напрямом для підготовки фахівців у сфері БпАС. Вона забезпечує наочне ознайомлення з будовою систем без використання ресурсів реальної техніки. Подальшим етапом має стати розробка спеціалізованого прототипу застосунку та його практичне тестування.

Данилюк А. М.
Військовий інститут Київського національного університету
імені Тараса Шевченка

ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ ТА БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ У ЗАВДАННЯХ МЕДИЧНОЇ ЕВАКУАЦІЇ, ПОРЯТУНКУ ЦИВІЛЬНОГО НАСЕЛЕННЯ ТА ВИВЕЗЕННЯ ТІЛ ЗАГИБЛИХ ДЛЯ ПОДАЛЬШОГО ОБМІНУ

Одним із найбільш людиноцентричних напрямів розвитку безпілотних технологій у поточній війні стало їх застосування не для ураження, а для порятунку – евакуації поранених військовослужбовців, цивільного населення та вивезення тіл загиблих. Насичення прифронтової смуги ворожими FPV-дронами й дронами-«ждунами» перетворило класичну евакуацію броньованим транспортом чи пішим порядком на надзвичайно ризиковану операцію, тоді як безпілотні платформи дозволяють виконувати ці завдання, мінімізуючи ризик для життя як евакуйованих, так і особового складу.

Найбільш системно розвинений напрям – медична евакуація наземними роботизованими комплексами (далі – НРК). Міністерство оборони України допустило до застосування логістично-евакуаційний комплекс «Вепр», здатний одночасно вивезти двох поранених. За даними системи ситуаційної обізнаності DELTA, кількість завдань НРК зросла більш ніж утричі за півроку, значною мірою завдяки евакуаційним і логістичним місіям. Паралельно розвивається повітряна евакуація важкими мультикоптерами в «сірій зоні», де рух броньованої техніки практично неможливий. Досвід Третього армійського корпусу та полку безпілотних систем «Kraken 1654» засвідчує, що евакуація цивільних і поранених НРК стає окремим напрямом роботи. Вивезення тіл загиблих є першою ланкою державного механізму репатріації та обміну.

Водночас нині ці рішення переважно існують як окремі платформи, що не об’єднані в єдину систему. Аналіз сучасних наукових публікацій з автономної медичної евакуації дозволяє виокремити інновації, які можуть забезпечити перехід від окремих засобів до цілісної системи евакуації.

Серед них:

Мультидоменна евакуаційна система, у якій безпілотні літальні апарати (далі – БпЛА) і НРК діють як єдиний комплекс: БпЛА веде розвідку маршруту,

НРК забирає постраждалого, за потреби повітряна платформа продовжує транспортування. Переваги: скорочується час евакуації; НРК рухається маршрутом, попередньо перевіреним з повітря; розподіл функцій між платформами підвищує живучість системи. Недоліки: ускладнюється керування кількома платформами, ця проблема може бути усунена частковим використанням штучного інтелекту; зростають вимоги до стійкого зв'язку в умовах радіоелектронної боротьби; потрібні підготовлені оператори та значні ресурси.

Евакуаційний модуль із вимірюванням життєвих показників і дистанційним медичним супроводом. Під час руху НРК модуль передає пульс, температуру, частоту дихання, стан свідомості, а медик на відстані оцінює стан постраждалого та визначає пріоритетність евакуації. Переваги: план дій щодо допомоги постраждалому ухвалюються ще до прибуття на медичний пункт; рішення ґрунтуються на об'єктивних даних; можливість автоматично фіксувати данні в документації. Недоліки: потрібен захищений канал передачі, невразливий до перешкод і перехоплення; датчики можуть давати хибні показники під час руху й вібрації; модуль збільшує масу, вартість і енергоспоживання НРК.

Вибір маршруту евакуації за допомогою штучного інтелекту за принципом human-in-the-loop. За допомогою БпЛА, що веде розвідку маршруту система обирає не найкоротший, а найбезпечніший маршрут з урахуванням прохідності, ризику ураження, перешкод і поточної обстановки, а рішення про евакуацію ухвалює оператор або медик. До цього можна додати єдиний цифровий запис кожного постраждалого чи загиблого: від місця виявлення до кінцевого пункту, що важливо й для подальшої репатріації тіл. Переваги: знижується ризик втрати платформи та постраждалого; людина зберігає контроль за ключовими рішеннями; полегшується облік. Недоліки: Ефективність рішень залежить від актуальності розвідувальних даних; швидка зміна обстановки ускладнює прогнозування ризиків; існує небезпека надмірної довіри оператора до рекомендацій системи.

Впровадження цих інновацій потребує стандартизації процедур, розширення номенклатури евакуаційних платформ і підготовки персоналу. Окремого значення набуває психологічний супровід операторів НРК і БпЛА та військовослужбовців, які працюють із тілами загиблих, оскільки саме вони несуть відповідальність за прийняття рішень, що спричиняє значне емоційне навантаження.

Говтва Д. С.
Військовий інститут Київського національного університету
імені Тараса Шевченка

ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ У ЗАВДАННЯХ ДИСТАНЦІЙНОГО МІНУВАННЯ ТА РОЗМІНУВАННЯ МІСЦЕВОСТІ

Мінна небезпека залишається однією з найбільш системних проблем, породжених повномасштабною війною. Безпілотні літальні апарати (далі – БпЛА) стали інструментом, що розв’язує одночасно два завдання – встановлення мінних загороджень і подальше розмінування місцевості.

Важкі дрони-бомбери («Кажан», «Вампір», «Немезида», «Королева Шершнів») фактично перебрали функції спеціалізованих систем дистанційного мінування. З дронів скидають протитанкові міни ТМ-62, ТМ-72, ПТМ-1, ПТМ-3 та дедалі частіше протипіхотні боєприпаси. Противник застосовує аналогічний підхід: зафіксовано скидання з дронів типу «Молнія» малопомітних мін «Пряник». Через це мінні поля постійно оновлюються й не завжди документуються.

Протилежний за спрямуванням напрям – застосування безпілотних засобів для розмінування. Міністерство оборони України кодифікувало наземний роботизований комплекс-сапер NEO-1 та запровадило спеціальність пілота-розміновувача. Показовим є досвід Третього армійського корпусу: на напрямку Шандриголового робот-розмінувальник розчистив тридцять кілометрів маршруту за дві ночі, тоді як двом ротам саперів знадобився б приблизно тиждень. Проте сертифікація нових зразків відстає від бойового попиту, а повне очищення територій України, за оцінками фахівців, потребуватиме щонайменше десяти років навіть за широкого залучення дронів.

Аналіз академічних оглядів останніх років показує, що найбільший потенціал має не окремий дрон із одним датчиком, а інтелектуальна система виявлення вибухонебезпечних предметів. Можна виокремити три інновації, а саме:

Першою інновацією є комплексне виявлення вибухонебезпечних предметів: БпЛА несе магнітометр, тепловізор і мультиспектральну або гіперспектральну камеру, а дані об’єднуються в геоінформаційній системі та

аналізуються методами машинного навчання. Переваги: різні сенсори компенсують слабкі сторони один одного (магнітометр виявляє металеві боєприпаси, тепловізор – температурні аномалії ґрунту, спектральна камера – зміни рослинності й ґрунту); зменшується кількість хибних спрацювань; обстеження відбувається без контакту із землею. Недоліки: збільшуються маса, вартість і складність обладнання; потрібні синхронізація й калібрування сенсорів; результат залежить від погоди, типу ґрунту та рослинності; для навчання моделей потрібні великі набори даних.

Другою інновацією є карта ймовірності мінної небезпеки, яку формує штучний інтелект. Замість бінарної відповіді «міна є / міни немає» система класифікує ділянки за рівнями ризику: із низькою ймовірністю небезпеки, ділянка, що потребують додаткової перевірки та з високою ймовірністю вибухонебезпечних предметів, а остаточне рішення приймає сапер. Переваги: сапери зосереджуються на найнебезпечніших ділянках; прискорюється аналіз даних; зберігається відповідальність людини за рішення. Недоліки: хибне віднесення небезпечної ділянки до безпечної має критичні наслідки; пороги ймовірності потрібно калібрувати для кожного типу місцевості; безпілотні засоби не замінюють сертифікований процес гуманітарного розмінування.

Третьою інновацією є динамічна цифрова карта («цифровий двійник») мінного поля з обробкою даних безпосередньо на борту БпЛА. Ланцюг має вигляд: БпЛА – сенсори – штучний інтелект – геоінформаційна система – цифрова карта – повторне обстеження – оновлення карти. На її основі можна формувати карту пріоритетності розмінування з урахуванням близькості населених пунктів, доріг, критичної інфраструктури, сільськогосподарських земель і маршрутів евакуації. Переваги: карта залишається актуальною, що важливо для недокументованих мінних полів; бортова обробка дозволяє передавати лише важливі фрагменти даних за нестійкого зв’язку; розмінування планується за гуманітарними пріоритетами. Недоліки: потрібні єдині стандарти даних і їх інтеграція із системами ситуаційної обізнаності; бортові обчислювачі мають обмежену потужність та споживають енергію; цифрові карти потребують кіберзахисту, а їхня достовірність залежить від якості первинних даних.

Таким чином, безпілотні авіаційні комплекси є двоцільовим інженерним інструментом, а запропоновані інновації переводять їх від «виявлення міни» до планування цілого комплексу завдань, включаючи розмінування. Необхідними умовами цього є стандартизація платформ і форматів даних та інтеграція з цифровими системами обліку мінної обстановки.

Виговська О. О.
Військовий інститут Київського національного університету
імені Тараса Шевченка

ПОВІТРЯНЕ ДЕСАНТУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

Наземні роботизовані комплекси (далі – НРК) перетворилися з допоміжного логістичного інструменту на самостійний бойовий засіб, здатний виконувати ударні, розвідувальні та інженерні завдання без ризику для життя особового складу. Ефективність їх застосування обмежує наземна мобільність, а саме: рух до об’єкта ускладнюють мінні поля, зруйновані дороги та ділянки, насичені ворожими FPV-дронами. Задля усунення даної проблематики доцільно застосовувати технологію повітряного перекидання («десантування») НРК важкими ударними безпілотними літальними апаратами (далі – БпЛА), масово застосована Збройними Силами України під час операції «Вівальді».

У світовій практиці такі системи отримали назву «marsupial» («сумчасті»). У Сполучених Штатах подібні розробки велися понад три десятиліття, однак не досягли бойового застосування, тоді як в Україні від задуму до першого використання пройшло десять днів. Створено НРК «Десантник» і систему його точного скидання з важкого дрона-бомбера «Грифон». Технологія дозволяє доставити НРК на понад десять кілометрів углиб тилу противника; за оцінкою операторів, успішність застосування становить близько 80%. Водночас дрон-носій залишається ціллю для ворожих засобів протиповітряної оборони, FPV-дронів і дронів-«ждунів», а точність скидання знижується за складних метеоумов, у темну пору доби..

Аналіз академічної літератури з гетерогенних повітряно-наземних систем дозволяє виокремити три інновації, які усувають ці недоліки, а саме:

Перша інновація – автономне десантування НРК із підтримкою штучного інтелекту під час вибору місця висадки. Система аналізує рельєф, перешкоди та метеоумови, пропонує оператору оптимальну зону, а коригувальні алгоритми керування скиданням зменшують похибку приземлення порівняно з некерованим скиданням. Переваги: вища ймовірність збереження НРК; менший час перебування носія в зоні ураження; менша залежність від досвіду оператора; можливість роботи в складних умовах. Недоліки: бортові датчики й обчислювач

збільшують масу носія та зменшують корисне навантаження; навігація вразлива до радіоелектронного придушення; помилки розпізнавання рельєфу можуть призвести до втрати комплексу.

Друга інновація – цифровий двійник повітряно-наземного роботизованого комплексу. Він дозволяє змоделювати політ носія, процес скидання, приземлення НРК, поведінку системи за різних умов і можливі відмови ще до реального застосування, а також використовувати модель для навчання операторів. Переваги: зменшуються витрати на випробування й втрати техніки; оптимізуються параметри скидання; забезпечується безпечне відпрацювання нестандартних та критичних сценаріїв застосування. Недоліки: точність моделі залежить від реальних даних, яких бракує; модель потребує перевірки в польових випробуваннях; існує ризик надмірної довіри до результатів моделювання.

Третя інновація – групова повітряно-наземна система за концепцією «людина – повітряний робот – наземний робот». Один носій доставляє кілька різнорідних НРК, які після висадки виконують взаємодоповнювальні функції, а людина ухвалює ключові рішення, передаючи роботам рутинні й небезпечні дії. Переваги: зростає масштаб і гнучкість застосування; одна доставка замінює кілька; людина зберігає контроль над результатом. Недоліки: обмежена вантажопідйомність носія; ускладнюється координація платформ за умов радіоелектронної боротьби; зростає когнітивне навантаження на оператора, що потребує спеціальної підготовки.

Досвід операції «Вівальді» доцільно розглядати як фундамент для розробки стандартних операційних процедур та випробування тактики застосування «сумчастих» безпілотних систем. Впровадження цих інновацій дозволить перейти від тактичного використання окремих безпілотних платформ до побудови стійких, високоавтономних гетерогенних комплексів. Зазначене зумовлює необхідність включення відповідної проблематики до програм підготовки курсантів (слухачів) і фахівців з інженерно-технічних та безпілотних систем.

Марич О. В.
Національний університет оборони України

ОБҐРУНТУВАННЯ СПОСОБІВ ЗАСТОСУВАННЯ РОТИ БЕЗЕКІПАЖНИХ НАЗЕМНИХ КОМПЛЕКСІВ У СКЛАДІ ЗАГАЛЬНОВІЙСЬКОВОЇ БРИГАДИ

Поширення безекіпажних наземних комплексів у діяльності підрозділів Сил оборони України формує передумови для переходу від використання окремих роботизованих платформ до їх системного застосування у складі спеціалізованих підрозділів. У межах загальновійськової бригади такий підрозділ має забезпечувати виконання завдань, пов’язаних зі зниженням ризику для особового складу, підвищенням стійкості забезпечення та розширенням можливостей виконання завдань у складних умовах обстановки. У цьому контексті актуальним є обґрунтування способів застосування роти безекіпажних наземних комплексів, які мають визначатися не лише технічними характеристиками платформ, а насамперед змістом завдань, місцем підрозділу в бойовому порядку та характером взаємодії з іншими елементами бригади.

Роту безекіпажних наземних комплексів доцільно розглядати як організаційно-функціональний елемент загальновійськової бригади, спроможності якого реалізуються через виконання визначених груп завдань. До них належать транспортно-логістичні, евакуаційні, інженерні, розвідувальні та інші завдання, виконання яких із застосуванням безекіпажних платформ дає змогу зменшити безпосередню участь особового складу в найбільш небезпечних ділянках бойової діяльності. Відповідно, спосіб застосування роти має відображати порядок використання її сил і засобів для досягнення конкретного результату в інтересах загальновійськових підрозділів.

Одним із базових способів доцільно вважати централізоване застосування роти в інтересах бригади, коли її сили і засоби використовуються за єдиним задумом для виконання найбільш пріоритетних завдань. Такий підхід створює умови для зосередження необхідної кількості комплексів на визначених напрямках, забезпечує централізоване управління, технічне обслуговування та відновлення. Його перевагою є можливість раціонального перерозподілу ресурсів відповідно до зміни обстановки та пріоритетності завдань. Водночас ефективність такого способу залежить від своєчасності управлінських рішень,

стійкості зв’язку та можливості оперативного переміщення комплексів між підрозділами.

Іншим способом є децентралізоване застосування окремих елементів роти в інтересах визначених підрозділів бригади. У цьому випадку частина сил і засобів може тимчасово використовуватися для підтримки конкретного батальйону або іншого елемента бойового порядку. Такий підхід підвищує оперативність реагування на потреби підрозділів, скорочує час між виникненням потреби та початком виконання завдання, а також сприяє кращому врахуванню особливостей конкретної ділянки місцевості й характеру дій. Водночас розосередження засобів ускладнює підтримання їх технічної готовності, управління та відновлення, що потребує чіткого визначення порядку підпорядкування і забезпечення.

Окремо доцільно виділити комбінований спосіб застосування, який поєднує централізоване управління основною частиною роти з тимчасовим виділенням окремих груп для підтримки підрозділів бригади. Такий підхід найбільшою мірою відповідає потребі в адаптивності, оскільки дозволяє зберігати резерв спроможностей на рівні бригади та водночас забезпечувати безпосередню підтримку підрозділів. Комбінований варіант може бути доцільним за умов нерівномірного навантаження на різних напрямках, зміни пріоритетності завдань та необхідності швидкого перерозподілу безекіпажних платформ.

Спосіб застосування роти має також визначатися характером конкретного завдання. Для транспортно-логістичних завдань ключового значення набувають вантажопідйомність, прохідність, тривалість автономної роботи та можливість повторного використання маршруту. Під час евакуаційних завдань зростають вимоги до надійності, стабільності руху та узгодженості дій із медичними й загальновійськовими підрозділами. Інженерне застосування потребує врахування особливостей місцевості, перешкод і можливості використання спеціалізованого обладнання. Таким чином, універсальний спосіб застосування для всіх типів завдань є малоефективним, а структура дій роти має адаптуватися до функціонального призначення залучених комплексів.

Важливою умовою результативного застосування є інтеграція роти БНК у систему управління загальновійськової бригади. Йдеться не лише про передачу команд, а й про отримання даних щодо обстановки, визначення пріоритетів, розподіл завдань, контроль їх виконання та своєчасне відновлення

готовності техніки. За відсутності такої інтеграції навіть достатня кількість сучасних платформ може використовуватися фрагментарно та не забезпечувати очікуваного ефекту.

На вибір способу застосування також впливають умови бойової обстановки, стан маршрутів, рівень технічної готовності комплексів, можливості управління та забезпечення, характер протидії противника. Тому доцільно передбачати не один фіксований порядок застосування роти, а декілька варіантів, які можуть змінюватися залежно від завдань і умов їх виконання.

Отже, обґрунтування способів застосування роти безекіпажних наземних комплексів має ґрунтуватися на поєднанні функціонального призначення підрозділу, характеру завдань, ступеня централізації управління та умов бойового застосування. Найбільш доцільним є використання гнучкої моделі, що передбачає централізоване, децентралізоване та комбіноване застосування сил і засобів роти залежно від потреб загальновійськової бригади. Такий підхід створює основу для подальшого обґрунтування структури підрозділу, визначення необхідних спроможностей та формування вимог до його оснащення і забезпечення.

Староконь Є. Г., канд. псих. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

ЛІДЕРСТВО ТА КОМАНДНА ВЗАЄМОДІЯ В ЕКІПАЖІ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА

Проблема лідерства в малих соціальних групах є найбільш значущою через процеси безпосереднього спілкування і відповідальної взаємодії в екіпажах безпілотних комплексів. В такій групі військовослужбовці перебувають у безпосередньому контакті, мають спільне завдання, встановлені правила взаємин та усвідомлюють свою належність до групи. І тому лідерство і командна взаємодія тут має особливе значення, оскільки рішення та поведінка одного військовослужбовця безпосередньо впливають на психологічні стани, поведінку та результати діяльності інших.

Основна психологічна проблема полягає в тому, що в екіпажі формальний командир і неформальний лідер можуть бути різними людьми. Коли, командир

призначений офіційно, але найбільший авторитет у групі має інший військовослужбовець і члени групи більше орієнтуються на його думку, то це створює багато проблем пов'язаних з виконанням завдань та виживанням, створює суттєві ризики для управління.

Але найкраща ситуація – це коли формальний командир одночасно є фактичним лідером групи. Саме він і ніхто інший спроможний ефективно нівелювати основні психологічні проблеми підлеглих. Серед найбільш небезпечних для ефективного функціонування екіпажу можна виділити хронічне нервово-психічне напруження, перевантаження когнітивної сфери (увага, сприймання, мислення, уява), втома та недосипання, стрес від високої відповідальності, емоційне виснаження, втрата БПЛА або невиконання завдання, професійне вигорання тощо.

Зрозуміло, що дані психологічні явища суттєво у негативному плані впливають на командну взаємодію: узгоджену роботу всіх членів екіпажу, за якої кожен розуміє свою роль, завдання інших, поточну ситуацію та порядок обміну інформацією.

Завдання лідера-офіційного керівника - забезпечити результативне та ефективне функціонування команди (екіпажу). Основою перетворення підрозділу на команду мають бути такі дії лідера:

- визначення функціональних ролей і сектору особистої відповідальності кожного члена екіпажу за виконання наказу;
- узгодження та координація дій членів екіпажу як єдиної бойової системи;
- налагодження взаємного контролю і самоконтролю з метою уникнення помилок або небезпечних явищ в команді;
- організація взаємодопомоги, взаємозамінності і підтримки членів екіпажу;
- відкрита комунікація в команді на основі довіри без страху критики чи покарання;
- колегіальне ухвалення рішень тощо.

Таким чином, командна взаємодія екіпажу БПЛА - це узгоджена діяльність його членів, яка засновується на чіткому розподілі функціональних ролей, взаємній довірі, позитивних міжособистісних стосунках, взаємному контролі та спільній відповідальності за виконання завдання.

На шляху до такого стану підрозділу перед лідером можуть стояти серйозні психологічні та організаційні перешкоди. Коротко охарактеризуємо найнебезпечніші з них:

1. Конкуренція формального та неформального лідерства. Досвідчений військовослужбовець із високим бойовим авторитетом може фактично впливати на групу сильніше ніж молодий командир. Тобто, неформальний авторитет в одній ситуації підтримує командира, але в іншій формує альтернативний центр впливу. І для підрозділу це дуже небезпечно.

2. Відсутність довіри. Недовіра породжує невпевненість, що критично впливає на морально-психологічний стан екіпажу і, як наслідок, на результати бойової діяльності.

3. Під впливом групового тиску може формуватися «неефективна» одностайність екіпажу при виробленні рішень. Конформізм, прагнення «бути як усі» може перешкоджати висловленню критичної думки, ефективних пропозицій.

4. Бойовий стрес, небезпечна ситуація швидко змінюють структуру взаємин. Командир, який був лідером у повсякденній діяльності, не завжди спроможний демонструвати тут лідерські якості.

Тому лідерство і командна взаємодія в екіпажі - це не лише здатність підлеглих працювати під тиском, витримувати стрес, а й уміння лідера-офіційного керівника впливати на соціально-психологічні процеси, що існують в команді.

Омельчук І. А.
Пількевич І. А., д-р техн. наук, проф.
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ ПЕРЕВАГ СЕРВОПРИВОДІВ ЕЛЕКТРОМАГНІТНОЇ СИСТЕМИ

Безпілотні літальні апарати (БпЛА) — це літальні засоби, які можуть виконувати політ без пілота на борту. Керування ними здійснюється дистанційно з наземної станції, з іншого повітряного судна або автоматично, відповідно до заздалегідь заданих алгоритмів і програм. Для забезпечення стабільного польоту та виконання команд керування БпЛА оснащуються системами зв’язку, засобами автоматичної стабілізації й контролю просторового положення, зокрема автопілотами та польотними контролерами. Важливу роль у цій системі відіграють виконавчі механізми, зокрема рульові приводи, які забезпечують зміну положення керувальних поверхонь.

За наявними даними, на виготовлення рульового приводу разом із джерелом живлення може припадати до 40% загальної трудомісткості виробництва безпілотного літального апарата. Така частка свідчить про важливість удосконалення конструкції приводних механізмів, зниження складності їх виготовлення та підвищення ефективності роботи. Тому пошук нових конструктивних рішень для рульових приводів залишається актуальним напрямом розвитку авіаційного машинобудування.

Під час проєктування рульових приводів для малорозмірних БпЛА необхідно враховувати низку вимог. До основних із них належать простота конструкції, невелике енергоспоживання, помірна вартість виготовлення, високі швидкодійність і динамічні характеристики. Крім того, привод повинен забезпечувати точне встановлення та утримання керувального органу в заданому положенні в межах усього робочого діапазону його переміщення.

Розроблення безпілотних літальних апаратів, сервоприводів і систем керування ними є предметом досліджень багатьох науковців та інженерів. Основна увага приділяється поліпшенню технічних характеристик літальних апаратів, удосконаленню алгоритмів керування та відповідного програмного забезпечення, підвищенню швидкодії й точності сервоприводів, а також забезпеченню плавності їх роботи. Водночас важливим завданням залишається пошук технічних рішень, які дають змогу зменшити масу, габарити та енергоспоживання приводів без погіршення їхніх експлуатаційних характеристик.

Для керування польотом безпілотних літальних апаратів застосовують різні аеродинамічні поверхні, зокрема кермо висоти, елерони та кермо напрямку. Залежно від конструкції й призначення літального апарата також можуть використовуватися гальмівні щитки та інтерцептори. Зміна положення цих елементів здійснюється за допомогою рульових приводів, які мають долати аеродинамічні навантаження, що виникають під час відхилення керувальних поверхонь. Значення цих навантажень залежать від типу та геометричних параметрів відповідного органу керування, а також від швидкості й режиму польоту.

Основні конструктивні рішення рульових приводів БпЛА можна поділити на дві групи. До першої належать приводи на основі електромагнітних перетворювачів, у яких переміщення рухомих елементів забезпечується почерговою зміною електромагнітних сил. Другу групу становлять електромеханічні приводи, в яких електродвигун працює разом із гвинтовими,

зубчастими або кулачковими механізмами. Такі механізми дають змогу змінювати передавальне відношення, збільшувати крутний момент і перетворювати обертальний рух відповідно до потреб системи керування. Сервоприводи є важливою складовою системи керування літальним апаратом, оскільки від їхньої точності, швидкодії та надійності значною мірою залежить ефективність керування польотом.

Окрему групу становлять рульові приводи на основі електромагнітних перетворювачів. Типову конструкцію сервоприводу з поляризованим електромагнітним перетворювачем, який працює в імпульсному режимі та забезпечує поворот якоря, наведено на рис. 1. Однією з особливостей такої конструкції є розміщення лише однієї обмотки на рухомому якорі. Це дає змогу спростити конструкцію та потенційно поліпшити масогабаритні характеристики пристрою.

Основними елементами імпульсного рульового приводу є: 1 — постійні магніти; 2 — магнітопровід; 3 — якір; 4 — керувальні поверхні; 5 — пружина; 6 — обмотка; 7 — вал.

Під час подавання керувального сигналу якір повертається навколо осі вала 7, змінюючи положення керувальних поверхонь. Після припинення дії сигналу пружина 5 сприяє поверненню рухомої частини механізму до початкового положення.

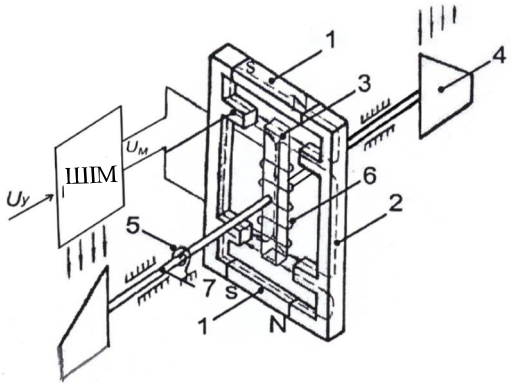


Рис.1. Схема електромеханічного приводу БпЛА

До основних переваг такого приводу належать компактність, конструктивна простота, надійність і висока швидкодія. Водночас його конструкція має певні обмеження. Зокрема, початкове положення рухомих елементів визначається переважно дією пружини, що може ускладнювати

забезпечення точного й стабільного позиціювання за наявності зовнішніх навантажень. Крім того, пружина створює протидійний момент під час відхилення якоря, через що частина електромагнітного моменту витрачається на подолання її опору. Це може знижувати корисний момент на валу та обмежувати можливості застосування таких приводів у системах керування безпілотними літальними апаратами.

Попри зазначені недоліки, розглянута конструкція має потенціал для подальшого вдосконалення. Зміна принципу формування та утримання початкового положення, а також оптимізація взаємодії електромагнітних і механічних елементів можуть сприяти поліпшенню характеристик приводу та розширенню сфери його застосування в системах керування польотом БпЛА.

Далі буде більш детально розглянуто особливості роботи електромагнітних приводів та особливості запронованого вдосконалення.

Ефективність запропонованого конструктивного рішення доцільно оцінювати за допомогою математичної моделі рульового електроприводу. Для цього необхідно розглянути рівняння, які описують роботу його основних елементів і взаємозв'язок між електричними та механічними параметрами системи.

Оскільки керування обмотками здійснюється за допомогою напруги постійного струму, для подальшого аналізу розглянемо модель сервоприводу на основі двигуна постійного струму. Такий підхід дає змогу описати електричні процеси в обмотці, формування електромагнітного моменту та рух механічних елементів, а також оцінити вплив параметрів конструкції на динамічні характеристики приводу.

На вхід підсилювача такого приводу надходить сигнал неузгодженості

$\Delta U = U_{\text{п}} - U_{\text{зз}}$.

де $U_{\text{п}}$ – напруга з підсилювача потужності;

$U_{\text{зз}}$ – сигнал зворотного зв'язку.

За умови що перетворення в електронних компонентах є безінерційними, то напруга подається на якір двигуна сервопривода буде обраховуватися наступним чином:

$U_{\text{я}} = k_y \Delta U,$

де k_y – коефіцієнт підсилення підсилювача

При малому вхідному опорі підсилювача, рівняння рівноваги напруг буде мати вигляд:

$$U_{\text{я}} = R_{\text{я}} i_{\text{я}} + L_{\text{я}} \frac{di_{\text{я}}}{dt} + c_e \Omega_{\text{дв}},$$

де $R_{\text{я}}$ – активний опір якоря;

$i_{\text{я}}$ – струм якоря;

$L_{\text{я}}$ – індуктивність якоря;

c_e – коефіцієнт протиелектрорушійної сили двигуна;

$\Omega_{\text{дв}}$, – частота обертання двигуна.

При протіканні струму через якір двигуна виникає електромагнітна взаємодія і механічний момент.

$$\mathrm{M}_{\text{дв}} = \mathrm{c}_{\text{м}} i_{\text{я}},$$

де $\mathrm{c}_{\text{м}}$ – коефіцієнт моменту двигуна;

$\mathrm{i}_{\text{я}}$ – струм якоря.

Для узгодження можливостей двигуна з потрібними величинами моментів і швидкостей на кермі застосовують механічний редуктор з коефіцієнтом передачі q (звичайно q>>1). У цьому випадку момент двигуна, приведений до вихідного вала (осі керма), має значення

$$\mathrm{M}_{\text{дв}} = \mathrm{M}_{\text{дв}} q.$$

де q – коефіцієнт передачі редуктора двигуна.

Враховуючи дані рівняння можна зазначити що в електромагнітному приводі відсутній один з елементів інерційності, а саме виникнення протиелектрорушійної сили двигуна, що значно покращує динамічні властивості такої схеми приводу.

Отже, з метою покращення динамічних характеристик приводів кермових поверхонь безпілотних літальних апаратів, доцільно використовувати електромагнітні системи повороту рулів, з фіксованими кутами відхилення як перспективні та такі, що мають шляхи вдосконалення та розвитку. Така система забезпечить швидке і однозначне переставляння рульових поверхонь в необхідне положення під час керування літальним апаратом, та наступне повернення їх в нейтральне. Даний спосіб приводу рулів дасть змогу забезпечити їх більшу динамічність та покращити параметри маневреності, безпілотних літальних апаратів.

Музичак А. З., канд. техн. наук, доц.
Чернов Є. В.
Військовий інститут танкових військ НТУ “ХПІ”

ФУНКЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ КЕРУВАННЯ РОЗВІДУВАЛЬНИМИ БЕЗПІЛОТНИМИ НАЗЕМНИМИ КОМПЛЕКСАМИ

Ще кілька років тому безпілотні наземні комплекси (БпНК) сприймалися на полі бою як екзотика, яка не має практичного впливу на реальний перебіг подій на полі бою. Проте сьогодні вони поступово стають окремим інструментом ведення війни, який дозволяє виконувати завдання, недоступні іншим технічним засобам, а також винести найризикованіші операції за межі прямої участі людини.

Кількість місій, що виконуються з використанням безпілотних наземних комплексів, постійно зростає (рис. 1). Лише протягом поточного 2026 року інтенсивність застосування БпНК зросла більш ніж у 3 рази.

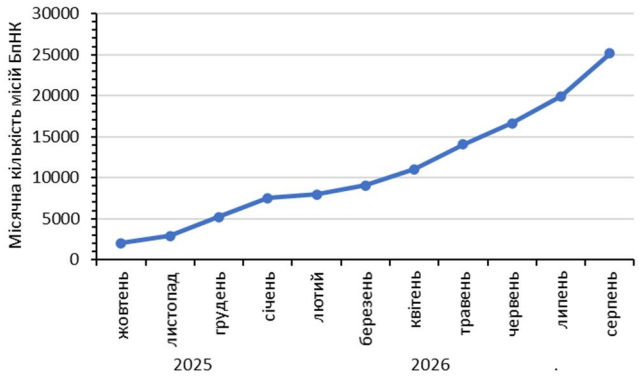


Рис. 1. – Динаміка зміни застосувань БпНК на фронті

Одночасно з кількісним зростанням розширюються також сфери застосування безпілотних наземних комплексів. На початках БпНК в основному залучали до вирішення логістичних та інженерних завдань а також місій камікадзе. Надалі, досить швидко додалися евакуаційні місії, які незважаючи на видиму подібність до логістичних, значною мірою від них відрізняються. А наступним важливим кроком стало залучення безпілотних наземних комплексів до виконання вогневих завдань, як в оборонному так і наступальному видах бою. Іншими напрямами, де безпілотні наземні комплекси ще не розкрили свій потенціал, є ведення спостереження, розвідка та патрулювання на лінії бойового зіткнення.

Слід відзначити, що в аналізах розвитку безпілотних наземних комплексів значну увагу приділяють технологічній складовій упускаючи з виду людський фактор. Проте будь-який безпілотний наземний комплекс працює у зв’язці з оператором, а точніше під його постійним управлінням. А отже успішність чи провал місії у першу чергу залежить від оператора.

Станом на сьогодні ефективність застосування БпНК значною мірою визначається майстерністю оператора, яка суттєво виходить за межі моторних навиків керування. Додатково, майстерність оператора включає вміння утримувати стійкий зв’язок, орієнтування на місцевості, використання технічних особливостей конкретної моделі БпНК. Також важливими є вміння швидко оцінювати обстановку, приймати зважені рішення, зберігати спокій за умов постійного психоемоційного навантаження тощо. Тому, частина військовослужбовців, які опанували технічні навики управління БпНК, так і не стають справді майстерними операторами. Як наслідок, нестача майстерності оператора частково гальмує подальше стрімке поширення безпілотних технологій у підрозділах.

Впровадження систем штучного інтелекту (ШІ) для керування БпНК може не лише сприяти вирішенню окресленої проблеми, а й підвищити ефективність застосування безпілотних наземних систем в загальному. Це зумовлено тим, що за багатьма параметрами системи штучного інтелекту перевершують людський мозок (табл. 1). Тобто, за умови добре навченого штучного інтелекту у людини-оператора практично немає шансів вийти з довобою переможцем.

Проте розроблення досконалого штучного інтелекту, здатного справитися з усіма викликами під час керування БпНК на сьогодні є по суті нездійсненним завданням. Технічно можливе лише делегування системам ШІ окремих елементів автономізації безпілотного наземного комплексу. При цьому наперед неможливо точно сказати, в котрому з обраних напрямів прорив станеться швидше.

Проте, можна впевнено стверджувати, що впровадження елементів штучного інтелекту в безпілотні наземні комплекси буде значною мірою відрізнятися від розвитку аналогічних функцій в безпілотних літальних апаратах (БпЛА). На сьогоднішній день основними функціями ШІ, що впроваджуються в БпЛА, є круїз-контроль (автономний проліт смуг активної дії РЕБ) та донаведення (знищення цілі в автономному режимі після її фіксації оператором). Також іде активна робота над функцією автономного пошуку цілей.

Таблиця 1

Порівняння швидкості реакції людини та системи штучного інтелекту

Тип реакції	Тривалість реакції		Примітка
	людина	система ШІ	
Розпізнавання об'єкта у відеопотоці	~0,5–2 с для простого випадку	~10–100 мс на кадр (залежно від потужності обчислювача)	ШІ може швидко класифікувати кадри
Вибір із кількох варіантів: вліво/вправо, ціль/не ціль	~300–800 мс і більше	~10–200 мс	у людини додається час розпізнавання, вибору й моторної відповіді
Рішення про ураження цілі	секунди – хвилини	технічно може бути мс, до кількох секунд	
Проста сенсорна реакція: побачив сигнал → натиснув кнопку	~200–350 мс	~1–50 мс після отримання сигналу	людина обмежена фізіологією нервової системи; проста візуальна реакція становить сотні мс.

Переміщення БпЛА з однієї точки в іншу є в основному рутинною операцією через практичну відсутність на шляху будь-яких перешкод, що значно спрощує вимоги як до параметрів нейроморфних (графічних чи тензорних) процесорів так і до архітектури нейронної мережі. Для безпілотного наземного комплексу переміщення із однієї точки в іншу навпаки, є однією з найскладніших частин місій. Це дозволяє припустити, що функції автономного переміщення БпНК будуть реалізовані в останню чергу, тоді як практичної автоматизації набуватимуть інші функції.

Усі функції, властиві безпілотному наземному комплексу, можна розділити на дві частини:

управління базовою платформою (колісною чи гусеничною),

управління функціональним модулем, що відображає специфіку застосування БпНК.

Стосовно розвідувального БпНК управління функціональним розвідувальним модулем може передбачати такі функції:

статичне спостереження за визначеною ділянкою на лінії бойового зіткнення та передача даних оператору,

перемикання між камерами та їх режимами, підбір оптимальних параметрів камер,

використання оптичного збільшення для детальнішого вивчення окремих елементів ландшафту.

У першу чергу на штучний інтелект можна перекласти функцію спостереження, включаючи аналіз відеопотоку, виявлення змін та їх підсвічування для оператора. На сьогоднішній день штучний інтелект достатньо добре справляється з такими завданнями, до того ж рівень його уваги не змінюється з плином часу, як це властиво людині. Впровадження такої функції бажане ще й тим, що подібні функції також активно розробляються як для FPV-дронів так і для зенітних дронів-перехоплювачів. Також штучний інтелект добре справиться із завданням підбору оптимальних параметрів камери (як денної так і тепловізійної).

Щодо інших дій, таких як аналіз підозрілого фрагменту ландшафту, зокрема з використання оптичного збільшення камери, тут бажане втручання оператора, оскільки у нього є загальне бачення ситуації, яке поки що відсутнє в ШІ.

Також за оператором найближчим часом залишиться практично усе керування базовою платформою, яке окрім переміщення з однієї точки в іншу також включає аналіз довкілля, вибір позиції, маскування тощо. Винятком може бути реалізація функції відслідковування стану акумуляторної батареї та регулярного переміщення до точки заряджання для відновлення її заряду. Таке переміщення може бути тим навчальним полігоном, де опираючись на неодноразове переміщення під керуванням оператора ШІ може практично відпрацьовувати та вдосконалювати майстерність переміщення змінним ландшафтом.

Висновок. Керування БпНК включає дві складові: керування базовою платформою та керування функціональними модулями. Найближчим часом можна очікувати поступову передачу функцій керування функціональним модулем штучному інтелекту, тоді як керування базовою платформою залишатиметься за оператором.

Островська – Бугайчук І. М., канд. пед. наук, доц.
Міскарян Д. С., курсант
Житомирський військовий інститут імені С. П. Корольова

МІЖНАРОДНО-ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ СИСТЕМ У СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТАХ

Широке впровадження безпілотних літальних апаратів, особливо після початку повномасштабного вторгнення росії в Україну, суттєво вплинуло на способи ведення бойових дій та назавжди змінило характер воєн. Тепер на полі бою з'явилися автономні пристрої для ураження, якими може керувати не лише людина, а і штучний інтелект.

На міжнародному арені відсутній єдиний нормативно-правовий акт котрий комплексно регулював би всі аспекти використання безпілотних літальних апаратів у збройних конфліктах. Правомірність їх застосування визначається сукупністю норм міжнародного гуманітарного права (МГП), міжнародного кримінального права, інших застосовних норм міжнародного права та національного законодавства відповідних держав. Оскільки спеціального загального договору саме щодо БПЛА поки що не існує, до них застосовуються ті самі правила, що й до традиційних видів озброєння.

Застосування безпілотних систем під час збройних конфліктів має відповідати чотирьом базовим принципам МГП:

1. **Принцип розрізнення (Distinction).** Оператори мають чітко розрізняти військових та цивільних, а також військові та цивільні об'єкти. Ідентифікація цілі перед ударом є прямим та критично важливим обов'язком.
2. **Принцип пропорційності (Proportionality).** Забороняється завдавати ударів по військових об'єктах, якщо шкода цивільним буде надмірною порівняно з потенційною військовою перевагою від такої атаки.
3. **Принцип запобіжних заходів під час нападу (Precautions in attack).**Сила може застосовуватися лише для досягнення законної військової мети, наприклад, для послаблення військового потенціалу ворога.
4. **Військова необхідність (Military Necessity).** Сторони зобов'язані робити все можливе, щоб мінімізувати шкоду для цивільного населення. З безпілотниками та їхніми оптичними системами спостереження цей принцип

теоретично виконується навіть краще, адже вони дозволяють тривалий час стежити за цілями та аналізувати ситуацію перед тим, як нанести удар.

Недотримання норм міжнародного гуманітарного права під час застосування безпілотних літальних апаратів може спричинити різні види юридичної відповідальності. Це стосується як безпосередніх виконавців, так і держав чи інших осіб, які планували, санкціонували або проводили такі операції. За порушення правил МГП відповідальність може нести як конкретна людина, так і командир, який віддав наказ, або вищі посадові особи, якщо буде доведено їхню причетність. При цьому відповідальність кожного суб’єкта встановлюється окремо відповідно до застосовних норм права.

Система відповідальності тут комплексна вона охоплює індивідуальну кримінальну відповідальність за воєнні злочини та інші міжнародні злочини за наявності відповідних підстав, дисциплінарну відповідальність військовослужбовців, а також міжнародно-правову відповідальність держав. У випадках, передбачених міжнародним правом, відповідальність може наставати й для командирів, які знали або мали знати про вчинення підлеглими правопорушень та не виконали покладених на них обов’язків щодо запобігання таким діям або реагування на них.

Міжнародно-правова відповідальність держави виникає в разі вчинення міжнародно-протиправного діяння, яке може бути приписане цій державі та становить порушення її міжнародного зобов’язання. Якщо незаконне використання БПЛА здійснюється державними органами або особами, чиї дії за міжнародним правом вважаються діями держави, то така держава несе відповідальність. Зокрема, вони можуть включати обов’язок припинити протиправне діяння, надати належні гарантії неповторення за відповідних обставин і забезпечити повне відшкодування заподіяної шкоди. Формами такого відшкодування можуть бути реституція, компенсація та сатисфакція.

Окрему проблему становить встановлення обставин правопорушення та визначення осіб, причетних до використання безпілотних літальних апаратів і тут важливим питанням є доведення вини особи чи суб'єкта при використанні безпілотників. Доказування відбувається згідно із загальними принципами кримінального та міжнародного гуманітарного права. Спочатку потрібно встановити сам факт правопорушення. Для цього вивчають обставини польоту, характер цілі, місце і час атаки, її наслідки, наявність цивільних осіб чи об'єктів

у зоні операції та те, чи відповідали дії нормам МГП. Далі потрібно встановити, хто саме керував БПЛА або брав участь в операції. Тут допомагають службові документи, журнали польотів, дані систем управління, записи телеметрії, відео з бортових камер, радіообмін, електронні листування та інші дані, що дозволяють пов'язати конкретну особу з конкретним завданням.

Отже, безпілотні літальні апарати стали невід'ємною частиною сучасних воєн, а інтеграція технологій штучного інтелекту розширює можливості їх застосування та водночас створює чимало складних юридичних питань. Незалежно від рівня автономності безпілотної системи, її використання повинно відповідати нормам міжнародного гуманітарного права, тому розвиток технологій потребує не лише технічного прогресу, а й постійного вдосконалення правових механізмів контролю та регулювання.

Важливими передумовами правомірного застосування безпілотних технологій є належна перевірка військових цілей, оцінювання можливих гуманітарних наслідків, забезпечення ефективного контролю за виконанням операцій і встановлення відповідальності за допущені порушення. Водночас розвиток автономних систем потребує вдосконалення правових механізмів, процедур перевірки нових засобів і методів ведення війни та способів документування можливих правопорушень. Таким чином, технологічний розвиток у військовій сфері має супроводжуватися послідовним дотриманням міжнародно-правових зобов’язань, спрямованих на обмеження наслідків збройних конфліктів і захист цивільного населення.

Островська – Бугайчук І. М., канд. пед. наук, доц.
Пензюр К. В., курсант
Житомирський військовий інститут імені С. П. Корольова

ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ АВТОНОМНИХ БЕЗПІЛОТНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВІЙ СФЕРІ

Однією з найбільш дискусійних проблем використання автономних систем у військовій сфері є визначення меж застосування штучного інтелекту (ШІ) під час ведення бойових дій і одне з ключових питань щодо використання

автономних систем полягає в тому, чи здатний штучний інтелект (ШІ) дотримуватися норм моралі та міжнародного права на полі бою.

Сьогодні технології штучного інтелекту в безпілотних літальних апаратах використовуються, зокрема, для аналізу даних із сенсорів, виявлення потенційних цілей, їх розпізнавання та супроводження. Залежно від рівня автономності конкретної системи, рішення щодо застосування зброї може ухвалювати оператор або сама система в межах визначених параметрів. Це зумовлює необхідність чіткого визначення ролі людини в процесі прийняття рішень і встановлення належних механізмів контролю за діями автономних технологій. Отже, ШІ виконує функцію допоміжного інструмента: він аналізує обстановку та моделює варіанти дій, проте остаточний вибір залишається за людиною.

Важливим аспектом застосування ШІ у збройних конфліктах є питання юридичної відповідальності. Згідно з нормами міжнародного гуманітарного права (МГП), відповідальність за воєнні злочини може нести лише фізична особа за наявності передбачених законом підстав. Водночас використання автономних систем не звільняє держави та учасників збройного конфлікту від обов’язку дотримуватися норм міжнародного гуманітарного права. Застосування таких технологій має здійснюватися з урахуванням ризиків помилкової ідентифікації цілей, невибіркових атак і заподіяння надмірної шкоди цивільному населенню.

У зв’язку з активним розвитком військових технологій держави та міжнародні організації приділяють значну увагу розробленню правових і етичних принципів використання штучного інтелекту в оборонній сфері. Особливе місце в цих дискусіях посідає питання допустимості передання машинам функцій вибору та ураження цілей. Противники повністю автономного застосування летальної сили наголошують, що рішення про позбавлення людини життя повинно залишатися під належним людським контролем, оскільки алгоритмічні системи не здатні повною мірою відтворити моральне судження людини та врахувати всі обставини конкретної бойової ситуації.

Головний аргумент опонентів автономних систем на основі ШІ полягає в тому, що передання алгоритму рішення про позбавлення людини життя принижує людську гідність. Крім того, наголошують, що алгоритм не здатний повною мірою застосовувати моральні норми та вимоги МГП.

У сучасному науковому дискурсі значна увага приділяється визначенню меж допустимого застосування ШІ в бойових діях і концепції значущого

людського контролю над такими технологіями. Міжнародна спільнота поступово формує відповідну нормативно-правову базу щодо використання ШІ у збройних конфліктах.

Окремі держави вже розробляють етичні засади застосування ШІ в оборонній сфері, зокрема власні принципи відповідального використання таких технологій. Особливого значення набуває дотримання принципу розрізнення, відповідно до якого сторони збройного конфлікту повинні розмежовувати цивільних осіб і комбатантів, а також цивільні об'єкти та військові цілі. Застосування систем штучного інтелекту в цьому контексті потребує оцінювання їхньої здатності правильно інтерпретувати інформацію, розпізнавати об'єкти в складних умовах і враховувати обставини, що можуть змінюватися безпосередньо під час бойових дій. Технічні помилки або некоректна класифікація об'єктів можуть спричинити тяжкі гуманітарні наслідки.

Отже, застосування автономних безпілотних систем і технологій штучного інтелекту у військовій сфері відкриває нові можливості для підвищення ефективності розвідки, виявлення цілей та виконання бойових завдань, водночас створюючи комплекс правових, етичних і гуманітарних викликів. Основною проблемою залишається забезпечення відповідності функціонування таких систем нормам міжнародного гуманітарного права, насамперед принципам розрізнення, пропорційності та вжиття запобіжних заходів під час нападу.

Перспективи правового регулювання військового застосування штучного інтелекту пов'язані з удосконаленням міжнародних норм, запровадженням належних механізмів людського контролю, проведенням правової оцінки нових систем озброєння та визначенням відповідальності за наслідки їх використання. Вирішальне значення має не лише технічна досконалість автономних систем, а й здатність забезпечити контрольованість їх застосування та мінімізувати загрози для цивільного населення. Таким чином, упровадження штучного інтелекту у військовій сфері повинно супроводжуватися комплексним правовим регулюванням, належним контролем з боку людини та неухильним дотриманням міжнародного гуманітарного права.

Островська – Бугайчук І. М., канд. пед. наук, доц.
Стецюк М. Є., курсант
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ ПРАВОВИХ НОРМ ЩОДО РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ АВТОНОМНИХ БЕЗПІЛОТНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВІЙ ДІЯЛЬНОСТІ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Сьогодні на полі бою все частіше використовують безпілотні апарати та технології штучного інтелекту (ШІ). Наша мета – з'ясувати, як норми міжнародного гуманітарного права (МГП) узгоджуються з такою новітньою зброєю. Для нашої держави це питання є надзвичайно актуальним: у 2024 році в Збройних Силах України офіційно з'явився новий рід військ — Сили безпілотних систем (СБС). Безпілотні апарати щодня виконують завдання з розвідки, доставки вантажів і знищення ворога. Технології ШІ при цьому допомагають швидше обробляти інформацію: розпізнавати техніку на місцевості, прокладати маршрути й пропонувати рішення командиру.

З юридичного погляду безпілотність і автономність не одне й те саме. Оператор безпілотної системи керує нею дистанційно й сам вирішує, чи застосовувати силу. В автономній системі частину функцій виконує програма, і від ступеня цієї автономії залежить, чи можна говорити про людський контроль. Найбільше суперечок викликають системи, що самі обирають і вражають цілі.

Міжнародні правила поширюються й на такі сучасні засоби. У статті 35 Додаткового протоколу I (1977 р.) прямо вказано, що воюючі сторони не мають безмежного права обирати будь-яку зброю та методи боротьби. Статті 48, 51 і 52 забороняють бити без розбору та зобов'язують чітко розрізняти військових і мирне населення, а стаття 57 вимагає завчасно вживати заходів, щоб не постраждали цивільні. Також діє застереження Мартенса: навіть якщо певні випадки ще не прописані в договорах, люди все одно захищені принципами гуманності. Складність у тому, що ці норми писали з розрахунку на людину, яка приймає рішення. Тому не очевидно, як оцінювати «практичну можливість» запобіжних заходів, коли вибір цілі робить алгоритм.

В Україні це регулюється законами «Про національну безпеку України», «Про оборону України» та документами Міноборони. Створення СБС

закріплено Указом Президента № 382/2024 на основі рішення РНБО від 25 червня 2024 року. Проте окремого закону суто щодо автономної зброї у нас наразі немає. Через це питання відповідальності та контролю доводиться вирішувати за загальними правилами, що створює труднощі для практики.

На міжнародному рівні дана проблематика розглядається в межах Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї (CCW) 1980 року. Тут працює Група урядових експертів із летальних автономних систем озброєння, яка у 2019 році погодила одинадцять керівних принципів, зокрема про те, що МГП застосовується до таких систем і що відповідальність не може бути перекладена на машину. Обов'язкового договору досі немає. У 2023 році Генеральна Асамблея ООН ухвалила першу резолюцію 78/241 з цього питання, але вона має рекомендаційний характер. Міжнародний комітет Червоного Хреста, зі свого боку, пропонує заборонити системи з непередбачуваними наслідками та обмежити решту.

За статтею 36 Додаткового протоколу I кожна країна повинна обов'язково проводити юридичну перевірку будь-якої нової зброї перед тим, як брати її на озброєння чи розробляти. Тобто безпілотники з технологіями ШІ мають пройти правову оцінку ще до фронту. Спільних для всіх країн правил такої експертизи досі немає. Крім того, складність виникає з системами, які здатні самонавчатися: після оновлення алгоритму програма може діяти зовсім не так, як під час початкових тестів.

Ризики технологій ШІ в бою добре відомі. Алгоритм може хибно ідентифікувати ціль, якщо навчальні дані були неповними чи не відповідали умовам застосування. Рішення системи часто неможливо пояснити, а коли шкоду завдано, важко встановити, хто відповідає: розробник, командир чи оператор. Для цивільних осіб, які опиняються в зоні дії такої системи, це може означати втрату захисту, на який вони мають право за МГП.

Підсумовуючи, можна виділити два головні кроки:

1. Запровадити обов'язкову юридичну експертизу нових комплексів із технологіями ШІ ще до передачі у війська відповідно до статті 36.
2. Завжди зберігати контроль людини за зброєю, щоб військовослужбовець міг оцінити ситуацію та вчасно зупинити атаку.

Чи вистачить для цього наявних законів, чи знадобиться новий міжнародний договір — це питання залишається відкритим для подальшого вивчення.

Отже, впровадження безпілотних систем зі штучним інтелектом вимагає обов'язкової правової експертизи ще до їхнього надходження у війська відповідно до вимог статті 36 Додаткового протоколу І. Водночас критично важливим залишається збереження контролю людини над застосуванням сили, щоб не допустити перекладання юридичної відповідальності на алгоритм. З огляду на це, подальший розвиток мілітарних технологій в Україні та світі потребує чіткішого законодавчого регулювання, яке захистить цивільне населення та збереже норми гуманності на полі бою.

Хмелевський С. І., канд. техн. наук, доц.
Большакова І. М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

НЕЧІТКІ МОДЕЛІ ОЦІНЮВАННЯ В УМОВАХ НЕВИЗНАЧЕНОСТІ: АВТОНОМНІСТЬ ТА ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ В БЕЗПІЛОТНИХ СИСТЕМАХ

Однією з основних проблем створення інтелектуальних систем є перетворення реальної інформації про об’єкт або середовище на форму, придатну для подальшого автоматизованого опрацювання. Для безпілотних систем (БпС) це особливо актуально, оскільки система повинна працювати в умовах динамічної зміни середовища, обмежених обчислювальних ресурсів та можливого погіршення якості інформаційного забезпечення.

Сучасні БпС є складними кіберфізичними комплексами, функціонування яких ґрунтується на взаємодії сенсорів, навігаційних засобів, обчислювальних модулів, каналів зв’язку та програмних алгоритмів. Розвиток технологій штучного інтелекту створює передумови для переходу від дистанційно керованих систем до систем із частковою або високою автономністю, здатних самостійно аналізувати обстановку, оцінювати власний стан, визначати пріоритети та формувати керуючі впливи.

Теорія нечітких множин, започаткована роботами Л. Заде, дає можливість описувати об’єкти не тільки через належність або неналежність певній множині, а й через ступінь цієї належності. Функція належності є основною

характеристикою нечіткої множини та визначає, наскільки конкретне значення змінної відповідає певній властивості. Функція належності може бути використана як проміжний механізм між показниками, отриманими від сенсорів, та алгоритмом прийняття рішення. При цьому особливого значення набуває спосіб її побудови, оскільки від відповідності функції належності безпосередньо залежить поведінка всієї нечіткої моделі.

Аналіз існуючих підходів показує, що функції належності можуть формуватися на основі статистичної інформації або за участю експертів. У першому випадку значення функції належності визначаються з урахуванням експериментальних або статистичних даних. У другому – ступінь належності визначається експертом або групою експертів відповідно до інтенсивності прояву певної властивості.

Для автономних БпС поєднання цих підходів є особливо перспективним. На етапі початкового створення моделі, коли статистичних даних недостатньо, функції належності можуть бути сформовані на основі експертних оцінок. У процесі експлуатації накопичені дані можуть використовуватися для коригування параметрів функцій та зменшення суб’єктивності початкової моделі.

Експертні методи побудови функцій належності поділяються на прямі та непрямі. До прямих методів належать безпосереднє задання значень функції, табличний, формульний та графічний способи.

Однак прямі методи мають суттєве обмеження – високий рівень суб’єктивності. Тому додатковою проблемою є тенденція експертних оцінок до полярних значень. Для автономної системи, яка повинна функціонувати стабільно та відтворювано, надмірна залежність від суб’єктивної оцінки є небажаною. Також прямі методи доцільно використовувати насамперед для початкового формування моделі або отримання експертних обмежень, після чого здійснювати їх уточнення за експериментальними даними.

Більш об’єктивними є непрямі методи побудови функцій належності. До цієї групи належать методи статистичних даних, парних порівнянь, експертних оцінок та інтервальних оцінок.

Серед них особливого значення для дослідження складних динамічних систем, зокрема автономних БпС, набуває метод статистичної інформації, який дає змогу формувати функції належності на основі фактичних даних про функціонування системи. У цьому випадку значення функції належності

формується на основі реальних або експериментальних даних. Наприклад, за наявності достатньої кількості записів польотів можна визначити залежність між параметрами польоту та фактичними результатами роботи системи. На основі таких даних формуються функції належності для оцінювання стабільності польоту, якості навігації, рівня навантаження на обчислювальну систему або достовірності розпізнавання об’єктів.

Іншим перспективним підходом є метод парних порівнянь. Його основою є матриця оцінок, яка відображає відносну перевагу або ступінь належності окремих елементів. Для БпС цей метод може використовуватися під час визначення пріоритетності факторів, що впливають на вибір режиму функціонування.

Важливе місце посідають інтервальні оцінки. Їх застосування є доцільним у ситуаціях, коли експерт не може визначити одне точне значення, але здатний встановити певний діапазон. Для автономної БпС це відповідає реальним умовам експлуатації, оскільки межа між “безпечним” і “небезпечним”, “стабільним” і “нестабільним” станом часто не є однозначною. Інтервальне представлення дає можливість відобразити не тільки значення параметра, а й невизначеність щодо цього значення. Це є особливо важливим під час роботи БпС в умовах похибок вимірювання або неповної інформації.

Окремим напрямом є статистичні методи, що ґрунтуються на експериментальних даних, зокрема методи нечіткої кластеризації та метод потенціалів. Для автономних БпС нечітка кластеризація може бути використана для автоматичного групування характерних станів системи. Наприклад, на основі набору параметрів польоту можуть бути сформовані кластери, які відповідатимуть типовим режимам: стабільний політ, політ із підвищеним навантаженням, нестабільний режим, критичний режим тощо.

Значний інтерес для автономних БпС становить вибір форми самої функції належності. На практиці застосовуються трикутні, трапецієподібні, гаусівські, дзвоноподібні, сигмоїдальні, поліноміальні, еліптичні та інші функції. Вибір конкретної форми повинен визначатися характером даних та вимогами до системи. Трикутні та трапецієподібні функції мають перевагу простоти реалізації та невисокої обчислювальної складності, що є важливим для бортових систем із обмеженими ресурсами. Гаусівські функції забезпечують плавний перехід між станами та можуть бути ефективними при моделюванні

природно розподілених параметрів. Сигмоїдальні функції доцільно використовувати для процесів, де існує асиметричний або монотонний перехід між станами.

Дослідження, наведені в наданому матеріалі, свідчать про те, що різні типи функцій належності суттєво відрізняються за точністю прогнозування та обчислювальною складністю. Зокрема, для систем ANFIS у низці задач гаусівська функція належності демонструвала високу точність при порівняно невеликій обчислювальній складності.

Адаптивна нейро-нечітка система ANFIS є одним із прикладів інтеграції нечіткої логіки та нейронних мереж. Її принципова перевага полягає в можливості автоматичного налаштування параметрів функцій належності за навчальною вибіркою. Для БпС це створює можливість переходу від статичної нечіткої моделі до адаптивної системи, яка може уточнювати свої параметри відповідно до накопичених даних. Разом із тим адаптивність не повинна розглядатися як безумовна перевага. Неконтрольоване переналаштування моделі на нових даних може призвести до втрати стабільності або погіршення результатів у раніше відомих сценаріях. Тому навчання та оновлення параметрів повинні здійснюватися за визначеною процедурою з використанням навчальної та тестової вибірок. Особливо важливим є питання перевірки відповідності сформованої нечіткої моделі. Нечітка модель, сформована на основі експертного досвіду, може бути лише початковою. Після отримання реальних даних її необхідно перевірити на незалежній вибірці, оцінити похибки та визначити випадки, у яких алгоритм приймає неправильні рішення.

Таким чином, доцільно сформувати багаторівневу процедуру побудови нечіткої моделі автономності БпС. На першому етапі визначаються вхідні параметри, які характеризують стан системи та зовнішнє середовище. На другому – формуються лінгвістичні змінні та відповідні функції належності. На третьому – експертні правила переводяться у формальну систему нечіткого висновку. На четвертому – модель перевіряється за експериментальними даними. На п’ятому – параметри функцій належності оптимізуються за результатами навчання. На завершальному етапі здійснюється незалежне тестування.

Перспективним є також використання багатовимірних функцій належності. Більшість традиційних методів передбачає представлення функції належності як функції однієї змінної. Проте реальні задачі автономного

управління характеризуються одночасною дією великої кількості факторів. Рішення щодо зміни режиму польоту, наприклад, може залежати одночасно від якості навігації, швидкості, висоти, залишку енергії, якості зв’язку та оцінки навколишнього середовища. Тому для складних БпС доцільним є перехід до багатовимірних функцій належності та моделей, які здатні враховувати взаємозв’язок між декількома змінними. Одним із шляхів автоматизації їх формування можуть бути методи нечіткої кластеризації.

Перевагою нечіткої логіки в контексті автономних систем є інтерпретованість. На відміну від деяких складних моделей машинного навчання, нечітка система може бути представлена у вигляді набору зрозумілих правил. Це спрощує аналіз поведінки системи та створює можливість контролю її рішень.

Водночас саме нечітка модель не вирішує всіх проблем автономності. Її ефективність залежить від якості вхідних даних, правильності визначення функцій належності та адекватності правил. За зміни умов експлуатації модель може потребувати переналаштування. Тому інноваційним є поєднання нечіткої логіки з машинним навчанням, нейронними мережами та статистичними методами.

Токар А. М., канд. техн. наук, ст. наук. співроб.
Попик В. І., курсант
Житомирський військовий інститут імені С. П. Корольова

КАСКАДНИЙ ОСЬОВИЙ ІМПЕЛЕРНИЙ РУШІЙ З ЕФЕКТОМ ВЕНТУРІ ДЛЯ КОМПАКТНИХ ЕЛЕКТРИЧНИХ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

Україна в умовах повномасштабної війни змушена шукати доступні та ефективні засоби для боротьби із ворогом. Одним із таких способів стали безпілотні авіаційні комплекси та безпілотні системи (БпАК / БпС). Їхня відносно низька вартість і можливість швидкого розгортання дозволили закрити частину потреб, однак існуючі конфігурації на базі відкритих гвинтів виявили суттєві обмеження: недостатню крейсерську швидкість, обмежену дальність при збереженні прийнятної вартості та значні втрати енергії на кінцевих вихорах лопатей. Сучасна фаза вимагає від компактних електричних апаратів здатності

ефективно долати значні відстані та прицільно наносити ураження по живій стилі та техніці противника. Це підвищує актуальність пошуку рішень, здатних забезпечити суттєве збільшення дальності та високі крейсерські швидкості для ураження логістики ворога.

Спроби простого збільшення потужності моторів або діаметра гвинтів у наявних схемах дають обмежений ефект і швидко впираються в зростання аеродинамічного опору та споживання. Виникла потреба не в черговому посиленні існуючого компонування, а в переосмисленні самої архітектури рушія. Прикладом таких модифікацій є перехоплювачі P1_Sun, D1L – Duck та інші.

Метою роботи є обґрунтування концепції автономного компактного електричного рушія сконструйованого з застосуванням повітряних гвинтів (роторів) каскадного осьового типу в конічній шахті з використанням ефекту Вентурі та пасивного колектора. Запропонована конфігурація спрямована на розширення діапазону крейсерських швидкостей та підвищення енергоефективності компактних БпАК у порівнянні з класичними відкритими гвинтами. Розрахунковий приріст тяги та оптимізація повітряного потоку створюють передумови для підвищення крейсерської швидкості та дальності польоту. Повноцінна оцінка енергетичного балансу та дальності буде здійснена за результатами стендових випробувань з урахуванням маси акумуляторних батарей і підйомної сили планера.

В основу покладено такі фізичні явища:

-усунення кінцевих вихорів лопаті замкнутим каналом;

-послідовне додавання імпульсу кількома роторами в одному потоці;

-закон нерозривності та геометричне прискорення повітря в конічному каналі;

-рівняння Бернуллі та утворення зони зниженого тиску у горлах Вентурі;

-пасивне підсмоктування зовнішнього повітря через кільцеві слоти;

-використання стагнаційного тиску носової точки для додаткового нагнітання;

-оптимізація солідності диска та числа Рейнольдса лопатей в умовах низьких Re;

-часткова компенсація закрутки потоку чергуванням напрямку обертання роторів у поєднанні зі статор-лопатками.

Конструктивно система (Рис. 1) являє собою чотири електричні ротори, розташовані послідовно в конічній шахті довжиною близько 660 мм з діаметрами ступенів від 82 мм до приблизно 40 мм і вихідним соплом 38–40 мм. Між ступенями розміщено модулі «статор – дифузор – конфузор Вентурі та повітрозабірник». Для ефективного використання швидкісного напору зустрічного потоку без додаткових

енерговитрат у конструкції шахти передбачено систему профільованих прямокутних повітрозабірників із внутрішніми похилими спрямовувачами (за принципом повітрозабірників NACA). Це забезпечує підвищення статичного тиску та примусове пасивне нагнітання зовнішнього повітря всередину каналу за рахунок зустрічного потоку. Додатково передбачено пасивний колектор від точки застою носа. Живлення — 12S. Крило розглядається як змінний модуль: для збереження максимальної швидкості рекомендується невелика площа (орієнтовно 200–250 см²) з використанням профілю малого потовщення і помірною стрілоподібністю крила.

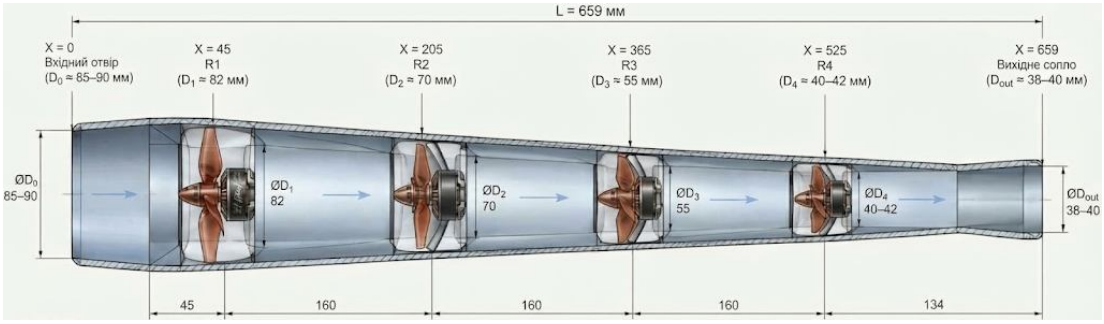


Рис. 1. Конструктивно система каскадного осьового імпелерного рушія з ефектом Вентурі для компактних електричних БпАК (створено за допомогою ШІ)

Аналітичні розрахунки виконано методами теорії диска-актуатора, рівняння Бернуллі, Теорія елементів лопаті (Blade Element Theory) та стандартної атмосфери ISA (International Standard Atmosphere — Міжнародна стандартна атмосфера). Важливо підкреслити: на даному етапі не враховано повну аеродинамічну модель корпусу та підйомну силу крила. Тому наведені нижче показники характеризують переважно рушійну установку і підлягають уточненню після включення аеродинаміки планера.

За розрахунками пасивний приріст тяги становить орієнтовно 15–20 % (з приблизно 3450 г до 4170 г) без зростання споживаної електричної потужності. За попередніми оцінками, це створює суттєвий потенціал для зростання крейсерської швидкості та дальності польоту. Остаточні висновки щодо досяжних швидкісних і кінематичних характеристик будуть зроблені після стендової верифікації та об’єднання рушія з планерною частиною. Додавання оптимального крила (після окремого врахування підйомної сили) здатне додатково знизити потрібну тягу на крейсері та збільшити дальність, однак ці ефекти поки що розглянуті лише якісно.

Аргументи на користь концепції.

Система внутрішньо узгоджена: кожне рішення відповідає конкретному фізичному обмеженню. Пасивні ефекти дають вимірюваний приріст тяги без додаткових витрат енергії джерела живлення. Фронтальна площа залишається мінімальною. Конфігурація зберігає модульність і орієнтована на доступну елементну базу. Розрахунки вказують на можливість суттєвого покращення швидкісних і енергетичних показників при збереженні вартості на рівні існуючих рішень. Потенційно збільшення розмірів каскаду призведе до збільшення ККД у 2 – 4 рази, але це потребує додаткових підтверджень на готових лабораторних стендах відповідних конфігурацій.

Об’єктивні слабкі місця та обмеження.

Аналітичні оцінки на низьких числах Рейнольдса мають помітну похибку. Реальні втрати на тертя, відриви в дифузорах, нерівномірність потоку між ступенями та точність виготовлення можуть зменшити теоретичний виграш. Система оптимізована під високі швидкості; на малих швидкостях перевага знижується. Повна аеродинамічна модель і підйомна сила крила ще не включені в розрахунки, тому остаточні висновки щодо дальності та енергоспоживання можливі лише після їхнього врахування. Конструкція складніша за класичний відкритий гвинт і вимагає ретельного юстування та стендової перевірки.

Таким чином, запропонована концепція є фізично обґрунтованою спробою підвищити ефективність компактних електричних рушіїв для БпАК. Вона розглядає кожен чинник (ефект каналу, каскад, Вентурі, колектор, геометрію лопатей) спочатку окремо, а потім у сукупності. Остаточний висновок про життєздатність можливий лише після стендової верифікації та включення повної аеродинамічної моделі. Подальша робота має розпочинатися з послідовних вимірювань тяги на стенді: відкритий ротор → канал → каскад → каскад з Вентурі → повна система з колектором.

Конечний М. Д.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ЗАСТОСУВАННЯ ІМПЕДАНСНИХ АНТЕН У БЕЗПІЛОТНИХ СИСТЕМАХ СИЛ ОБОРОНИ УКРАЇНИ

Повномасштабна війна зробила безпілотні системи (далі – БпС) одним із ключових засобів ведення бойових дій. Безпілотні літальні апарати (далі – БпЛА), наземні та морські роботизовані комплекси щодня виконують завдання розвідки, коригування вогню, логістики та ураження. Ефективність БпС значною мірою визначається надійністю радіоканалів керування, передавання відео та супутникової навігації. В умовах інтенсивного застосування засобів радіоелектронної боротьби (далі – РЕБ) противника саме антенно-фідерний тракт нерідко стає вирішальним чинником успішного виконання завдання та виживання особового складу. Водночас антена залишається елементом, якому приділяють менше уваги, ніж двигунам, акумуляторам чи системам керування, хоча в ній прихований значний резерв підвищення дальності та завадостійкості зв’язку.

Під імпедансним підходом до проєктування антен розуміють цілеспрямоване формування вхідного опору антени та параметрів її оточення, за яких забезпечується максимальна передача потужності між передавачем, фідером і випромінювачем у всій робочій смузі частот. Мірою узгодження слугують коефіцієнт відбиття та коефіцієнт стоячої хвилі (далі – КСХ). Якщо вхідний імпеданс антени відрізняється від хвильового опору тракту (зазвичай 50 Ом), частина потужності відбивається назад до передавача. Це зменшує реально випромінювану потужність, а отже й дальність зв’язку, спричиняє перегрів вихідного каскаду та може вивести його з ладу. Для малогабаритних БпЛА проблема загострюється: антена електрично мала, розташована поряд із вуглепластиковим каркасом, акумулятором і двигунами, які розстроюють її та змінюють імпеданс порівняно із заводськими даними. Пошкодження антени під час польоту чи посадки також різко підвищує КСХ, і дрон втрачає зв’язок навіть за наявності справного радіомодуля.

Окремий напрям становлять штучні імпедансні поверхні, зокрема високоімпедансні структури та штучні магнітні провідники. Традиційна антена, розміщена впритул до металевого корпусу, втрачає ефективність, оскільки

струми, що наводяться в корпусі, гасять випромінювання. Імпедансна поверхня дозволяє розмістити випромінювач на відстані кількох міліметрів від провідного корпусу без такої втрати. Це зменшує висоту та масу антени, дає змогу виконати її конформною, тобто такою, що повторює форму фюзеляжу, і знижує вплив планера на діаграму спрямованості. Для БпС це означає менший аеродинамічний опір, меншу демаскувальну ознаку та вищу механічну стійкість до ударів і вібрацій. Широкосмугові схеми узгодження дають змогу одній антені ефективно працювати у кількох діапазонах, що важливо для швидкої перебудови частот під час дії РЕБ противника.

У практиці Сил оборони України доцільно виділити кілька напрямів використання імпедансних рішень. По-перше, це канали керування та відеозв'язку БпЛА, де правильне узгодження антени з передавачем дає вимірний приріст дальності без збільшення потужності й, відповідно, без збільшення енергоспоживання та помітності джерела випромінювання. По-друге, це антени наземних станцій керування й ретрансляторів, де застосування узгоджених спрямованих антен допомагає зосередити енергію в потрібному секторі та послабити вплив ворожих завад із інших напрямків. По-третє, це приймачі супутникової навігації, для яких використовують багатоелементні антенні решітки з керованою діаграмою спрямованості: взаємний імпеданс між елементами решітки прямо впливає на глибину формування нулів у напрямку джерела завади. По-четверте, це адаптивні схеми узгодження, що автоматично компенсують розстроювання антени під час польоту, змінення температури чи пошкодження.

Практичне впровадження потребує дотримання кількох правил. Параметри антени слід вимірювати за допомогою векторного аналізатора кіл безпосередньо на зібраному виробі, а не окремо від нього, оскільки корпус і електроніка суттєво змінюють імпеданс. Як робочий критерій зазвичай приймають КСХ не гірше двох у всій використовуваній смузі, а для критичних каналів прагнуть до значень, близьких до одиниці. Конструкція антен має бути ремонтопридатною та придатною до виготовлення у польових умовах і в невеликих майстернях за допомогою друку на тривимірних принтерах та технологій друкованих плат. Це дозволяє швидко масштабувати виробництво й адаптувати його до потреб конкретних підрозділів.

Перспективним є використання методів автоматизованої оптимізації та штучного інтелекту для синтезу форми антен під конкретний планер, а також

створення типових методик випробувань, обов’язкових для приймання антенних модулів до експлуатації. Таким чином, застосування імпедансних антен у БпС Сил оборони України є ефективним і недорогим засобом підвищення дальності, завадостійкості та живучості безпілотних систем, а його системне впровадження – важливою складовою збереження технологічної переваги на полі бою.

Жук І. С.
Науково-дослідний центр ракетних військ і артилерії

ДОСВІД ЗАСТОСУВАННЯ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ БЕЗПІЛОТНИХ СИСТЕМ У СУЧАСНИХ БОЙОВИХ ДІЯХ

Російсько-українська війна засвідчила зростання ролі безпілотних систем у виконанні розвідувальних, ударних і забезпечувальних завдань. Вплинуло на характер бойових дій, організацію управління та вимоги до захисту особового складу. Досвід масового застосування безпілотних літальних апаратів став предметом вивчення й узагальнення у навчальних матеріалах НАТО. Особливого значення набуло поєднання технологічних розробок із практичним досвідом військових підрозділів.

Безпілотні системи охоплюють повітряні, наземні та морські платформи, засоби керування, зв’язку, оброблення інформації й технічного забезпечення. Тому їхні можливості необхідно розглядати з урахуванням працездатності всього комплексу. Навіть високі характеристики окремого апарата не гарантують результативного виконання завдань за відсутності стійкого керування, підготовленого персоналу та належного обслуговування.

Однією з визначальних особливостей застосування безпілотних систем є розширення можливостей спостереження за обстановкою. Повітряні платформи забезпечують отримання зображень місцевості та об’єктів, доповнюючи інформацію інших засобів розвідки. Водночас результативність такого спостереження залежить від своєчасності передавання даних, якості їх інтерпретації та перевірки. Це зумовлює потребу оцінювати не лише технічні можливості засобів спостереження, а й достовірність інформації, яка надходить до органів управління.

Іншою особливістю є різноманітність завдань, що покладаються на безпілотні платформи. Поряд із розвідкою та спостереженням вони використовуються як носії засобів ураження, а також можуть виконувати транспортні, ретрансляційні й інженерні функції. Наземні роботизовані комплекси дають змогу виконувати частину робіт без безпосередньої присутності людини в небезпечній зоні. Однак можливість заміни дій особового складу роботизованою платформою необхідно визначати окремо для кожного завдання з урахуванням умов місцевості, надійності техніки та обмежень керування.

Важливою рисою є швидка зміна умов застосування безпілотних систем. Розвиток засобів протидії спричиняє необхідність регулярного перегляду вимог до платформ, їхнього програмного забезпечення та допоміжного обладнання. У матеріалах Спільного центру НАТО–Україна з аналізу, підготовки та освіти зазначено, що темп розвитку безпілотних загроз потребує повторюваних циклів випробувань, навчання й адаптації. При цьому досвід України використовується для наближення експериментальних умов до реальних викликів сучасної війни.

Зазначена особливість підвищує значення постійного зворотного зв’язку між користувачами, розробниками та установами, які проводять випробування. Доцільно систематично узагальнювати відомості про технічні несправності, втрати керування, складність обслуговування та невідповідність заявлених характеристик фактичним умовам експлуатації. Такі дані можуть становити основу для уточнення технічних вимог і визначення пріоритетів удосконалення. Водночас результати окремих успішних застосувань не слід автоматично поширювати на всі умови використання відповідного зразка.

Суттєвим чинником залишається залежність безпілотних систем від умов зовнішнього середовища. Для повітряних платформ значення мають вітер, опади, температура повітря та видимість; для наземних — рельєф, стан ґрунту й наявність перешкод; для морських — хвилі та гідрометеорологічна обстановка. У зв’язку із цим оцінювання експлуатаційної придатності має охоплювати діапазон умов, у яких передбачається використання системи. Урахування зазначених чинників дає змогу обґрунтованіше визначати її можливості та обмеження.

Окремої уваги потребує людський чинник. Розширення застосування безпілотних систем формує потребу в підготовці операторів, технічних фахівців та персоналу з оброблення інформації. Автоматизація окремих функцій змінює

зміст їхньої роботи, посилюючи вимоги до контролю стану системи, розпізнавання помилок і прийняття рішень за неповної інформації. Відповідно, підготовку персоналу доцільно розглядати як безперервний процес, узгоджений з оновленням техніки та програмного забезпечення.

Для узагальнення досвіду застосування пропонується оцінювати безпілотні системи за сукупністю взаємопов’язаних показників: результативністю виконання завдань, технічною готовністю, надійністю, ремонтопридатністю, потребою в ресурсах і безпечністю експлуатації. Економічне оцінювання має враховувати витрати на закупівлю, навчання, обслуговування та відновлення. Такий підхід дозволить уникнути однобічних висновків, сформованих лише на основі вартості платформи або її паспортних характеристик.

Отже, особливостями застосування безпілотних систем за досвідом російсько-української війни є різноманітність виконуваних завдань, швидка адаптація технологій, залежність від інформаційного й технічного забезпечення та зростання вимог до підготовки персоналу. Подальше дослідження доцільно спрямувати на систематизацію експлуатаційних даних і вдосконалення методичних підходів до оцінювання цих систем. Результати таких досліджень стануть науковою основою для обґрунтування вимог до перспективних безпілотних систем і визначення пріоритетних напрямів їх удосконалення з урахуванням бойового досвіду .

Островська – Бугайчук І. М., канд. пед. наук, доц.
Кобилянський Н. О., курсант
Житомирський військовий інститут імені С. П. Корольова

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ: ВИКЛИК ТА ПЕРСПЕКТИВИ

Швидкий розвиток інтелектуальних обчислювальних технологій суттєво змінює характер сучасної війни. Автоматизоване оброблення оперативних даних, розпізнавання цілей і застосування автономних комплексів стають вирішальним чинником здобуття переваги над противником. Проте швидкість впровадження цих інновацій суттєво випереджає створення нормативної бази,

яка б на законодавчому рівні урегульовувала усі вище перераховані процеси та не блокувала оборонний потенціал і водночас відповідала нормам Міжнародного гуманітарного права (МГП). Таким чином, головне завдання юридичної сфери на сучасному етапі, це розробити дієвий правовий механізм, який забезпечуватиме дотримання норм міжнародного гуманітарного права без штучного гальмування оборонно-промислового сектору.

Аналізуючи міжнародні нормативно-правові акти можемо зробити висновок, що намір провідних держав, це розмежувати цивільне та військове використання штучного інтелекту. Так, специфіка європейського підходу: Регламент ЄС про штучний інтелект, а саме AI Act (Акт про штучний інтелект) як перший у світі комплексний закон щодо регулювання штучного інтелекту, ухвалений Європейським Союзом у 2024 році (Регламент ЄС 2024/1689) стаття 2 якого імперативно виключає зі сфери свого регулювання алгоритми, орієнтовані на сектор оборони та захисту національної безпеки. У пункті 3 статті 2 даного документу, чітко закріплено принцип так званого «військового винятку»: регламент не застосовується до систем штучного інтелекту, якщо вони розробляються, вводяться в експлуатацію або використовуються виключно для військових цілей, оборони чи національної безпеки.

Існує також колізія товарів подвійного призначення: значна частина військових програмних рішень розробляється комерційними ІТ-компаніями. Адаптація відкритого цивільного коду під бойові потреби породжує проблему правової невизначеності щодо корпоративної та державної таємниці.

У стратегії прецедентних та азійських юрисдикцій (США, Японія) ставка робиться на гнучкі оборонні стандарти та етичні дороговкази, що запобігає адміністративному тиску на військово-технічні стартапи.

В умовах російсько-української повномасштабної війни, Україна стала випробувальною платформою для автономних систем. Інтенсивна радіоелектронна боротьба (РЕБ) призводить до регулярної втрати каналів зв’язку між екіпажем та безпілотними літальними апаратами. Це зумовило поширення технологій машинного зору й автоматичного супроводу цілей на термінальній ділянці траєкторії. Водночас в Україні досі відсутнє спеціальне військово-технічне законодавство, яке б регламентувало межі автономності таких систем, адже Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України (№ 1556-р від 2 грудня 2020 року,

розроблена за ініціативи Міністерства цифрової трансформації) оборонну сферу не регулює. Тому було б ефективним прийняття на законодавчому рівні нормативно-правового акту який би визначив межі автономності бойових систем.

Формування системного законодавчого регулювання мілітарного штучного інтелекту є обов'язковою передумовою збереження правопорядку у війнах майбутнього. Для України цей процес має практичне значення: своєчасне нормотворення дасть змогу впроваджувати технологічні переваги в межах міжнародно визнаних стандартів, підтверджуючи репутацію держави, яка неухильно дотримується норм права війни.

Островська – Бугайчук І. М., канд. пед. наук, доц.
Федоришена О. В., курсантка
Житомирський військовий інститут імені С. П. Корольова

МІЖНАРОДНО-ПРАВОВІ ОБМЕЖЕННЯ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ СИСТЕМ ДЛЯ ДИСТАНЦІЙНОГО МІНУВАННЯ ТЕРИТОРІЙ

Сьогодні ми можемо спостерігати, що БПЛ стали головним інструментом доставки боєприпасів, у тому числі для мінування. Але якщо раніше міни ставили сапери або розкидала артилерія, то тепер це роблять повітряні дрони. Дана ситуація створює серйозні ризики для цивільного населення і автоматично ставить питання котрі пов’язані з кваліфікацією вищезгадуваних дій.

Основний нормативно правовий акт який регулює дану сферу діяльності, це Протокол II (1996) до Женевської конвенції заборони чи обмеження застосування певної традиційної зброї 1980 року. Стаття 2 якого визначає поняття: «дистанційно встановлена міна», це боєприпас, доставлений артилерією, ракетами або авіацією. Слів «дрон» чи «БПЛА» в тексті 1996 року немає (їх тоді так не використовували), але за змістом зрозуміло, що доставка міни безпілотником з повітря якраз і підпадає під це правило.

Отже важливий спосіб, а не сам БПЛА. Немає значення, міну скидає важкий ударний дрон, великий безпілотник-бомбардувальник чи швидкий FPV-дрон від першої особи. Якщо міну скинули з повітря в заданий квадрат, це дистанційне мінування. Навіть якщо БПЛА акуратно сів на землю й просто

залишив міну на дорозі, оператор все одно керував ним на відстані. Висока точність оператора не звільняє від дотримання правил.

Протокол II (стаття 3) прямо забороняє мінувати навмання або бити по цивільних об'єктах. Тобто точність БПЛА сама по собі не робить установку протипіхотних мін законною. Якщо міну доставили на відстані (стаття 6), вона обов'язково повинна мати механізм самознищення або самоліквідації через певний час, щоб не лежати роками. Також військові зобов'язані записувати координати таких ділянок і розміновувати їх після боїв.

Оттавська конвенція (Конвенція про заборону застосування, накопичення запасів, виробництва і передачі протипіхотних мін та про їхнє знищення, 1997 р.) запровадила повну глобальну заборону на протипіхотні міни: їх не можна виготовляти, тримати на складах і застосовувати взагалі. І доставка БПЛА це правило не обходить: протипіхотна міна залишається забороненою незалежно від того, як її скинули.

Через війну та дії російських військ на території України у липні 2025 року ВРУ було ухвалено Закон (№ 4519-IX) про зупинення дії Оттавської конвенції, посилаючись на докорінну зміну обставин. На міжнародному рівні, відносно даного факту, тривають юридичні суперечки, адже Оттавська конвенція не передбачає положень про призупинення, стаття 20 даного законодавчого акту допускає лише вихід, який не набуває чинності, доки держава перебуває у збройному конфлікті. Швейцарія та інші держави висловили заперечення проти призупинення. Згідно з Інститутом Лібера, Асамблея держав□сторін, що відбулася у грудні 2025 року, дійшла висновку, що Оттавська конвенція не передбачає призупинення.

Для нашої держави залишається чинним Протокол II, який Україна ратифікувала 15.12.1999 року. Саме його вимогами керується Україна, щоб мінування не вважалося порушенням законів ведення війни.

Таким чином, застосування безпілотних літальних апаратів для дистанційного мінування не виводить такі дії за межі міжнародного гуманітарного права, оскільки будь-яке скидання міни з повітря юридично підпадає під дію Протоколу II до Женевської конвенції 1980 року незалежно від точності оператора. Навіть в умовах вимушеного зупинення Україною виконання зобов'язань за Оттавською конвенцією через екзистенційну загрозу збройної агресії, використання БПЛА для мінування залишається законним

лише за умови збереження повного контролю людини-оператора над рішенням про скид, обов’язкового оснащення боєприпасів механізмами самоліквідації та суворої картографічної фіксації замінованих ділянок задля уникнення невибіркових жертв серед мирного населення. Будь-яка міна, скинута за допомогою БПЛА, юридично є дистанційно встановленою. Тому військові мають чітко фіксувати координати точок скидання та використовувати боєприпаси із самоліквідацією, щоб після нашої перемоги не страждало цивільне населення.

Козмуляк О. А.
Васильєв В. П
Житомирський військовий інститут імені С. П. Корольова

ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІНТЕРАКТИВНИХ КАРТ ПІД ЧАС ВИКОНАННЯ БОЙОВИХ ЗАВДАНЬ

Інтерактивні карти стали невід'ємною частиною сучасних бойових операцій, забезпечуючи численні переваги порівняно з традиційними паперовими картами. Основною особливістю таких систем є інтерактивність, що дозволяє динамічно змінювати масштаби карти, оперативно наносити нові дані, а також забезпечує високу точність визначення координат. Це суттєво знижує ризик помилок, пов’язаних із людським фактором, особливо при використанні GPS для орієнтації на місцевості.

Значною перевагою інтерактивних карт є можливість відображення та постійного оновлення розташування своїх військ і ворожих підрозділів, що сприяє ефективному плануванню операцій, швидкому прийняттю рішень і забезпеченню координації між підрозділами. Крім того, інтерактивні карти дозволяють виконувати розрахункові завдання, такі як визначення зон вогневого ураження чи коригування артилерійського вогню, з мінімальною затратою часу. Використання таких систем, як «Дельта» і «Кропива», демонструє ефективність інтерактивних карт у бойових умовах. Вони не лише відображають оперативну ситуацію в режимі реального часу, але й інтегруються з різними засобами розвідки, зокрема БПЛА, радіолокаційними та звукометричними системами. Це дозволяє створювати єдину цифрову екосистему для управління військовими операціями, що відповідає стандартам НАТО.

Згідно наказу Головнокомандувача Збройних Сил України від 28.10.2023 року №295 «Про запровадження використання у Збройних Силах України топографічних карт у світовій геодезичній системі WGS-84, картографічній проекції Меркатора (UTM)» та вважати таким, що не використовувати у Збройних Силах України з 01 червня 2024 року, топографічні карти, створені в Державній геодезичній референції системі координат УСК-2000 (СК-42).

Військові підрозділи (частини) під час виконання бойових завдань швидко та ефективно перейшли на використання система цілеуказання MGRS (Militagy Grid Reference System) без зниження бойової спроможності та ефективності ураження противника за допомогою використання програмного забезпечення «Дельта» та «Кропива».

Колотуша Я. В.
Військовий інститут Київського національного університету
імені Тараса Шевченка

ПЕРСПЕКТИВИ РОЗВИТКУ АВТОНОМНИХ БЕЗПІЛОТНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Російсько-українська війна стала одним із найбільших практичних випробувань сучасних безпілотних систем. За час широкомасштабної війни безпілотні літальні апарати пройшли шлях від відносно простих дистанційно керованих платформ до складних систем, які можуть виконувати окремі завдання в автоматичному або автономному режимі. Особливо швидко цей процес відбувається в Україні, де постійна зміна умов бойових дій змушує розробників та військових швидко вдосконалювати існуючі технології.

Одним із найбільш перспективних напрямів є використання штучного інтелекту для підвищення автономності безпілотних систем. Якщо раніше оператор повинен був безпосередньо керувати практично всіма етапами польоту, то сучасні системи поступово отримують можливість самостійно виконувати окремі завдання. До таких завдань належать орієнтування у просторі, обробка інформації з камер та інших сенсорів, виявлення об’єктів, їх розпізнавання та супровід.

Особливо важливого значення розвиток автономних технологій набув у боротьбі з російськими ударними безпілотниками типу “Shahed-136”. Їх

масоване використання росією створило для України потребу у великій кількості засобів протидії. Традиційні засоби протиповітряної оборони залишаються важливою складовою захисту повітряного простору, але їх можливості необхідно доповнювати іншими системами. Одним із таких рішень стали українські дрони-перехоплювачі.

Україна за час війни створила цілий напрям розробки безпілотників, призначених для перехоплення інших повітряних цілей. Серед відомих українських систем можна назвати P1-SUN, P1-SUN Long, STING, Bullet, Octopus та інші розробки. Їх поява показує, що безпілотник може використовуватися не тільки для розвідки чи ураження наземних цілей, а й як елемент системи захисту від повітряних загроз.

Насамперед варто розглянути розвиток P1-SUN та його подальшої версії P1-SUN Long. Ці системи є прикладом переходу від звичайного дистанційного управління до використання технологій штучного інтелекту. У нових системах частина роботи, яку раніше повинен був виконувати оператор, передається бортовим алгоритмам. Зокрема, йдеться про автоматичне виявлення та супровід повітряної цілі.

За повідомленнями Міністерства оборони України, у 2026 році українські дрони-перехоплювачі нового покоління вже використовували технології автономного наведення під час боротьби з «шахедами». При цьому оператор не зникає з процесу. Його роль змінюється: замість постійного ручного управління він контролює систему та визначає завдання, а окремі технічні операції виконує штучний інтелект.

Саме такий підхід можна вважати одним із найбільш реалістичних напрямів розвитку автономних безпілотних систем. Повністю автономний апарат, який самостійно приймає всі рішення, є складним технологічним завданням. Натомість система, в якій людина визначає загальне завдання, а штучний інтелект допомагає виконувати окремі етапи, уже сьогодні має практичне застосування.

Важливу роль у цьому процесі відіграє комп’ютерний зір. Камера безпілотника може передавати значний обсяг інформації, однак людині складно постійно аналізувати всі дані з високою швидкістю. Алгоритми штучного інтелекту можуть автоматично аналізувати зображення, знаходити характерні ознаки об’єктів та підтримувати їх супровід. Це дозволяє зменшити навантаження на оператора та швидше реагувати на зміни обстановки.

Для сучасної війни це особливо важливо через велику кількість безпілотників, які можуть одночасно перебувати в повітряному просторі. Якщо кожен апарат потребує постійного ручного управління, кількість операторів стає одним із головних обмежень системи. Автоматизація окремих функцій дозволяє змінити цю модель. У перспективі один оператор може контролювати декілька безпілотних систем, втручаючись лише тоді, коли це необхідно.

Таким чином, штучний інтелект дає можливість перейти від моделі "один оператор — один безпілотник" до більш складної моделі, у якій людина контролює групу автономних або напівавтономних систем. Це не означає повну відмову від оператора. Навпаки, його роль може стати ще важливішою, оскільки він відповідатиме за контроль, оцінку ситуації та прийняття ключових рішень.

Іншим важливим прикладом українського досвіду є розвиток дрона-перехоплювача STING. Ця система була створена українськими розробниками та активно розвивається саме в умовах війни. Її розвиток показує, наскільки швидко військові технології можуть змінюватися під впливом потреб. Конструкція та програмне забезпечення безпілотників постійно вдосконалюються відповідно до отриманого досвіду.

Подібна тенденція спостерігається і з іншими українськими перехоплювачами. Octopus, Bullet та інші системи є прикладами того, як в Україні формується окремий клас безпілотних систем для протидії повітряним цілям. Важливо, що розвиток цих систем відбувається не лише на рівні окремих виробників. У ньому беруть участь військові підрозділи, інженери, програмісти, волонтерські та приватні компанії. Така взаємодія дозволяє швидко перевіряти нові технології та враховувати отриманий досвід.

Український досвід також показує, що автономність не можна розглядати окремо від інших складових безпілотної системи. Для роботи штучного інтелекту потрібні сенсори, обчислювальні можливості, програмне забезпечення та надійна система управління. Якщо хоча б один із цих елементів працює недостатньо ефективно, можливості всієї системи зменшуються.

Однією з основних проблем є якість даних. Штучний інтелект навчається на великій кількості прикладів, тому від якості навчальних даних залежить його здатність правильно розпізнавати об'єкти. У реальних умовах ситуація може сильно відрізнятися від тієї, на якій навчалася модель. Освітлення, погода, перешкоди, різні типи цілей та інші фактори можуть впливати на результат роботи алгоритму.

Ще однією проблемою є постійна зміна умов війни. росія змінює конструкцію та способи застосування безпілотників, використовує нові модифікації та вдосконалює свої системи. Через це алгоритми штучного інтелекту також повинні постійно вдосконалюватися. Модель, яка добре працює сьогодні, може потребувати додаткового навчання після появи нових типів цілей.

Важливим питанням залишається і надійність автономної системи. Штучний інтелект може помилятися, тому його рішення не повинні сприйматися як абсолютно правильні. Особливо це важливо для систем, які працюють у складному та динамічному середовищі. Саме тому перспективним є поєднання автоматичних функцій із можливістю контролю з боку людини.

Український досвід показує, що найбільш практичною на сьогодні є саме часткова автономність. Оператор контролює роботу безпілотних систем, а штучний інтелект може самостійно виконувати окремі завдання. Такий підхід дозволяє одночасно використовувати переваги людини та машини.

Перспективним напрямом є також об’єднання декількох сенсорів. Наприклад, інформація з камери може доповнюватися даними від інших систем спостереження. Поєднання різних джерел інформації дозволяє отримати більш повне уявлення про навколишнє середовище. Для автономного безпілотника це особливо важливо, оскільки він повинен орієнтуватися не на один окремий сигнал, а аналізувати сукупність доступної інформації.

Ще одним напрямом розвитку є вдосконалення бортових обчислювальних систем. Для автономності необхідно обробляти значні обсяги інформації безпосередньо під час польоту. Тому сучасні безпілотники потребують потужніших, але водночас компактних та енергоефективних обчислювальних платформ. Розвиток таких технологій безпосередньо впливає на можливості автономних безпілотних систем.

Важливим напрямом у майбутньому може стати взаємодія декількох автономних систем. Замість використання одного безпілотника як окремого апарата можна створювати групи систем, які обмінюються інформацією та розподіляють між собою завдання. У такому випадку штучний інтелект може використовуватися не тільки для управління окремим безпілотними літальними апаратами, а й для координації всієї групи.

При цьому необхідно враховувати, що розвиток автономності має не тільки технічні, а й організаційні проблеми. Потрібно визначати рівень відповідальності оператора, порядок контролю автономної системи, вимоги до

її перевірки та критерії оцінювання надійності. Без вирішення цих питань навіть технічно досконала система не зможе повною мірою реалізувати свій потенціал.

Досвід російсько-української війни показує, що розвиток безпілотних систем відбувається дуже швидко. Те, що кілька років тому було перспективною технологією, сьогодні вже переходить до практичного використання. Окремі системи вже здатні самостійно виконувати значну частину завдань із пошуку та супроводу повітряних цілей. Український досвід створення та застосування P1-SUN, P1-SUN Long, STING, Bullet, Octopus та інших систем підтверджує, що технології штучного інтелекту вже переходять від експериментального використання до практичних завдань. Подальший розвиток цього напряму може стати одним із ключових чинників підвищення ефективності та масштабованості застосування безпілотних систем Силами оборони України.

Бубнов Т. Ю.
Військова частина А5111
Гаєвський С. О.
Житомирський військовий інститут імені С. П. Корольова

ДОСВІД ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ У НАСТУПАЛЬНІЙ ОПЕРАЦІЇ ТА НАПРЯМИ ЙОГО ВПРОВАДЖЕННЯ В ОСВІТНІЙ ПРОЦЕС

Насичення поля бою роботизованими засобами змінило порядок дій підрозділів: наземні роботизовані комплекси (далі – НРК) почали виконувати завдання замість особового складу, а не поряд із ним. Операція «Вівальді», проведена з вересня 2026 р. трьома послідовними етапами, є першим вітчизняним випадком реалізації цього принципу в масштабі операції армійського корпусу. Здобутий досвід зафіксовано описами окремих епізодів, які не дають ані переліку спроможностей, що підлягають формуванню, ані порядку дій, придатного до відпрацювання на занятті.

За даними станом на липень 2025 р., у структурі місій НРК у Сухопутних військах логістика та евакуація становлять 47 %, інженерні завдання – близько 25 %, бойові – 12 %. Дослідження тактичного застосування наземних

безпілотних систем доходить висновку, що визначальним обмеженням є не автономність платформи, а підготовка операторів, і рекомендує закріплювати оператора за взводом або ротою з визначеною відповідальністю за експлуатацію. Методологію вивчення та впровадження досвіду розроблено й нормативно закріплено, проте перенесення досвіду застосування НРК до змісту підготовки курсантів у ній не розглядалося. Мета роботи – визначити складники цього досвіду та сформулювати пропозиції щодо їх упровадження в освітній процес.

Першим складником є інформаційна складова задуму. Протягом операції підтримувалася інформаційна тиша, застосовувалися імітаційні дії та радіогра засобами НРК, через що противник утримував резерви на хибних напрямах; одночасно підрозділи безпілотних систем знищували антени та ретранслятори, позбавивши його розвідку засобів спостереження. Звідси випливає, що заходи введення противника в оману є визначальним, а не допоміжним елементом задуму і потребують окремого навчального відпрацювання.

Другим складником є багаторівнева побудова безпілотної системи: важкі безпілотні апарати десантували НРК на понад десять кілометрів у глибину, що дало змогу контролювати логістичні шляхи противника, а створені в системі ситуаційної обізнаності спеціалізовані шари обліку дистанційного мінування зробили застосування цих засобів керованим і підзвітним.

Третім складником є інженерне та медичне забезпечення, частка яких у структурі місій є найбільшою. Роботизовані розміновувачі прокладали коридори попереду піхоти, завдяки чому втрат серед саперів не допущено. Евакуацію поранених покладено на НРК, обладнані камерами з двостороннім зв’язком: постійний контакт із пораненим виявився самостійним чинником його морально-психологічного стану – обставина, не відображена в наявних дослідженнях, хоча ризик втрати зв’язку на маршруті в них зафіксовано.

Результатом операції є повернення під контроль близько ста сімдесяти шести квадратних кілометрів території та дев’яти населених пунктів. Показовим є те, що противник здавався в полон цілими підрозділами: позбавлення його логістики та управління виявилося дієвішим за вогневе ураження.

Для впровадження досвіду в освітній процес пропонується: увести тему застосування НРК у наступальному бою з відпрацюванням взаємодії «піхота – роботизований комплекс»; доповнити підготовку фахівців інженерних підрозділів дистанційним розмінуванням роботизованими засобами; унести до

медичної підготовки порядок дій під час евакуації такими засобами; відпрацьовувати заходи введення противника в оману окремим навчальним завданням; передбачити підготовку операторів до дій у деградованих режимах і переходу до ручного керування; сформувати банк документованих бойових епізодів операції як основу тактичних задач; забезпечити вивчення досвіду науково-педагогічними працівниками безпосередньо у військових частинах у порядку, встановленому.

Заміщення особового складу роботизованими комплексами є не технічним удосконаленням окремих зразків, а зміною порядку дій, що потребує відповідної зміни змісту підготовки. Подальші дослідження доцільно спрямувати на розроблення нормативів виконання завдань розрахунками НРК і методики оцінювання підготовленості таких розрахунків.

Голдобін С. М.
Ленський М. М.
Національна академія Служби безпеки України

МЕТОДИ НАВІГАЦІЇ ТА ОЦІНЮВАННЯ ПРОХІДНОСТІ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ В УРБАНІЗОВАНІЙ МІСЦЕВОСТІ

Використання наземних роботизованих комплексів в урбанізованій місцевості потребує врахування особливостей середовища, які безпосередньо впливають на навігацію, мобільність і достовірність отримуваної інформації.

Однією з основних проблем є визначення положення робота за умов недостатньої доступності супутникових навігаційних систем. У таких випадках виникає потреба використовувати дані бортових сенсорів, розпізнавання орієнтирів, оцінювання відносного переміщення та побудову карти середовища.

Для автономного переміщення в середовищі з рухомими перешкодами застосовують алгоритми планування маршруту та машинного навчання. Водночас ефективність маршруту залежить не лише від наявності перешкод, але й від фізичної прохідності поверхні.

Одним із підходів до розв’язання цієї проблеми є одночасна локалізація та картографування (SLAM). У загальному випадку НРК використовує послідовність сенсорних вимірювань для оцінювання власного руху та

формування представлення навколишнього середовища. Результат залежить від точності сенсорів, структури місцевості, наявності розпізнаваних орієнтирів і обчислювальних ресурсів.

Запропонована методика передбачає послідовне виконання п’яти етапів: отримання сенсорних даних, формування карти, оцінювання прохідності, планування маршруту та перевірка результатів переміщення. Така структура поєднує проблематику картографування, автономної навігації, оцінювання прохідності і взаємодії роботизованих платформ.

На першому етапі НРК отримує дані від наявних сенсорів. Залежно від конфігурації платформи це можуть бути лідар, камера, інерціальний вимірювальний модуль, енкодери приводів та інші засоби вимірювання. Фактичний склад сенсорів визначається експериментальною платформою.

На другому етапі виконуються локалізація та побудова карти. Для цього можуть застосовуватися SLAM, топологічне картографування або поєднання метричного й топологічного представлень.

На третьому етапі карта доповнюється інформацією про прохідність окремих ділянок.

Четвертий етап полягає у виборі маршруту, який відповідає обмеженням платформи та вимогам безпеки.

На п’ятому етапі фактична траєкторія порівнюється із запланованою, а показники виконання завдання реєструються для подальшого аналізу (рис.1).



Рис. 1. – Загальна схема навігації та планування руху НРК у урбанізованій місцевості

Для формалізації маршруту введемо граф $G=(V,E)$, де (V) – множина вузлів, що представляють характерні позиції або ділянки середовища; (E) – множина ребер, які відображають допустимі переходи між вузлами.

Для метричного представлення середовища може використовуватися сіткова карта, у якій кожна комірка характеризується оцінкою зайнятості та прохідності. Топологічний граф доцільно застосовувати для глобального планування, а сіткову карту – для локального маневрування. Поєднання цих представлень є запропонованим методичним рішенням, яке потребує перевірки на конкретній платформі.

Для кожного ребра e_{ij} визначимо вартість переходу $c_{ij} = \alpha d_{ij} + \beta r_{ij} + \gamma u_{ij} + \delta t_{ij}$, де d_{ij} – довжина переходу між вузлами (i) та (j); r_{ij} – оцінка ризику проходження; u_{ij} – невизначеність карти або локалізації; t_{ij} – прогнозований час переходу; $\alpha, \beta, \gamma, \delta$ – невід'ємні вагові коефіцієнти.

Перед агрегуванням показників їх необхідно нормалізувати, щоб уникнути некоректного порівняння величин із різними одиницями вимірювання. Вагові коефіцієнти визначаються відповідно до цільового завдання та мають бути зафіксовані до порівняльних випробувань.

Маршрут P визначимо як послідовність суміжних вузлів графа. Оптимальний за обраним критерієм маршрут можна подати у вигляді:

$$P^* = \arg \min_{P \in \rho} J(P) \tag{1}$$

де ρ – множина допустимих маршрутів, а $J(P)$ – сумарна вартість маршруту.

Для адитивної моделі

$$J(P) = \sum_{e_{ij} \in P} c_{ij} \tag{2}$$

У разі виявлення ділянок, що перевищують допустимий ризик або фізичні можливості платформи, відповідні переходи виключаються з множини допустимих ребер. Це дозволяє розділити оптимізацію маршруту та обмеження, пов'язані з безпекою руху.

Відповідно до систематизації методів оцінювання прохідності, наведеної в [4], характеристику ділянки можна формувати на основі геометричних ознак, візуальних властивостей поверхні та даних про стан платформи. У межах запропонованої методики для кожної ділянки i введемо коефіцієнт прохідності $\rho_i \in [0,1]$ де p_i=0 відповідає непрохідній ділянці, а p_i=1 – ділянці, яку за прийнятою моделлю оцінено як повністю прохідну.

Для прохідних ділянок можна сформувати штрафний показник $q_i = 1 - \rho_i$ Чим меншим є p_i, тим більшим буде штраф за проходження ділянки. Це

розмежування запобігає вибору маршруту через фізично непрохідні ділянки внаслідок недостатньо налаштованих вагових коефіцієнтів. Для підвищення надійності оцінювання доцільно поєднувати зовнішні сенсорні дані з вимірюваннями стану руху платформи.

Якщо доступні еталонні координати положення НРК, похибку локалізації в момент часу (k) можна визначити як

$$e_k = \sqrt{(\mathrm{x_k} - \hat{x}_k)^2 + (\mathrm{y_k} - \hat{y}_k)^2} \tag{3}$$

де (x_k, y_k) – еталонні координати; $\hat{x}_k, \hat{y}_k$ –координати оцінки НРК.

Середньоквадратичну похибку локалізації за N вимірюваннями визначимо як

$$RMSE = \sqrt{\frac{1}{N}\sum_{k=1}^{N} e_k^2}. \tag{4}$$

Додатково необхідно фіксувати максимальну похибку та її зміну в часі, оскільки середнє значення може приховувати короткочасні, але критичні відхилення. Для середовищ без доступної еталонної траєкторії слід застосовувати окремі методи оцінювання внутрішньої узгодженості траєкторії та карти, не ототожнюючи їх із прямим вимірюванням абсолютної похибки.

Якщо еталонна карта має відомий набір об’єктів або ділянок, повноту виявлення можна визначити як

$$C_m = \frac{N_{\mathrm{det}}}{N_{\mathrm{ref}}}, \tag{5}$$

де N_{det} – кількість правильно виявлених еталонних об’єктів; $\mathrm{N_{ref}}$ – загальна кількість об’єктів у контрольному наборі.

Показник $\mathrm{C_m}$ набуває значень від 0 до 1. Його не слід ототожнювати з повнотою картографування всього простору, якщо оцінювання виконується лише за окремими об’єктами. Для просторового оцінювання можна використовувати відношення площі правильно відображеної дослідженої області до площі контрольної області:

$$C_A = \frac{A_{\mathrm{matched}}}{A_{\mathrm{ref}}}, \tag{6}$$

де $A_{matched}$ – площа контрольної області, яка відповідає карті робота за встановленим критерієм; A_{ref} – площа еталонної області.

Вибір метрики повинен відповідати типу карти й завданню. Для пошуково-рятувальних сценаріїв, де важливими є доступні проходи та

розташування об’єктів, доцільно окремо оцінювати геометричну відповідність карти та її функціональну придатність.

Для порівняння алгоритмів введемо вектор показників

$$\mathbf{M} = (RMSE,\ C_m,\ C_A,\ L_P,\ T_P,\ N_c,\ S_P), \tag{7}$$

де L_P – довжина фактичного маршруту; T_P – час виконання завдання; N_c – кількість зіткнень; S_P – частка успішно пройдених ділянок. Показник успішності проходження визначимо як

$$S_P = \frac{N_{\text{succ}}}{N_{\text{attempt}}}, \tag{8}$$

де N_{succ} – кількість успішно пройдених ділянок; $N_{attempt}$ – загальна кількість ділянок, проходження яких оцінювалося.

Комплексний показник може бути сформований через нормалізацію окремих метрик:

$$K = \sum_{j=1}^{m} w_j z_j, \qquad \sum_{j=1}^{m} w_j = 1, \tag{9}$$

де z_j – нормалізовані показники результативності, орієнтовані в одному напрямку; w_j – їхні вагові коефіцієнти.

Для метрик, які потрібно мінімізувати, наприклад RMSE, довжини маршруту або часу, нормалізація має перетворювати менше значення на кращу оцінку. Для метрик, які потрібно максимізувати, наприклад повноти карти чи успішності проходження, напрямок нормалізації має бути протилежним. Нормалізація, набір показників і ваги повинні бути визначені до аналізу результатів, щоб забезпечити відтворюваність порівняння.

Зіткнення та порушення жорстких обмежень безпеки доцільно оцінювати окремо, а не компенсувати високими значеннями інших показників. Якщо алгоритм порушує встановлені обмеження безпеки, його не можна вважати кращим лише через коротший маршрут або менший час виконання.

Запропонована методика дає змогу перейти від оцінювання НРК за одним критерієм до комплексного аналізу його функціонування. Зменшення довжини маршруту саме по собі не свідчить про підвищення ефективності, якщо воно супроводжується зростанням кількості зіткнень, збільшенням похибки локалізації або вибором ділянок із невизначеною прохідністю. Аналогічно, висока повнота карти не гарантує її придатності для навігації, якщо геометричні похибки перевищують допустимі для конкретного робота значення.

Результати аналізу публікацій дають підстави розглядати навігацію, картографування, прохідність і координацію роботизованих платформ як взаємопов’язані, але окремо оцінювані складові. Топологічна карта може бути ефективною для глобального планування, тоді як локальне переміщення потребує детальнішої інформації про геометрію перешкод. Методи навчання з підкріпленням можуть забезпечувати адаптивне уникнення перешкод, але потребують перевірки на сценаріях, які не використовувалися під час навчання. Оцінювання прохідності має враховувати не тільки зовнішні ознаки поверхні, а й фізичні обмеження конкретної платформи.

Березовський А. І., канд. техн. наук, доц.
Університет трансформації майбутнього
Сухар В. В.
Махнюк О. В.
Центральний науково-дослідний інститут
озброєння та військової техніки Збройних Сил України

ШЛЯХИ ПОКРАЩЕННЯ ЕКСПЛУАТАЦІЇ НАЗЕМНИХ ЛОГІСТИЧНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ З УРАХУВАННЯМ БОЙОВОГО ДОСВІДУ ЗАСТОСУВАННЯ СИЛАМИ ОБОРОНИ УКРАЇНИ

Проведений аналіз відкритих джерел інформації щодо експлуатації та бойового застосування Силами оборони України наземних логістичних роботизованих комплексів (НЛРК) вказує на те, що на більшості з них відсутні сучасні засоби маскування, в окремих випадках застосовується звичайна маскувальна сітка, яка працює в оптичному діапазоні. Аналіз втрат НЛРК свідчить проте, що це мало ефективний спосіб маскування військової техніки, що застосовується як в тилу так і на лінії бойового зіткнення.

Тому постає проблема проведення робіт з проектування та розробки новітніх зразків систем та засобів маскування з врахуванням сучасних технологій та матеріалів.

В дослідженнях, що проводяться за зазначеним напрямком, пропонується розглянути один із методів зниження помітності НЛРК такий, як миттєва

постановка димових/аерозольних завіс. Прикладом системи для миттєвої постановки мультиспектральних димових завіс/екранів є система “Rosy” німецької компанії Rheinmetall’s. Принцип роботи “Rosy” до певної міри аналогічний принципу роботи системи “Туча”, що встановлюється на основні зразки бронетанкової техніки. Проте, на відміну від “Тучі” система “Rosy” ставить не димовий екран перед машиною для її захисту від наземних систем ураження, а димову завісу над машиною для її маскування від засобів повітряного ураження. Принцип роботи засновано на масованому застосуванні димових піротехнічних засобів (гранат) калібру 40 мм. Система дозволяє встановлення засобів виявлення БПЛА ворога та автоматичної постановки димової завіси.

Практична реалізація та впровадження результатів запропонованих наукових досліджень підприємствами вітчизняного оборонно-промислового комплексу на зразках наземних логістичних роботизованих комплексів суттєво підвищить їх живучість, забезпечить вчасне виконання завдань та зменшить втрати під час бойового застосування.

Майданюк В. А., Ph. D.
Вознюк В. В.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ЕВОЛЮЦІЯ ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ У російсько–УКРАЇНСЬКІЙ ВІЙНІ

Вступ

Російсько-українська війна стала одним із найбільш масштабних полігонів для практичного випробування безпілотних і роботизованих систем. Якщо на початкових етапах застосування наземних роботизованих платформ розглядалося переважно як перспективний напрям розвитку озброєння, то з часом вони почали займати цілком конкретне місце у структурі бойових дій.

Причина цього достатньо очевидна. Сучасне поле бою стало надзвичайно небезпечним для людини. Постійне спостереження з боку БпЛА, широке застосування FPV-дронів, артилерії та високоточних засобів ураження значно

ускладнили переміщення особового складу навіть у районах, які раніше вважалися відносно безпечними. У таких умовах виконання окремих завдань за допомогою роботизованих платформ дає можливість зберегти життя військовослужбовців та одночасно забезпечити виконання необхідних бойових і забезпечувальних функцій.

При цьому досвід війни показує, що розвиток НРК відбувається дещо інакше, ніж це передбачалося у класичних концепціях роботизації. Першими реально затребуваними виявилися не складні автономні бойові роботи, а відносно прості платформи, здатні доставити вантаж, евакуювати пораненого або виконати інше завдання замість військовослужбовця.

Основна частина

Умовно розвиток бойового застосування НРК у російсько-українській війні можна поділити на три основні етапи.

Перший етап - експериментальний, який охоплює період приблизно з 2014 до 2022 року. У цей час в Україні та Росії розроблялися окремі зразки наземних роботизованих платформ. Серед відомих російських розробок можна згадати «Уран-9», а в Україні - роботизовану платформу «Фантом». Проте їх застосування не мало масового характеру. Значна частина таких систем перебувала на стадії випробувань, а можливості їх використання в реальному бою залишалися обмеженими.

Повномасштабне вторгнення Російської Федерації у 2022 році суттєво змінило ситуацію. В умовах постійного артилерійського та мінометного ураження, а згодом і стрімкого поширення FPV-дронів виникла практична потреба виконувати завдання без безпосередньої участі людини.

Саме тому другий етап можна умовно назвати етапом практичного пошуку та «малої роботизованої логістики». У 2022–2023 роках почали з'являтися численні колісні та гусеничні платформи, частина яких створювалася невеликими виробниками, волонтерами або безпосередньо військовослужбовцями. Конструкції часто були досить простими, але відповідали конкретній потребі підрозділу.

На перший план вийшли доставка боєприпасів та інших матеріальних засобів, евакуація поранених, транспортування майна, мінування та розмінування. Фактично робот почав виконувати ту роботу, для якої раніше необхідно було відправляти військовослужбовця. Це стало одним із найбільш важливих практичних напрямів розвитку НРК.

При цьому саме бойовий досвід поступово показав, що можливості наземних платформ значно ширші. Якщо спочатку основна увага приділялася забезпеченню підрозділів, то у 2023–2024 роках почалися спроби застосовувати НРК безпосередньо для виконання бойових завдань.

Показовим у цьому відношенні є епізод, зафіксований у районі Бердичів на Авдіївському напрямку у березні 2024 року. Російська сторона застосувала гусеничні роботизовані платформи, оснащені автоматичними гранатометами АГС-17 та додатковими металевими елементами захисту. Роботизовані комплекси використовувалися як засоби вогневого впливу на позиції українських військових.

У відповідь оператори роти ударних безпілотних авіаційних комплексів 47-ї окремої механізованої бригади виявили роботизовані платформи та застосували проти них FPV-дрони. У результаті російські НРК були знищені.

Цей епізод є цікавим не тільки як факт знищення роботизованої техніки. Він демонструє важливу особливість сучасної війни: поява одного нового роботизованого засобу автоматично породжує пошук способів протидії йому іншими безпілотними системами. У цьому випадку повітряний FPV-дрон фактично виступив засобом боротьби з наземним роботом.

Тобто роботизація поля бою відбувається не ізольовано. Вона є частиною постійного протиборства систем «робот - робот», «робот - БпЛА», «робот - засоби РЕБ» та інших комбінацій. Саме тому перевага окремого зразка НРК визначається не лише його озброєнням або вантажопідйомністю, а всією системою його застосування.

Наступним етапом став перехід від окремих експериментів до організованого застосування НРК. У 2024 році у Силах оборони України почали формуватися штатні підрозділи, орієнтовані на використання наземних роботизованих систем. Зокрема, відповідні напрямки розвивалися у 3-й штурмовій бригаді та 47-й окремій механізованій бригаді.

Цей процес свідчить про важливу зміну підходу. НРК перестає бути просто технічним виробом, який окремий підрозділ отримує для виконання певного завдання. Поступово формується поняття роботизованого підрозділу, у якому сама техніка, оператори, засоби зв'язку, управління, розвідки та забезпечення розглядаються як єдина система.

Особливо важливим напрямом стало використання роботів у так званій «кілзоні» - зоні, де перебування військовослужбовця суттєво підвищує

ймовірність його виявлення та ураження. У таких умовах НРК можуть виконувати завдання з доставки боєприпасів, продовольства, води та іншого майна, не наражаючи на безпосередню небезпеку водія або вантажну групу.

У 2025–2026 роках спостерігається наступний етап — систематизація та спеціалізація роботизованих платформ. Замість універсального підходу починає формуватися ціла група спеціалізованих НРК. Одні платформи орієнтовані на логістику, інші - на евакуацію, мінування, розвідку або вогневу підтримку.

Серед українських розробок і платформ, які згадуються у відкритих матеріалах, можна виділити «TerMIT», «Тарган», «Рись PRO», «Воля Е» та інші системи. Їх поява свідчить про поступовий перехід від універсальної платформи до спеціалізованого роботизованого засобу, оптимізованого під конкретне завдання.

Змінюється також саме розуміння ролі НРК. Якщо раніше основним показником ефективності вважалися вантажопідйомність, запас ходу або можливість дистанційного управління, то сьогодні важливими стають інтеграція платформи у систему управління військами, стійкість каналів зв'язку, можливість роботи в умовах активного застосування засобів РЕБ, взаємодія з БпЛА та здатність діяти в єдиному інформаційному просторі.

Окремим напрямом стає озброєння НРК. Вогнева платформа дає можливість винести частину ризикованих бойових функцій за межі безпосереднього перебування людини. При цьому бойовий НРК не обов'язково повинен повністю замінювати традиційний засіб ураження. У багатьох випадках його перевага полягає саме у можливості наблизити засіб ураження до противника або виконати короткочасне завдання у зоні, де перебування людини є надто небезпечним.

Не менш перспективним є застосування НРК для мінування та розмінування. Роботизована платформа дозволяє перенести частину найбільш небезпечних операцій із людини на технічний засіб. У майбутньому саме такі завдання можуть стати одними з найбільш затребуваних напрямів роботизації.

Ще одна важлива тенденція - поступове збільшення дальності та тривалості роботи НРК. Якщо перші платформи використовувалися переважно поблизу переднього краю, то розвиток систем управління, зв'язку та навігації дозволяє розглядати їх як засоби, здатні працювати на значній відстані від оператора. Це особливо важливо для логістичних завдань, коли необхідно регулярно доставляти вантажі на передові позиції.

Таким чином, за декілька років НРК пройшли шлях від експериментального зразка до повноцінного елемента бойової системи. При цьому цей процес відбувався не стільки відповідно до наперед визначеної концепції, скільки під впливом реальних потреб фронту.

На наш погляд, головним результатом цього розвитку є зміна самої логіки використання роботизованої техніки. Якщо раніше ставилося питання: «де можна застосувати робота?», то сьогодні більш актуальним стає питання: «яке завдання доцільно передати роботу замість людини?»

Саме ця зміна підходу може визначити подальший розвиток НРК.

Висновки

Досвід російсько-української війни показує, що еволюція наземних роботизованих комплексів відбувається одночасно у технічному, організаційному та тактичному напрямах.

На першому етапі НРК були переважно експериментальними системами. З початком повномасштабної війни вони почали активно використовуватися для виконання допоміжних завдань, перш за все логістики та евакуації. У 2023–2024 роках відбувся перехід до їх безпосереднього застосування у бойових діях. Наступним кроком стало формування спеціалізованих роботизованих підрозділів та розширення переліку завдань, які виконуються без безпосередньої участі військовослужбовця.

Показовим є досвід бойового застосування НРК у районі Бердичів у березні 2024 року. З одного боку, він демонструє реальну можливість використання наземних роботизованих платформ як засобів вогневого впливу. З іншого - показує вразливість таких систем перед FPV-дронами та необхідність комплексного підходу до їх захисту.

У подальшому можна очікувати збільшення кількості НРК у підрозділах Сил оборони України, розширення їх спеціалізації та поступового переходу від дистанційно керованих платформ до систем із більш високим рівнем автономності.

Водночас основним критерієм розвитку НРК, на нашу думку, повинна залишатися не сама технологічність платформи, а її здатність реально зменшувати ризик для особового складу та підвищувати ефективність виконання бойового завдання. Саме бойовий досвід визначатиме, які із сучасних технічних рішень стануть перспективними, а які залишаться лише експериментальними зразками.

Маковський В. Ю.
Житомирський військовий інститут імені С. П. Корольова

АВТОНОМНІСТЬ ТА ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В БЕЗПІЛОТНИХ СИСТЕМАХ: МОЖЛИВОСТІ, ПЕРСПЕКТИВИ, ОБМЕЖЕННЯ

Стрімка еволюція штучного інтелекту (ШІ) трансформує безпілотні комплекси (повітряного, наземного та морського базування) із дистанційно керованих апаратів на повністю або частково самохідні робототехнічні системи. Впровадження алгоритмів машинного навчання, комп’ютерного зору та нейромережевих моделей дозволяє БПЛА реалізовувати складні місії за умов дефіциту зв'язку, інтенсивного радіоелектронного придушення (РЕБ) та мінливої обстановки.

Штучний інтелект в роботизованих системах має величезний потенціал щодо самостійної навігації та просторового орієнтування.

Візуальне просторове позиціонування (Visual Odometry & SLAM) - здатність визначати координати та маршрут за допомогою відеокамер та алгоритмів зіставлення рельєфу без залучення супутникових мереж (GPS/GLONASS).

Автоматичний обхід перешкод, завдяки аналізу потоку даних із LiDAR, оптичних датчиків та тепловізійних приладів у реальному часі задля прокладання безпечної траєкторії, а також комп’ютерний зір та автозахоплення об'єктів.

Автоматичне виявлення цілей, а саме: їх розпізнавання, систематизація та супровід (техніка, особовий склад, інфраструктура) в умовах обмеженої видимості або штучних завад.

Термінальне самонаведення (Terminal Homing), тобто автономне утримання та ураження цілей на прикінцевому етапі польоту без втручання оператора.

Оптимізація каналів зв'язку та керування

Стійкість до завад РЕБ. Оскільки рішення щодо маневрування та ураження ухвалюються безпосередньо бортовим обчислювачем, дрон отримує високу захищеність від придушення каналів управління, а також передачі трансляції відеосигналу.

Вектори розвитку та інноваційні тенденції: Ройовий інтелект (Swarm Intelligence) - Багатосегментна інтеграція (Повітря + Наземні комплекси + Морські сили) - Периферійний ШІ-обчислення (Edge AI) & Гібридне ухвалення рішень (Human-in-the-loop)

Ройовий інтелект (Swarm Intelligence) являє собою узгоджену роботу десятків або сотень автономних одиниць, які самостійно розподіляють між собою завдання (розвідка, ретрансляція сигнала, нейтралізація цілей) за відсутності централізованого командного пункту.

Периферійні ШІ-обчислення (Edge AI) передбачають застосування енергоефективних мікропроцесорів безпосередньо на борту беспілотного апарата для миттєвої обробки нейромереж без затримок на передачу даних до наземної станції.

Мультидоменна координація дає можливість синхронізувати дії безпілотних літальних апаратів (БПЛА) з наземними роботизованими комплексами (НРК), а також з безекіпажними катерами в єдиній інформаційній мережі.

Ключовими бар'єрами та викликами є: технічні та технологічні обмеження, а також етичні, правові та безпекові ризики.

Обчислювальні ресурси потребують значного енергоспоживання бортових ШІ-чипів за суворих лімітів на вагу, габарити та живлення (SWaP).

Чутливість оптичних та інфрачервоних систем до несприятливих погодних чинників (туман, злива, пилова буря) робить їх вразливими.

Існує непередбачувана ймовірність помилкової класифікації об’єктів у нестандартних або навмисно викривлених умовах (камуфляж, макети-пастки).

Етичні, правові та безпекові ризики

Визначення межі автономії під час ухвалення рішення про застосування летального озброєння (LAWS — Lethal Autonomous Weapons Systems) в рамках концепції „Human-in-the-Loop”.

Відсутність чітких міжнародних правових норм щодо встановлення винних (розробник, оператор чи командир) у разі збою або помилки автономного комплексу знімає юридичну відповідальність з таких осіб.

Кіберзагрози, а саме: ризик перехоплення управління через вразливості в алгоритмах машинного навчання або підміну вхідних даних (Adversarial Attacks).

Таким чином інтеграція технологій штучного інтелекту в роботизовані системи докорінно змінює концепцію їх використання, перетворюючи їх на високоточні автономні інструменти. Ключовим вектором подальшого поступу стане досягнення паритету між максимальною автономністю бортових обчислювачів та гарантованим контролем з боку людини, а також врегулювання етично-правових аспектів застосування автономної зброї.

Омельчук І. А.
Карпухін Р. Т., курсант
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ СТАНУ ВТОРИННОЇ ПЕРЕРОБКИ ПЛАСТИКУ НА СИРОВИНУ ДЛЯ 3D – ДРУКУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

На сьогодні в умовах повномасштабного вторгнення виникла необхідність в технологічному оснащення військ. Сучасний етап розвитку озброєння характеризується неухильним зростанням ролі безпілотних систем, що обумовлює необхідність інтенсифікації процесів проектування, створення та виробництва новітніх безпілотних комплексів різного функціонального призначення, та комплектуючих деталей до них. Це призвело до створення сил безпілотних систем, що в свою чергу потребує великої кількості виробничих і ремонтних потужностей, і також потребує відповідного оснащення та устаткування. Одним з видів такого устаткування є також і 3D принтери, але вони потребують великої кількості витратного матеріалу для друку - філаменту. Враховуючи йог велику вартість виникає потреба в швидкому і здешевленому поповненні матерів для друку комплектуючих і ремонтних частин для безпілотних комплексів. Тому ввторинна переробка пластику для потреб Збройних Сил України — це масштабний волонтерський та промисловий рух, який одночасно вирішує екологічні завдання та забезпечує фронт дефіцитним спорядженням. Пластикові відходи перетворюють на готові вироби двома основними шляхами: шляхом фінансової конвертації (монетизація втор сировини) або безпосереднім виготовленням деталей через 3D-друк та лиття.

Виготовлення філамента з пластикових пляшок — ідея не нова. Таку технологію застосовують в інших країнах. Так, під час аналізу існуючих методів виробництва філоменту було досліджєно та виявлено що найбільш розповсюдженими є декілька методів побутової переробки пластику серед яких можна виділити наступні:

Метод виготовлення філаменту для 3D-друку шляхом розпускання ПЕТ-пляшок на стрічку. Цей етод є доволі простим, та не поьребує додаткового подрібнення плящок на гранули, але в ньому можна отримати виключно стрічку пластику.

Основними превагами є низька собівартість та доступність сировини, простота конструкції саморобного обладнання, ввідсутність необхідності в складній грануляції.

До недоліків даного методу можна віднести обмеження по видах пластику Метод підходить переважно для ПЕТ (PET-E / 01) пластику.

Також можна виділити низьку швидкість виготовлення стрічки і складність їх з'єднання. Одна пляшка дає обмежену довжину стрічки (зазвичай 10–20 метрів). Для друку великих моделей потрібно зварювати кінці стрічок або прутків вручну чи за допомогою спеціальних термопаяльників. Іншим шляхом щодо виготовлення філоменту є метод виготовлення нитки для 3D-друку або виробництва виробів шляхом подрібнення пластику та екструзії. Перевагами даного методу є універсальність сировини. Можна переробляти практично будь-які термопласти, бо немає потреби обмежуватися лише циліндричними пляшками, та висока продуктивність виготовлення нитки. Продуктивність шнекового екструдера значно вища порівняно з повільним протягуванням стрічки від пляшок. Також до переваг варто віднести можливість вторинного подрібнення невдалих деталей браковані вироби можна знову відправити в подрібнювач і переплавити без втрати можливості подальшого друку.

Недоліками даного способу є необхідність точного сортування за типами пластику, оскільки змішування різних видів пластику призводить до розшарування матеріалу через різну температуру плавлення та хімічну несумісність.

Обмеження також стосуються і до розміру фракції при подрібненні. Пластик має бути подрібнений на рівномірні шматочки (зазвичай 3–5 мм). Занадто великі шматки не захоплюються шнеком, а надто дрібний пил забиває зону завантаження. Також при вторинній переробці спостерігається термічна деградація полімерів. При кожному циклі нагріву в екструдері полімерні ланцюги частково руйнуються. Пластик на кшталт PLA стає дуже крихким після кількох циклів плавлення, а ПЕТ починає активно втрачати в'язкість через гідроліз, якщо його попередньо ідеально не висушити.

На сьогоднішній день існує багато розробок щодо вторинної переробки пластику. Так, проєкт ARTME 3D, який спеціалізується на розробці компактного настільного обладнання для переробки пластикових відходів та виробництва власних ниток для 3D-принтерів пропонує набори та креслення для самостійного збирання настільних шнекових екструдерів, здатних переплавляти подрібнений пластик або гранули у філамент діаметром 1.75 або 2.85 мм. Ця інструкція описує створення саморобного шнекового екструдера для переробки пластику на філамент за допомогою металевої труби, нагрівальних елементів, терморегулятора (PID) та двигуна з довгим свердлом або шнеком усередині.

Виробник FilaFab з Великобританії також спеціалізується на розробці та виготовленні професійних настільних екструдерів і повних ліній для виробництва філаменту 3D-принтерів.

Але дані розробки та обладнання орієнтовано зазвичай бо на створення стрічки з пляшок, або на вже подрібрений пластик (гранульовану сировину), Тоді як сам процес подрібнення потребує додаткового обладнання та ускладнює процес переробки.

Перспективними напрямками вдосконалення даного напрямку є розробка проектів та реалізація установок, в яких процес подрібнення та плавлення сировини буде відбуватися одним нерозривним технологічним процесом. В такому випадку подрібнювач має мати одразу температуру, що необхідна для розплавлення пластикою перед подачею в шнековий екструдер. Така компоновка дозволить покращити та пришвидшити процес виготовлення філоменту та зменшити вартість даного обладнання.

Основними задачами при розробці даного проекту є забезпечення стабільної температури подрібнювача, та його достатньої міцності для забезпечення рівномірного перетворення конструкцій що відправляються на переробку в однорідну масу яка потраплятиме на шнек екструдера.

Саме створенню даного проекту та впровадженню технічних рішень для його реалізації таких як індуктивний спосіб розігріву шнеку та подрібнювача і буде присвячено подальші пошукові роботи та розробки.

Результатом розробки планується отримати пристрій в форматі для перобки шматків пластику та пляшок, без необхідності попереднього подрібнення, максимально здешевленим для застосування в силах оборони

Первак І. В.
Бондарчук В. Д.
Тимчук Г. М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ІНТЕГРАЦІЯ MESH-МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАВАДОСТІЙКОГО ЗВ'ЯЗКУ УДАРНИХ РАЗОВИХ СТРАТЕГІЧНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ІЗ ВОГНЕВОГО УРАЖЕННЯ ПРОТИВНИКА

Сучасна війна засвідчила, що ефективність вогневого впливу стратегічними безпілотними літальними апаратами (БпЛА) з метою ураження важливих військових, військово-промислових, енергетичних об’єктів, вузлів, комунікацій, об’єктів військового та державного управління противника в стратегічній глибині дедалі більше залежить від стійкості каналів управління БпЛА та вузлів зв'язку.

Противник насичує район бойових дій засобами радіоелектронної боротьби (РЕБ), створює зони придушення радіоліній і спотворення сигналів супутникової навігації. Традиційна система передачі сигналу “оператор – БпЛА” з єдиним каналом зв'язку є вразливою, придушення цього каналу призводить до втрати керованості, неможливості уточнення цілі та зриву виконання бойового завдання. Це зумовлює потребу в пошуку новітніх рішень, які забезпечують живучість зв'язку без нарощування потужності передавачів, що лише полегшує виявлення джерел випромінювання противником.

Mesh-мережа – це самоорганізована децентралізована система, у якій кожен вузол приймає, передає і ретранслює дані інших вузлів. На відміну від централізованої мережі передачі даних, вихід з ладу чи придушення окремого вузла або лінії не призводить до втрати зв'язності всієї мережі, оскільки трафік даних автоматично прокладається обхідними маршрутами. Для групи БпЛА кожен апарат одночасно є виконавцем завдання та ретранслятором, що дозволяє розподілити мережу та використовувати для зв'язку з оператором лише той вузол, який перебуває в найсприятливіших умовах поширення сигналу.

Підвищення завадостійкості до РЕБ за допомогою Mesh-мереж забезпечується комплексом взаємопов'язаних дій, а саме:

резервування маршрутів, що передбачає наявність кількох незалежних маршрутів між вузлами та адаптивна маршрутизація, що реагує динамічно на зміну якості ліній передачі даних, втрату вузлів і появу зон РЕБ;

різноманітність каналів, яка досягається поєднанням різних діапазонів частот каналів управління, видів модуляції та типів ліній зв'язку, що змушує противника розподіляти сили і засоби РЕБ і знижує ймовірність одночасного придушення всіх каналів;

зниження помітності випромінювання за рахунок використання спрямованих антен, малої потужності на коротких ділянках між вузлами, режимів радіомовчання та пакетної передачі, що ускладнює радіорозвідку й пеленгацію;

ретрансляція через вузли, розташовані поза зонами дії засобів РЕБ, зокрема з використанням окремих БпЛА-ретрансляторів.

Окремої уваги потребує інформаційна безпека такої мережі. Кожен вузол є потенційним вразливим елементом: у разі втрати чи захоплення апарата противник може отримати доступ до ключів, спробувати підміну інформації або впровадження хибних команд. Тому інтеграція Mesh-мереж має супроводжуватися автентифікацією вузлів, наскрізним шифруванням сигналу, періодичною зміною ключів і механізмами швидкого виключення ураженого вузла з мережі. Важливо також передбачити перевірку цілісності команд, що змінюють маршрут чи ціль, щоб унеможливити їх перехоплення та підміну.

Практична реалізація має наступну низку обмежень:

багатоетапна передача збільшує затримки та знижує пропускну здатність, що критично для передачі відеоданих, тому потрібно надавати більшу перевагу службовому трафіку, ніж інформаційному;

постійна робота приймально-передавальних модулів і постійний пошук маршрутів підвищують енергоспоживання та скорочують дальність польоту;

рухома мережа зв'язку в умовах високих швидкостей руху вузлів ускладнює підтримання зв'язку між БпЛА.

Ураховуючи зазначене Mesh-мережу доцільно розглядати як елемент багаторівневої системи, у якій обов'язковими елементами залишаються автономні режими, навігація за альтернативними джерелами та самостійне виконання завдання за повної втрати зв'язку.

Отже, інтеграція Mesh-мережі у систему зв'язку стратегічних БпЛА дозволяє перейти від вразливого єдиного каналу до стійкої розподіленої

структури, здатної зберігати керованість і обмін даними в умовах інтенсивного впливу РЕБ противника. Ефективність такого підходу визначається поєднанням гнучкої схеми зв'язку, різноманітності каналів, зниженої помітності випромінювання сигналів БпЛА та шифруванням вузлів передачі сигналу.

Грунович В. О.
Маліка А. А.
Національна академія Служби безпеки України

РОЗВИТОК СПОСОБІВ ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ З УРАХУВАННЯМ КОНСТРУКТИВНИХ МОЖЛИВОСТЕЙ ХОДОВОЇ ЧАСТИНИ

Сучасні умови ведення бойових дій обумовлюють постійне розширення сфер застосування наземних роботизованих комплексів (далі – НРК). Роботизовані платформи використовуються для транспортування матеріальних засобів, евакуації поранених, виконання інженерних завдань, спостереження та вогневої підтримки. Їх застосування дозволяє зменшити ризик для особового складу та забезпечити виконання окремих завдань у районах, де використання пілотованої техніки є небажаним або обмеженим.

Одночасно змінюються умови, у яких НРК повинні виконувати поставлені завдання. Підрозділи діють на різноманітній місцевості, яка може включати ґрунтові дороги, пересічену місцевість, схили, заболочені ділянки, зруйновану інфраструктуру та ділянки з природними і штучними перешкодами. Крім того, одна роботизована платформа може використовуватися для виконання декількох завдань, що передбачають різну масу корисного навантаження, різні маршрути та різні вимоги до мобільності.

За таких умов ефективність НРК визначається не окремою технічною характеристикою, а відповідністю конструкції платформи умовам її майбутнього застосування. Недостатня прохідність може унеможливити досягнення заданого району, нестійкість під час руху обмежує швидкість і безпечність переміщення, а надмірні динамічні навантаження можуть негативно впливати на роботу встановленого обладнання. Одночасно збільшення маси та складності ходової частини впливає на енергоспоживання, запас ходу та корисне навантаження.

Таким чином, виникає комплексна проблема узгодження конструктивних можливостей НРК із завданнями та умовами його застосування. Її особливість полягає у взаємозалежності основних характеристик платформи. Підвищення прохідності за рахунок збільшення кількості елементів ходової частини або застосування складнішої підвіски може призвести до збільшення маси та конструктивної складності. Використання активних систем підвіски розширює можливості адаптації до рельєфу, однак потребує додаткових приводів, систем керування та енергетичних ресурсів. Зменшення маси платформи, навпаки, позитивно впливає на запас ходу, але може обмежувати вантажопідйомність та стійкість.

Особливого значення зазначена проблема набуває для гусеничних НРК, оскільки їх здатність пересуватися складним рельєфом значною мірою визначається конструкцією ходової частини та підвіски. Положення опорних котків, довжина опорної поверхні, кінематична схема підвіски та характер переміщення її елементів впливають на контакт гусениці з поверхнею, розподіл навантаження та положення корпусу під час подолання перешкод.

На етапі проєктування гусеничного НРК можуть розглядатися різні конструктивні схеми ходової частини. Вибір конкретного рішення повинен здійснюватися з урахуванням призначення платформи, характеристик місцевості, маси корисного навантаження, необхідної мобільності та енергетичних можливостей.

Одним із найпростіших варіантів є жорстка ходова частина, у якій відсутні пружні елементи між корпусом та ходовою частиною. Така конструкція відзначається простотою, надійністю та малою масою, однак характеризується значними ударними навантаженнями та низькою адаптивністю до нерівностей поверхні. Тому її застосування доцільне переважно для платформ, призначених для руху по рівній або підготовленій поверхні.

Більш широкі можливості забезпечує незалежна пасивна підвіска, у якій опорні котки можуть переміщуватися індивідуально за рахунок пружних елементів. Така схема сприяє покращенню контакту гусениці з поверхнею та зниженню динамічних навантажень. Водночас збільшення кількості конструктивних елементів призводить до зростання маси та складності ходової частини. Подібні рішення можуть бути доцільними для багатоцільових НРК, які повинні виконувати завдання в різних умовах.

Для руху по пересіченій місцевості можуть застосовуватися балансирні схеми підвіски. У такому випадку група опорних котків встановлена на

спільному балансирі, що забезпечує рівномірніший розподіл навантаження та підвищує прохідність платформи. Основним обмеженням цієї схеми є обмежене незалежне переміщення окремих опорних котків, проте конструктивна простота та здатність адаптуватися до нерівностей роблять її придатною для відповідних умов експлуатації.

Ще вищу адаптивність до складного рельєфу можуть забезпечувати багатоланкові схеми. Їх конструкція передбачає використання кількох шарнірно з'єднаних елементів, переміщення яких дозволяє краще пристосовувати ходову частину до нерівностей поверхні та долати складні перешкоди. Водночас така схема характеризується складнішою кінематикою та підвищеними вимогами до конструкції шарнірних з'єднань. Її застосування доцільне для НРК, призначених для роботи на складному рельєфі.

Найбільші можливості адаптації забезпечують активні системи підвіски, у яких для керування положенням елементів ходової частини використовуються додаткові приводи. Це дозволяє змінювати положення підвіски відповідно до умов руху та стабілізувати корпус платформи. Разом із тим активна підвіска характеризується значною конструктивною складністю та додатковим енергоспоживанням, тому її застосування є найбільш доцільним для спеціалізованих високотехнологічних НРК, для яких можливості адаптації мають визначальне значення.

Таким чином, різні конструктивні схеми ходової частини забезпечують різне співвідношення прохідності, складності, маси та енергетичних витрат. Універсальної конструкції підвіски, яка однаково ефективно відповідала б усім способам застосування НРК, не існує. Для платформи, що переважно працює на підготовлених маршрутах, може бути достатньою проста ходова система. Для НРК, призначеного для роботи на пересіченій місцевості, пріоритетного значення набувають здатність копіювати рельєф, збереження контакту гусениці з поверхнею та зниження динамічних навантажень.

Для платформ, призначених для руху складним рельєфом, одним із перспективних напрямів є використання пасивних балансирних або багатоланкових схем підвіски. Їх застосування дозволяє забезпечити переміщення опорних елементів відносно корпусу та краще копіювати нерівності поверхні без використання додаткових приводів. Це має особливе значення для автономних платформ, для яких маса, енергоспоживання та надійність безпосередньо впливають на тривалість виконання завдання.

Разом із тим вибору лише типу підвіски недостатньо. Важливим є визначення її конкретних геометричних та кінематичних параметрів: положення опорних котків, координат шарнірів, довжин ланок, допустимих кутів переміщення та характеристик пружних елементів. Зміна цих параметрів впливає на траєкторію руху опорних елементів, контакт гусениці з поверхнею, положення корпусу та характер розподілу навантаження під час подолання перешкод.

У зв'язку з цим доцільним є застосування структурно-кінематичної оптимізації пасивної підвіски. Її сутність полягає у визначенні такої конфігурації ходової системи, яка забезпечує необхідну прохідність за одночасного дотримання обмежень щодо маси, габаритів, стійкості та навантаження на конструктивні елементи.

Як основні критерії оцінювання можуть використовуватися прохідність, стійкість корпусу, рівень динамічних навантажень та питомі енергетичні витрати. У загальному вигляді цільову функцію можна представити:

$$J(x) = w_1 J\ (x) + w_2 J\ (x) + w_3 J_d(x) + w_4 J_{\text{e}}(x) \rightarrow min,$$

де x – сукупність геометричних і кінематичних параметрів підвіски; J , J , J_d, J_{e} – критерії прохідності, стійкості, динамічних навантажень та енергетичних витрат; $w_1 - w_4$ – вагові коефіцієнти відповідних критеріїв.

При цьому співвідношення вагових коефіцієнтів повинно визначатися призначенням конкретної платформи. Для транспортного НРК більшу вагу може мати енергоефективність та здатність переміщувати задану масу вантажу. Для евакуаційного комплексу більш важливими є стійкість і зменшення динамічних навантажень. Для інженерної або спеціалізованої платформи, призначеної для роботи на складному рельєфі, пріоритетними стають прохідність та здатність долати перешкоди.

Такий підхід дозволяє пов'язати конструктивні параметри НРК із майбутнім способом його застосування. Послідовність формування конструктивного рішення може бути представлена як:

завдання → умови експлуатації → вимоги до мобільності → вибір ходової схеми → визначення параметрів підвіски → оцінювання можливостей платформи.

У результаті ходова частина розглядається не як окремий конструктивний елемент, а як складова загальної системи забезпечення виконання завдання. Прохідність платформи визначає доступні маршрути її переміщення, стійкість

впливає на можливість використання встановленого обладнання під час руху, а рівень динамічних навантажень визначає вимоги до міцності конструкції та надійності обладнання.

Зазначений взаємозв'язок має значення і для комплексного застосування різнорідних безпілотних систем. Авіаційний компонент може забезпечувати спостереження за маршрутом, оцінювання характеристик місцевості та інформаційне забезпечення наземного компонента, тоді як НРК безпосередньо виконує завдання на поверхні. У такій системі можливості наземної платформи визначають, чи може вона реалізувати отримане завдання за заданим маршрутом.

Наприклад, попереднє оцінювання маршруту за допомогою БпЛА дозволяє визначити ділянки з потенційними перешкодами, схилами або складними ґрунтовими умовами. На основі отриманої інформації можуть уточнюватися вимоги до руху НРК та обиратися відповідні режими його застосування. Таким чином, розвиток способів застосування авіаційних і наземних БпС передбачає не лише їх окреме вдосконалення, а й узгодження функціональних можливостей різних компонентів.

У цьому випадку конструктивні характеристики НРК безпосередньо впливають на організацію спільного застосування. Недостатня прохідність наземної платформи може обмежити можливість використання маршруту, визначеного за допомогою повітряного компонента. Аналогічно недостатня стійкість або надмірні коливання корпусу можуть обмежити застосування встановлених засобів спостереження, навігації чи зв'язку під час руху.

Отже, перспективним є перехід від підходу, за якого створюється універсальна роботизована платформа з подальшим визначенням способів її застосування, до підходу, за якого конструктивні характеристики формуються відповідно до визначених завдань та умов експлуатації. Це дозволяє ще на етапі проєктування встановити критичні вимоги до мобільності, вибрати відповідну схему ходової частини та визначити параметри підвіски.

Таким чином, розвиток способів застосування наземних роботизованих комплексів повинен відбуватися одночасно з розвитком їх конструктивних можливостей. Вибір та оптимізація ходової частини, зокрема підвіски гусеничних платформ, є одним із напрямів забезпечення відповідності НРК конкретним завданням та умовам експлуатації. Комплексне врахування прохідності, стійкості, динамічних навантажень, енергетичних витрат та характеристик корисного навантаження дозволяє сформувати конструкцію

платформи відповідно до визначеного способу її застосування та підвищити ефективність спільного використання наземних і авіаційних безпілотних систем.

Бондарчук В. Д.
Первак І. В.
Галепа О. Г.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

НАВІГАЦІЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ ПОДАВЛЕННЯ GNSS НА ОСНОВІ ВІЗУАЛЬНО-ІНЕРЦІЙНИХ МЕТОДІВ

Сучасні безпілотні літальні апарати (БпЛА) прямо залежать від глобальних навігаційних супутникових систем (Global Navigation Satellite System, GNSS). Сигнал таких систем на поверхні Землі слабкий, тому його легко подавити. У зоні бойових дій засоби радіоелектронної боротьби (РЕБ) створюють потужні завади та підміняють сигнал, через що БпЛА втрачає або отримує хибні координати. Наслідком цього є зрив польотного завдання, відхилення від маршруту та втрата БпЛА. Тому актуальним є створення автономних методів навігації, які не потребують зовнішніх радіосигналів і не вразливі до засобів РЕБ.

Одним із найперспективніших напрямів є візуально-інерційна навігація (Visual-Inertial Odometry, VIO), яка поєднує дані бортової камери та інерційного вимірювального блока (Inertial Measurement Unit, IMU). Інерційні датчики (акселерометри та гіроскопи) працюють із частотою в сотні герц і не залежать від зовнішнього середовища. Проте їхня похибка постійно накопичується з часом: помилка положення зростає майже квадратично, і за певний час автономного польоту відхилення стає критичним. Камера, навпаки, дає інформацію про навколишнє середовище, але працює з нижчою частотою, чутлива до освітлення та не дає масштабу без додаткових даних. Системи доповнюють одна одну: IMU безперервно вимірює рух між кадрами і визначає масштаб, а камера виправляє накопичену похибку відхилення.

Водночас класична VIO визначає лише відносне переміщення, тому її похибка все одно повільно зростає з пройденою відстанню. Для отримання абсолютних координат без GNSS доцільно використовувати двоетапну схему з

попереднім картографуванням місцевості, коли VIO доповнюється зіставленням із заздалегідь створеною тривимірною картою.

На першому етапі розвідувальний БпЛА виконує сканування території за заданим маршрутом. Це робиться тоді, коли GNSS ще доступна або коли застосовується наземна геодезична прив'язка опорних точок. Використовується оптична камера, а за наявності відповідної навантаги також лазерний сканер. Із послідовності знімків методами фотограмметрії та одночасної локалізації і картографування створюється тривимірна цифрова модель місцевості. Важливо, що карта містить не лише геометрію, до неї записуються візуальні ознаки такі як ідентифікатори характерних точок, контури будівель, дорожньої інфраструктури, ліній електропередач, берегової лінії. Кожна ознака прив'язана до координат у єдиній системі, і в результаті формується база орієнтирів для подальшого польоту.

На другому етапі БпЛА виконує місію в умовах придушення GNSS. Бортова камера знаходить у поточному кадрі характерні ознаки та зіставляє їх з картою. Для прискорення пошуку використовується орієнтовне положення, яке дає VIO: перевіряються лише ті ділянки карти, що потрапляють у зону невизначеності. За знайденими відповідностями "точка кадру – точка карти" розв'язується задача визначення положення камери за відомими просторовими точками. Її результатом є абсолютні координати та кути орієнтації апарата в системі координат карти. Отримані вимірювання надходять і об'єднуються з даними IMU. Інерціальний канал забезпечує безперервність оцінки між кадрами, а кожне успішне зіставлення з картою нівелює накопичене відхилення під час польоту. Висота польоту додатково уточнюється барометричним датчиком і порівнянням із цифровою моделлю рельєфу. Така систему дає змогу зберегти високу частоту навігаційних даних та обмежити похибку в часі, на відміну від автономної VIO.

Практична реалізація методу стикається з низкою проблем. Перша з них пов'язана зі зміною вигляду місцевості між скануванням і польотом: на нього впливають час доби, пора року, опади, тіні, а в бойових умовах ще й руйнування та нові укріплення. Друга проблема стосується однорідних поверхонь (поле, ліс, водойми, сніговий покрив), де бракує стійких ознак для зіставлення. Третя – різниця ракурсів і висот, через яку ознаки на карті та в кадрі виглядають по-різному. А також те, що бортовий комп'ютер БпЛА має обмежені обчислювальні ресурси та енергоспоживання, а карта великої території займає значний обсяг пам'яті.

Для підвищення стійкості застосовуються нейромережеві методи пошуку збігів ознак, які менш чутливі до зміни освітлення й сезону.

Представлення картографічних даних відбувається на різних масштабних рівнях: дрібномасштабні та середньомасштабні – для первинної прив’язки, великомасштабні – для уточнення. Хибні відповідності відсіюються алгоритмом випадкового узгодження, який перевіряє, чи підтверджує більшість знайдених збігів єдину модель положення камери.

Для роботи над однорідними ділянками доцільно планувати маршрут так, щоб він проходив поблизу виразних орієнтирів, а на ділянках без них покладатися на VIO та висотомір. Для зменшення навантаження на бортовий комп’ютер карта стискається, а для польоту завантажується лише коридор уздовж маршруту. Окремої уваги потребує оперативне оновлення карти за свіжими розвідувальними даними, щоб зміст відповідав поточному стану місцевості.

Отже, поєднання попередньо створеної тривимірної карти з візуально-інерційною навігацією дозволяє БпЛА визначати своє положення без GNSS із точністю до одиниць метрів, зберігаючи працездатність в умовах активної дії засобів РЕБ. Метод не випромінює сигналів, тому не демаскує апарат і не вразливий до завад та спуфінгу.

Пилипчук Т. І., курсант
Площик А. С.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ІНФОРМАЦІЙНІ СИСТЕМИ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ ПРО ПОВІТРЯНУ ОБСТАНОВКУ В ТАКТИЧНІЙ ЛАНЦІ СИЛ ОБОРОНИ УКРАЇНИ

Затримка між появою повітряної цілі та її відображенням на тактичному пульті визначає час реагування протиповітряної оборони. Акустичні датчики слугують альтернативним джерелом даних, проте низька швидкість звуку породжує затримку виявлення: на дальності 10 км вона сягає в середньому 29 с, за які крилата ракета долає 5,83–7,84 км, а БПЛА — 1,14 км. Крім того, додаткову затримку створює людський чинник — процес ручного

підтвердження та перевірки даних оператором: кожна хвилина такої перевірки додає 12–17,45 км прольоту ракети та 2,34 км прольоту БПЛА.

Потенціал військових геоінформаційних систем у повномасштабній війні реалізовано не повністю. Механізми систематичної інтеграції волонтерських рішень у єдину структуру управління потребують розробки. Низові практики, зокрема поєднання «Delta», інформаційно-аналітичні панелі, розвідки, спостереження, захоплення цілей та цілевказання і ролі чергового офіцера напрямку, не мають нормативного закріплення. У складних мережевих системах управління бою виникає непередбачувана сукупна поведінка, що спричиняє збої в розвідці та бездротових мережах. Бракує огляду, який поєднує акустичний, геоінформаційний і мережевий підходи.

Об'єктом дослідження є інформаційні системи ситуаційної обізнаності про повітряну обстановку в тактичній ланці Сил оборони України, а предметом дослідження — методи, алгоритми та засоби підвищення оперативності виявлення цілей і мінімізації часових затримок обробки даних у цих системах. Мета роботи – систематизувати наявні підходи та виявити консенсус, суперечності й обмеження сучасних досліджень. Дослідження виконано як порівняльний аналітичний огляд восьми публікацій 2022–2025 рр. Джерела охоплюють акустичний моніторинг, військову ситуаційну обізнаність, інформаційно-аналітичне управління бойовими діями, військові геоінформаційних систем, системи управління Повітряних Сил і сумісність з НАТО, непередбачувану сукупну поведінку в системах управління боєм. Зіставлено методи першоджерел: системно-архітектурний та розрахунково-аналітичний аналіз, програмно-системну розробку, аналіз сильних і слабких сторін, можливостей та загроз, аналіз бойових кейсів, порівняльний аналіз і декомпозицію, сценарійні та експертні методи, метакібернетичне моделювання. Результати згруповано за консенсусом авторів, дискусійними положеннями та заявленими обмеженнями.

Дослідження [Сідченко, 2024] кількісно окреслює межі акустичного моніторингу. Середня затримка виявлення на дальності 10 км становить 29 с. За цей час крилата ракета долає 5,83–7,84 км, а БПЛА лише 1,14 км. Тривалість перевірки та підтвердження даних оператором чинить різний за ступенем критичності вплив залежно від швидкості повітряної цілі: кожна хвилина затримки додає 12–17,45 км прольоту для крилатої ракети та лише 2,34 км —

для БПЛА. Таким чином, для високошвидкісних крилатих ракет така перевірка оператором є значно вагомішим чинником, ніж для малошвидкісних безпілотників.

На відміну від розрахункового підходу [Сідченко, 2024], робота [Kitsera, 2025] зосереджується на візуалізації. Інтерактивна карта відображає переміщення цілей у реальному часі за даними розподіленої мережі акустичних сенсорів і підвищує швидкість та обґрунтованість рішень операторів. Натомість перше джерело пропонує протокол обміну з спеціалізованим програмним забезпеченням «Віраж-Планшет», автоматичне розпізнавання сигналу та базу акустичних портретів [Сідченко, 2024].

Емпіричні дані показують, що поєднання «Delta», інформаційно-аналітичні панелі, розвідки, спостереження, захоплення цілей та цілевказання і ролі чергового офіцера напрямку синхронізує розвідку, командування та вогневе ураження в реальному часі. Вибірка обмежена одним об'єктом: зведеною оперативною групою 13-ї бригади НГУ. Класифікація та аналіз сильних і слабких сторін, можливостей та загроз охоплюють ширший спектр рішень і пояснюють їхню результативність синергією ІТ-фахівців і волонтерів. Дослідження [Kobzan, 2025] фіксує інший бік проблеми: потенціал військових геоінформаційних систем реалізовано не повністю, а інтеграція штучного інтелекту потрібна для концепції «розумного поля бою».

Позиції щодо ролі людини розходяться. Автори [Сідченко, 2024] розглядають оператора як джерело критичних затримок і наполягають на автоматизації класифікації. Натомість [Kret, 2025] та [Putrenko, 2024] підкреслюють аналітичний потенціал людини й гнучкі організаційні ролі, а [Kobzan, 2025] трактує ШІ як засіб підтримки рішень, не як заміну. Оцінка децентралізованих систем також неоднорідна: [Kret, 2025] і [Putrenko, 2024] бачать у них позитивний чинник, тоді як [Seizovic, 2022] попереджає про непередбачувану сукупну поведінку, здатну спричинити збої в розвідці та бездротових мережах.

Дослідження Повітряних Сил пропонують формалізовані моделі. Це триетапний метод (оцінка ефективності, оцінка сумісності з НАТО, синтез моделі за узагальненим показником) та сценарійний, багатокритеріальний і експертний інструментарій оцінки сумісності. Тактичні роботи [Kret, 2025; Kitsera, 2025] описують адаптивні ініціативи, що виникають знизу.

Автори сходяться в трьох положеннях. Потрібен відхід від радянських моделей командування та управління. Пріоритетом є рішення на основі даних

[Kitsera, 2025; Kobzan, 2025]. Системи мають бути сумісними з НАТО. Кількісних польових метрик ефективності, зокрема відсотка ураження цілей, більшість джерел не наводить. Моделі [Seizovic, 2022] потребують верифікації на реальному мережевому трафіку в умовах РЕБ.

Ефективність акустичного моніторингу обмежена фізичною затримкою виявлення та перевірки і підтвердження даних оператором. Затримка становить 29 с на дальності 10 км, а кожна хвилина перевірки та підтвердження даних оператором додає 12–17,45 км прольоту крилатої ракети та 2,34 км прольоту БПЛА. Пріоритетні напрями: автоматичне розпізнавання сигналу, повна база акустичних портретів і протокол обміну з спеціалізованим програмним забезпеченням «Віраж-Планшет». Візуалізація на інтерактивній карті підвищує швидкість і обґрунтованість рішень операторів.

Результативність мережевих платформ залежить від організаційної моделі. Поєднання «Delta», інформаційно-аналітичні панелі, розвідки, спостереження, захоплення цілей та цілевказання і ролі чергового офіцера напрямку забезпечує перехід до рішень на основі даних, однак потребує нормативного закріплення для масштабування на Сили оборони. Для інтеграції волонтерських розробок необхідні механізми систематизації. Інтеграція штучного інтелекту у військові геоінформаційні системи розглядається як засіб підтримки рішень у концепції «розумного поля бою». Мережеві системи управління бою водночас потребують контролю непередбачуваних сукупних ефектів.

Автори сходяться щодо відходу від радянських моделей командування та управління, пріоритету даних і сумісності з НАТО. Кількісні показники бойової ефективності в більшості джерел відсутні, тому наявні висновки мають концептуальний характер.

Відкритими залишаються питання кількісної оцінки ефективності цих систем у польових випробуваннях, верифікації теоретичних моделей на реальному мережевому трафіку в умовах РЕБ та узгодження автоматизації з роллю людини-оператора.

Таким чином, проведене дослідження дозволяє сформулювати такі основні підсумки:

1. Ключовим чинником, що обмежує оперативність виявлення повітряних цілей акустичними датчиками, є комбінація фізичної затримки поширення звуку та часових витрат на людський чинник. Для підвищення ефективності необхідна максимальна автоматизація розпізнавання сигналів та пряма інтеграція з спеціалізованим програмним забезпеченням «Віраж-Планшет».

2. Використання сучасних ситуаційних та аналітичних платформ довело свою дієвість на тактичному рівні, проте розгортання таких низових ініціатив потребує системного нормативно-правового закріплення та формалізованих механізмів інтеграції волонтерських розробок.

3. Перспективи подальшого розвитку систем ситуаційної обізнаності полягають упровадженні штучного інтелекту як засобу підтримки прийняття рішень, забезпеченні технічної та оперативної сумісності за стандартами НАТО, а також проведенні комплексних польових випробувань і верифікації моделей у складних умовах радіоелектронної боротьби.

Крутієнко О. В., курсант
Площик А. С.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ОСОБЛИВОСТІ ВИКОРИСТАННЯ АВТОНОМНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ АКТИВНОГО ПОДАВЛЕННЯ СИГНАЛІВ СУПУТНИКОВОЇ НАВІГАЦІЇ

Супутникові навігаційні системи залишаються вразливими до глушіння, підміни сигналу та повного блокування. Радіоелектронне придушення дезорієнтує БПЛА, унеможливлює виконання місії та загрожує безпеці польоту. Автори роботи (Detecting GNSS spoofing and Re-localization on UAV based on imagery matching(2024)) вважають підміну координат небезпечнішою за їх відсутність, адже апарат отримує хибні дані без ознак збою.

Дослідники сходяться в тому, що стандартних методів фільтрації недостатньо. Автономність потребує комплексування інерціальних систем, глибокого навчання, аналізу характеристик завад або кооперативних алгоритмів. Єдиного підходу немає: розбіжності стосуються статусу завади (загроза чи джерело даних), архітектури системи (одиночний БПЛА чи група) та сенсорної бази. Більшість результатів отримано в симуляції. Польові експерименти описано лише в одній праці (A Hierarchical Absolute Visual Localization System for Low-Altitude Drones in GNSS-Denied Environments(2025)).

Наукова проблема полягає у відсутності систематизованого зіставлення радіо-інерціальних і візуальних підходів до автономної навігації БПЛА за активного придушення супутникової навігаційної системи.

Аналіз наукових публікацій дозволяє систематизувати розробки за двома ключовими технологічними напрямами. Першу групу становлять радіо- та інерціальні підходи, що поєднують бортову сенсорику з обробкою радіосигналів: адаптивна навігація за сигналом завади (Aldosari W., 2026), де розширений фільтр Калмана оцінює потужність випромінювання, а глибоке навчання з підкріпленням оптимізує траєкторію; обхід зони придушення як фізичної перешкоди (Liu Y., Niu Q., 2026) за допомогою алгоритму штучних потенційних полів та інерціальної системи; локалізація джерел завад одиночним БПЛА (Luo Y. et al., 2026) без використання каналів зв'язку між бортами; а також кооперативний радіозахист групи бортів (Zhou J. et al., 2024) шляхом переносу частоти та формування віртуальної антенної решітки. Другу групу утворюють візуальні підходи, засновані на пасивній обробці зображень: побудова тривимірної карти та локалізація в реальному часі (Wu Y.-T., Huang Y.-C., 2026) за допомогою алгоритму тривимірного візуального картографування та камери глибини; ієрархічна абсолютна візуальна локалізація (Zhou Q. et al., 2025) за наземними орієнтирами; та нейромережеве виявлення підміни супутникових сигналів (Liu R. et al., 2024) шляхом зіставлення бортових аерофотознімків із супутниковими картами, що дозволяє виявити спотворення даних за 100 мс і відновити реальні координати. Порівняння виконано за чотирма критеріями: сенсорна база, архітектура системи, тип загрози та рівень емпіричної верифікації.

Порівняння робіт виявляє три розбіжності: у трактуванні завади, в архітектурі системи та в сенсорній базі.

Перша стосується статусу завади. Автор (Aldosari W.) використовує сигнал глушіння як джерело навігаційних даних. Розширений фільтр Калмана оцінює потужність передавача завад, рівень прийнятого сигналу та показник загасання траси, а алгоритм глибокого навчання з підкріпленням на цій основі оптимізує траєкторію. На відміну від цього, дослідження (Liu Y., Niu Q.) розглядає зону глушіння як небезпечну перешкоду. БПЛА літакового типу оминає її за допомогою модифікованого алгоритму штучних потенційних полів з віртуальними точками-перешкодами та навігаційною системою, зберігаючи

динамічні обмеження польоту. Обидві праці спираються на симуляцію, а абсолютних показників точності чи виживаності не наводять.

Друга розбіжність є архітектурною. Автори (Luo Y., Kong X., Wu C., Zeng M., Tian J., Jiang H., Xu G., Ren Z., Zhang L.) виходять з того, що придушення зв'язку унеможливлює обмін даними між бортами, тому локалізують джерела завад одним БПЛА. Схема локалізації джерел завад для малого БПЛА знижує похибку пеленгації на 87% відносно методу мінімальної дисперсії безвикривного відгуку та середньоквадратичну похибку локалізації на 32% відносно зваженого методу найменших квадратів. Швидкість локалізації при цьому зростає орієнтовно на 75%. Ці показники отримано в симуляції для конкретного співвідношення сигнал/шум. Натомість у роботі (Multi-UAV Cooperative Anti-Jamming for GNSS Signals Based on Frequency-Domain Power Inversion(2024)) обґрунтовано перевагу кооперативної групи: перенос частоти та ретрансляція сигналів поза діапазоном супутникових навігаційних систем об'єднують борти у «віртуальний» масив і збільшують просторові ступені свободи. Це твердження має суто теоретичний характер, кількісних даних немає.

Третя розбіжність стосується сенсорів. Візуальні підходи супроводжуються конкретнішими числовими оцінками. Система з однією камерою глибини та алгоритмом тривимірного візуального картографування у віртуальному середовищі симуляції з програмним моделюванням польоту дає середньоквадратичну похибку проходження траєкторії 0,195 м, 0,197 м і 0,420 м для низької, середньої та високої щільності перешкод відповідно. Середньоквадратична похибка повернення становить 0.295, 0.474 і 1.084 м. Похибка проходження зростає більш ніж удвічі. Ієрархічна візуальна локалізація є єдиною з розглянутих систем, перевіреною в реальних польотах. За результатами натурних польотних випробувань, проведених у дослідженні Zhou Q. et al. (2025), успішність ієрархічної системи абсолютної візуальної локалізації маловисотного БПЛА на чотирьох випробувальних траєкторіях склала 95,02%, 64,50%, 64,84% та 91,09%. Розкид понад 30 процентних пунктів вказує на залежність від рельєфу та типу маневру.

Окреме місце посідає праця (Detecting GNSS spoofing and Re-localization on UAV based on imagery matching.(2024)), присвячена спуфінгу, а не глушінню. Нейромережа зіставляє бортові знімки з відкритими супутниковими картами. Вона виявляє підміну з точністю 88.4% за 100 мс і відновлює координати з успішністю 88% та відхиленням менше 15 м. На відміну від розробок, що

потребують додаткових антен чи датчиків, цей метод працює зі стандартною камерою. Дані про вибірку й незалежну валідацію автори не наводять.

Загалом числові результати непорівнянні між собою: роботи використовують різні метрики, сценарії та рівні верифікації. Натурне підтвердження наявне лише в (A Hierarchical Absolute Visual Localization System for Low-Altitude Drones in GNSS-Denied Environments.(2025)).

Супутникова навігація не забезпечує стійкості БПЛА за активного придушення, тому проаналізовані роботи переходять до бортових рішень: радіопеленгації, інерціального комплексування, візуальної локалізації та кооперативної обробки сигналів. Стандартної фільтрації для цього недостатньо.

Підходи розходяться у трьох вимірах. Завада розглядається або як джерело навігаційних даних, або як перешкода, яку слід оминути. Локалізацію джерел завад виконує один БПЛА без радіообміну або кооперативна група. Сенсорна база охоплює радіосигнали й інерціальну навігаційну систему чи пасивні оптичні сенсори.

Кількісні оцінки є, але умови їх отримання різні. Схема локалізації джерел завад для малого БПЛА (Luo Y. et al., 2026) знижує похибку пеленгації на 87% та середньоквадратичну похибку локалізації на 32%, проте вказані результати досягнуто виключно в умовах симуляційного моделювання для конкретного співвідношення сигнал/шум. Ієрархічна система абсолютної візуальної локалізації (Zhou Q. et al., 2025) є єдиною розробкою, що пройшла перевірку в натурних польотах, показавши успішність від 64,50% до 95,02% залежно від рельєфу та складності траєкторії. Окреме місце посідає нейромережевий метод виявлення підміни супутникових сигналів (Liu R. et al., 2024), який досяг точності 88,4% за 100 мс. Проте даний підхід спрямований безпосередньо на протидію підміні навігаційних даних (спуфінгу), а не їх прямому радіоелектронному придушенню (глушінню).

Проаналізовані дослідження свідчать про відсутність універсального рішення для автономної навігації БПЛА в умовах придушення Супутникової навігаційної системи. Найбільш перспективним напрямом є відмова від моносенсорних систем на користь комплексування інерціальної навігації, візуального зіставлення орієнтирів та адаптивних алгоритмів оцінки радіозавад. Актуальними завданнями для подальших досліджень залишаються проведення натурних польотних випробувань симуляційних моделей, уніфікація метрик оцінки точності та створення комбінованих радіо-візуальних навігаційних систем.

Кудрявцева А. П.
Національна академія Служби безпеки України

ЗАХИЩЕНА MESH-МЕРЕЖА ДЛЯ ЗАБЕЗПЕЧЕННЯ РАДІОЗВ’ЯЗКУ МАЛИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ ЩІЛЬНОЇ МІСЬКОЇ ЗАБУДОВИ

Групи малих безпілотних літальних апаратів потребують надійного інформаційного обміну як між окремими БпЛА, так і з наземним пунктом керування. При цьому характеристики радіомережі безпосередньо впливають на можливість координації та передачі даних між елементами групи, а саме значною швидкістю переміщення вузлів, тривимірною топологією та швидкою зміною доступних радіоз’єднань. Проблема ускладнюється під час експлуатації малих БпЛА в щільній міській забудові. Висотні будівлі, екранування та зміна умов поширення радіосигналу можуть обмежувати прямий зв’язок між БпЛА та наземним пунктом керування. Тому використання лише прямого каналу не забезпечує необхідної гнучкості мережевої структури.

Одним із перспективних підходів є використання Mesh-архітектури, у якій БпЛА можуть виконувати функції проміжних вузлів та ретрансляторів.

Окремою складовою є захист інформаційної взаємодії. У захищених UAV-FANET (бездротова самоорганізовна мережа, яка створюється групою БПЛА) необхідно забезпечувати автентифікацію вузлів та контроль їхньої допустимості для участі в обміні даними. Отже, перспективним є поєднання multi-hop mesh network (передача сигналу через послідовність радіопереходів у мережній архітектурі з можливістю формування альтернативних маршрутів) з механізмом оцінювання довіри до вузлів.

В роботі наведено особливості моделювання трьох базових сценаріїв, що визначаються способом організації мережі.

1. Прямий радіозв’язок (Сценарій S1) у базовому сценарії кожний БпЛА встановлює пряме з’єднання з GCS. Проміжні вузли не використовуються. Група БпЛА та наземний пункт керування розглядаються як сукупність мережевих вузлів:

$$V(t) = \{\mathrm{u}_1, \mathrm{u}_2, ..., \mathrm{u}_{N_U}, \mathrm{GCS}\} \quad (1)$$

де N_U – кількість БпЛА;

u_i – i-й БпЛА;

GCS – наземний пункт керування.

Просторове положення кожного БпЛА в момент часу (t) визначається координатами $r_i(t) = [\mathrm{x_i(t), y_i(t), z_i(t)}]^{\mathrm{T}}$. Таким чином, зміна просторового стану групи БпЛА безпосередньо впливає на структуру доступних радіоз'єднань.

Для двох вузлів u_i та u_j доступність радіоканалу визначається характеристиками відповідного з'єднання. З урахуванням мінімально допустимої потужності сигналу та відношення сигнал/шум динамічна структура мережі задається графом (2).

$$G(t) = (V(t), E(t)), \quad E(t) = \{(\mathrm{i, j}) : \mathrm{P}_{r,i,j}(t) \geq P_{\min}, SNR_{ij}(t) \geq SNR_{\min}\}, \tag{2}$$

де $E(t)$ – множина доступних радіоканалів;

$\mathrm{P}_{r,i,j}(t)$ – потужність прийнятого сигналу між вузлами i та j;

$P_{\min}$ – мінімально допустима потужність прийнятого сигналу

$SNR_{ij}(t)$ – відношення сигнал/шум;

$SNR_{\min}$ – його мінімально допустиме значення.

Граф $G(t)$ є динамічним, оскільки зміна координат БпЛА, умов поширення радіосигналу або характеристик каналів призводить до зміни множини $E(t)$.

Для міського середовища ця залежність є принципово важливою. Однакове геометричне розташування БпЛА не гарантує однакових параметрів радіоканалів за різної конфігурації забудови. Тому модель мережі повинна враховувати просторову структуру середовища та її вплив на доступність каналів.

Динамічна модель дозволяє розглядати мережу не як фіксовану топологію, а як послідовність станів $G(t)$, між якими відбувається перебудова маршрутів. Такий сценарій необхідний як контрольний, оскільки дозволяє визначити початковий рівень якості радіозв'язку в заданому міському середовищі.

2. Multi-hop mesh-мережа (сценарій S2) характеризується формуванням за допогою БпЛА динамічної Mesh-мережі відповідно до послідовності

Маршрут між БпЛА-джерелом (u_s) та *GCS* задається послідовністю

$$R(t) = \{\mathrm{u}_s, \mathrm{u}_1, ..., \mathrm{u}_{h-1}, \mathrm{GCS}\} \tag{3}$$

де (h) – кількість радіопереходів маршруту.

Відповідно, один і той самий інформаційний потік може передаватися різними маршрутами залежно від поточного стану *G(t)*.

Принциповою перевагою Mesh-організації є можливість використання альтернативних маршрутів при погіршенні характеристик одного з каналів. За наявності декількох доступних маршрутів використовується критерій (4). БпЛА можуть виконувати функції проміжних ретрансляторів.

Водночас збільшення кількості переходів може підвищувати затримку та збільшувати кількість потенційних точок розриву маршруту. Тому критерієм оптимальності не повинна бути лише мінімальна кількість переходів. Оптимальним вважається маршрут із максимальним значенням $J(R,t)$.

$$J(R,t) = w_Q \bar{Q}_R + w_P \bar{P}_R + w_L \bar{L}_R + w_C \bar{C}_R + w_T \bar{T}_R + w_H \bar{H}_R, \qquad \sum w_i = 1, \tag{4}$$

де,

$\bar{Q}_R$ – якість радіоканалів;

$\bar{P}_R$ – показник доставки пакетів;

$\bar{L}_R$ – стабільність маршруту;

$\bar{C}_R$ – мережева зв’язність;

$\bar{T}_R$ – рівень довіри;

$\bar{H}_R$ – кількість переходів.

Надані характеристики нормуються до діапазону [0,1], що забезпечує коректне використання їх в одному інтегральному критерії:

$w_Q, w_P, w_L, w_C, w_T, w_H$ – вагові коефіцієнти

Таким чином, маршрутизація здійснюється не за одним параметром, а за сукупністю характеристик радіоканалу, мережі та безпеки. Такий підхід для прийняття рішення може одночасно використовуватися для характеристики мобільності, ресурсів, каналів та безпеки. Однак основним предметом порівняння є визначення того, наскільки використання альтернативних multi-hop маршрутів дозволяє зберегти зв’язність у ситуаціях, коли прямий канал БпЛА – GCS є нестабільним або недоступним.

3. UAV-FANET mesh-мережа (сценарій S3) - Захищена mesh-мережа є розширенням multi-hop архітектури. Її особливість полягає в тому, що технічна доступність радіоканалу не є єдиною умовою використання вузла.

Для кожного БпЛА визначається показник довіри $0 \le T_i(t) \le 1$. Значення $T_i(t)$ характеризує допустимість використання вузла в захищеній інформаційній взаємодії. Відповідно, для маршруту враховується узагальнений показник довіри $\bar{T}_R$, який входить до критерію (4).

У практичній реалізації механізм його формування може базуватися на результатах автентифікації, історії взаємодії, контролі цілісності або інших механізмах довіри. У цій роботі конкретний криптографічний алгоритм не фіксується, оскільки предметом дослідження є модель мережевої організації, а не порівняння конкретних криптографічних протоколів.

Важливим є те, що захист інтегрується саме в процедуру формування маршруту. Це дозволяє уникнути ситуації, коли стандартизований, але недовірений вузол автоматично отримує пріоритет лише через хороші характеристики радіоканалу.

Таким чином, захищена Mesh-мережа розглядається як система, у якій забезпечення радіозв'язку та контроль допустимості вузлів є взаємопов'язаними функціями. Для об'єктивного порівняння різних способів організації радіозв'язку необхідно забезпечити однакові зовнішні умови експерименту.

$$X_{S_1} = X_{S_2} = X_{S_3} = [N_U, M, R(t), R(t), T_{\text{exp}}], \qquad (5)$$

де N_U – кількість БпЛА; M – модель міської забудови; $R(t)$ – траєкторії руху БпЛА; $R(t)$ – параметри радіосистеми; T_{exp} – тривалість експерименту.

Це означає, що для всіх сценаріїв повинні бути незмінними кількість БпЛА, геометрія міського середовища, траєкторії польоту, параметри радіопередачі та тривалість експерименту рис. 1.

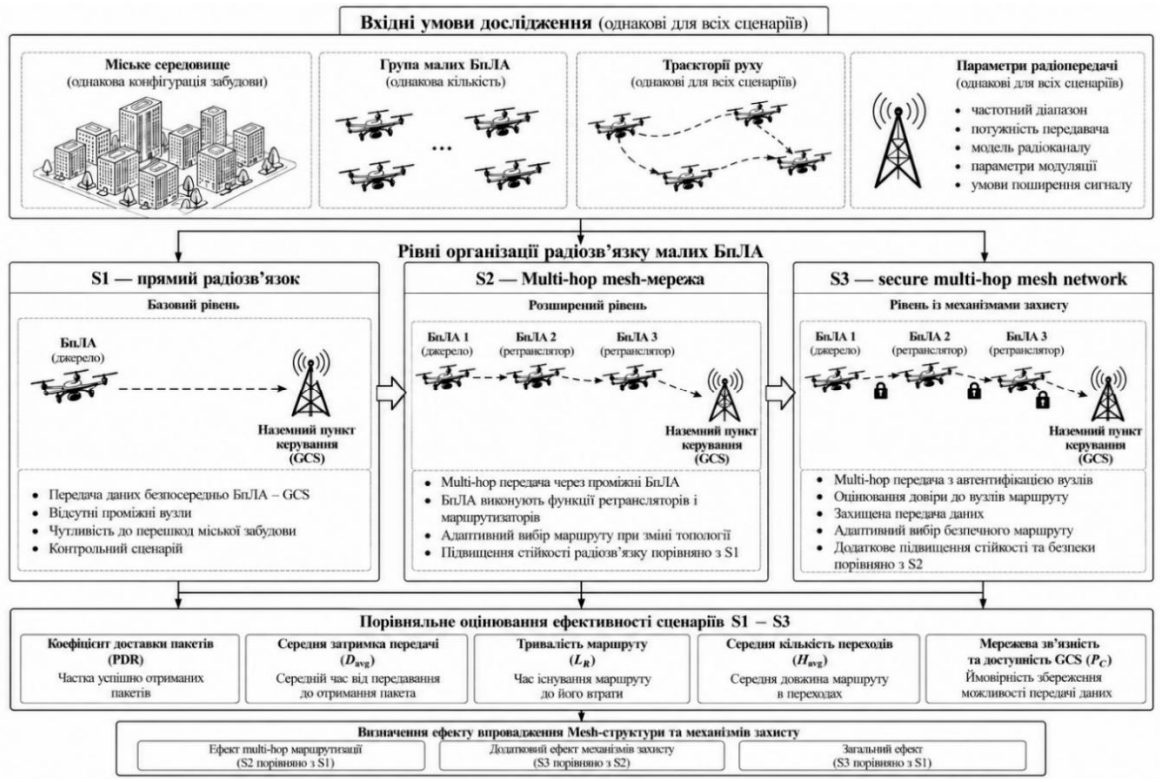


Рис. 1. Технічна схема сценаріїв Mesh-мережі БПЛА

У результаті вибір маршруту визначається одночасно технічними характеристиками радіоканалів та безпековими характеристиками вузлів

Запропонована методика дозволяє розділити результати дослідження на три рівні.

При цьому запропонована модель не прив’язується до конкретного криптографічного алгоритму. Це дозволяє надалі досліджувати різні механізми захисту без зміни математичної основи мережевої моделі.

Для міської забудови особливо важливим є поєднання просторової моделі та мережевої моделі. Саме зміна взаємного положення БпЛА та умов радіопоширення визначає, які маршрути існують у конкретний момент часу.

Таким чином, запропонований підхід створює основу для імітаційного дослідження, в якому можна варіювати щільність забудови, кількість БпЛА, траєкторії польоту, параметри радіоканалів та характеристики захисту, зберігаючи єдину методику порівняння.

Лемішко Л. С.
Ейдельштейн Г. Б.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ОБРОБЛЕННЯ ДАНИХ ПОВІТРЯНОЇ РОЗВІДКИ З ВИКОРИСТАННЯМ ЗГОРТКОВИХ НЕЙРОНИХ МЕРЕЖ

Повітряна розвідка генерує великі масиви EO/IR(Electro-Optical/Infrared) SAR(Synthetic Apertyre Radar) та мультиспектральних даних. Обробка данних у реальному часі перевищує можливості штатних розрахунків та стандартних наземних станцій управління (GCS), що призводить до затримок у системі командування та управління. Використання технологій згорткових нейроних мереж (CNN) дозволяє автоматизувати первинну селекцію, класифікацію та ранжування цілей, скорочуючи час від виявлення до прийняття рішення.

Розробити прикладну концепцію впровадження алгоритмів (CNN) у ланцюг обробки даних повітряної розвідки з урахуванням технічних вимог авіаційної інженерії, обмежень пропускної здатності каналів та стандартів сумісності з GIS/TDL (Geographic Information System/Tactical Data Link).

Основні завдання:

1.Визначити структуру даних, що підлягають автоматизованій обробці (EO/IR, SAR, LIDAR, телеметрія GNSS/INS) (Global Navigation Satellite System/ Inertial Navigation System).

2.Розробити архітектуру процесингового тракту: алгоритми попередньої обробки на борту та централізований алгоритмічний контур у наземних пунктах.

3.Забезпечити мультисенсорну інтеграцію та кореляцію даних для підвищення достовірності виявлення та відстеження об’єктів.

4.Розробити алгоритми пріорітетності та автоматичного виділення об’єкту для покращення роботи аналітиків.

5.Визначити протоколи людино-машинної взаємодії для верифікації результатів.

Методи та технічні рішення. Запропоновано двоступеневу систему:

Бортовий рівень: легкі нейромережеві модулі для попередньої фільтрації, виявлення змін та стискання даних з метою зниження навантаження на канал зв’язку.

Центральний рівень: система багатоканального аналізу з використанням архітектур для виявлення, класифікації та трекінгу об’єктів. Об’єднання даних здійснюється через алгоритми мультисенсорної інтеграції та просторово-часову кореляцію. Результати відображаються у GIS-шарах для оперативного використання.

Захист та експлуатація. Передбачається застосування шифрування каналів, контролю автентичності потоків та модулів виявлення аномалій для протидії інформаційним атакам. Реалізується принцип RBAC (Role-Based Access Control) із веденням аудиту рішень для подальшого аналізу. Система підтримує періодичну адаптацію моделей на основі нових датасетів та захищене оновлення програмного забезпечення.

Критерії ефективності. Зниження часу реагування, зростання точності детекції при контрольованому рівні, оптимізація обсягу переданих даних та скорочення навантаження на оператора. Планується апробація на навчальних польотах з паралельною ручною верифікацією результатів.

Висновок. Використання згорткових нейроних мереж (CNN) в обробці даних повітряної розвідки дозволяє створити операційно-придатний алгоритмічний контур з мінімальною латентністю, модульною архітектурою та гарантованою сумісністю з системами управління. Це відкриває перспективу для розробки дослідного зразка та проведення польових випробувань у реальних умовах.

Пасічнюк І. А.
Льова О. І.
Гром В. А.
Харківський університет Повітряних Сил
імені Івана Кожедуба

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ОБ’ЄКТІВ ОПТИКО-ЕЛЕКТРОННИМИ СИСТЕМАМИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ ЗНИЖЕННЯ ТЕМПЕРАТУРНОГО КОНТРАСТУ ОБ’ЄКТІВ ТА ВПЛИВУ АТМОСФЕРНИХ ЯВИЩ

Виходячи з аналізу проведення збройних конфліктів, ефективність застосування безпілотних літальних апаратів (БпЛА) в інтересах ведення повітряної розвідки (спостереження) і вогневого ураження суттєво залежить від можливостей бортових оптико-електронних систем (ОЕС). При цьому, значний влив на можливості ОЕС БпЛА створюють атмосферні явища (туман, задимлення, опади) та зниження температурного контрасту об’єктів спостереження і зовнішнього фону в ході ведення повітряної розвідки, особливо вночі.

Сучасні тенденції розвитку ОЕС БпЛА спрямовані на комплексування інформаційних каналів, зокрема використання інфрачервоних сенсорів, які фіксують обстановку у довгохвильовому інфрачервоному (ІЧ) діапазоні в поєднанні з оптичними сенсорами видимого спектру. Наприклад, зазначений підхід реалізований у мультиспектральній ОЕС RB-220 виробництва компанії M-FLY (Україна), масогабаритні характеристики (вага до 6 кг) якої дозволяють встановлювати зазначену ОЕС на тактичні БпЛА. За деякими характеристиками, використання ОЕС в довгохвильовому ІЧ діапазоні буде мати ряд переваг в порівнянні з ОЕС, які працюють у середньохвильовому ІЧ діапазоні, що пов’язано з принципом фіксації сигналів – у пасивному режимі і дозволяє виявляти об’єкти в умовах задимлення місцевості і густого туману.

Іншим шляхом підвищення ефективності виявлення об’єктів інтересу під час повітряного спостереження є використання алгоримів штучних нейронних мереж безпосередньо на борту літальних апаратів, в тому числі і на БпЛА. Сучасні нейромережові архітектури, наприклад, Unified Fusion, Deblurring and Detection на базі семейства YOLO (UFDT-YOLO) дозволяє здійснювати

детекцію і корекцію (покращення) зображень об’єктів інтересу, в тому числі розпізнавання малорозмірних цілей в умовах низького температурного контрасту. При цьому, використання технологій комп’ютерного зору, які функціонуватимуть на енергоефективних обчислювальних засобах для периферійних обчислень, наприклад, одноплатової електронної обчислюваної машини компанії NVIDIA (мінімальне споживання електроенергії знаходиться на рівні 7-15 Вт), забезпечить виконання завдань повітряної розвідки і вогневого ураження з БпЛА в режимі реального масштабу часу. Слід зазначити, що розрахункова пропускна здатність ідентифікації об’єктів знаходиться на рівні 19 кадрів за секунду, що відповідає сучасним версіям YOLOv11m, які працюють на стаціонарних обчислювальних засобах.

Таким чином, слід зазначити, що ефективність ОЕС БпЛА доцільно підвищувати комплексно, не лише за рахунок поєднання декількох інформаційних каналів, які працюють в різних діапазонах, але і за рахунок впровадження алгоритмів штучних нейронних мереж безпосередньо на борту літальних апаратів, які будуть стійкими для виявлення нечітких зображень в залежності від поточних метеорологічних умов та зниження температурного контрасту.

Чоларія Р. Г.
Стус А. В.
Слюсарєв М. Ф.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ВИКОРИСТАННЯ МОДЕЛЕЙ YOLO ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ОБ’ЄКТІВ ІНТЕРЕСУ У ВІДЕОПОТОЦІ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ

Сучасний розвиток безпілотних систем супроводжується розширенням їх функціональних можливостей та підвищенням рівня автономності під час виконання завдань розвідки та моніторингу. Великий обсяг інформації, який отримується оптико-електронними засобами БпАС (безпілотних авіаційних систем), потребує оперативної обробки та аналізу, що створює додаткове навантаження на оператора. У зв’язку з цим актуальним є застосування

технологій комп’ютерного зору та штучного інтелекту для автоматизованого виявлення і класифікації об’єктів безпосередньо під час виконання польотного завдання. Одним із перспективних підходів є використання моделей сімейства YOLO, які надають змогу здійснювати виявлення об’єктів у відеопотоці з високою швидкістю та забезпечувати отримання результатів у режимі реального часу.

Застосування YOLO на бортових системах БпЛА (безпілотний літальний апарат) дає можливість перенести частину функцій аналізу відеоінформації з оператора на обчислювальну систему безпілотного апарата. Це дає змогу автоматично визначати наявність об’єктів інтересу у полі зору камери, визначати їх положення в кадрі та формувати відповідну інформацію для використання іншими системами. Особливого значення набуває виконання первинної обробки даних безпосередньо на борту, оскільки це зменшує необхідність передавання повного відеопотоку на наземний пункт управління. Такий підхід має знизити навантаження на канал зв’язку та забезпечити збереження основної функціональності системи за умов нестабільного або обмеженого каналу передачі даних.

Пропонується дослідити можливості застосування моделей сімейства YOLO для підвищення автономності БпАС під час автоматизованого аналізу відеоінформації. Для цього потрібно сформувати навчальний набір даних, що містить зображення об’єктів за різних умов спостереження, та здійснити навчання і тестування моделі з подальшим її розгортанням на бортовій обчислювальній платформі. Оцінювання ефективності системи передбачається здійснювати за показниками точності виявлення, швидкості обробки кадрів, обчислювального навантаження та енергоспоживання.

Використання моделей сімейства YOLO на борту БпЛА забезпечують передумови для підвищення рівня автономності безпілотної авіаційної системи, оскільки результати аналізу можуть формуватися без постійної участі оператора. Але автономність не визначається виключно можливостями алгоритму виявлення об’єктів і залежить від продуктивності бортового обчислювального обладнання, доступної пам’яті, енергоспоживання та можливостей оптико-електронної системи. Застосування компактних та оптимізованих моделей має змогу зменшити обчислювальні витрати, однак надмірне спрощення моделі може призводити до зниження точності виявлення. Таким чином необхідно забезпечити баланс між точністю, швидкодією та енергоефективністю.

Основними обмеженнями використання моделей сімейства YOLO у БпАС є обмежені обчислювальні та енергетичні ресурси бортової платформи, залежність результатів виявлення від якості навчального набору даних та складність розпізнавання малорозмірних об’єктів. Додаткові труднощі виникають за час роботи в умовах недостатньої освітленості, туману, опадів складного фону або значної зміни масштабу об’єктів. Підвищення роздільної здатності відеопотоку сприяє виявленню малих об’єктів, однак одночасно збільшує обсяг оброблюваної інформації та навантаження на бортовий процесор. Тому ефективність використання моделей сімейства YOLO повинна оцінюватися не лише за точністю детектування, а й за комплексом технічних характеристик системи.

Майбутні дослідження треба зосередити на оптимізації моделей сімейства YOLO для роботи на бортових обчислювальних платформах, зменшенні їх обчислювальної складності та підвищенні енергоефективності. Головним напрямом є поєднання автоматизованого виявлення об’єктів із системами їх супроводження, навігації та іншими алгоритмами комп’ютерного зору. Увагу необхідно приділити підвищенню стабільності роботи моделей під час зміни умов спостереження та забезпеченню можливості функціонування системи за обмеженого каналу зв’язку.

Сотніков О. М., д-р техн. наук, проф.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба
Тюріна В. Ю., Ph. D.
Національний університет оборони України

МЕТОД СЕГМЕНТАЦІЇ ЗОБРАЖЕНЬ ДЛЯ СИСТЕМ НАВІГАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ ДЕФІЦИТУ ІНФОРМАТИВНИХ ОЗНАК

Сучасні системи технічного зору безпілотних літальних апаратів (БПЛА) зазнають дестабілізуючого впливу геометричних та атмосферних завад (туман, засніженість, низький контраст), що призводить до дефіциту локальних інформативних ознак об’єктів візування. Класичні кореляційні та нейромережеві алгоритми в таких умовах втрачають стійкість або вимагають

значних обчислювальних ресурсів бортового комп’ютера. Постає задача розробки завадостійкого аналітичного методу сегментації еталонних зображень, адаптованого до умов апріорної невизначеності.

Вперше розроблено метод аналітичного синтезу інваріантних еталонних зображень, який базується на пошуку оптимального просторово-частотного представлення вхідного кадру в базисі дробового перетворення Фур'є. На відміну від традиційного контурного чи текстурного аналізу, метод дозволяє виділити інтегральну фазову структуру об’єкта, яка зберігає високу інформаційну інваріантність навіть за критичного рівня шуму та часткового знищення локальних геометричних елементів ландшафту.

Синтез оптимального еталона зведено до двоетапної процедури оптимізації:

Перший етап: ітераційний пошук оптимального порядку дробового перетворення Фур'є за критерієм мінімізації структурної ентропії, що забезпечує максимальне геометричне фокусування енергії об’єкта.

Другий етап: застосування методу регуляризації Тихонова у спектральній області дробового перетворення Фур'є. Це дозволяє придушити стохастичні завади шляхом накладання стабілізуючих обмежень на гладкість еталона (норму похідних). Параметр регуляризації адаптивно налаштовується в реальному часі на основі робастної оцінки дисперсії шуму за методом Донохо-Джонстоуна.

Для верифікації методу введено критерій завадостійкості вимірювального контуру (максимізація відношення сигнал/шум відгуку з урахуванням крутизни піка) та регуляризований структурний критерій якості. Численне моделювання реальних сцен у середовищі Python (з використанням знімків із БПЛА DJI Mavic Pro з висот 50–200 м) довело, що за низьких значень відношення сигнал/шум метод синтезує чітку вирішальну функцію з вираженим центральним піком, забезпечуючи середньоквадратичне відхилення локалізації БПЛА на місцевості в межах 2–4 метрів. В аналогічних умовах класичні кореляційні алгоритми повністю втрачають працездатність.

Перехід від обробки зображень у координатному просторі до фазового простору дробового перетворення Фур'є дозволяє знизити навантаження на бортовий обчислювач. Для кадру розміром 128x128 пікселів кількість операцій зменшується з 268 мільйонів (у класичному просторовому підході) до 590 тисяч, що дає прискорення обчислень у 455 разів. Час обробки кадру не перевищує 25 мс, що гарантує роботу навігаційної системи БПЛА в реальному масштабі часу із частотою 30–40 кадрів за секунду.

Перегуда О. М., канд. техн. наук, ст. наук. співроб.
Ушаков С. І., канд. техн. наук
Житомирський військовий інститут імені С. П. Корольова

ІНТЕГРАЦІЯ БЕЗПІЛОТНИХ СИСТЕМ ТА ТРАДИЦІЙНИХ ЗРАЗКІВ ОЗБРОЄННЯ В ЄДИНІ ІННОВАЦІЙНІ РОЗВІДУВАЛЬНО-УДАРНІ КОНТУРИ СИЛ ОБОРОНИ УКРАЇНИ

Для сучасної збройної боротьби характерні стрімкий розвиток високотехнологічних засобів ураження, розвідки та управління, широке використання безпілотних систем і технологій штучного інтелекту. Досвід російсько-української війни засвідчує, що ефективність застосування озброєння та військової техніки (ОВТ) визначається не лише їхніми тактико-технічними характеристиками, а й здатністю підрозділів адаптувати форми й способи застосування до динамічних змін обстановки.

Одним із пріоритетних напрямів розвитку спроможностей Сил оборони України є перехід від платформоцентричного підходу до інтегрованого застосування взаємопов'язаних систем, тобто поєднання засобів розвідки, управління та ураження в єдиний розвідувально-ударний контур. Практичним прикладом є бойова система DELTA, яка забезпечує ситуаційну обізнаність і дає змогу за лічені хвилини координувати дії повітряних, наземних і морських безпілотних засобів, скорочуючи час між виявленням цілі та її ураженням.

Важливим напрямом інновацій є розвиток безпілотних авіаційних, наземних і морських систем, а також їх інтеграція з традиційними зразками ОВТ. Показовим є застосування Головним управлінням розвідки Міністерства оборони України морських дронів Magura-7, оснащених ракетами класу "повітря – повітря" AIM-9 Sidewinder: у травні 2025 р. ними над Чорним морем було збито два російські винищувачі Су-30. Ударні дрони стали одним з основних засобів вогневого ураження: як повідомив у квітні 2026 р. міністр оборони України, кожна четверта ціль на полі бою уражається підрозділами проєкту "Лінія дронів", що об'єднує понад 1000 екіпажів.

Особливого значення набуває впровадження мережецентричних принципів управління, за яких інформація про обстановку, отримана насамперед від безпілотних засобів розвідки, оперативно поширюється між взаємодіючими підрозділами. При цьому критично важливими залишаються

стійкість систем, зокрема каналів керування безпілотними засобами, до радіоелектронного впливу, кіберзагроз і втрати окремих елементів мережі.

У протиповітряній обороні дрони-перехоплювачі разом із мобільними вогневими групами, армійською авіацією та зенітними ракетними комплексами утворюють ешелоновану систему протидії ударним безпілотникам противника. У червні 2026 р. на перший ешелон перехоплення, представлений переважно дронами-перехоплювачами, припало 55% усіх знищених ударних безпілотників. Це дає змогу зберігати дефіцитні зенітні керовані ракети для ураження ракет противника.

Окремим чинником технологічної переваги є впровадження штучного інтелекту для оброблення розвідувальної інформації та автоматичного наведення безпілотних засобів на завершальній ділянці траєкторії. Зокрема, платформа Avengers, інтегрована в бойову систему DELTA, за даними Міністерства оборони України (вересень 2024 р.), щотижня автоматично виявляла на відео з дронів і стаціонарних камер близько 12 тис. одиниць техніки противника. Водночас рішення щодо застосування сили мають передбачати належний людський контроль і дотримання норм міжнародного гуманітарного права.

Реалізація зазначених підходів потребує вдосконалення не лише технічної складової, а й організаційних форм застосування ОВТ: адаптації доктринальних документів, розвитку міжвидової взаємодії, підготовки особового складу та швидкого узагальнення бойового досвіду. Прикладом організаційної інновації є створення Сил безпілотних систем, які в 2024 р. законодавчо визначено окремим родом сил Збройних Сил України.

Отже, перспективи підвищення ефективності застосування високотехнологічних зразків ОВТ Силами оборони України пов’язані насамперед з інтеграцією безпілотних систем і традиційних зразків озброєння в єдиний розвідувально-ударний контур, цифровізацією управління та адаптивними організаційними рішеннями. Визначальним чинником є не саме володіння сучасними технологіями, а здатність перетворювати їх на узгоджені оперативні спроможності.

Ушаков С. І., канд. техн. наук
Гаврилюк О. С.
Житомирський військовий інститут імені С. П. Корольова

РОЗВИТОК ТЕНДЕНЦІЙ МАСОВАНОГО ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ У ХОДІ СУЧАСНОЇ ЗБРОЙНОЇ БОРОТЬБИ

Наземні роботизовані комплекси (НРК) з початку відбиття широкомасштабної агресії рф проти України до теперішнього часу набули значний досвід від поодиноких експериментальних випадків до масованого застосування в якості новітніх високотехнологічних засобів ведення збройної боротьби.

Якщо у 2022 – 2023 роках їх застосування на фронті мало здебільшого епізодичний характер, то протягом 2026 року, за оцінками представників апарату Головнокомандувача ЗС України, підрозділи, оснащені зразками НРК, мали практично всі бойові бригади, а до експлуатації у Силах оборони України було допущено вже понад 200 моделей наземних роботизованих комплексів.

На 2026 рік було законтрактовано українськими бойовими підрозділами близько 25 тисяч серійних зразків НРК, що вдвічі більше ніж торік, при цьому лише в червні поточного року вони виконали більше 16,7 тисяч різноманітних бойових завдань.

Слід зазначити, що одночасно схожі за призначенням наземні роботизовані платформи на полі бою застосовує і противник. На початок травня 2026 року, за обліковими даними Генерального штабу ЗС України, налічувалось близько 1306 одиниць НРК противника різних класів, знищених Силами оборони України, чим підтверджується тенденція того, що наземні роботизовані комплекси перестають бути тільки допоміжною технікою та починають суттєво впливати на способи ведення бою та операцій.

Метою доповіді є визначення тенденцій і змін у тактиці та елементах оперативного мистецтва, зумовлених масованим застосуванням НРК.

Найпомітніші зміни проявлялись під час проведення наступальних дій підрозділів Сил оборони України.

Наприкінці 2024 року бригада Національної гвардії України “Хартія” знищила укріплення противника за допомогою декількох десятків наземних і

повітряних безпілотних засобів, не втративши через спротив противника жодної одиниці безпілотних комплексів.

У липні 2025 року 3-тя окрема штурмова бригада (3 ошбр) повідомила про перший підтверджений штурм позицій противника при застосуванні виключно безпілотних роботизованих платформ: укріплення ворога вражали НРК-камікадзе з протитанковими мінами та FPV-дрони зі спецзарядами, а двох військовослужбовців противника, які здалися в полон, було виведено до розташування позицій української бригади за допомогою ескортування полонених виключно безпілотними літальними апаратами (БпЛА).

У липні 2026 року 33-й окремий штурмовий полк знищив противника в будівлях населеного пункту силами двох НРК із великокаліберними кулеметами та важкого БпЛА з потужними підривними зарядами після того, як розвідувальні українські квадрокоптери перевірили маршрут висування наземної техніки на наявність засідок від FPV-дронів противника (так званих “ждунів”). Отже, таким чином формується ”новий” порядок штурму: розвідка маршруту повітряними засобами, ураження й прорив ліній оборони першим безпілотним ешелоном, закріплення захоплених позицій піхотою.

За рішенням командира 3-го армійського корпусу, під час подальших штурмів позицій противника, попереду української піхоти тепер завжди висуваються БпЛА і НРК.

В обороні зразки НРК дедалі частіше заміщують особовий склад піхотних підрозділів на окремих передових позиціях. Ударний НРК 3 ор із кулеметним модулем півтора місяця чергував на позиції замість піхоти, противнику так і не вдалося прорвати цю ділянку. Наземні платформи застосовують також для дистанційного мінування маршрутів противника: один розрахунок, за даними 3-го армійського корпусу, може замінувати до 200 м території на добу. Це дає змогу розріджувати бойові порядки, зменшувати кількість людей у “кіл-зоні”, глибина якої сягає від 15 до 30 км, і вивільняти піхоту для резервів, хоча утримання позиції виключно самими роботами поки є винятком.

Змінюється й забезпечення бою. Під час наступальної операції “Вівальді” НРК 3-го армійського корпусу за дві ночі розмінували маршрути висування протяжністю близько 30 км, на що, за оцінкою представників корпусу, двом ротам саперів знадобиться тиждень, а загалом роботизовані комплекси знімають близько 60% протипіхотних мін у смузі відповідальності корпусу.

У логістиці НРК перебрали на себе основне підвезення на “останній милі”: у 28-й окремій механізованій бригаді на них припадає близько 70% логістичного забезпечення. Узагальнені зміни способів дій наведено в табл. 1.

Таблиця 1

Зміни способів дій підрозділів, зумовлені застосуванням НРК

Вид дій	**Зміна способу дій**	**Вплив на бойовий порядок**
Наступ	безпілотний перший ешелон (розвідка БпЛА, ураження й прорив НРК)	піхота діє в другому ешелоні й закріплює захоплене
Оборона	вогневі НРК на окремих позиціях; дистанційне мінування	розрідження бойових порядків, менше людей на позиціях
Інженерне забезпечення	розмінування маршрутів без участі саперів	скорочення часу підготовки маршрутів
Логістика й евакуація	підвезення й евакуація без руху людей у “кіл-зоні”	менші втрати під час підвезення та ротацій

Масоване застосування НРК породило й зворотну тенденцію. Противник створив “дронові” підрозділи, що спеціалізуються на ураженні засобів логістики, зокрема НРК, і влаштовує засідки FPV-дронів на маршрутах, тому в окремих бригадах наземні роботизовані комплекси втрачаються майже щодня. У відповідь застосування НРК поєднують із попередньою повітряною розвідкою маршруту, рухом лише неспостережуваними маршрутами та маскуванням у тепловому діапазоні, а рота ударних НРК 3 ошбр застосовувала групи до п'яти комплексів різного призначення.

На оперативному рівні зміни відбуваються насамперед в організації проведення планування застосування НРК.

З 2025 року у складі бойових бригад Сил оборони України розгортаються окремі ”роботизовані” підрозділи, для яких розробляються доктринальні документи, штати, посади й система підготовки операторів.

НРК стали ресурсом, який потрібно планувати на рівні угруповань: окремі підрозділи потребують по 30–60 логістичних комплексів, цикл постачання зразків НРК від виробника сягає іноді до півроку, а на одного навченого та спеціально підготовленого оператора припадає щонайменше близько десяти осіб забезпечення.

Новим у розподілі кількісних ресурсів НРК між підрозділами став “механізм” впровадження системи бонусних балів, які нараховують, зокрема, за виконання числа та складності місій НРК та в подальшому обмінюють на потрібну техніку через маркетплейс Brave1 Market, яким вже скористалися понад 400 підрозділів Сил оборони України.

Взяття у квітні 2026 року позиції противника виключно безпілотними платформами без участі піхоти свідчить про можливість переходу від окремої роботизованої підтримки до роботизованих тактичних дій.

Слід особливо відмітити досвід десантування потрібної кількості НРК в тилову зону оборонних порядків противника в ході першого та другого етапів проведення контрнаступальної операції 3-го армійського корпусу під кодовою назвою “Вівальді” у серпні-вересні 2026т року на Лиманському напрямку.

Вважаємо, що масове застосування НРК зумовлює три головні зміни в тактиці застосування військ: появу безпілотного першого ешелону в наступі, часткове заміщення особового складу на позиціях в обороні та перенесення найнебезпечніших завдань забезпечення (підвезення, евакуації, розмінування) на роботизовані засоби.

На оперативному рівні НРК перетворюються на плановий ресурс угруповання, що потребує формування штатних підрозділів, удосконалення системи підготовки, ремонту й постачання, а протидія застосуванню НРК противника – на самостійне завдання. Водночас утримання позицій і захоплення території лише роботизованими засобами є поки що поодинокими випадками, тому вирішальною залишається взаємодія НРК із піхотою та повітряними безпілотними засобами.

Перспективними напрямами подальших досліджень є обґрунтування раціонального складу й порядку застосування змішаних груп НРК і БпЛА в наступі та обороні, розроблення методики планування визначення потреби в чисельності зразків НРК для озброєння угруповання військ на напрямку з урахуванням втрат комплексів і їх ремонту, а також способів протидії роботизованим засобам противника.

Бондаренко А. Ю.
Національний університет оборони України

ПОБУДОВА ЦИКЛУ БОЙОВОГО ЗАСТОСУВАННЯ БРИГАДИ БЕЗПІЛОТНИХ СИСТЕМ В ОПЕРАЦІЯХ УГРУПОВАННЯ ВІЙСЬК

Масштабне впровадження безпілотних систем у діяльність військ суттєво змінює не лише набір засобів, що використовуються під час операції, а й саму логіку організації їх бойового застосування. За умов одночасного використання значної кількості різнотипних безпілотних платформ результат визначається не стільки характеристиками окремого засобу, скільки спроможністю поєднати отримання інформації, її оброблення, прийняття рішення, виконання завдання та оцінювання результату в єдиний функціональний процес.

Тому бригаду безпілотних систем доцільно розглядати як складну організаційно-функціональну систему, бойове застосування якої реалізується через послідовний цикл взаємопов’язаних дій.

Необхідність виокремлення такого циклу обумовлюється специфікою застосування безпілотних систем. На відміну від використання окремого технічного засобу, діяльність бригади БПС охоплює одночасне виконання різних за змістом завдань, накопичення значних обсягів інформації, їх узгодження із завданнями угруповання військ, визначення пріоритетності об’єктів та подальше використання результатів попередніх дій. Відповідно, ефективність визначається не лише кінцевим результатом окремого застосування, а й безперервністю, узгодженістю та адаптивністю всього циклу.

Під циклом бойового застосування бригади БПС пропонується розуміти сукупність взаємопов’язаних процесів від отримання завдання та визначення необхідного результату до оцінювання його досягнення і формування рішення щодо подальшого застосування сил і засобів. Такий підхід дозволяє поєднати управлінську, інформаційну та виконавчу складові в межах єдиної логічної моделі.

Початковим елементом циклу є отримання та уточнення завдання. На цьому етапі визначається, який результат має бути забезпечений застосуванням бригади БПС в інтересах операції. Важливо, щоб постановка завдання не обмежувалася визначенням окремого технічного засобу чи способу його використання. Вихідним має бути саме необхідний результат - отримання

інформації, забезпечення спостереження, створення умов для впливу, підтримка дій інших складових угруповання або інший визначений ефект від застосування.

Наступним елементом є формування потреби в інформації. Для виконання завдання необхідно встановити, яких даних не вистачає для прийняття рішення, які об’єкти або райони потребують спостереження, які характеристики обстановки потрібно додатково уточнити. На цьому етапі відбувається формування зв’язку між завданням операції та конкретними інформаційними потребами бригади БПС.

Подальший етап охоплює пошук, виявлення та первинне оцінювання об’єктів. Його зміст полягає у використанні доступних засобів для отримання необхідної інформації, її перевірки та уточнення. Результативність цього етапу значною мірою визначає якість подальших рішень, оскільки помилки або затримка в отриманні інформації можуть знижувати доцільність подальших дій.

Після накопичення необхідних даних здійснюється оцінювання та пріоритезація отриманої інформації. На цьому етапі важливо співвідносити виявлені об’єкти, зміни обстановки та наявні можливості бригади з потребами операції.

Подальшим елементом циклу є вибір варіанта застосування сил і засобів, який має проводитись з урахуванням характеру поставленого завдання, доступних ресурсів, технічної готовності, часу, умов обстановки та очікуваного результату. При цьому вибір конкретної платформи або групи засобів є похідним від завдання, а не навпаки.

На етапі безпосереднього виконання завдання реалізується обраний варіант застосування, забезпечується управління діями залучених сил і засобів, здійснюється взаємодія з іншими елементами угруповання військ.

Завершальним, але не кінцевим за змістом елементом є оцінювання отриманого результату. Його значення полягає не лише у встановленні факту виконання або невиконання завдання, а й у визначенні причин отриманого результату, уточненні стану об’єкта впливу, оцінюванні доцільності повторного застосування та коригуванні подальших дій.

Варіант загальної структури циклу представлено на рис.1.

Принциповою особливістю запропонованої структури є те, що цикл не завершується після виконання окремого завдання. Результати одного етапу формують вихідні дані для наступного, а оцінювання отриманого ефекту одночасно створює інформаційну основу для нового циклу. Саме тому бойове

застосування бригади БПС доцільно розглядати як безперервний адаптивний проце**с**, а не як сукупність окремих епізодів застосування безпілотних систем.

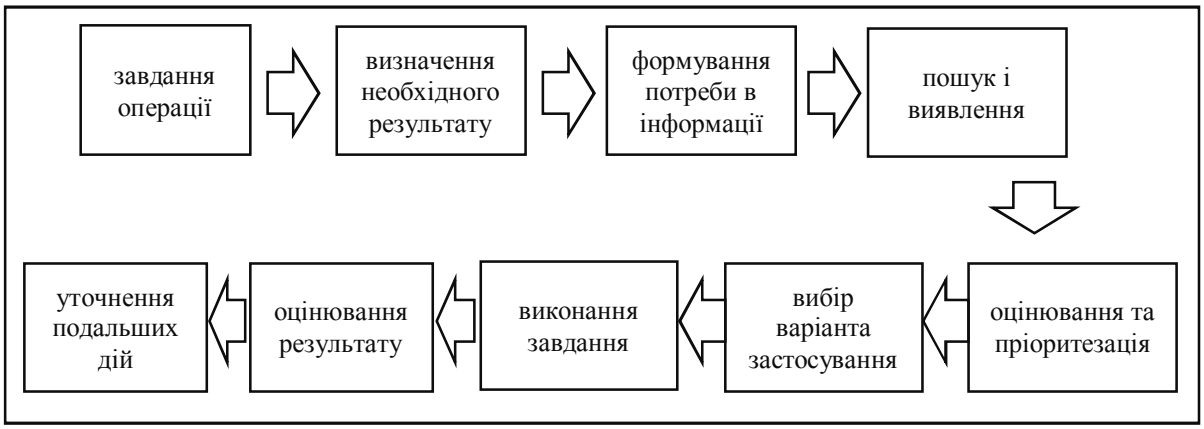


Рис. 1. Узагальнена структура циклу бойового застосування БрБПС

Для характеристики циклу важливим є також часовий параметр, його тривалість у спрощеному вигляді може бути представлена:

$$T_{\text{ц}} = T_{\text{з}} + T_i + T_B + T_p + T_{\text{заст}} + T_{\text{оц}} \ , \qquad (1)$$

Де:

$T_{\text{ц}}$ — загальна тривалість циклу бойового застосування;

$T_{\text{з}}$ — час на уточнення завдання;

T_i — час на отримання та оброблення інформації;

T_B — час на виявлення й оцінювання об’єкта;

T_p — час на прийняття рішення;

$T_{\text{заст}}$ — час безпосереднього виконання завдання;

$T_{\text{оц}}$ — час на оцінювання отриманого результату.

Наведена залежність не є завершеною математичною моделлю, а відображає вплив тривалості окремих етапів циклу на загальну результативність бойового застосування. Затримки під час отримання й оброблення інформації, визначення пріоритетності або прийняття рішення можуть знижувати ефективність навіть за високих технічних характеристик безпілотних систем.

Тому доцільно оцінювати не лише тривалість окремих етапів, а й їх узгодженість та функціональний взаємозв’язок, за якого результат кожного етапу є вихідними даними для наступного процесу. Функціональний зміст такого взаємозв’язку наведено в табл. 1.

Таблиця 1. Функціональний зміст етапів циклу застосування Бр БПС

Етап циклу	Основний зміст	Результат етапу
Уточнення завдання	Визначення необхідного результату	Сформульована потреба застосування
Формування інформаційної потреби	Визначення необхідних даних	Перелік інформаційних завдань
Пошук і виявлення	Отримання інформації про обстановку	Виявлені та уточнені об’єкти
Оцінювання і пріоритезація	Визначення значущості отриманої інформації	Пріоритетність подальших дій
Вибір варіанта застосування	Співвіднесення завдання з наявними можливостями	Обґрунтований варіант дій
Виконання завдання	Реалізація визначеного варіанта	Отриманий результат
Оцінювання результату	Визначення ступеня досягнення мети	Підстава для повторного циклу

Наведена структура показує, що функціонування бригади БПС не може зводитися лише до процесу виявлення – застосування. Між цими елементами знаходяться етапи оцінювання, пріоритезації та вибору варіанта дій, які значною мірою визначають раціональність використання наявного ресурсу в ході виконання завдання.

Характер бойових дій, технологічна протидія, зміна доступних каналів управління, погодні умови, технічний стан платформ та інші чинники можуть швидко змінювати початкові умови. Тому цикл має передбачати можливість повернення до попередніх етапів, уточнення завдання або зміни варіанта дій без завершення всієї послідовності.

Наприклад, якщо на етапі виконання завдання виявлено зміну умов, що суттєво впливає на можливість досягнення необхідного результату, доцільним є не механічне продовження попередньо визначеного варіанта, а повернення до оцінювання ситуації та формування нового рішення. Таким чином, запропонований цикл має бути не лінійним, а замкненим і коригованим за результатами постійного зворотного зв’язку.

Ще однією важливою характеристикою є інформаційна безперервність. Результати розвідки, виконання завдань та оцінювання ефекту повинні накопичуватися і використовуватися під час планування наступних дій. Відсутність такого зв’язку призводить до повторення однакових дій без урахування їх попередньої результативності.

Побудова циклу створює передумови для подальшого оцінювання ефективності застосування бригади БПС, де об’єктом оцінювання може бути не лише кінцевий результат, а й функціонування окремих етапів. Це дозволяє визначати, де саме виникають затримки, втрати інформації, нераціональне використання ресурсу або зниження результативності.

Таким чином, цикл бойового застосування бригади безпілотних систем доцільно розглядати як послідовність взаємопов’язаних процесів. Його принциповими характеристиками є безперервність, адаптивність, функціональний взаємозв’язок етапів та наявність зворотного зв’язку.

Практичне значення запропонованого підходу полягає в переході від розгляду окремих фактів застосування безпілотних систем до аналізу функціонування бригади БПС як цілісної системи. Побудова такого циклу створює основу для подальшого визначення показників його результативності, виявлення найбільш критичних етапів та обґрунтування рекомендацій щодо підвищення ефективності застосування бригади безпілотних систем в операціях угруповання військ.

Круковський І. А., канд. техн. наук, Ph. D., ст. наук. співроб.
Александров А. К.
Сімаков В. Л.
Громадська організація
«Міжнародний науково-дослідний центр «Синергія»»

ПРО ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ КОНСАЛТИНГОВИХ МАТЕРІАЛІВ КОМПАНІЙ IDC, GARTNER, FORRESTER RESEARCH ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМ ПІДТРИМКИ РІШЕНЬ НА ОСНОВІ BUSINESS INTELLIGENCE В СИЛАХ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

В умовах ведення сучасних мережецентричних дій та інтенсивного впровадження інформаційних технологій у сферу безпеки і оборони України, якість та швидкість прийняття рішень на основі аналізу оборонної і безпекової інформації стають критичними чинниками ефективної діяльності. Активно реалізуються заходи цифрової трансформації, зокрема впроваджують автоматизовані системи управління військами на основі С2 (C4ISR, C5ISR) та

системи підтримки прийняття рішень (Decision Support System, DSS) на розширеній основі Business Intelligence (Data Warehouse, OLAP, Data Mining, Text Mining (Sentiment Analysis, Opinion Mining, ets), Dashboards, Image Mining, Video Mining, генеративний штучний інтелект, ін).

Проте розробка таких комплексних систем на основі «самописних» програм в умовах обмеженості часу, ресурсів та специфіки воєнного стану супроводжується значними ризиками (технологічним старінням, помилками архітектури, хибним визначенням пріоритетів). Тому є актуальним вірне вирішення проблемних питань використання готової експертизи, методологій та аналітичних матеріалів світових лідерів у сфері консалтингу інформаційно-аналітичних систем — від компаній Gartner, IDC та Forrester Research, Panorama Software, etc.

1. Потенціал та специфіка застосування матеріалів провідних консалтингових компаній у сфері Business Intelligence.

Кожна з названих глобальних консалтингових аналітичних компаній володіє унікальною методологічною базою, яка може бути адаптована під потреби сектору безпеки і оборони.

- **Компанія Gartner (методології Magic Quadrant, Hype Cycle, ITScore).** Дозволяє здійснювати обґрунтований вибір технологічних платформ, програмного забезпечення та вендорів для побудови архітектури СППР. Аналіз кривих ажіотажу (Hype Cycle) допомагає уникнути інвестицій у переоцінені технології або вчасно інтегрувати перспективні рішення (штучний інтелект, предиктивна аналітика, хмарні обчислення, Big Data). У сфері Analytics and Business Intelligence черговий опублікований звіт - це «2026 Gartner® Magic Quadrant™ for Analytics and Business Intelligence Platforms». Необхідно враховувати, що назви консалтингових документів дискретно-безперервно змінюються, для прикладу звіти компанії Gartner: 2006–2012: «Magic Quadrant for Business Intelligence Platforms»; 2013–2017: «Magic Quadrant for Business Intelligence and Analytics Platforms»; з 2018 і до сьогодні: «Magic Quadrant for Analytics and Business Intelligence Platforms».
- **Компанія IDC (міжнародна ринкова аналітика, прогнози ІСТ).** Надає глибоку статистичну базу щодо розвитку ринку корпоративного софту, кібербезпеки та інфраструктурних рішень. Для сил оборони і безпеки ця

інформація корисна для розробки архітектури системи, її функцій, плануванні життєвого циклу, оцінці масштабованості рішень та забезпеченні їх сумісності зі стандартами НАТО (STANAG). У сфері Analytics and Business Intelligence черговий опублікований звіт - це «2025 IDC MarketScape for Business Intelligence and Analytics Platform»

- **Компанія Forrester Research (дослідження UX, Wave, Zero Trust).** Фокусується на методологіях оцінки ефективності взаємодії користувача з системою (UX), що є критично важливим для DSS у екстремальних умовах. Крім того, напрацювання Forrester Research у сфері концепції Zero Trust (Нульової довіри) є фундаментальними для забезпечення кібербезпеки військових інформаційних систем. У сфері Analytics and Business Intelligence черговий опублікований звіт - це «The Forrester Research Wave™: Business Intelligence Platforms, Q2 2025».

2. Ефект синергії від інтеграції консалтингових даних у процес створення DSS BI

Використання матеріалів IDC, Gartner та Forrester Research у діяльності органів безпеки і оборони та у науково-дослідних установах забезпечує такі переваги:

1. Мінімізація ризиків та економія ресурсів. Завдяки використанню кращих практик (Best Practices) усувається дублювання розробок і значно знижується ймовірність закупівлі неефективних технологій. Так, пропозиції ГО МНДЦ «Синергія» у 2011 році залишаються вірними і у 2026 році, з урахуванням їх оновлення і доповнення генеративним штучним інтелектом (ШІ), та іншими технологіями, які активно увійшли в практику за останні роки.
2. Застосування еталонних архітектурних підходів. Моделі Enterprise Architecture (наприклад, TOGAF) дозволяють забезпечити інтероперабельність створюваних DSS BI між військовими підсистемами та структурами країн НАТО.
3. Прискорення циклу OODA. Оптимізуються потоки інформації в штабах, перетворюючи первинні дані моніторингу та логістики на якісні рекомендації для керівництва.
4. Інтеграція передових трендів. Вчасно інтегруються алгоритми машинного навчання (ML), генеративний ШІ та цифрові двійники (Digital Twins).
5. Удосконалення таксономій, концепцій, технологій, програмних засобів і методик їх оцінки, розробки й удосконалення разом з

удосконаленнями, які щороку чи раз на два роки публікують компанії Gartner, IDC та Forrester Research для мільйонів користувачів у всьому світі.

6. Полегшення перевірки достовірності й удосконалення базових пропозицій Gartner, IDC та Forrester Research - за допомогою підготовлених корпоративних вчених та IT-працівників. Власні корпоративні вчені потрібні у тому числі щоб розібратися зі складними інформаційно-аналітичними технологіями з елементами управління кінетичними системами, щоб організувати їх вибір, підтримку, впровадження, використання, удосконалення і заміну протягом усього життєвого циклу.

3. Виклики та обмеження

Під час використання аналітики IDC, Gartner та Forrester Research та інших у сфері оборони слід враховувати:

- **Комерційну спрямованість.** Звіти орієнтовані на цивільний сектор і вимагають глибокої адаптації під специфіку управління у силах оборони і безпеки та вимоги охорони державної таємниці.
- **Обмеженість доступу.** Доступ до преміум-аналітики вимагає значних ресурсів, що може вирішуватися через механізми міжнародної технічної допомоги та партнерства.
- **Іноземний вплив на сферу Analytics & Business Intelligence.** 1. У РФ є суттєві напрацювання і консалтингові ресурси у сфері Business Intelligence та дезінформуючий вплив на конкурентів - за рахунок тривалої співпраці із західними компаніями на рівнях держави, окремих компаній і фахівців, порушення правил безпеки інформації користувачів і постачальників програмного забезпечення і консалтингових послуг. Для прикладу, у Москві раніше проходили консалтингові заходи компаній IDC, розміщувався головний офіс ТОП-компанії у сфері Analytics and Business Intelligence SAP у країнах СНД. У 2022 році у зв`язку з війною РФ проти України компанії IDC, Gartner, Forrester Research - згорнули свою діяльність у РФ. 2. У США діють суворі обмеження на збір та аналіз атрибутів інформації про людей, але тільки для громадян США.

Висновки

Використання аналітичних матеріалів і методологій компаній IDC, Gartner та Forrester Research та інших (виходять за межі цієї публікації) при

реалізації DSS BI у силах оборони і безпеки України є високодоцільним. Це дозволяє скоротити час на проектування складних ІТ-систем, зменшити технологічні помилки, підвищити рівень кібербезпеки та забезпечити сумісність вітчизняних оборонних рішень зі стандартами армій країн НАТО.

Перспективою подальших досліджень є розробка методики адаптації стандартів IDC, Gartner, Forrester Research та інших під специфіку управління силами безпеки і оборони. Більш широко тематика досліджень розкрита у публікаціях мультисайтів ГО МНДЦ «Синергія» (rdc-synergy.org) та DOBRUDJA.eu з 2011 року по 20226 рік. Запрошуємо до співпраці.

СЕКЦІЯ 2
Протидія безпілотним авіаційним системам противника

Джемула О. М.
Черниш О. В.
Удовицький В. В.
Предчук В. А.
Житомирський військовий інститут імені С. П. Корольова

ДОСВІД ПІДГОТОВКИ ФАХІВЦІВ ІЗ ПРОТИДІЇ БЕЗПІЛОТНИМ АВІАЦІЙНИМ КОМПЛЕКСАМ ПРОТИВНИКА

В сучасних умовах ведення бойових дій в російсько-українській війні ударні безпілотні авіаційні апарати противника різних типів (БпЛА зі скидами, дрони-камікадзе типу FPV) стали чи не найбільшим викликом і ризиком для життя і здоров’я особового складу, живучості зразків ОВСТ і, як результат, успішного виконання бойового завдання в цілому.

Переваги ударних БпЛА над іншими засобами вогневого ураження очевидні вони маневрені і швидкі (дозволяють уражати виявлену ціль із непередбачуваного напрямку із високою точністю), і, що найнебезпечніше, є непередбачуваними. Про це свідчить аналіз своїх втрат, який дозволяє стверджувати, що левова частка вогневого ураження припадає на ударні дрони, переважно БпЛА зі скидами та FPV-дрони.

Таким чином, виживання особового складу на полі бою залежить насамперед від рівня навченості, дисципліни і вміння правильно діяти в разі виявлення БпЛА противника. Так, у критичний момент ми діємо не на максимумі своїх розумових можливостей, а на автоматизмі (м’язовій пам’яті). Тобто наша реакція і правильність дій на БпЛА противника напряму залежить від рівня навченості й отриманого бойового досвіду.

Таким чином, протидія БпЛА противника реалізується шляхом виконання взаємопов’язаних і послідовних заходів, що організуються і виконуються як на рівні військової частини (підрозділу), так і окремими військовослужбовцями

і передбачають:

а) своєчасне виявлення БпЛА;

б) оповіщення про загрозу його застосування противником;

в) і безпосередню протидію.

Остання реалізується виконанням активних і пасивних заходів.

Способи виявлення і оповіщення про БпЛА противника

Першочергове значення має виявлення (організація виявлення) БпЛА противника військовослужбовцем (у військові частині, в підрозділі, бойовій групі). Це завдання зазвичай вирішується:

а) шляхом ведення постійного спостереження за повітрям призначеними спостерігачами;

б) використанням засобів електронної підтримки (т.зв. "аналізаторів спектру" і "детекторів дронів") (далі – засобів електронної підтримки);

в) використанням наявних засобів радіолокаційної та радіотехнічної розвідки (організується у військовій частині (підрозділі) старшими командирами (начальниками);

г) організацією взаємного оповіщення в підрозділі (бойовій групі, підгрупі).

Крім виявлення БпЛА противника за звуком або візуально – спостереженням, особовим складом бойових груп (підгруп) використовуються наявні в підрозділі засоби електронної підтримки (засоби перехоплення відео FPV-дронів (які виявляють і відображають відео).

Використання цих засобів дозволяє зірвати неочікуваний для особового складу удар противника із використанням ударних БпЛА різних типів. Разом з тим варто розуміти й те, що знання частот роботи БпЛА противника означає "бачити те, чого не видно"

Це дає можливість діяти на випередження.

Під час дій у складі малих груп піхоти (бойових підгруп) типова голосова команда оповіщення типу *"Повітря"* не забезпечує необхідної інформативності. Доцільніше використовувати короткі голосові команди (сигнали), які будуть одночасно зрозумілі всьому особовому складу і, в той же час, містити мінімально-необхідну інформацію про напрямок і висоту польоту БпЛА противника. Рекомендований формат віддачі команди повинен бути максимально стислий і спрямований на практичні дії, наприклад: ***"Увага! FPV на 12; висота 30; дальність 100"*** *або* ***"Увага! Дрон на 9; низько; дальність 50"****,* де:

"12" і "9" відповідно – це напрямок за годинниковою на безпілотний апарат противника відносно свого місцеположення або напрямку руху;

"30" – орієнтовна висота польоту БпЛА противника в метрах;

“100” і “50” відповідно – дальність до БпЛА противника в метрах відносно свого місцеположення.

Безпосередня протидія БпЛА противника ґрунтується на швидкості і узгодженості дій особового складу. Вона передбачає дотримання вимог тактичного маскування, застосування доступних засобів ураження а також підтримку дій засобами старшого командира (зі складу системи протидії БпЛА).

За умови дотримання нижче зазначених рекомендацій та усвідомлення того, що противник веде за вами постійне (цілодобове) спостереження з повітря – ви беззаперечно підвищите живучість особового складу.

Боротьба із БпЛА противника передбачає комплексний підхід, а виконання (дотримання) активних і пасивних заходів протидії їм мають бути реалізовані як на рівні військових частин (підрозділів), так і окремими військовослужбовцями малих груп піхоти.

Протидія БпЛА із використанням засобів РЕБ ближньої дії.

На тактичному рівні підсистема РЕБ з БпЛА противника з використанням засобів РЕБ ближньої дії є ешелонованою зонально-об’єктовою підсистемою в єдиній системі протидії БпЛА противника.

Технічну складову підсистеми РЕБ складають комплекси (системи, засоби) ЕП та радіоподавлення (далі – РП) БпЛА, що відрізняються за дальністю виявлення, радіоелектронного подавлення, мобільністю, в залежності від характеристик об’єктів і ділянки місцевості, що прикриваються.

Радіоподавлення каналів управління ударних БпЛА противника здійснюється після їх виявлення, перехоплення відеосигналу засобами ЕП та визначення напрямку його польоту.

Подавлення каналу управління БпЛА здійснюється послідовним випромінюванням радіоперешкод.

Для тимчасової зупинки польоту ударного БпЛА противника здійснюється радіоподавлення його каналу управління (каналу передавання даних), як правило, засобами РЕБ ближньої дії у відповідних частотних діапазонах. В результаті впливу засобами РЕБ ближньої дії на БпЛА противника мультироторного типу у нього активується протокол 1001-ї прошивки, під час якого дрон стрімко набирає висоту та за рахунок втрати візуального контролю процесу подавлення і поривів вітру виходить з-під дії засобів РЕБ ближньої дії. Це забезпечує відновлення зв’язку дрону з пультом керування, але зриває його

польотне завдання та створює можливість для його ураження стрілецькою зброєю (зокрема гладкоствольною рушницею).

Протидія БпЛА із використанням гладкоствольних рушниць і стрілецької зброї.

В сучасних умовах ведення бойових дій гладкоствольні рушниці 12-го калібру набувають дедалі більшого значення.

За умов активного застосування противником БпЛА різних типів, зокрема FPV-дронів і ударних БпЛА зі скидами (в т.ч. з використанням оптоволоконного каналу управління), гладкоствольні рушниці є ефективним засобом протидії їм.

Варто звернути увагу й на той факт, що постійне вдосконалення противником БпЛА, зміна частот управління ними значно ускладнює або робить неефективним використання засобів РЕБ ближньої дії нашими підрозділами.

Гладкоствольні помпові і напівавтоматичні рушниці є доступним та ефективним засобом боротьби із дронами на малих висотах і відстанях. Висока щільність і площа ураження досягається саме завдяки використанню шроту, який дозволяє знищувати дрон з одного або декількох пострілів, навіть за умови його польоту на великій швидкості.

В сучасних умовах ведення бойових дій і спірної ефективності засобів РЕБ ближньої дії, гладкоствольні рушниці стали ефективним рішенням для боротьби піхоти із БпЛА противника. Кожен військовослужбовець повинен бути готовим до швидкого реагування на появу дронів противника, мати необхідні навички стрільби по рухомим повітряним цілям і використовувати відповідні боєприпаси для досягнення максимального ефекту.

Для ефективної протидії ударним БпЛА противника (в т.ч. й на оптоволокні) в кожному відділенні (малій групі піхоти) доцільно призначати стрільця із гладкоствольною напівавтоматичною рушницею, який діє у взаємодії із спостерігачем і керується його командами. Спостерігач забезпечує своєчасне виявлення і оповіщення (попередження) про повітряну ціль, а стрілець займає позицію для контролю верхньої напівсфери та заздалегідь визначає найбільш ймовірні напрями підльоту й т. зв. “можливі вікна ураження” над траншеєю, підходами до бліндажу тощо.

Вогонь з рушниці відкривається переважно в момент зависання БпЛА або на випередження, уникаючи передчасного демаскування, після чого стрілець може змінювати своє місце (позицію для стрільби) з метою зниження ризику ураження.

Найкращий результат у протидії ударним БпЛА противника (FPV-дронам) забезпечує застосування гладкоствольної напівавтоматичної рушниці у

поєднанні із засобами РЕБ. Останні створюють умови для зриву наведення і примушують БпЛА знижуватися або втрачати стабілізацію, в той час як стрілець фізично знищує ціль з мінімальної відстані.

Крім того, ефективною є організація короткочасних вогневих засідок у місцях, де БпЛА складно маневрувати, а також у районах (на маршрутах прольоту), які противник регулярно обирає для ударів по важливим елементам оборони.

Таким чином, для ефективної протидії БпЛА противника із використанням гладкоствольних рушниць, кожен військовослужбовець повинен оволодіти основними базовими навичками:

швидкого приготування до стрільби і здійсненням прицільного пострілу;

бінокулярного прицілювання – прицілювання обома очима дозволяє краще оцінити висоту і швидкість цілі;

швидкого перезаряджання зброї;

виносу точки прицілювання;

перенесенням вогню між секторами спостереження і стрільби;

ведення стрільби по БпЛА, що заходять на ціль різними траєкторіями (під різними кутами по відношенню до стрільця).

Адаменко А. А., канд. техн. наук, ст. наук. співроб.
Порохончук О. М.
Григоренко Є. О.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ПІДСИСТЕМА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗАСТОСУВАННЯ ПІДРОЗДІЛІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

За роки протистояння російській агресії Збройні Сили (ЗС) України здобули значний досвід боротьби з безпілотними літальними апаратами (БпЛА) противника, зокрема, шляхом комплексного застосування підрозділів радіоелектронної боротьби (РЕБ) та протиповітряної оборони (ППО).

Їх ефективне комплексне застосування вимагає постійної обізнаності про повітряну обстановку та оперативної координації дій при протидії БпЛА противника у спільній зоні відповідальності. Це можливе, зокрема, за рахунок

автоматизації процесів оперативного збору, обробки та обміну розвідувальною інформацією про повітряного противника, а також обміну іншою інформацією, необхідною для якісного виконання бойового завдання.

В доповіді презентовано програмний модуль “АРМ-РЕБ” для створення закритої (без інформаційного обміну із іншими системами) або відкритої підсистеми інформаційного забезпечення бойового застосування підрозділів РЕБ, зокрема, у кооперації із підрозділами ППО, що використовують інформаційно-комунікаційну систему (ІКС) ситуаційної обізнаності про повітряну обстановку “Віраж-Планшет” (далі – ІКС “Віраж-Планшет”).

Основні завдання програмного модуля “АРМ-РЕБ”:

- нарощення загальної інформації про повітряну обстановку за рахунок автоматизованого збору, обробки та внесення інформації про застосування БпЛА, що отримана підрозділами РЕБ;

- автоматизація та інформаційне забезпечення завдань управління комплексним застосуванням засобів РЕБ по повітряним об’єктам противника підрозділом(ми) РЕБ;

- оперативне оповіщення підпорядкованих підрозділів (постів управління засобами) РЕБ про застосування противником БпЛА;

- обмін інформацією про повітряну обстановку з іншими ІКС ЗС України.

Модуль “АРМ-РЕБ” входить до складу програмного комплексу ІКС “Віраж-Планшет”, а його функціональні можливості щодо отримання, обробки, відображення, обміну та захисту інформації про повітряну обстановку, а також об’єктивного контролю та роботи з картографічним матеріалом відповідають загальним аналогічним можливостям цієї системи.

В залежності від призначення та функціональних режимів використання програмний модуль “АРМ-РЕБ” може бути використаний для організації автоматизованих робочих місць (АРМ) користувачів підрозділу РЕБ наступних типів:

- АРМ командира (оперативного чергового) підрозділу РЕБ;

- АРМ оператора ручного введення розвідувальної інформації від підпорядкованих постів РЕБ;

- АРМ оператора (бойової обслуги) посту РЕБ з автоматизованим або ручним введенням пеленгів на ціль;

- АРМ оповіщення абонентів (видачі повітряної обстановки на АРМ підрозділу, штатні АРМ систем та засобів РЕБ, АРМ зовнішніх інформаційних систем);

- АРМ абонента оповіщення.

Відповідно до цього функціонал програмного модуля “АРМ-РЕБ” надає змогу розгортання локальної мережі автоматизованих робочих місць органів військового управління РЕБ різного рівня, бойових розрахунків та постів РЕБ (із різнорідними засобами РЕБ), а також її інформаційного спряження з ІКС “Віраж-Планшет” та ІКС електронної підтримки з метою дозованого контрольованого оперативного обміну розвідувальною інформацією про повітряну обстановку та координації дій між підрозділами РЕБ та ППО при комплексній протидії БпЛА противника.

Програмний модуль “АРМ-РЕБ” самостійно та у складі ІКС “Віраж-Планшет” успішно пройшов відповідні експертизи та дослідну експлуатацію, а також випробування органами військового управління Повітряних Сил та підрозділами РЕБ ЗС України в реальних умовах експлуатації в бойовій обстановці.

Лаврик С. В.
Науково-дослідний центр ракетних військ і артилерії

ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ ВІД УРАЖЕННЯ УДАРНИМИ БЕЗПІЛОТНИМИ АВІАЦІЙНИМИ СИСТЕМАМИ

У сучасних умовах ведення бойових дій противник продовжує нарощувати кількість та щільність застосування ударних безпілотних авіаційних систем (далі – БпАС) у тактичній зоні наших військ. Їх застосування противником забезпечує ураження до 80% від усієї кількості ураженого озброєння і військової техніки (далі – ОВТ) артилерійських підрозділів на вогневих позиціях (далі – ВП), а також особового складу.

Показник результативних влучань у ціль вказаного засобу ураження складає до 40%, а їх кількість для гарантованого знищення артилерійського зразка ОВТ становить більше 3 одиниць. Разом з тим, досвід ведення бойових дій вказує на те, що після виявлення противником гармати та її обслуги на ВП для їх ураження застосовується 5-6 одиниць ударних БпАС.

З метою протидії зазначеним засобам ураження противника, збереження боєздатності артилерійських підрозділів шляхом підвищення живучості особового

складу, ОВТ, систем управління та забезпечення застосовується комплексна система захисту артилерійських підрозділів (далі – КСЗ АП).

КСЗ АП є інтегрованою системою здійснення ефективних пасивних та активних заходів захисту.

Основними вимогами до КСЗ АП є:

безперервність – цілодобовий моніторинг обстановки, а також цілодобове виявлення загроз та чергування груп безпеки;

проактивність – завчасне та своєчасне виявлення загроз;

багаторівневість – поєднання та одночасне застосування заходів захисту;

адаптивність та гнучкість – здатність своєчасно реагувати на зміну дій противника;

взаємодія – постійний обмін інформацією, підтримка та узгодження дій між частинами та підрозділами.

Планування та організація КСЗ АП регламентується бойовими наказами (розпорядженнями) командирів артилерійських частин та підрозділів.

З метою здійснення централізованого управління вказаною системою на командних пунктах артилерійських частин, а також тимчасово створених формувань артилерійських підрозділів розгортається та функціонує група (секція) безпеки застосування військ. До її складу входять два офіцери (начальник та офіцер групи), які ведуть цілодобове позмінне чергування безпосередньо в кімнаті бойового управління. Район відповідальності групи охоплює зону від лінії бойового зіткнення на глибину розташування ВП артилерійських підрозділів. Група здійснює планування, організацію, координацію та контроль комплексного застосування усіх існуючих пасивних та активних заходів захисту. Вказана група у взаємодії з іншими групами (секціями), зокрема радіоелектронної боротьби, протиповітряної оборони, цілодобового здійснює моніторинг обстановки у єдиному інформаційному контурі, акумулюючи дані, отримані від старшого начальника (засоби радіоелектронної розвідки (далі – РЕР) дальнього попередження до 200 км), сил та засобів РЕР артилерійських частин (середня дистанція виявлення до 50 км), а також засобів РЕР артилерійських підрозділів на ВП (безпосередня зона детекції до 5 км). Отримані дані передаються та відображаються у режимі реального часу у інформаційних системах “Skymap”, “Віраж”, “Графіт”, “Дамба” та “Неон”. ВП артилерійських підрозділів АГ та зони дії засобів РЕБ відображаються на електронних картах інформаційних систем “Ліра” та “Айсберг”.

Основними пасивними заходами КСЗ АП є вибір та інженерне обладнання ВП, їх розосередження та маскування, влаштування хибних ВП з відтворенням демаскуючих ознак для імітації присутності та діяльності військ, встановлення на зразки ОВТ додаткового захисту, вибір та облаштування шляхів пересування, радіоелектронний захист. Активними заходами є моніторинг та розвідка повітряної обстановки, застосування засобів радіоелектронної боротьби, а також кінетичного впливу на засоби ураження противника.

Бойовий досвід застосування частин та підрозділів артилерії СВ ЗС України вказує на те, що найефективнішим засобом кінетичного впливу на ударні БпАС противника є застосування безпілотних літальних апаратів (далі – БпЛА)-перехоплювачів, а для досягнення належного рівня

ефективності здійснення прикриття кожної гармати з обслугою необхідно залучати мінімум два екіпажі БпЛА-перехоплювачів.

Гусаківський А. В.
Мазур В. П.
Уваров Ю. Г.
Житомирський військовий інститут імені С. П. Корольова

ШЛЯХИ ВДОСКОНАЛЕННЯ МЕТОДИКИ ПІДГОТОВКИ ОСОБОВОГО СКЛАДУ ЗІ ЗНИЩЕННЯ FPV- ДРОНІВ ЗІ СТРІЛЕЦЬКОЇ ЗБРОЇ

Актуальність удосконалення методики підготовки особового складу до знищення FPV-дронів зі стрілецької зброї зумовлена радикальною зміною характеру сучасних бойових дій, де масоване використання БпЛА-камікадзе стало одним із ключових чинників ураження живої сили та техніки. А саме:

масовість та дешевизна загрози: FPV-дрони застосовуються на тактичному рівні безперервно. Оскільки засобів РЕБ чи спеціалізованих зенітних комплексів на кожну позицію чи відділення не вистачає, стрілецька зброя залишається останнім і найбільш доступним рубежем самооборони піхотинця;

специфіка цілі – дрон рухається на швидкостях від 60 до 150+ км/год, може різко змінювати траєкторію, висоту та заходити на ціль із мертвих зон (із тилу, з-за дерев або зі сторони Сонця). Звичайна інтуїтивна стрільба без знання правил випередження є неефективною;

психологічний тиск: звук наближення FPV-дрона викликає сильний стрес. Військовослужбовець має за лічені секунди подолати заціпеніння, виявити ціль, оцінити її швидкість, напрямок і відкрити прицільний вогонь. Без автоматизму дій, напрацьованого на тренуваннях, це неможливо;

еволюція тактики ворога: тактика застосування БпЛА постійно змінюється (скиди, тарани, синхронні атаки кількох дронів). Методика підготовки має випереджати ці зміни. Звичайні колишні правила стрільб не враховують специфіку боротьби з малорозмірними високошвидкісними та маневреними повітряними цілями, що вимагає негайної адаптації навчального процесу.

На наш погляд, щоб навчання давало реальний результат у бою, програму підготовки особового складу необхідно трансформувати у таких напрямках:

1. Теоретична база та тактична обізнаність.

Вивчення балістики та випередження: впровадження чітких математичних та візуальних таблиць випередження (на скільки корпусів дрона чи силуетів потрібно виносити точку прицілювання залежно від дальності та швидкості руху БпЛА).

Анатомія дрона: вивчання бійцями вразливх місць БпЛА (акумулятор, пропелери, бойова частина) для підвищення ефективності ураження.

2. Зміна матеріально-технічної бази тренувань.

Використання стендової стрільби: запровадження елементів спортигну (стрільби по тарілочках) для розвитку навичок супроводження рухомої цілі та стрільби на випередження.

Макети та тренувальні мішені: застосування реальних дешевих FPV-дронів (із захистом гвинтів та без вибухівки) як рухомих мішеней на полігонах для створення реалістичної картини бою.

VR-симулятори: впровадження тренажерів віртуальної реальності, які дозволяють без витрати боєприпасів тисячократно відпрацювати наведення зброї на дрони з різними траєкторіями польоту та в різних погодних умовах.

3. Вогнева тактика та групова взаємодія.

Створення «антидронових розрахунків»: навчання взаємодії у парі чи трійці, де один боєць (спостерігач) за допомогою аналізатора частот чи візуально виявляє дрон і вказує напрямок, а інші ведуть щільний вогонь.

Зосереджений вогонь відділення: відпрацювання створення «стіни вогню» (загороджувального вогню) силами всього підрозділу, що різко підвищує ймовірність збиття або пошкодження БпЛА на підльоті.

4. Психологічна стійкість та акустична адаптація.

Аудіосупровід на тренуваннях: використання потужних динаміків на стрільбищах, які відтворюють специфічний звук (дзижчання) FPV-дронів різних типів, щоб бійці звикали до звуку та вчилися орієнтуватися за ним на слух.

Удосконалення цієї методики – це не просто заміна мішеней на полігоні, а створення комплексної системи (від теорії балістики до психотренінгу), яка перетворює хаотичну стрільбу в бік дрона на системне, спокійне та ефективне його знищення на безпечній відстані. Це потребує наявності навчального часу, розробки програми навчання, підготовки інструкторсько-викладацького складу та необхідної навчально-матеріальної бази.

Баталов М. А.
Науково-дослідний центр ракетних військ і артилерії

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ АРТИЛЕРІЙСЬКОГО ПІДРОЗДІЛУ

Сучасний характер бойових дій характеризується широким застосуванням безпілотних літальних апаратів (далі – БпЛА) для ведення розвідки, спостереження, визначення місцеположення об’єктів та забезпечення їх ураження. Для артилерійських підрозділів це створює постійну загрозу виявлення та вогневого впливу і потребує не окремого застосування засобів захисту, а їх узгодженого функціонування в межах комплексної системи.

Комплексна система захисту (далі – КСЗ) артилерійського підрозділу являє собою сукупність взаємопов’язаних організаційних, тактичних, технічних та логістичних заходів, спрямованих на збереження боєздатності підрозділу, особового складу, озброєння і військової техніки та забезпечення виконання поставлених завдань в умовах вогневого впливу противника.

Актуальною проблемою є відсутність узагальненого оцінювання ефективності застосованих заходів (процесів). Оцінювання лише окремих характеристик, таких як маскування, маневр, технічна помітність або стійкість забезпечення, не дозволяє визначити загальний рівень захищеності підрозділу. Тому доцільним є формування методичного підходу, який забезпечує кількісне оцінювання ефективності застосування КСЗ артилерійського підрозділу.

У запропонованому підході ефективність КСЗ артилерійського підрозділу оцінюється через рівень захищеності артилерійського підрозділу, який формується сукупним впливом чотирьох складових (таблиця 1).

Таблиця 1 – Складові та показники оцінювання ефективності комплексної системи захисту артилерійського підрозділу

Складова КСЗ артилерійського підрозділу	Основний зміст оцінювання
Організаційна	управління, координація, своєчасність реагування, контроль виконання заходів захисту
Тактична	маскування, використання захисних властивостей місцевості, розосередження, маневр, протидія БпЛА
Технічна	зниження радіоелектронної, теплової та оптичної помітності, виявлення загроз, технічний контроль
Логістична	стійкість постачання, розосередження матеріальних засобів, евакуація, ремонт та відновлення

Організаційні заходи спрямовані на забезпечення управління системою захисту, координацію дій посадових осіб і підрозділів, своєчасне отримання та оброблення інформації про загрози, а також організацію реагування на їх виникнення.

Тактичні заходи спрямовані на зниження вразливості артилерійського підрозділу. До них належать заходи щодо приховування та маскування, використання захисних властивостей місцевості, розосередження, маневру, зміни районів розташування та організації протидії БпЛА противника.

Технічні заходи спрямовані на зниження можливості виявлення підрозділу технічними засобами противника та підвищення спроможності своєчасного виявлення загроз. При цьому враховуються радіоелектронна, теплова, оптична та інші технічні ознаки, які можуть сприяти виявленню об’єктів.

Логістичні заходи забезпечують стійкість системи постачання, накопичення матеріальних засобів, евакуації, ремонту та відновлення. Їх результативність безпосередньо впливає на здатність підрозділу зберігати боєздатність після вогневого впливу противника.

Для кількісного оцінювання кожної складової формується система часткових показників, значення яких після нормування приводяться до єдиного діапазону від 0 до 1. Узагальнена оцінка захищеності визначається за формулою:

$$K_{\text{зах}} = w_{\text{орг}}K_{\text{орг}} + w_{\text{так}}K_{\text{так}} + w_{\text{тех}}K_{\text{тех}} + w_{\text{лог}}K_{\text{лог}}, \quad (1)$$

де $K_{\text{зах}}$ – інтегральний показник захищеності артилерійського підрозділу;

$K_{\text{орг}}, K_{\text{так}}, K_{\text{тех}}, K_{\text{лог}}$ – нормовані оцінки організаційної, тактичної, технічної та логістичної складових;

$w_{\text{орг}}, w_{\text{так}}, w_{\text{тех}}, w_{\text{лог}}$ – їх вагові коефіцієнти, сума яких дорівнює одиниці.

Використання вагових коефіцієнтів дозволяє врахувати неоднаковий вплив окремих складових на загальний рівень захищеності. Їх значення доцільно визначати на основі експертного оцінювання, статистичних даних, результатів моделювання та практичного досвіду. Запропонована залежність є методичною моделлю, яка потребує подальшої перевірки та уточнення.

Оцінювання ефективності застосування КСЗ артилерійського підрозділу доцільно здійснювати шляхом порівняння рівня захищеності за різних станів обстановки або варіантів організації захисту. Це дозволяє визначити, які зміни в організаційних, тактичних, технічних чи логістичних заходах забезпечують найбільший приріст загального показника.

При цьому захищеність не є сталою характеристикою. Її рівень змінюється залежно від активності засобів розвідки та ураження противника, тривалості перебування підрозділу в районі виконання завдання, стану озброєння і військової техніки, особового складу та системи забезпечення. Тому оцінювання КСЗ артилерійського підрозділу доцільно здійснювати періодично та використовувати його результати для своєчасного коригування організації захисту.

Запропонований підхід створює можливість перейти від переважно якісного оцінювання окремих заходів КСЗ артилерійського підрозділу до кількісного визначення їх сукупної результативності. Практичним результатом такого оцінювання може бути визначення складових, які найбільше впливають на захищеність підрозділу, та обґрунтування пріоритетних напрямів удосконалення системи.

Ефективність застосування КСЗ артилерійського підрозділу визначається не наявністю окремих заходів захисту, а їх узгодженим впливом на загальний рівень захищеності артилерійського підрозділу. Запропонований підхід дозволяє представити цей вплив через чотири взаємопов’язані складові та сформувати на їх основі інтегральну кількісну оцінку.

Використання показника захищеності створює основу для порівняння різних варіантів організації КСЗ артилерійського підрозділу, визначення

найбільш суттєвих чинників її результативності та обґрунтування напрямів подальшого вдосконалення. Подальші дослідження мають бути спрямовані на уточнення системи часткових показників, методів їх нормування та визначення вагових коефіцієнтів з подальшою перевіркою методичного підходу за результатами практичного застосування.

Телегін В. В.
Кошкін М. А.
Шульга В. В.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ СИСТЕМ ОБРОБКИ РАДІОЛОКАЦІЙНОЇ ІНФОРМАЦІЇ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX В УМОВАХ ІНТЕНСИВНОГО ПОТОКУ ДАНИХ

Масоване застосування противником ударних безпілотних авіаційних комплексів (БпАК) стало одним з основних способів ураження об’єктів на території України. Під час таких атак у зоні відповідальності радіолокаційних засобів одночасно можуть перебувати десятки цілей, унаслідок чого істотно зростає обсяг радіолокаційної інформації (РЛІ), який автоматизоване робоче місце (АРМ) оператора має прийняти, обробити та відобразити за один період огляду.

Специфіка БпАК як цілей створює додаткове навантаження. Виявлення малорозмірних цілей на малих висотах відбувається в умовах відбиттів від місцевості та за зниженого порога виявлення, що збільшує кількість хибних відміток, які також підлягають обробленню. Часта зміна курсу ускладнює зав’язування та супроводження трас. Крім того, атака може тривати кілька годин, що висуває вимоги до стабільності роботи програмного забезпечення АРМ без накопичення затримок.

Перспективним напрямом є побудова АРМ на серійних обчислювальних засобах під керуванням Linux. Під час вибору апаратної конфігурації таких АРМ недостатньо орієнтуватися на загальні характеристики, оскільки оброблення РЛІ навантажує апаратні компоненти нерівномірно. Мережевий адаптер разом із мережевим стеком ядра забезпечує приймання потоку

повідомлень, центральний процесор (ЦП) – їх декодування, вторинне та третинне оброблення РЛІ, оперативна пам’ять – зберігання поточної обстановки та історії руху цілей, графічний процесор (ГП) – відображення. Якщо хоча б один із компонентів не встигає за періодом огляду, оператор отримує обстановку із запізненням саме тоді, коли час на прийняття рішення є мінімальним.

Мета дослідження – обґрунтування методики оцінювання продуктивності апаратних компонентів Linux-платформи за інтенсивності потоку РЛІ, характерної для масованого застосування БпАК, та визначення компонента, що обмежує продуктивність системи загалом.

Контрольоване навантаження створюється програмним імітатором джерела РЛІ з поступовим збільшенням кількості цілей у сценарії. На кожному кроці фіксуються такі показники:

– завантаження кожного ядра ЦП окремо, оскільки однопотокове оброблення може повністю зайняти одне ядро за низького середнього завантаження процесора;

– обсяг оперативної пам’яті, який використовує процес оброблення, і його зміна протягом тривалої роботи (для виявлення витоків пам’яті);

– завантаження ГП і фактична частота оновлення зображення;

– інтенсивність вхідного потоку та кількість відкинутих мережевих пакетів.

Показники отримуються штатними засобами Linux (файлова система /proc, утиліти пакета sysstat, профілювальник perf) та утилітами виробника ГП. Граничним вважається навантаження, за якого тривалість оброблення даних одного оберту антени перевищує період огляду або виникають втрати пакетів.

Аналіз архітектури Linux дає підстави очікувати, що компонентом, який обмежує продуктивність, не завжди буде найбільш завантажений. Так, втрати вхідних пакетів можуть виникати через переповнення приймального буфера сокета ще до повного завантаження ЦП, а затримка відображення залежить не лише від ГП, а й від графічного стеку (сервера відображення, драйвера).

Отже, продуктивність Linux-платформи для оброблення РЛІ в умовах масованого застосування БпАК доцільно оцінювати за кожним апаратним компонентом окремо з урахуванням відповідних підсистем ядра, а не за усередненим завантаженням системи. Запропонована методика дає змогу визначити граничну кількість цілей для конкретної конфігурації, виявити компонент, що обмежує продуктивність, та обґрунтувати вимоги до апаратного забезпечення АРМ.

Пасічник В. М., канд. військ. наук
Слюсаренко М. О., канд. техн. наук, ст. досл.
Центральний науково-дослідний інститут Збройних Сил України

АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ ТА МОЖЛИВОСТЕЙ БАРАЖУЮЧИХ БОЄПРИПАСІВ (ТИПУ “ЛАНЦЕТ-1” (“ЛАНЦЕТ-3”), “МОЛНІЯ”, “КУБ-БЛА”)

Узагальнений аналіз можливостей баражуючих боєприпасів (типу “Ланцет-1” (“Ланцет-3”), “Молнія”, “КУБ-БЛА”) показав, що до переліку основних факторів, які впливають на характер загроз зразкам ОВТ на полі бою від цих БпЛА, належать:

тривалість польоту – понад 30 хв, дальність польоту – понад 40 км, висота польоту: максимальна – 3–5 км, перед переходом в атаку (пікірування) – 0,7–1,5 км; швидкість польоту: горизонтального – в межах 65–130 км/год (18–36 м/с); під час пікірування на об’єкт (ціль) – до 300 км/год (до 84 м/с);

дальність виявлення цілі – 1260–12700 м;

дальність ідентифікації цілі: до типу – 110–1100 м; до класу – 145 – 1500 м;

ймовірність виявлення типових зразків ОВТ¬ – 0,8 (на дальностях до 1,2 км);

ймовірність ідентифікації цілей – 0,8 (на дальностях до 200 м);

дальність, з якої здійснюється пікірування на ціль – 0,3–1,5 км;

кути атаки на ціль – від 100 до максимально наближених до 900;

точність влучення в ціль – до 5 м (кругове імовірне відхилення), яка суттєво залежить від точності цілевказань розвідувальних БпЛА;

висока надійність ураження цілі: для кумулятивних бойових частин (БЧ) – при безпосередньому контакті з її корпусом; для осколкових (осколково-фугасних, та термобаричних) БЧ – на відстані до 3 м від цілі;

відносно великі габаритні розміри, що зумовлюють їх достатньо високу контрастність як об’єктів виявлення та ураження.

На основі аналізу даних щодо досвіду застосування противником баражуючих боєприпасів (типу “Ланцет” та “Молнія”), що надані підрозділами Сухопутних військ (СВ) ЗС України, встановлено наступні особливості їх польоту:

на основному етапі – політ на висотах 100–1000 м із крейсерською швидкістю 80–185 км/год;

на етапі атаки – перехід у динамічне пікірування під кутами атаки

40–60° із підвищенням швидкості до 150–300 км/год. Це забезпечує максимальну кінетичну енергію для пробиття броні та ускладнює перехоплення засобами протиповітряної оборони (ППО) чи стрілецькою зброєю.

Таким чином, проведений аналіз свідчить про доцільність формування параметрів (сценаріїв) загроз зразкам ОВТ від баражуючих боєприпасів (типу “Ланцет”), що враховують як їх можливості, так і практичний досвід застосування.

З огляду на можливості застосування баражуючих боєприпасів загрози зразкам ОВТ від них формуються на основі таких параметрів:

для зразків ОВТ, що захищаються КГАЗ, на основному етапі польоту – горизонтальний політ з незначним маневруванням за курсом та висотою на середніх (1–4 км) та частково великих висотах (4–5 км) та на дальностях, з яких ці БпЛА спроможні самостійно виявляти цілі, починають перетинати дальню межу зони виявлення КГАЗ (6 км) і перебувають в її середині (на віддаленнях 1,5–6 км від зразка ОВТ), здійснюючи політ на середніх швидкостях 80–110 км/год (22–31 м/с);

для зразків ОВТ, що захищаються КГАЗ та КАЗ на кінцевому етапі польоту, – пікірування з малих (0,5–1 км) та частково середніх висот (1 – 1,5 км), з дальностей, з яких ці БпЛА починають ідентифікувати ціль (0,15 – 1,5 км) та атакувати її з верхньої напівсфери під кутами 100–870 здійснюючи політ на максимальних швидкостях 250–300 км/год (70–84 м/с).

З огляду на практичний досвід застосування баражуючих боєприпасів, загрози зразкам ОВТ доцільно скоригувати з урахуванням таких параметрів:

на основному етапі – політ на висотах 100–1000 м із крейсерською швидкістю 80–185 км/год (22–52 м/с);

на кінцевому етапі – перехід у динамічне пікірування під кутами атаки 40–60° із підвищенням швидкості до 150–300 км/год (41–84 м/с).

Коростельов В. А.
Науково-дослідний цент ракетних військ і артилерії

ПРОТИДІЯ БЕЗПІЛОТНИМ АВІАЦІЙНИМ СИСТЕМАМ ПРОТИВНИКА

Досвід сучасних збройних конфліктів свідчить про суттєве зростання ролі безпілотних авіаційних систем (далі – БпАС) у виконанні завдань розвідки,

спостереження, цілевказання, коригування вогню та безпосереднього ураження об’єктів противника. Масове застосування безпілотних літальних апаратів (далі – БпЛА), їх технологічне вдосконалення та інтеграція із засобами розвідки й ураження призвели до істотного скорочення часу між виявленням об’єкта та здійсненням вогневого впливу. За таких умов протидія БпАС противника є одним із ключових чинників забезпечення живучості підрозділів, збереження особового складу, озброєння і військової техніки та підтримання спроможності до виконання бойових завдань.

Особливої актуальності зазначене питання набуває для артилерійських підрозділів. Їх вогневі позиції, пункти управління, засоби артилерійської розвідки, транспортні засоби та елементи логістичного забезпечення є пріоритетними об’єктами розвідки і ураження. У комплексній системі захисту артилерійських підрозділів протидія ударним БпЛА визначається як один із основних напрямів забезпечення їх живучості та боєздатності.

Протидію БпАС противника доцільно розглядати не як застосування окремого засобу боротьби, а як комплекс взаємопов’язаних організаційних, тактичних, технічних та інженерних заходів. Їх реалізація має забезпечувати послідовне вирішення завдань щодо зниження ймовірності виявлення підрозділу, своєчасного виявлення БпЛА противника, оповіщення про повітряну загрозу, зниження ефективності функціонування безпілотних систем та мінімізації наслідків їх застосування.

Важливою передумовою ефективної протидії є організація безперервного моніторингу повітряної обстановки та своєчасного оповіщення підрозділів. Інформація про повітряну обстановку повинна надходити від усіх доступних джерел, узагальнюватися та оперативно доводитися до відповідних елементів бойового порядку. Система оповіщення має забезпечувати своєчасне реагування особового складу на появу розвідувальних та ударних БпЛА, а також створювати інформаційні передумови для застосування наявних засобів протидії.

Не менш важливим напрямом є зниження помітності підрозділів. Застосування маскувальних засобів, використання захисних властивостей місцевості, обмеження демаскуючих ознак, періодична зміна позицій та дотримання маскувальної дисципліни ускладнюють виявлення і розпізнавання об’єктів засобами повітряної розвідки. Водночас інженерне обладнання позицій, створення укриттів і захисних конструкцій сприяють зменшенню наслідків застосування ударних БпЛА та боєприпасів, що скидаються з них.

Технічна складова протидії БпАС передбачає комплексне використання засобів виявлення, радіоелектронної боротьби та протиповітряної оборони. Засоби виявлення мають забезпечувати своєчасне отримання інформації про появу малорозмірних повітряних цілей, а засоби радіоелектронної боротьби — знижувати можливості противника щодо управління окремими типами БпЛА, передачі даних та використання супутникової навігації. Засоби протиповітряної оборони та інші засоби ураження доповнюють систему протидії, забезпечуючи фізичне знищення повітряних цілей у межах визначених спроможностей.

Принципове значення має взаємодія підрозділів із силами та засобами протиповітряної оборони, радіоелектронної боротьби, розвідки, інженерного забезпечення та іншими елементами бойового порядку. Ізольоване застосування окремих засобів не забезпечує достатнього рівня захисту. Тому засоби виявлення, оповіщення, радіоелектронної протидії, фізичного ураження, маскування та інженерного захисту мають функціонувати як взаємопов’язані елементи єдиної системи.

Окремої уваги потребує забезпечення стійкості власних систем управління та зв’язку в умовах одночасного застосування засобів радіоелектронної боротьби. Організація протидії БпАС не повинна створювати критичного взаємного впливу на власні канали зв’язку, навігації та автоматизовані системи управління. Це обумовлює необхідність координації застосування засобів радіоелектронного впливу, постійного контролю електромагнітної обстановки та забезпечення резервування критично важливих систем.

Таким чином, протидія безпілотним авіаційним системам противника повинна ґрунтуватися на комплексному та системному підході. Її ефективність визначається не лише кількістю наявних засобів боротьби з БпЛА, а насамперед здатністю об’єднати розвідку, виявлення, оповіщення, маскування, інженерний захист, радіоелектронну боротьбу та засоби протиповітряної оборони в єдиний функціональний контур. Подальше вдосконалення такої системи має бути спрямоване на скорочення часу реагування на повітряну загрозу, підвищення стійкості управління, адаптацію заходів захисту до зміни способів застосування БпАС противником та забезпечення живучості підрозділів у сучасному бойовому середовищі.

Задорожний І. С., д-р. техн. наук, проф.
Байцурак С. І.
Швиденко А. В., канд. тех. наук, доц.
Шинкаренко О. М., канд. економ. наук, доц.
Державний науково-дослідний інституту випробувань і сертифікації
озброєння та військової техніки

ТРАНСФОРМАЦІЯ ПОВІТРЯНИХ ЗАГРОЗ ТА ФОРМУВАННЯ НОВИХ ВИМОГ ДО СИСТЕМ АКТИВНОГО ЗАХИСТУ НАЗЕМНИХ ВИРОБІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Досвід сучасного збройного протиборства свідчить про швидку зміну характеру повітряних загроз для наземних виробів ОВТ. Безпілотні літальні апарати, які раніше розглядалися переважно як засоби ураження із заздалегідь визначеною траєкторією польоту, поступово перетворюються на складні багатофункціональні системи, що поєднують носій, навігацію, сенсори, засоби протидії радіоелектронним перешкодам, мережеві компоненти та бойове оснащення.

Особливого значення набуває поява реактивних варіантів Shahed/Герань. За наданими вихідними даними, для окремих представників сімейства заявляються швидкості від 300-370 км/год для Герань-3 до 450-600 км/год для Герань-5, а також бойові частини масою до 50–90 кг. Одночасно розвиваються засоби навігації та підвищення стійкості до радіоелектронних перешкод, включаючи CRPA, а в окремих варіантах – оптико-електронні засоби та мережеві компоненти.

Отже, вимоги до систем активного захисту наземних виробів ОВТ не можуть формуватися лише на основі одного узагальненого параметра «тип БпЛА» або його бойової частини.

Розглянемо принципову зміну трансформації повітряної загрози, яку можна представити переходом:

БпЛА як боєприпас → БпЛА як інтегрована система загрози.

У сучасному варіанті загрозу доцільно розглядати як:

Shahed/Герань = носій + навігація + сенсори + стійкість до РЕБ + бойова частина + система масованого застосування.

Відповідно, активний захист наземного виробу повинен протидіяти не одному фізичному об'єкту, а сукупності його властивостей. Основні трансформації повітряної загрози та їх наслідки наведено в таблиці.

Фактор загрози	Основна зміна	Наслідок для системи захисту
Швидкість	Перехід до реактивних варіантів	Скорочення доступного часу реагування
Висота	Розширення просторової зони застосування	Підвищення вимог до виявлення та супроводження
GNSS + INS CRPA / anti-jam	Багатоканальна навігація Підвищення стійкості до РЕБ	Зменшення ефективності лише GNSS-пригнічення
Оптичні сенсори, Мережеві компоненти	Можливість уточнення об'єкта/траєкторії. Обмін даними та функціональна інтеграція	Підвищення вимог до маскування та зниження помітності
Різні бойові частини	Зміна характеру ураження	Диференційовані вимоги до живучості
Масоване застосування	Потік одночасних цілей	Обмеження пропускної здатності C-UAS/КАЗ.

Таким чином, сучасна загроза характеризується переходом від одиничного об'єкта до динамічної багатофакторної системи, що адаптується до засобів протидії.

Для практичного формування вимог до наземних виробів ОВТ доцільно здійснити перетворення параметрів загрози на вимоги до активного захисту, застосовувати послідовність:

параметр загрози → фізичний вплив → вимога до системи → вимірюваний показник → випробування**.**

Такий підхід дозволяє уникнути формального перенесення характеристик БпЛА безпосередньо у технічні вимоги.

Розглянемо детальніше наступні параметри:

- швидкість загрози та час реагування;
- висота та просторові можливості виявлення;
- стійкість загрози до РЕБ;
- оптико-електронні сенсори та помітність наземного виробу;
- бойова частина та живучість.

1. Швидкість загрози та час реагування. Зі зростанням швидкості БпЛА доступний час для його виявлення, прийняття рішення та застосування засобу протидії скорочується:

$$V_{загр} \uparrow \Rightarrow T_{доступ} \downarrow.$$

Час реагування можна представити:

$$T_{реакції} = T_{виявл} + T_{супр} + T_{ріш} + T_{залучення}.$$

і вимагати:

$$T_{виявл} + T_{супр} + T_{ріш} + T_{залучення} \leq T_{доступ},$$

або, якщо $T_{доступ}$ - час від моменту виявлення до точки перехоплення:

$$T_{доступ} = T_{перех} - T_{виявл}.$$

Для випробувань доцільно використовувати ймовірнісний показник:

$$P\square = P_r(T_{реакції} \leq T_{виявлен}).$$

Доповнювальними показниками є середній час виявлення, 95-й перцентиль часу реакції, час передачі інформації оператору, час формування рішення та час переходу засобу захисту у готовий режим. Такий підхід дозволяє безпосередньо пов'язати швидкість загрози з інформаційно-управлінським контуром активного захисту.

2. Висота та просторові можливості виявлення**.** Збільшення висоти польоту загрози змінює геометрію її виявлення та супроводження. Тому вимогу до системи недоцільно задавати лише як фіксовану максимальну висоту.

Методично коректнішою є вимога забезпечення необхідної ймовірності виявлення у визначеній області дальностей і висот:

$$P_{det}(H,D) \geq P_{det},min.$$

Основними випробувальними показниками можуть бути: дальність виявлення D_{det}; ймовірність виявлення $P_{det}(H,D)$; ймовірність супроводження $P_{track}(H,D)$; час стійкого супроводження T_{track}.

Таким чином, характеристика загрози «висота» трансформується у просторову вимогу до сенсорної системи активного захисту.

3. Стійкість загрози до РЕБ**.** Розвиток CRPA та інших засобів підвищення стійкості навігації змінює підхід до оцінювання радіоелектронної протидії. Наявність засобу РЕБ сама по собі не повинна вважатися достатньою умовою захисту.

Вимогу доцільно формулювати як забезпечення заданого ефекту протидії за визначеного рівня стійкості загрози до радіоелектронного впливу:

$P_{EW} = P_r$(необхідний ефект протидії | задана EW-стійкість загрози),

де EW – стійкість до радіоелектронного впливу; P_{EW} – імовірність досягнення заданого ефекту радіоелектронної протидії за заданого рівня стійкості загрози до РЕП.

До складу показників можуть входити: $P_{track}|EW$ – ймовірність збереження супроводження; $T_{recovery}$ – час відновлення після порушення; $P_{navigation}$-loss – імовірність втрати ефекту протидії; P_{EW}-fail – ймовірність відмови протидії.

Для критичних систем показників необхідні умови:

$$P_{EW} \geq P_{EW} - \min,$$

доцільно розглядати як GATE-вимогу, тобто обов'язкову умову проходження системою встановленого рівня придатності.

4. Оптико-електронні сенсори та помітність наземного виробу. Застосування бортових камер та інших сенсорів означає, що оцінювання захищеності наземного виробу повинно виходити за межі лише радіолокаційної помітності.

Доцільно розглядати узагальнений профіль:

$$\text{Signature} = (\text{Radar, EO, IR, Thermal}),$$

де Radar – радіолокаційна, EO – оптико-електронна, IR – інфрачервона, Thermal – теплова складові помітності.

Випробувальними показниками можуть бути дальність та ймовірність оптико-електронного й інфрачервоного виявлення, контрастність об'єкта, імовірність хибної ідентифікації та нормований коефіцієнт зниження помітності $K_{signature}$.

Отже, маскування необхідно розглядати не тільки як конструктивну властивість виробу, а як кількісно вимірювану складову його захищеності.

5. Бойова частина та живучість. Збільшення маси бойової частини саме по собі не є достатнім показником небезпеки. Для наземного виробу принциповим є характер наслідків впливу:

$$E_{impact} \rightarrow (P_{crew}, P_{mission}, P_{critical}, K_{res}).$$

Тому доцільно оцінювати:

$$P_{surv} = P_r(\text{екіпаж і система зберігають задану функцію});$$

$$P_{crit} = P_r(\text{критична втрата функції});$$

$$K_{res} = P_{mission,after} / P_{mission,before}.$$

де $P_{mission,after}$ та $P_{mission,before}$ – ефективність виробу до та після впливу.

Додатковим показником є $T_{restore}$ – час відновлення бойової функції.

Такий підхід переводить оцінювання від простої характеристики «маса бойової частини» до оцінювання функціональних наслідків ураження.

Суттєвою особливістю сучасної загрози є можливість масованого застосування БпЛА. У цьому випадку оцінювання одиничного акту перехоплення вже не характеризує повною мірою ефективність системи.

Для опису потоку загроз доцільно використовувати інтенсивність:

$$\lambda_{UAS} = N / \Delta t,$$

де N – кількість загроз, що надходять за час Δt.; λ_{UAS} – інтенсивність надходження загроз, [цілей/с];

Для просторової характеристики може використовуватися щільність:

$$\rho = N / A,$$

де A – площа відповідної зони; ρ_{UAS} – просторова щільність загроз, [цілей/м²].

Розглянемо узагальнену модель вимог до систем активного захисту. На основі проведеного аналізу захищеність наземного виробу від повітряних загроз доцільно представити як комплексну характеристику:

$$S_{UAS} = w□S_{detect} + w□S_{EW} + w□S_{kinetic} + w□S_{survive},$$

де w□ + w□ + w□ + w□ = 1; S_{detect} – спроможність своєчасного виявлення та супроводження БпЛА; S_{EW} – стійкість і ефективність протидії авіаційним та інформаційним можливостям загрози; $S_{kinetic}$ – здатність протистояти фізичному впливу; $S_{survive}$ – здатність зберігати бойову функцію після ураження. Всі складові попередньо нормовані до [0;1], причому:

$$S_i \geq S_i,min,$$

для критичних властивостей:

$$S_i \geq S_i,GATE,$$

де GATE – критична обов'язкова вимога, невиконання якої виключає можливість визнання системи.

Сучасна трансформація повітряних загроз полягає у формуванні інтегрованої багатофакторної загрози, що поєднує носій, навігацію, сенсори, стійкість до РЕБ, бойову частину та можливість масованого застосування.

Королюк Н. О. канд. техн. наук, доц.
Рудь Б. С.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ОСОБЛИВОСТІ ПОБУДОВИ ЕШЕЛОНОВАНОЇ СИСТЕМИ ПРОТИПОВІТРЯНОЇ ОБОРОНИ ВІД УДАРІВ ПОВІТРЯНОГО ПРОТИВНИКА

Досвід збройної агресії рф проти України свідчить, що противник в останній час застосовує комбіновані масовані ракетно-авіаційні удари, у яких поєднуються ракети різних типів. Так, у ніч на 17 вересня 2026 року було зафіксовано 197 повітряних цілей (ПЦ), які запускалися з різних напрямків, на різних висотах протягом тривалого часу, щоб максимально ускладнити роботу протиповітряної оборони (ППО). В таких умовах забезпечення надійного прикриття наземних об’єктів є технічно малоймовірним.

Необхідним в сучасних умовах є підвищення стійкості ППО шляхом побудови багатоешелонованої системи, у якій зенітні ракетні комплекси перехоплюють засоби повітряного нападу (ЗПН) на різних дистанціях і висотах. Зовнішній рубіж формують комплекси великої дальності (“Patriot”, “Samp/T”), здатні уражати високошвидкісні цілі, зокрема балістичні та крилаті ракети; зокрема “Patriot” може одночасно уражати до 8 ПЦ на дальності до 80 км і висоті до 24 км. Наступний ешелон складають комплекси середньої дальності (“Iris-T”, “Nasams”, “Бук-М1”): “Iris-T” уражає цілі на дальності до 25 км, “Nasams” – до 40 км, а “Бук-М1” здатний діяти по 6 безпілотним літальним апаратам одночасно з імовірністю ураження 0,7–0,9. Завершальний ешелон утворюють комплекси малої та ближньої дії, переносні зенітні ракетні комплекси, зенітні самохідні та артилерійські установки (“Avenger”, “Oca”, “Stinger”, “Ігла”, “Gepard”, ЗУ-23-2), які безпосередньо прикривають важливі об’єкти та ефективні при знищенні малорозмірних цілей.

Перевагою даної побудови багатоешелонованої системи є те, що прорив ПЦ через один рубіж компенсується перехопленням у наступному ешелоні. Склад засобів ППО повинен бути збалансованим за класами, дальністю та висотою ураження, з високою мобільністю підрозділів.

Досвід бойових дій свідчить, що збільшення кількості та різноманітності вогневих засобів підвищує навантаження на органи управління. У зоні поразки зенітної ракетної бригади (*зрбр*) може одночасно перебувати до 10–30 ПЦ, у зоні ураження зенітного ракетного дивізіону (*зрдн*) – до 5–10 цілей, а час на рішення по кожній з них обмежується 5–8 секундами. Ефективність ППО визначається не лише тактико-технічними характеристиками засобів ураження, а й рівнем автоматизації процесів прийняття рішень при управлінні огневими засобами. Існуючі комплекси засобів автоматизації переважно вирішують розрахункові задачі, тоді як логіко-аналітичні (оцінка задуму противника, визначення напрямку головного удару, виявлення хибних цілей, пріоритезація цілей) виконуються бойовим розрахунком без автоматизації.

Наявні аналітичні моделі спираються на спрощені припущення та орієнтовані на кількісну інформацію, тоді як значна частина задач управління має якісний, нечіткий і неповний характер. Тому доцільно застосовувати декларативні методи представлення знань, які передбачають формалізацію процесу розподілу вогню на основі класифікації подій, ознакової інформації та функціональних мереж. Такий підхід дозволяє об’єднати логіко-аналітичні, розрахункові та пошукові задачі в єдину систему, встановлювати черговість знищення ПЦ і обирати *зрдн* з урахуванням його тактичного призначення та бойових можливостей, редагувати базу знань без перебудови програмного забезпечення.

Особливості застосування засобів ППО в сучасній війні підтверджують важливість мобільності, багатоешелонованості та інтеграції засобів у єдину систему управління. Сучасні ЗПН характеризуються високою швидкістю та маневреністю, складними тактичними прийомами, веденням радіоелектронної боротьби. Кожен ешелон системи ППО повинен бути пов’язаний із відповідною ланкою повітряного простору. Інакше збільшення кількості засобів ППО супроводжується дублюванням вогню по одних цілях і пропуском інших.

Таким чином, збільшення складу засобів ППО різного класу створює необхідну глибину та кількість вогневих каналів ешелонованої оборони, а автоматизоване вироблення рекомендацій на розподіл вогню забезпечує їх узгоджене використання в умовах дефіциту часу. Поєднання цих напрямків дозволяє підвищити ефективність відбиття масованих ракетно-авіаційних ударів противника.

Ушаков С. І., канд. техн. наук
Костиря О. О., д-р техн. наук, ст. наук. співроб.
Черкес О. П.
Тіора В. А.
Зубелевич Д. І.
Житомирський військовий інститут імені С. П. Корольова

ТЕНДЕНЦІЇ ВДОСКОНАЛЕННЯ ЗАСОБІВ ПРОТИДІЇ УДАРНИМ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТАМ ТИПУ FPV

Досвід відсічі широкомасштабної збройної агресії рф проти України засвідчив, що ударні безпілотні літальні апарати (БпЛА) типу FPV (англ. First Person View – вид від першої особи) стали одним з основних засобів ураження озброєння та військової техніки (ОВТ) у тактичній зоні. Такі БпЛА дешеві, їх застосовують масово, а завдяки високій маневреності вони влучають у найвразливіші місця навіть добре захищених зразків ОВТ.

Тривалий час основу захисту ОВТ від ударних БпЛА типу FPV становили засоби радіоелектронної боротьби (РЕБ) та пасивного захисту – антидронові екрани, сітки, маскування. Пасивні засоби лише знижують імовірність ураження або тяжкість його наслідків, проте збільшують масу ОВТ і можуть обмежувати сектори обстрілу озброєння. Ефективність РЕБ суттєво знизило поширення БпЛА з волоконно-оптичним каналом керування, які не піддаються радіоелектронному придушенню і не виявляються засобами радіотехнічної розвідки.

За цих умов захищеність ОВТ залежить передусім від того, чи вдасться своєчасно виявити та знищити БпЛА ще на підльоті до зразка. Це завдання виконує комплекс активного захисту (КАЗ) ОВТ – сукупність взаємопов'язаних засобів виявлення, ураження та керування. На відміну від пасивного захисту, КАЗ запобігає самому влучанню.

Метою доповіді є визначення тенденцій удосконалення засобів протидії ударним БпЛА типу FPV, пов'язаних з інтеграцією систем виявлення та ураження в КАЗ ОВТ.

Узагальнену структуру КАЗ ОВТ від ударних БпЛА типу FPV наведено на рис. 1. Сірим виділено складові, що розглядаються в доповіді, зокрема обробку даних на основі штучного інтелекту (ШІ).



Рис. 1. Узагальнена структура КАЗ ОВТ від ударних БпЛА типу FPV

На нашу думку, КАЗ ОВТ доцільно створювати як поєднання засобів групового та індивідуального прикриття. Групове прикриття забезпечують радіолокаційні станції (РЛС) малої дальності, кулеметні установки з комбінованим радіолокаційно-оптичним виявленням і наведенням, засоби акустичної та радіотехнічної розвідки, РЕБ і пункт управління. Засоби індивідуального прикриття розміщуються на зразку ОВТ: мікрохвильові датчики руху або оптико-електронні засоби виявляють БпЛА, а блоки сіткометів і вогнепальні засоби, встановлені по периметру зразка або на турелі, уражають його автоматично за командою контролера. Засоби РЕБ для такого прикриття малоперспективні через високе енергоспоживання, погіршення електромагнітної сумісності та значну масу й габарити антен. Засоби виявлення суттєво відрізняються за дальністю дії, скритністю роботи та ефективністю щодо БпЛА з волоконно-оптичним керуванням (табл. 1; наведені значення орієнтовні).

Таблиця 1

Порівняльна характеристика засобів виявлення БпЛА

Засіб (дальність)	**Переваги**	**Недоліки та обмеження**
РЛС малої дальності	всепогодність; велика дальність; точні координати	“мертва зона”; вразливість до РЕБ; демаскування; висока вартість
Засоби радіотехнічної розвідки (до 3 км)	скритність роботи; мала маса; перехоплення відеосигналу	не визначають дальність; не виявляють БпЛА з волоконно-оптичним керуванням; потребують оновлення частот
Акустичні засоби (сотні метрів)	скритність роботи; працездатність поза прямою видимістю	мала дальність; запізнювання даних; похибки пеленгування через вітер

Засіб (дальність)	Переваги	Недоліки та обмеження
Оптико-електронні засоби із ШІ	скритність роботи; незалежність від каналу керування	залежність від погоди й освітленості; вузьке поле зору; вразливість ШІ до маскування
Мікрохвильові датчики руху (десятки метрів)	низька вартість; визначення сектора загрози	мала дальність; хибні спрацювання (не розпізнають тип цілі)

Жоден із цих засобів окремо не забезпечує надійного виявлення. Тому отримані дані доцільно комплексувати, а розпізнавання БпЛА на тлі завад, класифікацію загрози та прогнозування траєкторії цілі покласти на алгоритми ШІ.

Розподіл функцій між засобами групового та індивідуального прикриття визначається умовою своєчасного ураження БпЛА:

$$t_в + t_к + t_ц + t_у \le (D_в - D_{min}) / V,$$

де $t_в$, $t_к$, $t_ц$, $t_у$ – час виявлення, класифікації, цілевказання та ураження; $D_в$ – дальність виявлення; D_{min} – мінімальна безпечна дальність ураження; V – швидкість БпЛА.

За швидкості БпЛА типу FPV 30–40 м/с і дальності виявлення засобами групового прикриття 1–5 км на цикл протидії залишається від кількох десятків секунд до 2–3 хв, чого достатньо, щоб зберегти людину в контурі прийняття рішення. Для засобів індивідуального прикриття з дальністю виявлення в кілька десятків метрів цей час не перевищує 1 с, і оператор фізично не встигає втрутитися. До того ж в екіпажі ОВТ немає окремої особи, яка могла б постійно вести спостереження за повітряною обстановкою та керувати засобами КАЗ. Тому цикл протидії засобів індивідуального прикриття має бути повністю автоматичним у заданих екіпажем секторах ураження, а вирішального значення набувають достовірність розпізнавання цілей і безпека власних сил. Виконати умову можна насамперед скороченням $t_к$ і $t_ц$, тобто автоматизацією й інтеграцією засобів виявлення та ураження.

Більшість наявних засобів протидії діють роз'єднано або лише з автоматизованим цілевказанням, проте в бойових умовах вже використовуються й інтегровані комплекси. Станом на теперішній час відомо (за даними відкритих джерел) про використання підрозділами Збройних Сил України малих турелей із ШІ, які автономно виявляють і супроводжують БпЛА та розраховують його траєкторію, а оператору залишається лише дати дозвіл на ураження. Створюються й автоматичні модулі із сіткометами для індивідуального прикриття ОВТ.

Зарубіжні (зокрема російські) розробки наведено в табл. 2 (за відкритими джерелами та заявами виробників).

Таблиця 2

Зарубіжні розробки КАЗ ОВТ і комплексів протидії ударним БпЛА

Комплекс (країна, розробник)	**Засоби виявлення**	**Засоби ураження**	**Особливості**
“Арена-М” (рф, КБМ)	РЛС ближньої дії	захисні боєприпаси	на танках Т-72Б3 і Т-90М; у бою з 2026 р.
LPD-2000 (рф, “Лабораторія ППШ”)	РЛС, оптико-електронний приціл	кулемети, лазер, засіб РЕБ	автоматичний або напівавтоматичний режим; до 2 км
“Титан” (рф)	нейромережеве розпізнавання цілей	дробова турель, лазер, РЕБ	стаціонарний; доопрацьовується для мобільних систем
Trophy (Ізраїль, Rafael)	РЛС кругового огляду	захисні боєприпаси	на танках M1 Abrams, Merkava; з 2024 р. заявлено захист від БпЛА
ForceField (Ізраїль, Axon Vision)	пасивні сенсори кругового огляду, ШІ	штатна зброя	автономний; розрахований і на БпЛА з волоконно-оптичним керуванням
Bullfrog (США, Allen Control Systems)	оптико-електронний сенсор із ШІ	кулемет M240 на турелі	пасивне виявлення; автоматичний режим; до 800 м

Класичні КАЗ, створені для протидії протитанковим керованим ракетам і реактивним гранатам, адаптуються до загрози з боку БпЛА типу FPV, проте їх ефективність обмежена. Відомості про бойове застосування КАЗ “Арена-М” у 2026 р. неоднозначні: у липні зафіксовано влучання в танк без видимого спрацювання захисту, а в серпні, за повідомленнями, один комплекс перехопив 7 БпЛА до вичерпання боєкомплекту. Новіші системи ґрунтуються на пасивних оптико-електронних засобах виявлення з алгоритмами ШІ та кінетичних засобах ураження з низькою вартістю пострілу. У рф також заявлено про розробку пневматичного сіткомета для захисту верхньої проєкції танка.

Узагальнивши розглянуті зразки, виокремлюємо такі тенденції:

– об'єднання засобів виявлення, оцінювання загрози та ураження в єдиному контурі з автоматизацією всіх етапів циклу протидії;

– зростання ролі пасивних засобів виявлення (оптико-електронних, акустичних), ефективних і щодо БпЛА з волоконно-оптичним керуванням;

– комплексування даних різнорідних засобів виявлення з розпізнаванням і супроводженням цілей на основі ШІ;

– використання кінетичних засобів ураження з низькою вартістю пострілу – блоків сіткометів і вогнепальних засобів (кулеметних, дробових), зокрема на наземних роботизованих комплексах;

– мережева інтеграція бортових КАЗ із засобами групового прикриття через уніфіковані інтерфейси (наприклад, протокол SAPIENT, визначений НАТО основою стандарту технічної сумісності);

– розвиток зброї спрямованої енергії (лазерної, надвисокочастотної), яка згодом може доповнити кінетичні засоби ураження у складі КАЗ.

Вважаємо, що основна тенденція удосконалення засобів протидії ударним БпЛА типу FPV полягає в переході від пасивного захисту й роз'єднаних засобів до КАЗ ОВТ із замкнутим контуром “виявлення – ураження”, що поєднують засоби індивідуального та групового прикриття, притому перші мають діяти повністю автоматично. Їх ефективність визначається насамперед комплексуванням даних засобів виявлення на основі ШІ та застосуванням кінетичних засобів ураження з низькою вартістю пострілу й боєкомплектом, розрахованим на відбиття групових атак. Засоби РЕБ і надалі потрібні, проте самі такого захисту вже не забезпечують. Оскільки в рф аналогічні комплекси активно розробляються, вітчизняні КАЗ необхідно створювати випереджальними темпами.

Перспективними напрямами подальших досліджень є обґрунтування раціонального складу бортового КАЗ за критерієм “ефективність – вартість”, розроблення стійких до навмисних впливів противника алгоритмів розпізнавання малорозмірних цілей на основі ШІ та визначення вимог до його спряження із засобами групового прикриття з урахуванням стандартів НАТО.

Чорномаз О. А.
Центральне управління інноваційної діяльності Збройних Сил України

КОМПЛЕКСНИЙ ПІДХІД ДО ПРОТИДІЇ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТАМ - ПЕРЕХОПЛЮВАЧАМ ДЛЯ ПІДВИЩЕННЯ ЖИВУЧОСТІ БАГАТОРАЗОВИХ УДАРНИХ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

І. Вступ та актуальність проблеми

Багаторазові ударні безпілотні авіаційні комплекси (БпАК) є важливою складовою спроможностей Сил оборони України з ураження об’єктів противника та вогневої підтримки підрозділів. На відміну від одноразових ударних засобів, ефективність їх застосування залежить не лише від виконання бойового завдання, а й від збереження безпілотного літального апарата (БпЛА) та його повернення для повторного застосування.

Досвід бойового застосування свідчить про значні втрати багаторазових БпЛА внаслідок комплексного впливу засобів радіоелектронної боротьби (РЕБ), протиповітряної оборони, вогневих засобів та БпЛА-перехоплювачів. Поширення останніх формує додаткову загрозу ураження БпЛА безпосередньо в повітрі як під час виконання бойового завдання, так і на маршруті повернення.

Систематичні втрати багаторазових БпЛА скорочують наявний парк, збільшують потребу в його відновленні та знижують спроможність підрозділів до інтенсивного і тривалого застосування багаторазових БпАК. Відповідно, підвищення їх живучості є актуальним науково-практичним завданням, вирішення якого потребує комплексного підходу до виявлення загроз і протидії їм протягом усього циклу бойового застосування.

ІІ. Основні ідеї

У роботі розглядається комплексний підхід до підвищення живучості багаторазових ударних БпАК в умовах застосування противником БпЛА-перехоплювачів та інших засобів протидії. Вихідним припущенням є те, що окремий засіб захисту не забезпечує протидію всьому спектру загроз, а необхідний рівень живучості має досягатися поєднанням взаємодоповнюючих засобів виявлення, оцінки загрози та реагування.

У ході дослідницьких випробувань перевірено технічні рішення за чотирма основними напрямами: бортові засоби радіоелектронної розвідки

(РЕР) та РЕБ, акустичне виявлення загроз, зниження помітності БпЛА та активна фізична протидія. Технічні рішення перевірялися після інтеграції на конкретні БпАК-носії, що дозволило оцінити їх працездатність, ефективність у визначених умовах та особливості взаємодії з бортовими системами.

Результати випробувань підтвердили працездатність окремих технологічних рішень, водночас не підтвердили наявність універсального засобу, здатного самостійно забезпечити необхідний рівень захисту БпАК. Встановлено, що практична ефективність протидії залежить не лише від характеристик окремого засобу, а й від своєчасності виявлення загрози, часу реагування та якості інтеграції з БпАК-носієм.

З урахуванням отриманих результатів пропонується будувати захист багаторазового БпАК як єдиний функціональний контур: виявлення загрози - її ідентифікація та оцінка - прийняття рішення - застосування відповідного способу протидії - оцінка результату. Перспективним напрямом є формування інтегрованого бортового комплексу оборони, який об’єднує різнотипні засоби виявлення, обробку інформації та засоби протидії з поетапним підвищенням рівня автоматизації реагування.

Самозахист багаторазового БпАК та активне перехоплення БпЛА противника доцільно розглядати як окремі взаємодоповнюючі спроможності. Самозахист має забезпечувати збереження БпАК-носія під час виконання основного бойового завдання, тоді як активне перехоплення доцільно реалізовувати спеціалізованими безпілотними платформами.

ІІІ. Висновки

Підвищення живучості багаторазових ударних БпАК потребує переходу від застосування окремих засобів захисту до їх функціональної інтеграції в єдину систему. Основою такої системи має бути замкнений цикл виявлення, оцінки загрози, прийняття рішення, протидії та оцінки результату.

Перспективним напрямом є створення інтегрованого бортового комплексу оборони з поетапною автоматизацією процесів виявлення, оцінки загроз та реагування. При цьому самозахист БпАК і активне перехоплення БпЛА противника мають розвиватися як окремі, але взаємопов’язані спроможності.

Подальший розвиток систем забезпечення живучості доцільно здійснювати за адаптивним принципом: фактичні дані про втрати та пошкодження БпАК - аналіз актуальних загроз - формування вимог - розробка

та випробування технічних і тактичних рішень - впровадження - оцінка результатів бойового застосування. Такий підхід забезпечує системне оновлення засобів і способів захисту відповідно до зміни характеру загроз.

Савчук Д. В.
Шостак Р. С.
Науково-дослідний центр ракетних військ і артилерії

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ ЗА ДОСВІДОМ ВЕДЕННЯ БОЙОВИХ ДІЙ

Масове застосування противником безпілотних літальних апаратів (далі – БпЛА) різних типів, зокрема ударних, а також застосування високоточної зброї, засобів радіоелектронної боротьби та комплексів технічної розвідки суттєво змінюють умови бойового застосування артилерійських підрозділів. Скорочення циклу від виявлення об’єкта до його ураження противником підвищує вразливість елементів бойового порядку артилерійських підрозділів та висуває додаткові вимоги до забезпечення їх живучості. За таких умов застосування окремих, не пов’язаних між собою заходів захисту не забезпечує належного рівня захищеності підрозділів, що зумовлює необхідність формування комплексної системи захисту (далі – КСЗ).

Зазначеному питанню нині приділяють особливу увагу. За результатами роботи військово-наукової групи Науково-дослідного центру ракетних військ і артилерії у військових частинах (підрозділах) РВіА розроблено описову модель комплексної системи захисту артилерійських підрозділів, вимоги до її функціонування та рекомендації щодо його забезпечення.

Під КСЗ артилерійських підрозділів доцільно розуміти сукупність взаємопов’язаних та взаємоузгоджених заходів, об’єднаних єдиними процесами управління, інформаційного обміну та реагування на загрози і спрямованих на забезпечення живучості та боєздатності підрозділів, збереження особового складу, озброєння і військової техніки, підтримання безперервності управління та виконання бойових завдань.

Метою функціонування КСЗ є зниження ймовірності виявлення та ураження артилерійських підрозділів противником, зменшення можливих втрат,

збереження їх боєздатності та забезпечення стійкого управління під час виконання бойових завдань. Досягнення зазначеної мети потребує комплексного залучення наявних сил і засобів військових частин (підрозділів), а також узгодження їх дій із підрозділами протиповітряної оборони (далі – ППО), радіоелектронної боротьби (далі – РЕБ), інженерними та загальновійськовими підрозділами.

З урахуванням характеру сучасних загроз комплексну систему захисту артилерійських підрозділів доцільно формувати за чотирма взаємопов’язаними групами заходів: організаційними, тактичними, технічними та логістичними. Їх комплексне та взаємоузгоджене застосування дає змогу реалізувати єдиний цикл захисту: виявлення загрози, її оцінювання, оповіщення підрозділів, визначення необхідного способу реагування, застосування відповідних сил і засобів та оцінювання результатів здійснених заходів.

Організаційні заходи становлять основу функціонування КСЗ та охоплюють планування заходів захисту, координацію дій із залученими силами і засобами, моніторинг обстановки та оповіщення, а також контроль виконання визначених заходів.

Планування захисту артилерійських підрозділів має здійснюватися одночасно з плануванням їх бойового застосування та передбачати оцінювання характеру й рівня можливих загроз, визначення необхідного складу сил і засобів захисту, вибір районів розташування та вогневих позицій, маршрутів маневру, порядку інженерного обладнання, маскування і прикриття. Плани захисту повинні оперативно уточнюватися відповідно до змін бойової обстановки та можливостей противника.

Важливою умовою функціонування КСЗ є координація заходів захисту з іншими силами та засобами. Досвід бойових дій свідчить, що артилерійські підрозділи не можуть повною мірою забезпечити власний захист виключно штатними силами та засабами. Необхідний рівень захищеності досягається шляхом інтеграції можливостей підрозділів ППО, РЕБ, інженерних, загальновійськових та інших підрозділів у єдину систему захисту.

Моніторинг обстановки має передбачати безперервне спостереження за повітряною, наземною та радіоелектронною обстановкою із залученням усіх доступних джерел інформації. Отримані дані повинні забезпечувати своєчасне виявлення ознак виникнення загроз, оцінювання їх характеру та оперативне доведення відповідної інформації до елементів бойового порядку. Система оповіщення при цьому повинна бути безперервною, стійкою до

радіоелектронного впливу та передбачати використання основних і резервних каналів зв'язку.

Контроль виконання заходів захисту має здійснюватися командирами відповідних рівнів під час планування та ведення бойових дій. Його основним змістом є перевірка повноти, своєчасності та якості реалізації запланованих заходів, оцінювання їх ефективності, виявлення недоліків та оперативне коригування планів відповідно до змін обстановки.

Тактичні заходи реалізуються безпосередньо під час підготовки та ведення бойових дій і спрямовуються на зниження ймовірності виявлення та ураження артилерійських підрозділів, а також на формування у противника хибного уявлення щодо їх складу, положення та характеру дій. До основних тактичних заходів доцільно віднести введення противника в оману, використання маскувальних властивостей місцевості, періодичну зміну районів і позицій, а також заходи інженерної підтримки, безпосередньо спрямовані на підвищення захищеності підрозділів.

Введення противника в оману реалізується шляхом демонстративних дій, дезінформації та імітації. Застосування хибних позицій, макетів озброєння і військової техніки та інших засобів імітації має забезпечувати відволікання розвідувальних і вогневих засобів противника від реальних елементів бойового порядку.

Важливе місце у забезпеченні захисту артилерійських підрозділів належить інженерній підтримці. Основними її заходами в межах КСЗ є інженерна розвідка місцевості та об'єктів, фортифікаційне обладнання вогневих позицій, пунктів управління, рубежів і районів, улаштування та утримання інженерних загороджень, а також приховування діяльності підрозділів. Реалізація зазначених заходів має забезпечувати використання захисних і маскувальних властивостей місцевості, зниження демаскувальних ознак та підвищення стійкості підрозділів до вогневого впливу противника.

Технічні заходи передбачають застосування радіоелектронних, оптико-електронних, програмно-апаратних та інших комплексів, систем і засобів, призначених для зниження ймовірності виявлення та ураження артилерійських підрозділів. До основних напрямів їх реалізації належать протидія БпЛА, протидія високоточній зброї та радіоелектронний захист.

Протидія БпЛА повинна здійснюватися комплексно та охоплювати їх своєчасне виявлення, оповіщення про повітряну загрозу, застосування засобів

РЕБ, ППО та інших засобів протидії. Ефективність зазначених заходів значною мірою залежить від інтеграції засобів виявлення, оповіщення та протидії в єдиний інформаційно-функціональний контур.

Протидія високоточній зброї має бути спрямована на зниження ефективності процесів виявлення, супроводження та наведення засобів ураження противника. Важливого значення набуває комплексне використання маскування, хибних позицій та об’єктів, засобів оптико-електронної протидії, РЕБ і ППО.

Радіоелектронний захист має забезпечувати стійке функціонування засобів зв’язку, управління, навігації та передачі даних в умовах радіоелектронного впливу противника. Особливого значення набувають забезпечення електромагнітної сумісності власних засобів РЕБ із системами зв’язку та управління, підвищення їх завадостійкості, а також створення резервних каналів зв’язку та навігації.

Логістичні заходи в межах КСЗ доцільно спрямовувати на безперервне матеріально-технічне забезпечення артилерійських підрозділів. До них належать розосереджене розміщення запасів ракет, боєприпасів, пального та інших матеріальних засобів, приховане їх підвезення, використання основних і запасних маршрутів, а також своєчасна медична евакуація поранених та евакуація пошкодженого озброєння і військової техніки.

Розосередження запасів має зменшувати ймовірність одночасної втрати значної кількості матеріальних засобів унаслідок одного вогневого впливу та забезпечувати необхідний рівень автономності підрозділів. Організація підвезення повинна враховувати необхідність мінімізації демаскувальних ознак транспортних засобів і маршрутів руху, а евакуації – забезпечувати своєчасне вивезення поранених та виведення пошкоджених зразків ОВТ із небезпечних районів та їх подальше відновлення.

Таким чином, комплексна система захисту артилерійських підрозділів повинна являти собою не просту сукупність окремих заходів, а взаємоузгоджену систему організаційних, тактичних, технічних і логістичних заходів, об’єднаних єдиними процесами управління, інформаційного обміну та реагування на загрози. Її функціонування має забезпечувати зниження ймовірності виявлення та ураження підрозділів, зменшення можливих втрат, збереження їх боєздатності та спроможності безперервно виконувати бойові завдання.

Водночас практична реалізація запропонованого підходу потребує вирішення низки проблемних питань, зокрема забезпечення електромагнітної сумісності засобів РЕБ із системами зв'язку та бойового управління, інтеграції різнорідних засобів виявлення, оповіщення та протидії, а також скорочення часу реагування на виявлені загрози. Перспективним напрямом подальших досліджень є обґрунтування структури та алгоритмів функціонування КСЗ, розроблення методичного апарату оцінювання її ефективності, а також автоматизація процесів розподілу загроз між засобами захисту з урахуванням умов обстановки та можливостей противника.

Варава В. В.
Науково-дослідний центр ракетних військ і артилерії

РЕКОМЕНДАЦІЇ ЩОДО ФУНКЦІОНУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ ПІД ЧАС ПЛАНУВАННЯ ТА ВЕДЕННЯ БОЙОВИХ ДІЙ

Досвід ведення бойових дій під час російсько-української війни засвідчив суттєву зміну умов бойового застосування артилерійських підрозділів, зумовлену широким використанням противником безпілотних літальних апаратів (далі – БпЛА), високоточної зброї, засобів радіоелектронної боротьби (далі – РЕБ) та технічної розвідки. Постійне вдосконалення засобів розвідки та ураження, скорочення часу від виявлення об'єкта до завдання по ньому удару значно підвищують вразливість особового складу, озброєння і військової техніки (далі – ОВТ), пунктів управління та підрозділів забезпечення артилерійських підрозділів. За таких умов застосування окремих, неузгоджених між собою заходів захисту не забезпечує належного рівня живучості та збереження боєздатності артилерійських підрозділів, що зумовлює необхідність комплексного підходу до організації їх захисту під час планування та ведення бойових дій.

Комплексну систему захисту (далі – КСЗ) артилерійських підрозділів доцільно розглядати як сукупність взаємопов'язаних заходів, спрямованих на зниження ймовірності виявлення й ураження, зменшення наслідків вогневого впливу противника, збереження стійкості управління та безперервності виконання бойових завдань. Її функціонування має забезпечуватися

узгодженим застосуванням організаційних, тактичних, технічних і логістичних заходів. Такий поділ є функціональним: окремі заходи можуть одночасно належати до кількох груп.

Організаційні заходи рекомендується спрямовувати на узгоджене планування захисту, організацію взаємодії, підтримання ситуаційної обізнаності та контроль виконання прийнятих рішень. Планування захисту необхідно здійснювати одночасно з плануванням бойового застосування артилерії з урахуванням характеру загроз, наявних ресурсів, захисних властивостей місцевості й можливостей суміжних підрозділів. У відповідних документах доцільно визначати відповідальних виконавців, порядок взаємодії та критерії готовності до виконання заходів захисту.

Координацію рекомендується забезпечувати шляхом узгодження дій із підрозділами протиповітряної оборони (далі – ППО), РЕБ, інженерного забезпечення та загальновійськовими підрозділами. Особливого значення набуває електромагнітна сумісність власних засобів зв’язку, управління і РЕБ, оскільки неузгоджене застосування технічних засобів може обмежувати функціонування власних систем. Організація інформаційного обміну й оповіщення має передбачати своєчасне доведення достовірних відомостей про загрози та наявність резервних способів передавання інформації.

Контроль виконання організаційних заходів доцільно здійснювати за показниками повноти реалізації запланованих рішень, своєчасності оповіщення, готовності сил і засобів та стійкості управління. Результати перевірок слід використовувати для уточнення планів захисту й усунення виявлених недоліків.

Тактичні заходи рекомендується спрямовувати на зниження помітності та вразливості підрозділів, використання захисних властивостей місцевості, інженерну підтримку та введення противника в оману. Їх зміст необхідно визначати відповідно до характеру бойових завдань, умов місцевості та встановлених вимог щодо прихованості дій.

У межах інженерної підтримки доцільно передбачати інженерну розвідку місцевості, оцінювання захисних і маскувальних властивостей районів, фортифікаційне обладнання місць розташування особового складу, ОВТ, пунктів управління й матеріальних засобів. Обсяг і вид захисних споруд слід обґрунтовувати очікуваними загрозами та фактичними можливостями

підрозділів. Наявність фортифікаційних споруд зменшує вразливість, проте не забезпечує абсолютного захисту від усіх засобів ураження.

Для зменшення демаскувальних ознак рекомендується комплексно використовувати маскувальні властивості місцевості, штатні засоби маскування, фарбувати ОВТ під фон місцевості та дотримання маскувальної дисципліни. Ефективність маскування необхідно оцінювати з урахуванням можливостей оптичних, тепловізійних і радіолокаційних засобів спостереження противника: один спосіб маскування не забезпечує однакового ефекту в усіх діапазонах.

Заходи введення противника в оману доцільно розглядати як складову загального задуму захисту, узгоджену з іншими діями підрозділів. Їх реалізація має бути підпорядкована зменшенню достовірності розвідувальної інформації противника без створення додаткових ризиків для власних сил. Відповідні заходи повинні плануватися й контролюватися уповноваженими органами управління.

Технічні заходи рекомендується спрямовувати на своєчасне виявлення загроз, підвищення захищеності ОВТ та стійкості систем управління, зв’язку й навігації. Основними функціональними напрямами є протидія БпЛА, зниження вразливості від високоточної зброї та радіоелектронний захист.

Протидію БпЛА доцільно забезпечувати поєднанням доступних засобів виявлення, оповіщення, захисту та взаємодії з підрозділами ППО і РЕБ. Під час визначення необхідних технічних засобів слід ураховувати типи повітряних загроз, можливості власних систем і обмеження їх застосування. Зокрема, ефективність радіоелектронного впливу залежить від способів керування та навігації конкретного БпЛА; тому такі засоби не можуть розглядатися як універсальний захист.

Для зниження наслідків ураження доцільно передбачати застосування захисних конструкцій та інженерних укриттів із перевіреними характеристиками. Вибір конструкцій повинен враховувати їхню сумісність з експлуатаційними вимогами ОВТ і безпекою особового складу. Захист від високоточної зброї необхідно обґрунтовувати відповідно до характеру загрози й принципу наведення засобу ураження, уникаючи припущення про універсальну ефективність окремих технічних рішень.

Радіоелектронний захист рекомендується забезпечувати підвищенням завадостійкості засобів зв’язку та навігації, захистом інформаційного обміну, використанням резервних засобів управління та контролем електромагнітної

сумісності. Результатом реалізації зазначених заходів має бути зниження ризику втрати керованості підрозділів за умов радіоелектронного впливу.

Логістичні заходи в КСЗ доцільно спрямовувати не лише на постачання ресурсів, а насамперед на зниження вразливості системи забезпечення та підтримання її працездатності за умов втрат і порушення комунікацій. До основних напрямів належать захист запасів матеріальних засобів, забезпечення безперервності постачання, відновлення ОВТ та організація евакуації.

Збереження матеріальних запасів рекомендується забезпечувати шляхом раціонального розподілу ресурсів, застосування захищених місць зберігання, обліку наявності й контролю умов зберігання. Розосередження запасів доцільно застосовувати з урахуванням потреб підрозділів, транспортних можливостей та вимог безпеки. Надмірне розосередження без належної координації може ускладнювати забезпечення, тому відповідні рішення потребують обґрунтування.

Стійкість постачання доцільно підвищувати завдяки плануванню резервних способів забезпечення, узгодженню потреб із фактичними запасами та підтриманню готовності транспортних засобів. Відновлення боєздатності ОВТ має передбачати своєчасне технічне обслуговування, діагностування, ремонт і організацію евакуації несправних або пошкоджених зразків з урахуванням безпеки персоналу.

Оцінювання логістичних заходів доцільно здійснювати за здатністю підтримувати забезпечення підрозділів, зберігати критично важливі ресурси та відновлювати працездатність техніки. Конкретні нормативні значення показників мають визначатися на підставі відповідних документів і фактичних даних.

Отже, функціонування КСЗ артилерійських підрозділів потребує не механічного поєднання окремих засобів захисту, а їх узгодженого планування, застосування та контролю. Організаційні заходи створюють основу управління системою; тактичні зменшують помітність і вразливість; технічні підвищують можливості виявлення загроз і стійкість функціонування; логістичні підтримують ресурсну забезпеченість і відновлення підрозділів. Комплексна реалізація цих рекомендацій має сприяти збереженню живучості, боєздатності та безперервності виконання бойових завдань. Кількісне підтвердження результативності потребує окремого оцінювання за визначеними показниками.

Перспективним напрямом подальших досліджень є розроблення методичного підходу до оцінювання ефективності функціонування КСЗ артилерійських підрозділів.

Храпач Д. О.
Науково-дослідний центр ракетних військ і артилерії

ПРОТИДІЯ БЕЗПІЛОТНИМ АВІАЦІЙНИМ КОМПЛЕКСАМ ПРОТИВНИКА

Досвід сучасних бойових дій зобов'язує шукати шляхи вирішення питання боротьби з БпЛА противника, що вимагає комплексної інтеграції розвідки, радіоелектронної боротьби та засобів вогневого ураження.

Для виявлення безпілотних авіаційним системам противника необхідно:

застосовувати РЛС, які здатні засікати малорозмірні об'єкти з низькою ефективною площею розсіювання;

використовувати камери видимого спектра та тепловізорів для верифікації цілей у складних умовах;

розгортати мережі акустичних датчиків для фіксації специфічного шуму двигунів БпЛА на малих висотах;

перехоплювати сигнали керування та телеметрії для визначення координат БпЛА та оператора, який ними керує.

Засоби радіоелектронної боротьби застосовувуються для:

придушення каналів керування зв'язку між БпЛА та наземною станцією керування шляхом постановки завад на робочих частотах;

супутникового спуфінгу та підміни навігації – спотворення сигналів GPS/GLONASS/Galileo для дезорієнтації БпЛА або примусової зміни його маршруту.

Також для боротьби з безпілотними авіаційними системами противника потрібно застосовувати вогневі засоби ураження, а саме :

малокаліберну зенітну артилерію – швидкострільні гармати із програмованими боєприпасами дистанційного підриву (шрапнельні снаряди);

стрілецьку зброю та турелі – оснащати позиції кулеметами на мобільних платформах, підсилених тепловізійними прицілами та лазерними далекомірами;

ракетні комплекси ППО – легкі ракетні системи ближньої дії виключно для ураження висотних або швидкісних ударних БпЛА.

Таким чином, застосування технічних засобів розвідки, радіоелектронної боротьби та вогневого ураження допоможе підрозділам вирішувати питання протидії БпЛА противника.

Балакірева С. М., канд. техн. наук, ст. досл.
Ковзало І. Г.
Додурич О. Б.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ ПІДВИЩЕННЯ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ ПРО ПОВІТРЯНУ ОБСТАНОВКУ В ПРОТИДІЇ УДАРНИМ БЕЗПІЛОТНИМ АПАРАТАМ

В умовах масованого застосування противником ударних безпілотних літальних апаратів (БпЛА) типу «Shahed», ракет і керованих авіабомб швидкість обробки даних про повітряну обстановку на пунктах управління Повітряних Сил забезпечують цифрові засоби ситуаційної обізнаності (СО). Ці засоби спрощують роботу офіцера бойового управління, який у реальному часі сприймає, розуміє та прогнозує повітряну обстановку за даними радіолокаційних станцій (РЛС), постів спостереження та акустичних датчиків. В сучасній високоінтенсивній війні найбільш розповсюдженими та корисними у застосуванні на теперішній час при виконанні бойових завдань стали наступні розробки.

Delta – національна система СО, створена за стандартами НАТО. Модуль Delta Monitor відображає на електронній карті рух повітряних цілей, а інші модулі забезпечують аналіз відеопотоків та розподіл цілей. Система дає наскрізну картину обстановки для всіх рівнів командування, проте залежить від стійкості зв’язку та кіберзахисту.

Пункт управління тактичної групи протиповітряної оборони “Кречет” на броньованому автомобілі, за даними розробника, об’єднує до п’яти РЛС і до десяти мобільних вогневих груп та супроводжує до 250 цілей. Перевагою є автономність, обмеженням – прив’язка до броньованого носія.

Мобільний застосунок “Віраж-ППО” використовується на робочому місці офіцера бойового управління для отримання даних від інформаційно-комунікаційної системи “Віраж-Планшет” і безпосередньо від РЛС, та передачі даних для наведення БпЛА-перехоплювачів, за допомогою захищеного VPN-тунелем зв’язку.

Інформаційна система оповіщення “Графіт” доводить попередження про наближення БпЛА та керованих авіабомб до окремих військовослужбовців,

розширюючи СО поза межі стаціонарного командного пункту, але виконує лише попереджувальну функцію.

Тактична система командування та управління Sky Map (Sky Fortress), поєднує дані РЛС із мережею понад 14 тисяч акустичних датчиків, що дає змогу виявляти малорозмірні БпЛА на малих висотах і визначати їхні координати методом тріангуляції. Ефективність системи залежить від густоти мережі датчиків.

Отже, системи Delta та Sky Map формують наскрізну картину обстановки, "Віраж-ППО" забезпечує обробку радіолокаційної інформації на командному пункті, "Кречет" – автономне управління тактичною групою протиповітряної оборони, а "Графіт" відповідно – індивідуальне оповіщення. Жодна з систем окремо не забезпечує повного циклу підтримки СО, тому максимальний ефект досягається за рахунок взаємодоповнювальної інтеграції цих систем на всіх рівнях управління. Крім того, не вирішеними залишаються питання повної інтеграції систем, розрив між швидкістю обробки радіолокаційної інформації на командному пункті і доведенням рішень командирів до виконавців, а також обмежене використання штучного інтелекту для підтримки прийняття рішень.

Малишев О. А., канд. техн. наук, доц.
Арасланов М. Р., канд. техн. наук, ст. наук. співроб.
Примак Р. Є.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ОГЛЯДОВИХ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ L-ДІАПАЗОНУ ЗА РАХУНОК УДОСКОНАЛЕННЯ ДІАГРАМИ СПРЯМОВАНОСТІ АНТЕНИ

Одним із характерних чинників сучасної російсько-української війни є широке застосування безпілотних літальних апаратів (БпЛА) різних класів. Частина таких БпЛА використовує сигнали глобальних навігаційних супутникових систем, зокрема GPS та ГЛОНАСС. Одним із заходів протидії є застосування засобів радіоелектронної боротьби (РЕБ), які можуть створювати навмисні радіозавади приймачам супутникової навігації у відповідних частотних смугах L-діапазону.

У L-діапазоні також працюють деякі оглядові радіолокаційні станції (РЛС) Сил оборони України. За наявності спектрального перекриття або недостатньої частотної розв’язки випромінювання засобів РЕБ може впливати на приймальні тракти РЛС. Це знижує відношення сигнал/(шум + завада), ускладнюючи виявлення та супроводження повітряних цілей.

Для зменшення впливу засобів РЕБ на РЛС застосовують організаційні та технічні заходи. До організаційних належить раціональний вибір позиції РЛС, щоб в основному секторі відповідальності не знаходилися засоби РЕБ. Однак цього може бути недостатньо, якщо потужна завада надходить до приймача РЛС через бічні або задні пелюстки діаграми спрямованості антени (ДСА) та істотно знижує відношення сигнал/(шум + завада).

Отже, актуальним є завдання підвищення захищеності оглядових РЛС від активних шумових завад (АШЗ), які можуть створюватися засобами РЕБ своїх підрозділів.

Відомо, що для захисту РЛС від активних завад застосовуються різні технічні способи. Серед них окреме місце займає просторова селекція, яка базується на використанні розбіжностей між напрямками приходу ехосигналів та активної завади.

Одним з варіантів реалізації просторової селекції є зниження рівня бічних пелюсток ДСА шляхом корекції її форми. Зробити це можна завдяки зміні амплітудно-фазового розподілу (АФР) поля на апертурі антени.

За умови точного фазування антенної решітки рівень бічних пелюсток значною мірою визначається амплітудним розподілом поля на апертурі. В існуючих оглядових РЛС РТВ зазвичай використовуються такі його види: рівномірний, косинусний, “косинус на п’єдесталі”.

Для таких розподілів існує компроміс між шириною головної пелюстки та рівнем бічних пелюсток ДСА: зниження рівня бічних пелюсток, як правило, призводить до розширення головної пелюстки, тоді як її звуження супроводжується підвищенням рівня бічних пелюсток.

Розширення головної пелюстки ДСА може погіршувати кутову точність та роздільну здатність РЛС за кутовою координатою. Підвищення рівня бічних пелюсток, у свою чергу, збільшує чутливість РЛС до активних завад, що надходять з бічних напрямків.

Відомо, що для лінійних та плоских антенних решіток може бути використаний дольф-чебишевський амплітудний розподіл, який забезпечує

формування оптимальної діаграми спрямованості з рівновисокими бічними пелюстками заданого рівня. Під оптимальною розуміється така ДСА, у якої при заданому рівні бічних пелюсток ширина головної пелюстки є мінімально можливою. При цьому значення амплітудного розподілу поля на розкриві антени визначаються на основі поліномів Чебишева.

Запропоновано для РЛС L-діапазону типу "СНОВ", антенна система якої виконана у вигляді циліндричної цифрової фазованої антенної решітки, застосувати чебишевський принцип синтезу комплексних вагових коефіцієнтів на елементах кільцевої решітки з урахуванням їх розташування в азимутальній площині.

Це дозволить сформувати ДСА зі зниженим рівнем бічних пелюсток, зменшити вплив активних шумових завад, що надходять через бічні пелюстки, та підвищити завадостійкість станції за прийнятного співвідношення між рівнем бічних пелюсток, шириною головної пелюстки та роздільною здатністю за азимутом.

Королюк Н. О. канд. техн. наук, доц.
Бутенко А. Ю.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

АНАЛІЗ МЕТОДІВ УПРАВЛІННЯ ВОГНЕВИМИ ЗАСОБАМИ ПІДРОЗДІЛІВ ЗЕНІТНИХ РАКЕТНИХ ВІЙСЬК НА ОСНОВІ ПОРІВНЯННЯ БАГАТОКРИТЕРІЙНИХ АЛЬТЕРНАТИВ

Досвід війни свідчить, що противник зосереджує основні зусилля на руйнуванні ключових об'єктів державного управління, військового командування, енергетичної та транспортної інфраструктури. Активне використання та постійне вдосконалення засобів повітряного нападу забезпечує вирішення противником завдання стратегічного масштабу, що підкреслює важливість побудови ефективної протиповітряної та протиракетної оборони як основного стримуючого фактора.

Автоматизація процесу прийняття рішень на управління вогневими засобами підрозділів Повітряних Сил можлива шляхом створення нових та вдосконалення існуючих методів цілерозподілу на основі сучасних інформаційних технологій, зокрема – інтелектуальних систем підтримки

прийняття рішень. Інтелектуалізація передбачає застосування знань, вмінь осіб, що приймають рішення, комплексом засобів автоматизації при вирішенні завдань управління в умовах інтенсивних бойових дій.

У зв’язку зі зростанням вимог до якості управління підрозділами зенітних ракетних військ в умовах ведення війни виникає необхідність у вдосконаленні існуючих алгоритмів управління вогневими засобами на основі прогнозування варіантів розвитку бойової обстановки та тактики повітряного противника.

Пропонується, в умовах інтенсивного нальоту, масованого ракетно-авіаційного удару здійснювати ранжуванні цілей (групи об’єктів локальної системи повітряного базування) із формуванням скалярних або векторних показників узагальнених (потенційних та/або реальних) збитків, яких можна уникнути. Зазначений підхід є особливо важливим під час організації протиповітряної оборони, де просторово-часові обмеження досягають граничних значень, а ціна помилки вимірюється втратою боєздатності техніки та особового складу.

Для вибору оптимального математичного апарату при ранжуванні повітряних цілей проведений аналіз методів прийняття багатокритеріальних рішень, що застосовуються в системах управління засобами протиповітряної оборони. Отже, жоден із комбінаторних підходів не відповідає повною мірою вимогам для вирішення задачі ранжування повітряних цілей автоматизованим методом в умовах масованого ракетно-авіаційного удару.

Метод прямої бальної оцінки та метод зваженої суми критеріїв (WSM) характеризуються високою швидкістю обчислень, проте спрощена лінійна структура не дозволяє коректно опрацьовувати складні, різнорозмірні та взаємозалежні показники збитків, враховувати динамічні параметри цілей. У свою чергу, група методів ELECTRE забезпечує гнучкість розрахунків, але створює неприпустиму затримку в обчислювальному контурі засобів автоматизації через зростання алгоритмічної складності, виникнення часовомістких колізій (циклічних переваг).

Отже, проведений аналіз методів вирішення багатокритеріальних задач підтвердив, що для автоматизованих систем управління підрозділами зенітних ракетних військ в умовах інтенсивного нальоту противника найбільш обґрунтованим є застосування модифікованого методу аналізу ієрархій. На відміну від спрощених лінійних моделей, складних методів групи ELECTRE,

метод аналізу ієрархій забезпечує необхідний баланс між точністю опрацювання взаємозалежних параметрів збитків і швидкістю розрахунків у реальному часі.

Запропонований підхід, що базується на комбінації статичного ранжування цілей локальної системи повітряного базування, дозволяє формувати адаптивний цілерозподіл вогневих засобів, оптимізувати послідовність ураження повітряних об’єктів та мінімізувати потенційні втрати боєздатності підрозділів Повітряних Сил Збройних Сил України в умовах жорстких просторово-часових обмежень.

Королюк Н. О., канд. техн. наук, доц.
Чопенко Я. Р.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба
Луценко А. С.
Харківський національний університет радіоелектроніки

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗПІЗНАВАННЯ ПОВІТРЯНОГО ПРОТИВНИКА В УМОВАХ ВЕДЕННЯ БОЙОВИХ ДІЙ

Повітряні Сили (ПС) Збройних Сил (ЗС) України здійснюють радіолокаційний контроль повітряного простору в межах чергового радіолокаційного поля та диспетчерський контроль на командних пунктах за повітряним рухом на всій території України.

Радіолокаційний контроль полягає в спостереженні за допомогою радіолокаційних станцій за польотами повітряних цілей (ПЦ) і визначенні їх державної належності по системі радіолокаційного впізнавання. Контроль повітряного простору вимагає детального знання обстановки для своєчасного виявлення порушень та потенційних загроз, на підставі обробки усієї інформації, що поступає до розвідувально-інформаційного центру. При цьому одним з основних завдань чергових сил з протиповітряної оборони є відбиття ударів повітряного противника. Це передбачає розпізнавання ПЦ за відповідними класифікаційними ознаками, тобто проведення класифікації повітряних об’єктів (ПО). Об’єктами класифікації при вирішенні задач

контролю повітряного простору є літальні апарати, гідрометеори, аномальні явища в атмосфері, тощо. Класифікація ПО у ПС ЗС України здійснюється у процесі бойової роботи на розвідувально-інформаційному центрі командних пунктів.

Результатом розпізнавання типів ПЦ у повітрі є присвоєння відповідним цілям індексів належності (категорій), тобто класифікація ПЦ.

Досвід повномасштабної збройної агресії проти України свідчить, що повітряний простір став ключовою ареною збройної боротьби, де ворог постійно удосконалює тактику повітряних нападів. Сучасні повітряні атаки характеризуються масованістю, застосуванням комбінованих ударів, активним використанням засобів радіоелектронної боротьби та маскування, а також масовим запуском фальш-цілей.

В умовах інтенсивного бойового чергування радіотехнічні війська та бойові обслуги командних пунктів ПС ЗС України змушені приймати рішення дуже швидко – в умовах жорсткого дефіциту часу, перевантаження інформаційних каналів, а також наявності нечітких, суперечливих чи фрагментарних даних від радіолокаційних станцій через активну протидію противника. Це призводить до зростання навантаження на бойову обслугу, що підвищує ризики помилок через людський фактор та свідчить про нагальну потребу створення та впровадження інтелектуальних систем підтримки прийняття рішень, здатних автоматизовано класифікувати ПО в умовах невизначеності.

Класифікація є інформаційним процесом, що реалізовується деяким перетворювачем інформації (інтелектуальним інформаційним каналом, системою розпізнавання), що має вхід і вихід. На вхід системи подається інформація про те, які ознаки мають ПЦ. На виході системи відображається інформація про те, до яких класів (узагальненим образам) віднесені розпізнані об'єкти.

Розпізнаванням є перетворення вхідної інформації, у вихідну, таку, що є висновком про те, до якого класу відноситься дана ситуація.

Але своєчасність розпізнавання ситуацій у повітрі для прийняття рішення залежить від низки факторів, оскільки організація контролю використання повітряного простору України є складним процесом, що має суттєві недоліки, які знижують її ефективність та підвищують небезпеку у повітрі.

Створення та впровадження удосконаленої системи розпізнавання класів ПО на основі нечіткої та неповної інформації дозволить підвищити ступінь

автоматизації процесів управління на командних пунктах ПС ЗС України, забезпечити своєчасне виявлення загроз та підвищити загальну ефективність відбиття повітряних ударів противника.

Стеценко С. М.
Дорохов О. М.
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

ДОСВІД ПІДГОТОВКИ ФАХІВЦІВ АРТИЛЕРИСТІВ ІЗ ПРОТИДІЇ БЕЗПІЛОТНИМ АВІАЦІЙНИМ КОМПЛЕКСАМ ПРОТИВНИКА

Забезпечення живучості артилерійських підрозділів на сучасному етапі збройної боротьби вимагає кардинального перегляду підходів до організації оборони вогневих позицій від повітряних загроз. Стрімкий розвиток безпілотних авіаційних систем, які поєднують у собі функції глибокої розвідки, коригування вогню та безпосереднього ударного ураження, перетворив небо на простір постійної небезпеки. Раніше артилерія могла почуватися відносно захищеною на значній відстані від переднього краю, розгортаючи класичні вогневі позиції та зосереджуючись виключно на виконанні вогневих завдань.

Сьогодні ж кожен артилерійський розрахунок стає першочерговою ціллю для ворожих розвідувальних крил та масованих роїв ударних дронів, які здатні діяти автономно та знаходити замасковану техніку за тепловим або радіовипромінюванням. Це визначає гостру потребу в трансформації всієї системи підготовки фахівців, де навички протидії безпілотним комплексам мають стати не додатковим елементом навчання, а базовим компонентом виживання та бойової ефективності. Проблема полягає в тому, що традиційні методи протиповітряної оборони великого радіуса дії часто виявляються безсилими проти малорозмірних, низьколітаючих та високоманеврених засобів, що змушує артилеристів брати справу захисту у власні руки.

Метою цієї доповіді є комплексний аналіз практичного досвіду впровадження нових програм підготовки особового складу, які дозволяють поєднати виконання основних вогневих завдань із ефективною самообороною та збереженням людських життів та матеріальної частини.

Аналіз реальних бойових дій показує, що тривале перебування артилерійського підрозділу на одній точці є гарантованим шляхом до його знищення, оскільки час від моменту виявлення гармати ворожим безпілотником до прильоту першого снаряда чи ударного дрона скоротився до кількох хвилин. У зв'язку з цим першочерговим елементом оновленої підготовки фахівців є перехід до концепції граничної мобільності, коли розрахунки діють за принципом швидкого виходу на позицію, швидкого виконання вогневого завдання, бажано до чотирьох хвилин та негайного залишення вогневої позиції. Навчання особового складу тепер будується навколо жорстких часових нормативів, де кожна секунда зволікання при згортанні системи безпосередньо впливає на виживання людей. Розрахунки самохідних та причіпних гармат тренуються діяти в умовах постійного дефіциту часу, при цьому велика увага приділяється розосередженню техніки, адже скупчення навіть кількох машин стає занадто привабливою ціллю для ворога. Крім зміни тактики маневру, критично важливим аспектом підготовки стало освоєння засобів радіоелектронної боротьби безпосередньо на рівні кожної гармати чи автомобіля постачання. Сучасний артилерист повинен не лише досконало знати будову своєї гармати, а й уміти правильно розгортати та експлуатувати окопні станції перешкод, визначати їх ефективну зону дії та вчасно перемикати частоти для придушення каналів керування ворожих дронів.

Важливим елементом підготовки є також навички візуального та акустичного спостереження за повітрям, оскільки в умовах щільної роботи засобів радіоелектронного придушення технічні системи виявлення можуть давати збої або демаскувати власну позицію. Розрахунки навчаються розпізнавати специфічні звуки наближення різних типів безпілотних апаратів, оцінювати напрямок їхнього руху та миттєво подавати сигнали тривоги для приведення в готовність засобів вогневого прикриття. Вогнева підготовка артилеристів зазнала суттєвих змін через необхідність створення штатних або позаштатних мобільних вогневих груп усередині самих батарей. Тепер кожен військовослужбовець проходить інтенсивний курс стрільби по рухомих малорозмірних цілях з використанням гладкоствольної мисливської зброї, яка довела свою високу ефективність проти низьколітаючих дронів-камікадзе на коротких відстанях. Також розрахунки відпрацьовують групове ведення вогню з автоматичної зброї та кулеметів на спеціально обладнаних турелях, що

дозволяє створювати щільну стіну вогню на шляху підльоту повітряної загрози. Окремим і надзвичайно складним напрямком є психологічна підготовка особового складу, адже постійне перебування під загрозою атаки з неба створює колосальний тиск на психіку солдатів. Навчальні центри впроваджують у програми елементи стрес-тестування, коли під час виконання навчально-бойових завдань над головами розрахунків постійно кружляють дрони, імітуючи скидання вибухових пристроїв та звукові ефекти реального бою. Це дозволяє подолати первинний страх, навчити людей не панікувати при появі повітряної цілі, а чітко виконувати алгоритм дій із маскування, укриття або знищення об'єкта. Інженерне обладнання позицій також отримало абсолютно нове наповнення в процесі навчання, оскільки класичні бліндажі та окопи тепер обов'язково мають обладнуватися антидроновими сітками, екранами та спеціальними навісами, які здатні затримати або передчасно підривати кумулятивну бойову частину ворожого безпілотника. Фахівці вчяться створювати складні системи хибних позицій та макетів техніки, які повторюють не лише візуальний вигляд реальної гармати, а й її теплове випромінювання за допомогою спеціальних хімічних чи електричних підігрівачів, що дозволяє вводити противника в оману та виснажувати його запаси безпілотних засобів ураження. Командний склад підрозділів додатково навчається здійснювати безперервний моніторинг радіоелектронної обстановки та координувати дії своїх підлеглих із сусідніми підрозділами протиповітряної оборони

Впровадження передових методик підготовки та інтеграція засобів протидії безпілотним авіаційним системам безпосередньо у повсякденну діяльність артилерійських підрозділів є єдиним дієвим способом збереження боєздатності підрозділу у сучасній війні високої інтенсивності. Досвід показує, що успіх виконання вогневого завдання сьогодні однаково залежить як від точності стрільби по цілях, так і від здатності захистити власну вогневу позицію від ударів з повітря. Перетворення навчальних програм, яка базується на розвитку мобільності, освоєнні засобів радіоелектронної боротьби, веденні щільного вогню та інженерного обладнання позицій, дозволяє значно знизити рівень втрат серед особового складу та техніки. Подальший розвиток артилерійської науки та практики підготовки кадрів має йти шляхом ще тіснішої інтеграції технологічних засобів захисту та автоматизації процесів виявлення повітряних загроз, щоб випереджати стрімку еволюцію безпілотних систем противника та забезпечувати безумовне вогневе домінування на полі бою.

Кошкін М. А.
Телегін В. В.
Першин О. В.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

РОЗРОБКА МЕРЕЖЕВОЇ СИСТЕМИ ІМІТАЦІЇ ДЖЕРЕЛА РАДІОЛОКАЦІЙНИХ ПОВІДОМЛЕНЬ ІЗ ВИКОРИСТАННЯМ ПРОТОКОЛУ ASTERIX

Підготовка осіб бойової обслуги засобів оброблення радіолокаційної інформації (РЛІ) потребує відпрацювання дій за різною повітряною обстановкою. Використання реальних радіолокаційних станцій (РЛС) для проведення таких занять не завжди є доступним, обмежене ресурсом станції, потребою виходу на випромінювання та залежить від наявності в зоні огляду відповідних повітряних об'єктів, а повторити ту саму обстановку для кожної обслуги в реальних умовах неможливо. Одним із шляхів розв'язання цієї проблеми є розроблення програмних засобів імітації джерел РЛІ, які формують інформаційні повідомлення відповідно до стандартизованих протоколів обміну даними.

Для забезпечення сумісності з різними засобами оброблення РЛІ доцільно використовувати протокол ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange), який визначає структуру та правила кодування повідомлень спостереження. Застосування цього протоколу дає змогу створювати програмні джерела даних, здатні взаємодіяти з інформаційними системами, що підтримують відповідні категорії ASTERIX.

Мета роботи – розробка мережевої системи імітації джерела радіолокаційних повідомлень, яка формує керований потік повідомлень у форматі ASTERIX для навчання осіб бойової обслуги.

В імітаторі реалізовано певні категорії ASTERIX для передачі повідомлень про повітряні об’єкти (ПО) від окремого радіолокатора та службові повідомлення про його роботу. Сформовані блоки даних передаються в локальну мережу за протоколом UDP (User Datagram Protocol).

Перед початком роботи в систему вводяться вхідні дані: кількість ПО, їхні траєкторії, швидкості та висоти. Це дає змогу відтворювати типові атаки: одночасний підліт великої кількості ПО з кількох напрямків, політ на малих

висотах і малих швидкостях, зміну курсу для обходу районів, прикритих засобами протиповітряної оборони, поступове нарощування кількості ПО протягом тривалого часу. Параметри можна змінювати, а імітацію — запускати повторно, тому кожна така ситуація відтворюється стільки разів, скільки потрібно.

Отже, розроблена система призначена для навчання осіб бойової обслуги та дає змогу відтворювати задану повітряну обстановку, у тому числі масовані нальоти ПО, необхідну кількість разів за однакових умов, без залучення РЛС, задіяних у бойовій роботі. Оскільки дані передаються у стандартному форматі ASTERIX через протокол UDP, система сумісна з іншими засобами, що підтримують відповідні категорії ASTERIX. Напрямами подальшої роботи є моделювання хибних відміток і пропусків виявлення, характерних для малорозмірних цілей.

Мирончук Ю. А., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

ФОРМУВАННЯ ВИМОГ ДО БЕЗПІЛОТНИХ ПЕРЕХОПЛЮВАЧІВ РЕАКТИВНИХ УДАРНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРОТИВНИКА

В умовах бойового протистояння розвиток безпілотної авіації у прискореному темпі проходить ті ж самі історичні етапи, які пройшла пілотована авіація – від перших дерев’яних аеропланів з перкалевою обшивкою до сучасних реактивних надзвукових винищувачів 5-го покоління. Зі сторони противника відбувся закономірний перехід від застосування тихохідних радіокерованих гвинтомоторних ударних БпЛА дальньої дії до застосування швидкісних БпЛА з турбореактивними двигунами, які виконують польотні завдання під керуванням програмного забезпечення бортових комп’ютерів, без потреби підтримання зв’язку з наземними станціями керування.

Для системи протиповітряної оборони (далі – ППО) швидкохідність і висотність таких цілей обнулила ефективність традиційних методів боротьби з ними – кулеметного вогню мобільних вогневих груп та перехоплення радіокерованими безпілотними перехоплювачами. Основна причина – швидкість реакції людини-оператора недостатня для своєчасного реагування на

зміни параметрів польоту таких цілей. Відповідно, постала гостроактуальна потреба розроблення методів боротьби з реактивними БпЛА противника, які б відповідали їх швидкісним і висотним характеристикам. Застосування високовартісної ракетної зброї економічно не оправдане, особливо в умовах затяжної війни на виснаження. Тому пошук нових методів протиповітряної оборони повинен бути спрямований на застосування безпілотних перехоплювачів. Очевидно, що для забезпечення належної швидкохідності такі безпілотні перехоплювачі повинні бути споряджені турбореактивними або ракетними двигунами. Важливо наголосити, що створення таких перехоплювачів не повинне проводитись у режимі «самостійної» розробки. Вони від самого початку повинні створюватись як повноцінна складова частина, тісно інтегрована до єдиної системи ППО й здатна виконувати перехоплення цілі у повністю автоматичному режимі.

Система ППО повинна забезпечувати:

- своєчасне виявлення повітряної цілі на дальніх підступах, її ідентифікацію та встановлення основних параметрів руху (координати, курс, швидкість, висота, тип цілі);

- автоматичне виконання оцінювальних розрахунків щодо можливості перехоплення та видачу команди на старт того перехоплювача, територіальне розташування стартової позиції якого дозволяє здійснити успішний маневр перехоплення;

- наведення по радіоканалу перехоплювача у розрахункову зону зустрічі з ціллю до моменту захоплення цілі бортовою системою донаведення перехоплювача (оскільки перехоплення проводиться на віддаленні від лінії бойового зіткнення, завади від засобів РЕБ можна вважати відсутніми).

Масо-габаритні параметри та енергоозброєність малих безпілотних перехоплювачів не дозволяють розміщувати на їх борту радіолокаційне обладнання. Тому бортова система донаведення перехоплювача для виявлення і захоплення цілі може застосовувати тільки відеокамери різних спектральних діапазонів. Після відеозахоплення цілі перехоплювач повинен переходити у автономний режим її атаки. Враховуючи швидкохідність цілі й перехоплювача, обмеженість бортового енергоресурсу перехоплювача та потребу знищення цілі в найкоротший час, система наведення повинна забезпечувати перехоплення і методом “паралельного зближення” – рис. 1.

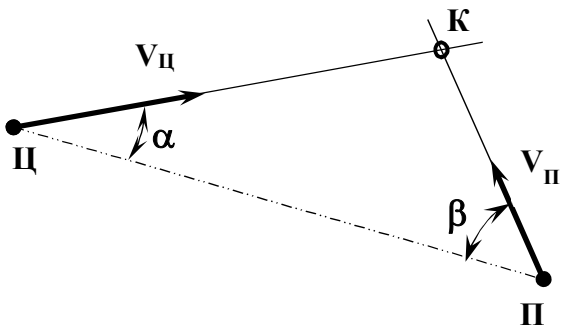


Рис. 1. Траєкторії перехоплювача й цілі при перехопленні методом “паралельного зближення”
Ц – позиція повітряної цілі.
П – позиція перехоплювача.
К – розрахункова точка контакту перехоплювача зціллю.

Розрахунок маневру перехоплення методом паралельного зближення вимагає розв’язку системи рівнянь

$$\begin{cases} V_{Ц} \cdot Sin(\alpha) = V_{П} \cdot Sin(\beta) \\ \tau \cdot \left(V_{Ц} \cdot Cos(\alpha) + V_{П} \cdot Cos(\beta)\right) = \left|ПЦ\right| \\ \left|ПК\right| \le R_{Д} \end{cases}$$

де: Ц – поточні координати цілі;
П – поточні координати перехоплювача;
К – координати розрахункової точки контакту;
$V_{Ц}$ - вектор швидкості цілі;
α - напрям польоту цілі;
$V_{П}$ - вектор швидкості перехоплювача;
β - напрям польоту перехоплювача;
τ - тривалість перехоплення;
$R_{Д}$ - дальність польоту перехоплювача.

На початковому етапі наведення інформація про поточні параметри руху цілі отримується засобами системи ППО і передається на борт перехоплювача. На кінцевому етапі, після захоплення цілі бортовою відеосистемою перехоплювача, інформація про параметри руху цілі повинна отримуватись повністю на основі аналізу бортових сенсорів перехоплювача, без потреби зв’язку з наземними засобами системи ППО.

Для розрахунку параметрів траєкторії маневру перехоплення математичні алгоритми бортової обчислювальної системи перехоплювача повинні на основі даних бортових сенсорів, без використання супутникових навігаційних систем, уміти:

- будувати поточну траєкторію польоту перехоплювача;
- будувати поточну траєкторію польоту цілі з опорою на поточну траєкторію польоту перехоплювача;
- на основі аналізу взаємної конфігурації поточних траєкторій вираховувати оптимальну траєкторію подальшого руху перехоплювача та видавати відповідні команди для органів керування перехоплювачем;
- приймати рішення про момент активації бойової частини.

Задача побудови поточної траєкторії перехоплювача може бути вирішена числовим інтегруванням по часу миттєвих значень вектору повітряної швидкості перехоплювача. Миттєві значення величини і напряму вектору вимірюються сенсором повітряної швидкості та магнітометром через проміжки часу, задані таймером.

Для побудови траєкторії цілі необхідно знати миттєві значення пеленгів на ціль та відстаней до цілі, виміряних у ті ж миті часу, що й значення величини і напряму вектору руху перехоплювача. Для визначення пеленгу достатньо на відеоматриці визначити координати тих пікселів, на які потрапляє зображення цілі. Технічно значно складнішою є задача визначення відстані від цілі. Для її вирішення у ряді публікацій пропонується досить широкий набір різноманітних методів аналізу зображень – отриманих як монокулярним, так і бінокулярним способами. Для технічної реалізації більш надійним і ефективним є застосування бінокулярних відеосистем, які дозволяють з високою точністю визначати відстані до об’єктів, які знаходяться на ближніх дистанціях. На дальніх дистанціях точність бінокулярних методів падає до співставимої з точністю монокулярних методів.

На дальніх дистанціях існує проблема відеозахоплення об’єкту. Для надійного утримання захопленого об’єкту необхідно щоб його проекція на поверхню відеоматриці мала достатньо великі розміри (у кількості пікселів). При малій кількості пікселів зображення об’єкту нечітке, системи комп’ютерного зору не можуть виконати його надійне виділення на фоні та надійно утримувати, зокрема, при зміні умов освітленості (тінь від хмари) чи зміні форми контуру зображення (виконання об’єктом маневру). Тому для надійного захоплення і утримання на великих відстанях вимагається застосування довгофокусних оптичних систем, які мають вузький кут огляду.

Таким чином, для можливості надійного захоплення і утримання цілі на різних дистанціях оптична система перехоплювача повинна бути комбінованою

з різних типів камер – монокулярна довгофокусна для супроводу цілі на дальніх дистанціях та бінокулярна короткофокусна (ширококутна) для супроводу на ближніх дистанціях.

Обов'язковою умовою автономного наведення перехоплювача на ціль є постійне утримання цілі в полі зору оптичної системи перехоплювача, причому, зображення цілі повинне потрапляти у центральну частину поля зору, оскільки при утриманні цілі в периферійних ділянках виникає висока ймовірність втрати цілі при здійсненні нею несподіваного різкого маневру. Враховуючи, що ударні БпЛА противника споряджаються детекторами атак перехоплювачів, оптична система перехоплювача повинна мати "запас" поля зору для можливості відслідковування маневрів ухилення.

Серед різноманіття можливих конфігурацій траєкторій цілі й перехоплювача типовою є група таких конфігурацій, у яких перехоплювач змушений наздоганяти ціль, рухаючись обіч неї – рис. 2.

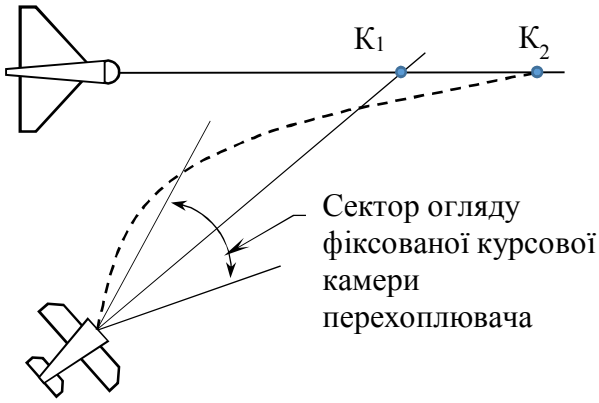


Рис. 2. Вплив напрямку і кута сектору огляду оптико-електронної системи перехоплювача на вибір траєкторії зближення з ціллю.
$К_1$ – точка контакту з ціллю при поворотній камері перехоплювача.
$К_2$ - точка контакту з ціллю при фіксованій камері перехоплювача

Для таких конфігурацій, якщо оптична система перехоплювача жорстко закріплена "по курсу", то застосування методу "паралельного зближення" неможливе, оскільки положення цілі випадає за межі сектора огляду відеосистеми перехоплювача. В подібних випадках (при жорсткому закріпленні оптичної системи) для зближення з ціллю перехоплювач змушений застосовувати метод "погоня" та рухатись по криволінійній траєкторії – щоб утримувати ціль в межах сектора огляду відеосистеми. Очевидно, що зближення по криволінійній траєкторії вимагає більше часу і простору, що створює підвищену загрозу зриву перехоплення із за передчасної витрати бортового енергоресурсу. Для уникнення таких небажаних ситуацій оптична

система перехоплювача повинна бути поворотною по рисканню – це надаватиме перехоплювачу можливість надійного атакування цілі, яка рухається збоку від його.

Підсумовуючи, створення ефективного перехоплювача реактивних ударних БпЛА противника вимагає системного підходу, знання і врахування особливостей побудови й функціонування системи ППО та тактики виконання перехоплень. Літальний апарат повинен створюватись та застосовуватись як невід’ємна інтегральна складова системи ППО.

Заєць Ю. О.
Ольшанський М. А.
Солопій І. А.
Житомирський військовий інститут імені С. П. Корольова

НАУКОВО-МЕТОДИЧНІ ЗАСАДИ МОДЕРНІЗАЦІЇ 70-мм НЕКЕРОВАНИХ АВІАЦІЙНИХ РАКЕТ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УРАЖЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Інтенсифікація застосування засобів повітряного нападу типу «Герань – 4/5» та крилатої ракети S8000 «Бандероль» актуалізує задачу розробки асиметричних, економічно доцільних систем протиповітряної оборони (ППО) тактичної ланки. Використання 70-мм некерованих авіаційних ракет (НАР) із бойовими частинами спрямованого осколкового поля (типу «Thales FZ123») у складі наземних мобільних комплексів є перспективним напрямком. Проте досягнення необхідної ймовірності ураження цілі ($P_{\text{ур}} \geq 0{,}85$) за умови пуску з наземних платформ потребує глибокої модернізації бортових систем ракети та оптимізації параметрів її бойового спорядження.

Головними чинниками, що обмежують ефективність базового комплексу, є квадратичне зростання лінійної помилки дальності підриву на траєкторії та недостатня кінетична енергія готових вражаючих елементів (ГВЕ) сферичної форми на граничних відстанях розльоту хмари. Метою роботи є теоретичне обґрунтування та розробка технічних рішень за двома ключовими напрямками: автоматизація програмування дистанційного підриву бойової частини ракети та оптимізація фізико-геометричних параметрів бойової частини.

Напрямок 1. Розробка та інтеграція системи тахометричного індукційного програмування дальності підриву.

Для усунення балістичних помилок за дальністю та відмови від дороговартісних оптико-електронних головок самонаведення, обґрунтовано впровадження системи динамічного програмування часового запізнення підривача на зрізі пускової напрямної.

Математична модель та алгоритм системи управління вогнем: Наземна система управління вогнем (СУВ) за даними радіолокаційного або оптико-електронного супроводження цілі обчислює просторові координати точки зустрічі. Бортовий обчислювач СУВ у реальному часі розв'язує пряму задачу балістики для визначення польотного часу:

$$T_{\text{пол}} = \int_0^{D_{\text{цілі}}} \frac{1}{V_r(x)}\, dx$$

Де $T_{\text{пол}}$ – сумарний польотний час ракети від моменту її сходу з пускової установки (виходу з напрямної) до моменту досягнення координати цілі (точки зустрічі), вимірюється в секундах (с);

$\int_0^{D_{\text{цілі}}}$ – знак визначеного інтеграла за просторовою координатою від (0) (зріз пускового ствола) до ($D_{\text{цілі}}$). Він означає математичне підсумуваннння нескінченно малих часток часу на кожній елементарній ділянці дистанції польоту;

$D_{\text{цілі}}$ – просторова дальність (дистанція) від пускової установки до точки зустрічі з БпЛА вздовж траєкторії, вимірюється в метрах (м). Визначається в режимі реального часу за даними тривимірного супроводження цілі радіолокатором або оптико-електронною станцією комплексу;

$V_r(x)$ – функція поточної швидкості ракети залежно від пройденої відстані x, вимірюється в метрах за секунду (м/с);

x – поточна просторова координата ракети на траєкторії, вимірюється в метрах (м);

dx – диференціал просторової координати, який означає нескінченно малий приріст відстані вздовж траєкторії польоту.

Технічна реалізація. Інформаційна взаємодія між системою управління вогнем та ракетою реалізується безконтактним способом за допомогою індукційного програматора, інтегрованого в передню частину напрямної труби пускової установки. Під час проходження ракети крізь котушку зв'язку на приймальну антену бортового підривача передається кодована часова мітка з точністю до $\leq 10^{-4}$ с.

Мінімізація похибок. Застосування тахометричного принципу дозволяє коригувати час підриву безпосередньо в момент старту, нівелюючи вплив нестабільності початкової швидкості ракети (Δ V□), зумовленої коливанням температури порохового заряду. Це звужує лінійну помилку підриву вздовж траєкторії до меж $\Delta L \leq \pm 2\ldots5$ метрів, що повністю перекривається геометрією осколкового поля.

Напрямок 2. Оптимізація аеродинамічних характеристик бойової частини та модернізація геометрії готових вражаючих елементів.

Перехід від повітряного базування (з високою початковою швидкістю носія) до наземного старту суттєво змінює балістичні умови та висуває жорсткіші вимоги до аеродинамічної якості ракети.

Аеродинамічне балансування: Інтеграція важкої осколкової бойової частини зміщує центр мас $X_{цм}$ ракети вперед, що за незмінної площі стабілізаторів призводить до надмірної статичної стійкості та зростання чутливості до вітрових збурень (ефект «флюгера»). На основі розрахунків методів обчислювальної гідрогазодинаміки (CFD) визначено доцільність зміни форми носового обтічника з конічної на оживальну (за кривою O give) з відносним подовженням λ = 3,5. Це дозволяє оптимізувати розподіл тиску, знизити коефіцієнт лобового опору C_x на надзвукових режимах (M=1,5–2,2) на 12–15% та стабілізувати положення центра тиску $X_{цм}$.

Модернізація уламкового наповнення (заміна готових вражаючих елементів): Традиційні сферичні елементи мають незадовільний балістичний коефіцієнт і швидко втрачають швидкість за законом:

$$V_r(x) = V_{\text{підр}}\, e^{-\frac{\rho_{\text{пов}} C_x S}{2m} r}$$

Пропонується заміна сталевих кульок на кубічні елементи з важких вольфрамових сплавів з щільністю $\rho \approx 18{,}0\ldots18{,}5$ г/см^2.

Науковий ефект модернізації готових вражаючих елементів**:**

Збереження енергії. Завдяки високій поперечній щільності кубічні елементи з важких вольфрамових сплавів зберігають кінетичну енергію на відстанях до 15–20 метрів від точки підриву, забезпечуючи надійне пробиття титанових та дюралевих елементів планера БпЛА.

Оптимізація об'єму. Висока щільність вольфраму дозволяє зменшити геометричний об'єм бойової частини при збереженні її маси, що вивільняє простір для інтеграції електронного підривача та покращує загальне центрування ракети.

Реалізація запропонованих науково-технічних рішень дозволяє трансформувати некеровану ракету у високоточний засіб ураження ближньої зони із фіксованою вартістю пострілу. Впровадження індукційного програмування у поєднанні з оптимізацією балістичних характеристик бойової частини забезпечує щільне накриття цілі уламковим полем з оптимізованими параметрами пробивної дії, що є критично важливим для побудови ешелонованої системи протидії масованим загрозам БпЛА.

Maidaniuk V. A., Ph. D.
Vahnin O. V.
Hetman Petro Sahaidachnyi National Army Academy

HIGH-POWER MICROWAVE WEAPONS AS A MEANS OF COUNTERING ENEMY UAVs

Abstract. The paper considers the prospects of using high-power microwave (HPM) weapons as a means of countering enemy unmanned aerial vehicles (UAVs). The specific features of high-power microwave effects on UAV electronic systems are analyzed, and the main advantages and limitations of this approach are identified. The possibilities of using HPM systems against the mass and swarm employment of UAVs are considered. Modern foreign developments are analyzed, and promising directions for further development of HPM-based counter-UAV systems are identified.

Keywords: high-power microwave weapons, HPM, UAVs, counter-UAS, counter-drone systems, directed-energy weapons, electronic warfare.

Problem Statement

The experience of modern armed conflicts demonstrates the continuously increasing role of unmanned aerial vehicles. UAVs are widely used for reconnaissance, surveillance, fire adjustment, target engagement, and other missions. At the same time, the development of technologies makes it possible to produce relatively inexpensive UAVs in large quantities, which significantly changes approaches to countering them.

One of the main problems of modern counter-UAS systems is the cost ratio between the target and the means used to defeat it. The mass employment of

inexpensive UAVs may create a situation in which the use of traditional kinetic means against each individual target becomes economically inefficient. At the same time, an increasing number of UAVs in the air places an additional burden on systems responsible for their detection, tracking, and engagement.

In this context, considerable attention is being paid to the development of directed-energy weapons. One of these directions is the use of high-power microwave (HPM) radiation designed to affect the electronic systems of unmanned aerial vehicles.

The U.S. Air Force Research Laboratory (AFRL) considers HPM technology to be one of the promising directions for developing non-kinetic countermeasures against groups of UAVs. In particular, the THOR system was developed specifically to counter UAV swarms and is designed to engage multiple targets.

Purpose of the Study

The purpose of this study is to analyze the capabilities of HPM weapons for countering enemy UAVs and to determine their role among modern means of combating unmanned aerial vehicles.

Main Part

Unlike kinetic weapons, which engage targets through the physical impact of ammunition, HPM weapons use electromagnetic energy. The primary target of this type of weapon is the electronic systems of the UAV.

A modern UAV is a complex electronic system whose operation is supported by onboard control, navigation, communication, information-processing systems, and other electronic components. Therefore, disruption of critical electronic components may result in the UAV losing its ability to perform its assigned mission.

The AFRL describes THOR as a directed-energy weapon prototype designed to disable UAV electronics. The system was specifically developed with the need to counter multiple targets simultaneously in mind.

One of the main advantages of HPM weapons is their potential ability to affect groups of UAVs. In 2023, AFRL reported a demonstration of THOR against a group of unmanned aerial vehicles. During the test, the system used high-power microwave pulses to produce a non-kinetic effect on the targets.

This capability is particularly important when an adversary employs UAV swarms. When a traditional kinetic weapon is used against each individual UAV, a separate munition is normally required for each target. An HPM system, in contrast, has the potential to affect multiple electronic targets without such a direct one-to-one relationship between a target and a munition.

Therefore, the main potential of HPM weapons lies not so much in replacing traditional air-defense systems as in providing an additional layer of counter-UAS capability.

Advantages and Limitations of HPM Weapons

The main advantages of HPM systems include the possibility of non-kinetic effects against UAVs, rapid generation of electromagnetic energy, and the potential ability to engage multiple targets.

AFRL states that THOR uses high-power microwave pulses to create an electronic effect, while its design is specifically focused on countering swarm attacks by UAVs. During the 2023 demonstration, the laboratory reported the use of the system against groups of targets and emphasized its potential for scenarios involving UAV swarms.

Another important advantage is that HPM weapons do not necessarily require the physical destruction of each UAV. To neutralize a target, it may be sufficient to produce the required electromagnetic effect on its electronic systems.

At the same time, HPM weapons have significant limitations. One of the main challenges is the need for a substantial amount of electrical energy. This directly affects the design of the system, including its weight, dimensions, cooling requirements, and mobility.

Furthermore, the effectiveness of HPM employment depends on the design of the electronic systems of a particular UAV and on measures that may be used to increase their resistance to electromagnetic effects. Therefore, the development of HPM weapons will inevitably be accompanied by the development of technologies for protecting electronic equipment against such effects.

HPM Weapons as Part of an Integrated Counter-UAS System

HPM weapons should be considered in combination with other counter-UAS capabilities. A modern counter-UAS system should provide target detection, identification, tracking, and engagement using different methods depending on the specific situation.

In this context, an HPM system can occupy an intermediate position between traditional kinetic weapons and electronic warfare capabilities. Its distinctive feature is the directed energy effect on the electronic systems of UAVs.

The use of HPM systems as part of a multilayered counter-UAS architecture appears promising. Such an architecture may combine electronic warfare, kinetic weapons, directed-energy systems, and other capabilities. This approach makes it

possible to reduce dependence on a single countermeasure and increase the resilience of the overall system to changes in the adversary's UAV employment tactics.

Modern Foreign Developments

Practical interest in the development of HPM weapons is confirmed by the implementation of relevant programs in the United States.

One of the best-known projects is **THOR (Tactical High Power Operational Responder)**, developed by the Air Force Research Laboratory. The system is designed to protect military facilities against group UAV attacks and uses high-power microwave radiation to produce non-kinetic effects on UAV electronics.

Another important development is **Leonidas**, developed by Epirus. In 2023, the company announced that the U.S. Army had awarded it a contract to develop HPM system prototypes under the Indirect Fire Protection Capability – High-Power Microwave (IFPC-HPM) program. In 2024, Epirus reported the delivery of four IFPC-HPM systems to the U.S. Army and the completion of engineering developmental testing against UAVs and groups of UAVs.

Thus, HPM technology is gradually moving from experimental demonstrators toward systems being considered for practical military applications.

The further development of IFPC-HPM is also noteworthy. In 2025, Epirus announced that it had received another U.S. Army contract for second-generation IFPC-HPM systems, demonstrating the continuation of efforts to increase the capabilities of this technology.

Another area of interest is the development of HPM capabilities against new types of UAVs. In 2026, Epirus announced a demonstration of Leonidas against a UAV controlled through a fiber-optic link. According to the company, the system demonstrated an electromagnetic effect against this type of target during the test.

This area is particularly relevant because the proliferation of fiber-optic FPV UAVs creates additional challenges for conventional electronic warfare systems. At the same time, the reported test results require further independent assessment and evaluation of the actual capabilities of HPM systems against different types of UAVs.

Prospects for Further Development

Analysis of current developments makes it possible to identify several promising directions for further development of HPM weapons.

The first is improving the energy efficiency of systems while reducing their weight and dimensions. This would enable the development of more mobile systems capable of operating directly with combat units.

The second direction is improving radiation-control and guidance systems. Modern developers are moving toward software-controlled systems capable of adjusting the parameters of electromagnetic effects according to target characteristics.

The third direction is the integration of HPM systems with detection and battle-management systems. Such integration would allow HPM capabilities to be used not as an isolated weapon but as part of an integrated counter-UAS system.

The fourth direction is the development of capabilities against UAV swarms. The ability to affect multiple unmanned systems is one of the key potential advantages of HPM weapons compared with many traditional counter-UAS means.

Conclusions

HPM weapons represent one of the promising directions in the development of modern counter-UAS capabilities. Their fundamental feature is the possibility of producing non-kinetic effects on UAV electronic systems through high-power electromagnetic radiation.

The greatest potential of HPM systems may be realized under conditions of mass UAV employment. Their potential ability to affect multiple targets makes them particularly relevant for countering swarm attacks, where traditional systems may face the problem of a large number of targets and high ammunition expenditure.

At the same time, HPM weapons should not be regarded as a universal replacement for traditional systems. Their effectiveness depends on the system's energy capabilities, UAV electronic architecture, employment conditions, and other factors. Therefore, the most reasonable approach is to use HPM systems as one element of a multilayered counter-UAS architecture.

The development experience of U.S. systems such as THOR and Leonidas demonstrates the gradual transition of high-power microwave technology from experimental demonstrators toward practical military systems. Further research should focus on assessing HPM effectiveness against different classes of UAVs, determining appropriate employment conditions, and establishing the optimal role of HPM systems within an integrated counter-UAS architecture.

Дроздов М. О., канд. фіз.-мат. наук, доц.
Шкурпіт О. М., Ph. D.
Небесний С. О.
Військова академія (м. Одеса)

ПЕРСПЕКТИВИ ПЕРСОНАЛЬНОГО ЗАХИСТУ ВІД FPV–БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА НА ПОЛІ БОЮ

Актуальною є проблема персонального захисту військовослужбовців або їх невеликих груп від FPV-БпЛА на полі бою в процесі виконання бойових завдань. Сьогодні втрати особового складу від дій FPV-БпЛА на полі бою помітно високий. Тому, заради збереження бійців, все більша увага віддається застосуванню на полі бою повітряних, наземних, надводних та підводних роботизованих комплексів (РТК). Слід відзначити, що самозахист від загроз БпЛА є неефективним через обмеженість можливостей індивідуальних засобів протидії БпЛА, а також через те, що виконавцям бойових завдань доводиться виконувати невластиві ним доволі складні і напружені дії по відстежуванню повітряного простору. При цьому, можливе зіткнення відбувається в умовах більш сприятливих для нападника.

Авторами пропонується концепція персонального захисту на полі боя за допомогою спеціалізованої БпЛА платформи з використанням штучного інтелекту (ШІ) у виконанні завдань персонального захисту. В разі використання БпЛА перевагою є краща тактична позиція в повітрі та мала помітність. Бортові засоби придушення атак БпЛА можуть бути напочатку подібними до тих, які використовуються в індивідуальному захисті сьогодні, але, як це властиво цифровим платформам можна передбачити їх швидкий розвиток та вдосконалення в практиці застосування. Нема сумніву, що такі роботизовані бойові платформи можуть з часом стати амфібійними з метою найкращого пристосування до особливостей поля бою та характеру тактичних завдань. На користь даної концепції виступає значно більша ніж у людини швидкодія автоматизованих пристроїв, звільнення від невластивих функцій і зайнятих виконанням конкретних бойових завдань бійців, значно більший потенціал майбутнього удосконалення бойових платформ персонального захисту (БППЗ) у порівнянні з можливостями удосконалення індивідуальних засобів протидії БпЛА окремого бійця або невеликої групи.

Завданнями, що вирішуються БППЗ, можуть бути: ідентифікація взятих під захист бійців та бойових одиниць противника; розвідувальна робота за визначенням та постійним спостереженням (моніторинг) повітряної, наземної,

надводної обстановки поля бою; передача розвідувальних даних та цілевказівок наземним комплексам та інтеграційним платформам ситуаційної обізнаності (наприклад DELTA, «Кропива», «Арта»); видача цілевказівок бійцю або групі бійців, взятих під захист від БПЛА противника та надання ним рекомендацій на оперативні дії із застосуванням зброї в разі неможливості уникнення зіткнення; відпрацювання тактики обходу противника або способу та порядку його знешкодження; можливість ведення ефективної інтелектуальної РЕБ по відношенню до сил противника; можливість самостійного знищення або знешкодження БПЛА чи інших сил противника, що створюють загрозу бійцям; доставка (підвіз) боєприпасів и навіть евакуація загиблих чи поранених.

Перспективним є озброєння БППЗ зброєю гостроспрямованої когерентної електромагнітної дії у надвисокочастотному (НВЧ) діапазоні, розробка та випробування якої є перспективною через можливість досягнення високої ефективності та різкого зменшення масогабаритних характеристик. При цьому найбільш ефективними є два конкретні діапазони: S-діапазон (від 2 до 4 ГГц) та X-діапазон (від 8 до 12 ГГц).

S-діапазон забезпечує вплив, який можна назвати «Вхід через антени». Цей діапазон є ідеальним для так званого «функціонального ураження» через власні приймальні канали дрона. Надпотужний когерентний імпульс на цих частотах проходить крізь штатні антени та фільтри дрона з фізичним пошкодженням електронного обладнання дрона. Наслідком є втрата навігації та зв'язку із оператором.

X-діапазон забезпечує вплив, який можна назвати забезпечує вплив, який можна назвати «Вхід через корпус». Цей діапазон має значно меншу довжину хвилі (близько 2.5–3.7 см), що дає йому можливість проникнення всередину корпусу дрона через будь-які технологічні отвори, щілини в пластику чи металі, а також по дротах живлення.

Для формування гостроспрямованого когерентного випромінювання НВЧ високої потужності можливо застосування технологій активних фазованих антенних решіток (АФАР) на базі твердотільних напівпровідників.

Для створення перспективної БППЗ важливою є розробка легкої та водночас потужної бортової системи електроживлення з первинним джерелом, яким може бути високочастотний компактний турбогенератор або спеціалізовані літій-іонні акумулятори з високою швидкістю розряду, та буферним накопичувачем з використанням, наприклад, графен-полімерних суперконденсаторів. Сучасні технології дозволяють виконати розробку та виробництво БППЗ.

Парфенюк В. Г., канд. техн. наук, доц.
Григорєв І. С.
Житомирський військовий інститут імені С. П. Корольова

ЦИФРОВЕ ПЕРЕНАЛАШТУВАННЯ ЧАСТОТИ У FHSS-СИСТЕМАХ ІЗ ЗАСТОСУВАННЯМ SDR-ТЕХНОЛОГІЇ

Системи з псевдовипадковим переналаштуванням робочої частоти (ППРЧ, *Frequency Hopping Spread Spectrum*, *FHSS*) широко застосовуються для підвищення завадостійкості, забезпечення низької ймовірності виявлення факту існування сигналу в ефірі та перехоплення, а також електромагнітної сумісності. У *SDR*-реалізаціях критичним стає час переналаштування частоти, точність і повторюваність стрибків, а також простота синхронізації. Традиційне переналаштування аналогового генератора несучої радіотракту має принципові обмеження за швидкодією, фазовими перехідними процесами та небажаними спектральними складовими. Тому актуальним є пошук способів, які дозволяють реалізувати високу швидкість переналаштування частоти, що особливо актуально для військових *FHSS*-систем (потребують десятки тисяч стрибків частоти на секунду), так як це один із способів протидіяти сучасним засобам радіоелектронної боротьби.

У доповіді пропонується реалізувати високу швидкість переналаштування частоти та широкий діапазон зміни частоти *FHSS*-систем гібридним способом із використанням *SDR*-пристроїв. Суть цього способу полягає в поєднанні грубого переналаштування аналогового синтезатора частоти аналогової ФАПЧ з точним цифровим зсувом частоти.

Синтезатор частоти *SDR*-пристрою встановлюється на фіксованій центральній частоті вибраного діапазону переналаштування частоти $f_{ц}$, а зміна частоти в межах діапазону реалізується цифровим шляхом – множенням комплексної обвідної сигналу на сформовану цифровим способом комплексну експоненту необхідної частоти.

На приймальній стороні радіотракт має налаштовуватись на частоту $f_{ц}$ та виконуватись обернена операція «дехопінг (*dehopping*)» множенням на комплексно-спряжену експоненту з тим самим законом зміни частоти.

Перевагами даного способу можуть бути:

час переналаштування у межах діапазону визначається не швидкодією ФАПЧ, а **темпом оновлення** *NCO* (*Numerically Controlled Oscillator*), який формує комплексну синусоїду шляхом накопичення фази з заданим кроком, та може становити один або кілька відліків;

висока точність і повторюваність значення частоти та детермінована затримка;

відсутність перехідних процесів аналогового синтезатора частоти;

можливість адаптивної послідовності стрибків частоти;

гнучка реконфігурація через ПЛІС або програмне забезпечення.

Очікується, що гібридний спосіб матиме і певні обмеження щодо застосування. По-перше діапазон переналаштування має вкладатися в миттєву смугу *SDR*-пристрою. Також підвищуються вимоги до лінійності, динамічного діапазону та *SFDR* АЦП/ЦАП. Окрім того потрібні ефективні цифрові фільтри та, за потреби, дизеринг (*phase dithering*) фази *NCO* (додавання псевдовипадкової послідовності до молодших розрядів слова фази) для зменшення паразитних спектральних складових (спурів, *spurs*).

Подальше теоретичне та експериментальне дослідження гібридного способу може полягати в вирішення наступних завдань.

Як забезпечити надійне входження приймача в синхронізм за часом, частотою та фазою стрибків, і які алгоритми дають мінімальний час входження?

Як вибирати початкову фазу *NCO* і методи дизерингу, щоб мінімізувати розриви фази, спури при заданій розрядності?

Якою є оптимальна архітектура *NCO* для ПЛІС (*LUT*, *CORDIC*, поліноміальна), що забезпечить найкращий компроміс між ресурсами, швидкодією та енергоспоживанням?

Як узгодити широку миттєву смугу АЦП/ЦАП з високим *SFDR* і динамічним діапазоном?

Як кількісно оцінити стійкість до навмисних завад, перехоплення та пеленгації порівняно з аналоговою побудовою?

Передбачається, що гібридний спосіб дозволить реалізувати швидкі *FHSS*-системи із фіксованим центральним гетеродином у смузі переналаштування. Його реалізація усуне основні обмеження аналогового способу, забезпечить високу точність і гнучкість керування частотою.

СЕКЦІЯ 3
Засоби ураження безпілотних систем

Черняєв С. І.
Павленко К. І.
Житомирський військовий інститут імені С. П. Корольова

ЗАСОБИ РОЗВІДКИ ТА УРАЖЕННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ ПРОТИВНИКА МЕХАНІЗОВАНИХ ПІДРОЗДІЛІВ

Механізованим підрозділам необхідні власні засоби розвідки та ураження БпАК противника через те, що сучасне поле бою стало повністю прозорим, а загроза з повітря — масовою та безперервною. Без ефективної протидії дронам будь-яка бронетехніка та жива сила стають легкою мішенню.

Актуальність цієї потреби визначається докорінною зміною характеру сучасної російсько-української війни, де БпАК перетворилися на головний інструмент розвідки, коригування вогню та безпосереднього ураження на полі бою. Сьогодні наявність таких засобів у механізованих підрозділів – не просто питання технологічної переваги, а єдина умова виживання підрозділу та збереження його боєздатності. Якщо механізований підрозділ не має засобів виявлення та збиття розвідувальних дронів противника, він автоматично стає мішенню для артилерії, касетних авіаційних бомб чи ракет за лічені хвилини після виходу на позицію.

Сучасний комплекс протидії БпАК у механізованих підрозділах поділяється на дві основні складові: засоби розвідки (виявлення та попередження) та засоби ураження (кінетичне та радіоелектронне знищення). Головне завдання засобів розвідки полягає у виявленні дрону до того, як він підлетить на відстань атаки. До засобів розвідки належать портативні аналізатори спектра та сканери частот, малогабаритні радіолокаційні станції, оптико-електронні та акустичні системи. Сучасні засоби ураження БпАК механізованих підрозділів поділяються на радіоелектронні (нелетальні) та кінетичні (фізичне знищення).

Механізованим підрозділам засоби розвідки та ураження БпАК противника необхідні насамперед для збереження боєздатності, захисту бронетехніки та забезпечення можливості здійснювати будь-які маневри в

умовах сучасної війни. Засоби розвідки та ураження БпАК для механізованих військ це інструмент, який повертає бронетехніці її роль на полі бою, захищаючи її від дешевого, але смертоносного повітряного асиметричного бачення та ударів противника.

Білоус Г. П.
Смоляр О. І.
Інститут Військово-Морських Сил
Національного університету «Одеська морська академія»

УДОСКОНАЛЕННЯ ФОРМ І СПОСОБІВ ПРОТИДІЇ МАСОВОМУ ЗАСТОСУВАННЮ УДАРНИХ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ ПРОТИВНИКА З УРАХУВАННЯМ ДОСВІДУ БОЙОВИХ ДІЙ НА ПІВДНІ УКРАЇНИ

Сучасні бойові дії характеризуються стрімким зростанням ролі безпілотних авіаційних систем у складі засобів повітряного нападу. рф систематично нарощує масштаби застосування ударних безпілотних літальних апаратів (БпЛА), удосконалює способи їх бойового використання, збільшує кількість одночасно задіяних засобів та поєднує їх із ракетним і авіаційним озброєнням. Унаслідок цього безпілотні системи перетворилися з окремого тактичного засобу на один із ключових компонентів систематичного повітряного впливу на Сили оборони України та об’єкти військової, транспортної, енергетичної й портової інфраструктури.

Досвід бойових дій на півдні України протягом вересня – початку жовтня 2026 року підтверджує стійку тенденцію до високої інтенсивності застосування противником ударних БпЛА. Упродовж окремих діб кількість застосованих у зоні відповідальності угруповання військ "Південь" безпілотних засобів досягала близько двох тисяч і більше, а на початку жовтня зафіксовано подальше збільшення масштабів їх застосування. Така динаміка свідчить не лише про кількісне нарощування повітряного нападу, а й про зміну підходів противника до його організації, що проявляється у використанні різнотипних безпілотних систем та їх поєднанні з іншими засобами ураження.

Масоване застосування БпЛА створює додаткове навантаження на систему протиповітряної оборони та підвищує вимоги до її спроможності

одночасно виявляти, супроводжувати, класифікувати та уражати значну кількість повітряних цілей. За таких умов ефективність протидії визначається не тільки кількістю знищених або подавлених БпЛА, а насамперед здатністю системи забезпечувати своєчасне отримання інформації про повітряну обстановку, визначення пріоритетності цілей, раціональний розподіл наявних засобів та безперервність управління. Отже, подальше підвищення ефективності протидії потребує удосконалення не лише технічних характеристик окремих засобів, а передусім форм і способів їх комплексного застосування.

Перспективним напрямом є формування багаторівневої системи протидії ударним БпЛА, у якій засоби виявлення, розвідки, ситуаційної обізнаності, радіоелектронної боротьби та вогневого ураження функціонують як взаємопов’язані елементи. Така система має забезпечувати отримання інформації про повітряну обстановку з різних джерел, її оперативне узагальнення, класифікацію повітряних цілей, визначення рівня їх загрози та вибір найбільш доцільного способу протидії. При цьому ефективність системи доцільно оцінювати не за ізольованими показниками окремих засобів, а за її спроможністю забезпечувати безперервне виявлення, супроводження, розподіл та ураження повітряних цілей.

Важливим напрямом удосконалення є диференційований вибір засобів протидії залежно від характеру повітряної загрози. Масоване застосування противником значної кількості безпілотних систем потребує раціонального використання наявного ресурсу. Перспективна система протидії має передбачати поєднання вогневого ураження, радіоелектронного впливу, мобільних вогневих засобів, спеціалізованих безпілотних систем-перехоплювачів та інших технологічних рішень. Застосування різнорідних засобів за єдиним задумом дозволить підвищити стійкість системи до зміни способів дій противника та зменшити залежність від окремого виду засобів протидії.

Окремим перспективним напрямом є розвиток БпЛА-перехоплювачів як додаткового компонента системи протиповітряної оборони. Їх застосування потенційно дозволяє сформувати додатковий рівень ураження повітряних цілей та зменшити навантаження на окремі традиційні засоби протидії. Водночас ефективність такого способу залежить від своєчасності виявлення цілі, швидкості передачі інформації, оперативності прийняття рішення та можливості інтеграції перехоплювачів у загальну систему управління. Тому

БпЛА-перехоплювачі доцільно розглядати не як окремий засіб, а як складову комплексної системи протидії масованому застосуванню безпілотних систем противника.

Необхідною умовою підвищення ефективності протидії є вдосконалення інформаційного забезпечення. За одночасного застосування значної кількості різнотипних повітряних цілей особливого значення набуває скорочення часу від їх виявлення до прийняття рішення щодо способу протидії. Для цього необхідно розвивати автоматизовані системи ситуаційної обізнаності, забезпечувати інтеграцію інформації від різних джерел, автоматизоване супроводження цілей, їх класифікацію та визначення пріоритетності. Застосування сучасних інформаційних технологій та елементів штучного інтелекту доцільно спрямовувати насамперед на прискорення обробки значних обсягів інформації, виявлення закономірностей у діях противника та підтримку прийняття рішень.

Особливого значення набуває забезпечення адаптивності системи протидії до постійної зміни способів застосування противником безпілотних систем. Удосконалення тактики застосування БпЛА, зміна їх кількісного та якісного складу, використання різних типів повітряних цілей та поєднання їх з іншими засобами повітряного нападу потребують постійного аналізу результатів застосування сил і засобів протидії. Це обумовлює необхідність систематичного узагальнення бойового досвіду, удосконалення алгоритмів оцінювання повітряної обстановки та оперативного коригування способів застосування наявних засобів. Тому система протидії має розвиватися як адаптивна система, здатна своєчасно реагувати на зміни характеру повітряної загрози.

Таким чином, досвід бойових дій на півдні України свідчить, що подальше масштабування застосування противником ударних БпЛА потребує переходу від переважно реактивного знищення окремих повітряних цілей до комплексної, адаптивної системи протидії їх масованому застосуванню. Основними напрямами її удосконалення мають бути інтеграція засобів виявлення, розвідки, радіоелектронного впливу та вогневого ураження в єдиний інформаційний контур, диференційований вибір способів протидії, розвиток БпЛА - перехоплювачів, автоматизація оцінювання повітряної обстановки та розподілу цілей, а також підвищення оперативності управління. Такий підхід забезпечить своєчасне реагування на зміни характеру повітряної загрози, раціональніше використання наявних ресурсів та підвищення стійкості системи протиповітряної оборони до подальшого розвитку засобів і способів повітряного нападу противника.

Брановицький В. В.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ ЗАЛИСТУВАННЯ ТЕРИТОРІЇ ПРОТИВНИКА ЯК СПОСІБ ПСИХОЛОГІЧНОГО ВПЛИВУ НА ЦІЛЬОВУ АУДИТОРІЮ

В умовах відсічі збройної агресії російської федерації проти України психологічний вплив залишається критичним складником ведення війни. Там, де відсутні інтернет і мобільний зв’язок, майже єдиним каналом впливу на визначену цільову аудиторію (ЦА) є залистування території візуальними матеріалами впливу – листівками з інструкціями, закликами, інформаційними повідомленнями.

Традиційний спосіб цього завдання – агітаційні снаряди калібрів 122 мм і 220 мм розраховані на покриття відносно великих площ від 0,25 км², що відповідає масштабу опорного пункту взводу, роти чи фрагмента району оборони. Сучасна тактика противника полягає в діях невеликих штурмових груп і закріпленні на компактних опорних пунктах. Виникає розрив між характеристиками штатного засобу доставки друкованих матеріалів і просторовим масштабом. За оцінкою похибка залистування агітаційними снарядами сягає від 500–700 м. Розкриття на значній висоті спричиняє розліт матеріалів поза ЦА та запланованою зоною скиду. Агітаційних снарядів у військах залишилося обмаль, залучення артилерійських систем створює ризик їх виявлення, сильний вітер та опади зміщують зону розповсюдження, отож, агітаційні снаряди не відповідають вимогам сьогодення, щодо точкового впливу на малу групу противника.

Досвід тактичних груп підтвердив доцільність застосування безпілотних літальних апаратів (БПЛА) із пристроєм скидання листівок. Друковані матеріали розповсюджувалися не "килимом" по квадрату місцевості, а адресно: поблизу позицій ворожої піхоти, вздовж імовірних маршрутів атак і в районах можливого просування противника. Такий вибір точок розповсюдження листівок відповідає тактиці малих груп: візуальний матеріал має бути на шляху руху противника або в місці укриття конкретної ЦА, а не на порожній ділянці місцевості між позиціями.

Індикатором ефекту від залистування стає зворотний зв’язок від військовополонених військовослужбовців збройних сил російської федерації. Зі слів полонених підтверджено факт ознайомлення зі змістом листівок у опитаних, що листівки мотивували їх до добровільної здачі в полон. Водночас фіксується ланцюг "друк листівок – доставка друкованих матеріалів за допомогою БПЛА – ознайомлення ЦА з листівкою – зміна поведінки (здача в полон)".

Одним з технічних засобів при залистуванні застосовують безпілотний авіаційний комплекс (БпАК) "AVENGER" українського виробництва, версія "Бомбер". Для залистування з БпАК був розроблений спеціальний лоток під друковані матеріали та передбачено відсік корисного навантаження до 4 кг. Для підвищення точності скидання листівок їх розміщують у картонному оздобленні з прикріпленим вантажем: це зменшує некерований розліт листівок після скидання з БПЛА.

Принциповими для впливу на ЦА є точність скидання, автономність і здатність проходити зони радіоелектронної боротьби (РЕБ). Гарантована дальність польоту БпАК "AVENGER" – 80 км, швидкість – 80 км/год, час розгортання – близько 10 хв. Інерційне позиціонування і режим радіомовчання дають змогу виконати автономний політ і повернення без радіоканалу управління та телеметрії.

Окремою умовою впливу на ЦА є оформлення листівки за правилами першого контакту, відпрацьованими в зоні бойових дій: яскраві кольори, щоб листівка вирізнялася на ґрунті, снігу чи в окопі; пряме звернення до ЦА, а не абстрактне "солдатам"; конкретне проблемне питання, актуальне для цієї ЦА в даний момент; покрокова інструкція, зокрема щодо порядку здачі в полон і виходу до позицій Сил оборони України.

Отже, розповсюдження листівок на ЦА за допомогою БПЛА є актуальним, особливо за відсутності на даній місцевості інтернету та мобільного зв’язку. Бойовий досвід тактичних груп підтверджує дієвість адресного залистування з БПЛА. Перехід спеціальних підрозділів на безпілотну доставку візуальних матеріалів є не лише доцільним, а практично невідкладним організаційно-технічним завданням. Перспективними напрямами є індикатори ефективності, інструментальне вимірювання розльоту листівок залежно від висоти, вітру та способу пакування.

Пількевич І. А., д-р техн. наук, проф.
Лобода Р. І.
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ БОЄПРИПАСІВ ДЛЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ІЗ МОДУЛЕМ КОРИГУВАННЯ ТРАЄКТОРІЇ ПОЛЬОТУ

Сучасний розвиток безпілотних систем супроводжується розширенням номенклатури боєприпасів та підвищенням вимог до точності їх застосування. Перспективним напрямом є розроблення і впровадження боєприпасів, конструктивно та функціонально адаптованих до застосування з безпілотних літальних апаратів (БпЛА) і здатних після відокремлення від носія здійснювати коригування траєкторії польоту.

Необхідність розвитку таких боєприпасів зумовлена тим, що точність скидання звичайних боєприпасів із БпЛА значною мірою залежить від параметрів руху носія, метеорологічних умов, висоти польоту, характеристик системи скидання, динаміки боєприпасу після його відокремлення, а також від практичних навичок оператора БпЛА. Одночасний вплив зазначених чинників може спричиняти розбіжність між фактичною та розрахунковою точками влучання. Використання функції коригування траєкторії дозволяє компенсувати похибки та підвищити прогнозованість результату застосування. Тобто якщо після скиду на боєприпас діє боковий вітер і відхиляє від точки прицілювання, то модуль коригування дає команди на виконавчі механізми і спрямовує його в ціль.

У цьому дослідженні під боєприпасом із модулем коригування траєкторії польоту розуміється боєприпас, оснащений електронним обладнанням і механізмами, що після його відокремлення від БпЛА забезпечують можливість зміни параметрів польоту відповідно до закладених алгоритмів, зовнішніх команд або інформації, отриманої від бортових сенсорів, з метою зменшення відхилення від розрахункової точки влучання. На відміну від некоригованих боєприпасів, траєкторія яких після відокремлення переважно визначається початковими умовами та впливом зовнішнього середовища, кориговані мають додатковий модуль керування. Зі зростанням рівня автономності підвищуються вимоги до надійності програмного забезпечення, коректності алгоритмів, захищеності інформаційного обміну та стабільності функціонування системи.

Важливою умовою ефективного застосування таких боєприпасів є забезпечення їх функціональної та технічної сумісності з конкретним типом БпЛА. Вона охоплює масо-габаритні параметри, кріплення, допустимий вплив на центрування та аеродинамічні характеристики БпЛА, енергетичну сумісність, інформаційний обмін та узгодженість із системами керування. Зміна маси або конфігурації навантаження може впливати на тривалість польоту, маневреність і загальну стійкість БпЛА, тому оцінювання коригованого боєприпасу окремо від носія має обмежену практичну цінність.

Ключове значення для коректного функціонування системи має точність визначення навігаційних параметрів і достовірність інформаційного забезпечення. Коригування траєкторії передбачає наявність достовірної інформації про просторове положення боєприпасу, параметри його руху або положення визначеної точки. Неточність навігаційної інформації, часові затримки її передавання, нестійкість каналів зв'язку та дія зовнішніх перешкод можуть суттєво обмежувати функціональну ефективність модуля коригування.

Модулі коригування відрізняються насамперед способом формування команд керування. В одних варіантах зміна траєкторії відбувається за наперед заданим алгоритмом, в інших – з урахуванням інформації, яку система отримує від бортових датчиків або зовнішніх джерел. Окремий інтерес становлять комбіновані рішення, коли початкові параметри польоту задаються заздалегідь, а надалі уточнюються залежно від фактичного руху боєприпасу та умов зовнішнього середовища.

Практичне застосування модулів коригування значною мірою визначається обмеженнями за масою, габаритами та доступним енергетичним ресурсом. Коригований боєприпас додатково містить елементи керування, обчислення та живлення, що збільшує складність конструкції. Це зумовлює необхідність пошуку компромісу між розширенням функціональних можливостей системи та обмеженням маси додаткового обладнання. Для тактичних БпЛА цей чинник набуває особливого значення, оскільки навіть незначне збільшення маси корисного навантаження може суттєво впливати на характеристики носія. Ефективність застосування таких систем доцільно оцінювати комплексно. Одного показника точності недостатньо. Розглянемо, що до системи критеріїв входять: стабільність функціонування, повторюваність результатів, надійність, стійкість до зовнішніх впливів, сумісність із носієм,

вплив на льотно-технічні характеристики БпЛА, технічна готовність, простота експлуатації та ресурсна ефективність.

$$E = f(K_{\text{т}}, K_{\text{н}}, K_{\text{с}}, K_{\text{ст}}, K_{\text{р}}),$$

де E – узагальнена ефективність застосування; $K_{\text{т}}$ – показник точності; $K_{\text{н}}$ – показник надійності; $K_{\text{с}}$— показник сумісності з носієм; $K_{\text{ст}}$ –показник стійкості до зовнішніх впливів; $K_{\text{р}}$ – показник ресурсної ефективності.

Такий підхід дозволяє уникнути ситуації, коли система визнається ефективною лише за однією характеристикою, тоді як інші її параметри істотно обмежують практичну придатність.

Вагоме значення має проведення випробувань у складі конкретного безпілотного авіаційного комплексу. Лабораторне підтвердження працездатності окремих компонентів не може повністю характеризувати поведінку системи в реальних умовах. У процесі комплексного оцінювання необхідно враховувати зміни параметрів носія, зовнішні метеорологічні чинники, вібраційні та електромагнітні впливи, похибки інформаційних систем, а також стабільність роботи при повторному застосуванні. Особливого значення набуває верифікація програмного забезпечення та навігаційних компонентів, від коректності функціонування яких залежить точність і надійність роботи системи. Оскільки коригування траєкторії залежить від програмно-апаратної обробки даних, помилки алгоритмів або некоректні вхідні параметри можуть істотно впливати на кінцевий результат. Доцільно передбачити послідовну перевірку працездатності системи: спочатку за результатами математичного та імітаційного моделювання, а після позитивних результатів – шляхом експериментальної перевірки в контрольованих умовах.

Подальший розвиток цього напряму пов’язаний із використанням багатосенсорної обробки даних, підвищенням автономності та впровадженням алгоритмів адаптивного керування. і зростанням рівня автономності підвищуються вимоги до надійності програмного забезпечення, коректності алгоритмів керування, захищеності інформаційного обміну та стабільності роботи системи в різних умовах застосування.

Таким чином, застосування боєприпасів для БпЛА з модулем коригування траєкторії польоту є перспективним напрямом розвитку безпілотних авіаційних систем, спрямованим на підвищення точності та прогнозованості результатів застосування. Разом із тим ефективність таких систем визначається не окремим

технічним рішенням, а якістю інтеграції всіх складових комплексу. Їх подальше вдосконалення має здійснюватися на основі системного підходу, комплексного моделювання, випробувань у складі конкретного носія, стандартизації та об’єктивного оцінювання функціональної надійності й сумісності.

Онищенко В. М., канд. техн. наук
Терещенко О. П.
Долинюк В. В., курсант
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

МОДЕЛЮВАННЯ ЗБУРЕННОГО РУХУ ТА НАВАНТАЖЕННЯ КОНСТРУКЦІЇ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА ПІД ЧАС СТРІЛЬБИ

Сучасний досвід ведення бойових дій демонструє необхідність розробки ефективних технічних засобів та інженерних рішень для протидії масованим загрозам з повітря. Одним із перспективних напрямів створення безпілотного літака для боротьби з ворожими цілями виступає застосування мобільних повітряних платформ, обладнаних спеціалізованими засобами виявлення, зближення з ціллю та вогневого ураження. Разом із тим інтеграція артилерійського озброєння на борту безпілотних літальних апаратів (БпЛА) породжує вирішення комплексного науково-технічного завдання.

Під час виконання вогневих завдань на планер літального апарата діють виражені імпульсні сили віддачі, які у поєднанні з обумовленими атмосферною турбулентністю аеродинамічними збуреннями провокують виникнення інтенсивних динамічних коливань. Подібні вібраційні процеси здатні за відносно короткий проміжок часу призвести до прискореного утомного руйнування елементів силового набору, зниження рівня експлуатаційної міцності конструкції, а також погіршення точності наведення та стрільби.

З огляду на суттєві матеріально-технічні витрати та часові обмеження, які супроводжують проведення повномасштабних натурних випробувань, критично важливого значення набувають методи комп'ютерного та математичного моделювання.

Розроблена математична модель нестаціонарного явища аеропружності базується на сумісному рішенні у часі диференціальних рівнянь динаміки польоту, деформування конструкції планера та співвідношень внутрішньої балістики руху снаряда в каналі ствола. Для розрахунку динамічного відгуку конструкції застосовано метод заданих форм, згідно якого пружні деформації повітряного судна розкладаються за симетричними та кососиметричними формами вільних коливань. Аеродинамічні характеристики обчислюються на підставі квазістаціонарної гіпотези, що дає змогу коректно враховувати збурений рух апарата відносно базового режиму польоту.

На основі сформованих математичних моделей різного рівня складності, виконані параметричні дослідження щодо впливу параметрів стрільби та умов закріплення зброї на динамічну реакцію літака. Вони дають змогу детально проаналізувати динамічний стан конструкції БпЛА залежно від жорсткісно-масових характеристик планера, частоти пострілів та тривалості черги. Результати чисельних експериментів підтверджують, що збільшення тривалості вогневого впливу призводить до зростання амплітуди кутової швидкості та перевантажень у центрі мас літака. При цьому найбільші змінні перевантаженя конструкції спостерігаються на кінцях крила внаслідок виникнення високочастотних пружних коливань.

Сумісна дія сил віддачі та зовнішніх атмосферних поривів суттєво збільшує амплітуду змінних напружень, що підвищує темп витрати ресурсу планера.

Таким чином, запропонований розрахунковий комплекс забезпечує прогнозування допустимих режимів стрільби та оптимізацію компонувальних рішень для збереження міцності БпЛА.

Третяк Д. А., Ph. D.
Яромій А. В.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ УДАРНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ТА ТИПИ БОЄПРИПАСІВ ДЛЯ ЇХ ОСНАЩЕННЯ

Широке застосування безпілотних літальних апаратів (далі – БпЛА) у сучасних бойових діях суттєво змінило підходи до ведення розвідки, спостереження та ураження цілей. Одним із поширених напрямів стало використання багаторазових БпЛА мультироторного типу, які у практиці бойового застосування отримали назву «бомбери». Їх основною особливістю є можливість транспортування та скидання боєприпасів із подальшим поверненням апарата до місця запуску.

Актуальність дослідження зумовлена необхідністю узагальнення сучасного досвіду застосування таких БпЛА, визначення їх основних технічних можливостей та систематизації типів боєприпасів, які використовуються як корисне навантаження. Офіційні матеріали Сил оборони України виділяють «бомбери» в окремий напрям застосування БпЛА із можливістю скидання боєприпасів, а сучасні військові публікації підтверджують їх застосування для виконання широкого спектра подібних завдань.

БпЛА типу «бомбер» – це переважно багаторазові мультироторні платформи, обладнані засобами дистанційного керування, відеоспостереження та системою кріплення корисного навантаження. За конструктивними характеристиками вони можуть істотно відрізнятися від відносно легких коптерів до важких багатороторних платформ, здатних транспортувати значно більшу масу корисного навантаження. Тому поняття «бомбер» характеризує насамперед функціональне призначення БпЛА, а не конкретну модель чи уніфікований технічний клас.

Основною особливістю тактики застосування таких БпЛА є поєднання повітряного спостереження, доставки корисного навантаження, його скидання та подальшого контролю результатів. Багаторазовість платформи дає змогу використовувати один апарат із можливістю його повернення для виконання множини завдань, що відрізняє «бомбери» від одноразових ударних FPV-дронів.

У сучасних умовах вони можуть застосовуватися як самостійно, так і у взаємодії із розвідувальними БпЛА, засобами вогневого ураження та іншими безпілотними системами.

Однією із характерних особливостей є можливість використання БпЛА для виконання завдань у різних умовах обстановки та на різних ділянках місцевості. Залежно від поставленого завдання «бомбер» може застосовуватися для ураження визначених об’єктів, підтримки підрозділів, виведення з ладу техніки та нейтралізації особового складу противника, а також для дистанційного мінування ділянок місцевості. Окремі підрозділи також використовують важкі БпЛА як багатоцільові платформи, здатні не тільки переносити боєприпаси, а й виконувати логістичні завдання.

Важливою складовою застосування «бомберів» є вибір відповідного корисного навантаження. Український досвід свідчить, що з БпЛА типу «бомбер» здійснюються скидання боєприпасів різного типу, зокрема уламкової, фугасної та протитанкової дії. Водночас конкретна номенклатура залежить від вантажопідйомності платформи, конструкції системи кріплення та характеру поставленого завдання. Дослідження Харківського національного університету Повітряних Сил зазначає, що для скидання з БпЛА застосовуються боєприпаси як спеціально створені для таких носіїв, так і адаптовані раніше розроблені зразки.

За характером дії боєприпаси доцільно класифікувати на кілька основних груп. Уламкові боєприпаси забезпечують ураження цілей переважно за рахунок дії уламків, що утворюються під час вибуху. Фугасні боєприпаси характеризуються переважною дією продуктів вибуху та ударної хвилі й застосовуються для ураження цілей (озброєння, військова техніка та інші матеріальні засоби) та руйнування об’єктів (укриття, фортифікаційні споруди, будівлі). Протитанкові боєприпаси призначені для боротьби з броньованими цілями спрямованою дією кумулятивного струменя. Окремо варто виділити інженерні боєприпаси, зокрема міни, призначені для створення мінно-вибухових загороджень і обмеження дій противника на визначених ділянках місцевості.

Окремої уваги потребують боєприпаси різних калібрів. Їх використання із застосуванням БпЛА має певні конструктивні та експлуатаційні обмеження. Зокрема, характеристики боєприпасу, його підривника та умови застосування мають відповідати можливостям конкретної платформи. Результати практичних досліджень у сфері застосування боєприпасів із БпЛА вказують на необхідність

забезпечення сумісності між боєприпасом і носієм, оскільки особливості їх конструкцій можуть впливати на безпечність та надійність застосування.

Тактика застосування «бомберів» також значною мірою залежить від протидії противника. Однією з основних загроз для застосування БпЛА такого типу є активне використання засобів радіоелектронної боротьби, протиповітряних засобів та засобів вогневого ураження. Тому сучасні безпілотні підрозділи приділяють значну увагу стійкості каналів зв'язку, управління та навігації, а також спостереженню за повітряною обстановкою та організації взаємодії між різними екіпажами БпЛА. Розвиток технологій призводить до постійної адаптації безпілотних систем до нових засобів протидії.

Таким чином, ефективність застосування БпЛА типу «бомбер» визначається не лише характеристиками самого апарата. Важливе значення мають організація роботи екіпажу, наявність розвідувальної інформації, відповідність корисного навантаження поставленому завданню та технічним характеристикам апарата, можливість повторного використання платформи та стійкість до впливу засобів протидії. Саме комплексне поєднання цих показників перетворює «бомбер» із простого носія боєприпасу на багатоцільовий елемент сучасної безпілотної системи.

Подальший розвиток тактик застосування БпЛА типу «бомбер» буде пов'язаний із підвищенням їхньої стійкості до засобів радіоелектронної боротьби, удосконаленням систем спостереження та управління, розвитком спеціалізованого корисного навантаження та вдосконаленням організації взаємодії між розвідувальними й ударними безпілотними системами (підрозділами).

Перспективним напрямом досліджень залишається систематизація бойового досвіду застосування багаторазових БпЛА типу «бомбер» та визначення оптимальних підходів до їх використання у складі підрозділів сил безпеки і оборони України.

Тучемський В. С.
Лобода Р. І.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ ПІДРИВАЧІВ ІЗ ЗАТРИМКОЮ СПРАЦЮВАННЯ

Під час застосування боєприпасів із БпЛА важливим є не лише факт спрацювання бойової частини, а й момент, у який це відбувається. За певних умов миттєве спрацювання при контакті з перешкодою не дає можливості повною мірою реалізувати властивості боєприпасу. Тому в окремих конструкціях застосовується короткочасна затримка між моментом контакту та ініціюванням бойової частини.

Такий підхід дає змогу змістити момент основної дії боєприпасу відносно точки первинного контакту. Його результативність залежить від характеристик перешкоди, положення боєприпасу в момент зустрічі з нею, швидкості руху, міцності корпусу та стабільності роботи підривача. Через це сам час затримки не може розглядатися як окремий критерій ефективності.

За своїм призначенням короткочасна затримка може застосовуватися у випадках, коли необхідно забезпечити спрацювання бойової частини після проходження або часткового подолання зовнішньої перешкоди. На відміну від миттєвого режиму, основна дія в такому випадку реалізується вже після завершення початкової фази взаємодії боєприпасу з конструкцією об’єкта.

Окремо слід ураховувати особливості застосування боєприпасів кумулятивної дії у складі БпЛА одноразового застосування. За високої швидкості зіткнення з ціллю надмірна затримка спрацювання може призвести до невідповідності моменту ініціювання умовам, необхідним для повноцінної реалізації дії бойової частини. Унаслідок цього ефективність ураження може знижуватися. Тому для таких систем принципове значення має узгодження моменту спрацювання підривача з динамікою зіткнення та конструктивними особливостями бойової частини.

Для боєприпасів, що застосовуються з БпЛА, це питання має додаткову специфіку. Умови відокремлення від носія можуть відрізнятися залежно від положення апарата, параметрів його руху, метеорологічної обстановки та конфігурації корисного навантаження. Через це однаковий режим роботи підривача не завжди забезпечує однаковий результат у різних умовах застосування.

У військово-технічному аспекті значення має не стільки номінальна величина затримки, скільки її відповідність характеру взаємодії боєприпасу з перешкодою. Якщо момент спрацювання не узгоджений із перебігом цієї взаємодії, очікуваний результат може бути суттєво нижчим. Тому характеристики такого режиму мають визначатися за результатами моделювання та випробувань.

Не менш важливою є повторюваність роботи підривача. За однакових початкових умов момент його спрацювання повинен залишатися стабільним, оскільки значний розкид часових характеристик безпосередньо впливає на передбачуваність результату. Саме тому під час випробувань слід оцінювати не лише факт спрацювання, а й сталість роботи пристрою після впливу механічних, температурних і вібраційних навантажень.

У науковому тексті доцільніше використовувати поняття «короткочасна затримка спрацювання після контакту з перешкодою», оскільки воно точніше передає фізичний зміст процесу та не прив'язує його до конкретного числового діапазону.

Таким чином, затримку спрацювання слід розглядати як один із параметрів, що визначає момент реалізації дії бойової частини після контакту з перешкодою. Для боєприпасів, які застосовуються з БпЛА, цей параметр має оцінюватися разом із характеристиками носія, умовами відокремлення та стабільністю роботи підривача.

Пантєлєєва Н. М., д-р. екон. наук, канд. техн. наук, проф.
Лайське Є. В., канд. техн. наук
Хуторна М. Е., д-р. екон. наук, проф.
Державний науково-дослідний інститут випробувань і сертифікації
озброєння та військової техніки

ЕКСПЕРИМЕНТАЛЬНА АПРОБАЦІЯ ІНТЕГРАЦІЇ "ВЕРТОЛІТ – БЕЗПІЛОТНИЙ АВІАЦІЙНИЙ КОМПЛЕКС" ДЛЯ ПРОТИДІЇ БЕЗПІЛОТНИМ ПОВІТРЯНИМ ЗАГРОЗАМ

В умовах особливого періоду для підвищення результативності боротьби з масштабними атаками ворожих безпілотних літальних апаратів (БпЛА) на критичну інфраструктуру та цивільні об'єкти виникає необхідність розширення

бойових можливостей пілотованих літальних апаратів щодо виявлення, супроводу та перехоплення повітряних цілей [1].

Одним із перспективних напрямів є інтеграція вертолітних платформ з БпЛА-перехоплювачами. Технічно і функціонально така інтеграція реалізується відповідно до принципів концепції Manned–Unmanned Teaming (MUM-T), яка передбачає розподіл функцій між пілотованою та безпілотною платформами в межах єдиного інформаційно-управлінського контуру [2]. У контексті протидії безпілотним загрозам інтегрована система “вертоліт – БпАК” може розглядатися як складова багаторівневої системи Counter-Unmanned Aircraft Systems [3]. Доцільність такої інтеграції визначається можливістю функціонального розподілу завдань між платформами. Інтегрований БпАК забезпечує інформаційне та організаційно-технічне супроводження виконання завдання, тоді як БпЛА-перехоплювач виконує політ після відділення від вертольота та реалізує функцію перехоплення повітряної цілі. Вертоліт виконує функції мобільної повітряної платформи, засобу розгортання БпАК та елемента управління місією. Такий розподіл дозволяє частково компенсувати обмеження БпЛА-перехоплювачів, пов’язані з дальністю та тривалістю польоту, швидкістю і висотою застосування, а також забезпеченням стійкого каналу управління, одночасно розширюючи функціональні можливості вертолітної платформи. При цьому інтеграція “вертоліт–БпАК” змінює не лише функціональні можливості окремих платформ, а й структуру бойової системи, інформаційні потоки, розподіл функцій між екіпажем і оператором БпЛА-перехоплювача, вимоги до каналів зв’язку, надійності та безпеки застосування. Тому підтвердження технічної сумісності та оцінювання ефективності такої інтеграції потребують проведення цілеспрямованих наземних і льотних дослідних випробувань.

Мета дослідження полягає в експериментальній апробації моделі інтеграції БпАК на вертолітній платформі шляхом проведення наземних і льотних випробувань та оцінювання показників безпеки відділення, функціонування БпЛА-перехоплювача, інформаційної взаємодії, точності наведення і ефективності виконання цільового завдання.

З метою експериментальної апробації моделі інтеграції БпАК на вертолітній платформі та оцінювання її ефективності було розроблено програму і методику дослідних випробувань. Згідно програми випробувань об’єктом є модернізований вертоліт типу Ми-8, дообладнаний БпАК, призначеним для

виконання завдань протидії безпілотним повітряним загрозам. Метою випробувань визначено можливості та безпеки застосування інтегрованої системи "вертоліт–БпАК" за призначенням. Основний метод дослідних випробувань зразка згідно програми – натурний експеримент (наземний та льотний). Додаткові методи доведення відповідності (розрахунок, аналіз, моделювання) застосовуються для комплексних характеристик зразка, які неможливо та/або недоцільно кількісно оцінювати на етапах натурного експерименту (електро-магнітна сумісність, міцність, льотно-технічні характеристики тощо). При проведенні наземних випробувань передбачено здійснення оцінки комплектності та достатності експлуатаційної документації (вертольоту, БпАК), схеми розміщення та якості монтажу БпАК на вертольоті, працездатності БпАК під час наземного опробування двигунів та інше. Льотні випробування включають перевірку міцності вузлів кріплення в польоті, рекогносцировки району (маршрутів) польотів на місцевості, працездатності БпАК та іншого обладнання вдень і вночі, ефективності та безпеки застосування БпАК не тільки у штатному режимі, а й в бойових умовах, а також навантаження екіпажу і надійність взаємодії. Крім цього враховуються інші умови реального застосування, зокрема зміни метеорологічних умов і прояв таких критичних чинників, як погіршення роботи каналу зв'язку, затримка передачі інформації або часткова її втрата.

У методиці випробувань запропоновано метод оцінювання ефективності інтегрованої системи "вертоліт–БпАК", який включає: 1) формування багаторівневої стохастично-сценарної моделі на основі системи показників; 2) сценарне та імітаційне моделювання з одержанням прогнозованих значень оцінювання показника інтегральної ефективності системи та інших часткових показників; 3) ризик-орієнтований аналіз; 4) експериментальні льотні випробування зі збором первинних даних; 5) валідація моделі за експериментальними даними та оцінювання її адекватності; 6) надання рекомендацій щодо удосконалення моделі, потреби проведення подальших випробувань, прийняття рішень стосовно застосування дослідного зразка. Відмітимо, що в єдиному інтегральному критерії поєднані показники експлуатаційної надійності, сумісності платформ, якості інформаційної взаємодії, ефективності взаємодії за системою "людина-машина", бойової і часової ефективності виконання завдання за призначенням. Це забезпечує комплексне оцінювання інтегрованої системи "вертоліт–БпАК", враховуючи

випадкові процеси її функціонування, ризики виникнення відмов, сценарну невизначеність і результати імітаційного моделювання. За прийнятими вхідними даними, сценарним підходом та імітаційним моделюванням одержано прогнозовані значення показників оцінювання ефективності системи “вертоліт–БпАК”, які показали істотну залежність ефективності виконання інтегрованою системою місії від умов її функціонування. Зокрема, при зміні сценарію прослідковується механізм деградації ефективності, а саме зменшення значень експлуатаційної ефективності за методологією RAMS, якості інформаційної взаємодії та сумісності компонентів інтегрованої системи, що призводить до зменшення Ефективність виконання місії за конкретним сценарієм. Оцінювання інтегральної ефективності системи “вертоліт–БпАК” за всіма сценаріями за результатами імітаційного моделювання дозволило довести сценарно залежний характеру її функціонування, кількісно визначити ймовірності переходу між рівнями ефективності, а також виявити найбільш чутливі компоненти інтеграції та обґрунтувати доцільність їх подальшого доопрацювання.

У 2026 р. уперше проведено дослідницькі випробування, де досліджено процес повітряного старту БпЛА-перехоплювача з різних точок підвіски вертольота-носія. Покадровий аналіз показав, що після повітряного старту формується просторове розходження БпЛА-перехоплювача з вертольотом-носієм із характерним поперечним відходом назовні від фюзеляжу (рис.1).



Рис. 1. Характер початкового просторового розходження БпЛА з вертольотом-носієм після повітряного старту

На дослідженій початковій ділянці тенденції до повторного зближення БпЛА-перехоплювача з вертольотом не виявлено.

Під час подальших випробувань підтверджено можливість переходу БпЛА-перехоплювача до самостійного польоту та його зближення з рухомою повітряною мішенню. У досліджених реалізаціях спостерігалося стійке скорочення горизонтальної дальності до мішені з подальшим навмисним відводом БпЛА-перехоплювача після завершення етапу зближення (рис. 2).



Рис. 2. Візуальне спостереження рухомої повітряної мішені на етапі зближення БпЛА

Результати натурних випробувань показали доцільність розгляду повітряного старту, початкового просторового розходження, переходу до самостійного польоту та подальшого зближення з рухомою повітряною мішенню як взаємопов’язаних етапів єдиного процесу застосування БпЛА-перехоплювача з вертольота-носія, а також експериментально підтвердили працездатність такої схеми в заданих умовах.

Подальші випробування доцільно спрямувати на розширення області початкових умов і визначення раціональних режимів спільного застосування пілотованої і безпілотної авіаційних платформ.

Отже, запропонований метод щодо експериментального оцінювання інтегрованої системи типу “вертоліт–БпАК”, на відміну від існуючих, комплексно враховує технічну надійність, якість інформаційного обміну, взаємодію екіпажу і результативність виконання місії за різних сценаріїв застосування. Його практична значимість полягає в застосуванні як інструменту аналізу та порівняння варіантів інтеграції, дослідження впливу окремих факторів, оцінювання сценарних ризиків і підтримки прийняття рішень за результатами експериментальних випробувань, а також у формуванні основи для валідації багаторівневої стохастично-сценарної моделі за результатами експериментальних польотних даних, що слугує підгрунтям для подальшого вдосконалення інтегрованої системи типу “вертоліт–БпАК” за концепцією MUM-T.

Синявський А. А., курсант
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ЗАСОБИ УРАЖЕННЯ БЕЗПІЛОТНИХ СИСТЕМ

Повномаштабне вторгнення принесло в Україну новий вид терору - масовані атаки дронами-каміказе типу "Шахед".

Вони дешеві у виробництві проте не надто швидкі, до 150-180 км/год. Вони можуть літати на далекі відстані та завдавати ударів по інфраструктурі. У більшості випадків витрати на збиття одного шахеда перевищують його вартість. Тому Україна часто для збиття шахедів використовує кулемети, переносні зенітно-ракетні комплекси та FPV-дрони.

Але після появи реактивних безпілотників ворога, які мають значно вищу швидкість, класичні рішення перехоплювачів втрачають свою ефективність, тому почалося оперативне розгортання реактивних дронів-перехоплювачів. Реактивні дрони-перехоплювачі, здатні впевнено наздоганяти та знищувати будь-які високошвидкісні повітряні цілі.

За словами Президента України в вересні 2026 року було знищено близько 57% таких безпілотників, тоді як звичайних - приблизно 85-90%. Випробовують п’ять моделей. Одна вже дійшла до етапу, коли до кінця жовтня Україна розраховує виготовити близько 400 перехоплювачів. Решта чотири ще проходять випробування.

Одна з головних проблем із масштабуванням - двигуни. Значну їх частину Україна імпортує, є і власне виробництво, однак нинішніх обсягів недостатньо. Бракує також фінансування.

Саме бойове застосування більших партій має показати, які моделі варто запускати у справді масове виробництво.

Німецька оборонна компанія Quantum Systems у рамках спільного підприємства з українською WIY (Quantum WIY Industries) підписала лист про наміри щодо постачання Україні десятків тисяч нових швидкісних дронів-перехоплювачів SPYS, розроблених на основі бойового досвіду експлуатації БПЛА STRILA. Перші тисячі цих безпілотників надійдуть уже цього року, а подальше масштабування виробництва на наявних потужностях дозволить випускати по кілька тисяч одиниць щомісяця для системного знищення російських реактивних БПЛА “Герань-4” та “Герань-5”.

Дрон SPYS розганяється до 480-600 км/год, піднімається на висоту до 6000 м, має дальність до 12 км і час польоту до 4 хвилин, а також оснащений 300-грамовою бойовою частиною, денною чи тепловізійною камерою та ШІ-системою термінального наведення з автоматичним захопленням цілі за даними від радарів.

Звичайні механічні перехоплювачі без вибухового заряду можуть розганятися до швидкості 450 км/год, із бойовим зарядом до 300 км/год. На 3D принтері друкується модель ракети з пластику, дрон із карбоновою рамою перевертається пропеллерами до низу і зверху прикріпляється модель ракети. В моделі робиться гострий кут на кінчику та на кінцях лапок дрона, для боротьби з аеродинамікою, що значно зменшить опір повітря на дрон. Камера розташовується на кінчику ракети так, щоб за допомогою сервоприводу можна було керувати кутом нахилу камери з пульта. Це зробить зручний пошук БпЛА в повітрі та зменшить використання енергії батареї.

Інаціатор боєприпасу- це пристрій, який при замкненні електричного кола запускає вибухову реакцію. Активація боєприпасу відбувається за рахунок електричного запалу, який спрацьовує при подачі струму.

Батарею потрібно закріпити знизу конструкції, та надійно закріпити її стяжками для батареї. Батарею потрібно вибирати з достатньо великою ємністю, так як чим швидше дрон рухається тим більше він використовує електроенергії, але якщо батарея буде занадто велика, це може призвести до сильних вібрацій та навіть вихід дрона або його двигунів з ладу. Антену відеопередавача потрібно розмістити вертикально, так щоб вона не заважала батареї та була максимально далеко від пропеллерів дрона. Це зменшить опір повітря та збільшить швидкість дрона. На FPV-дрон потрібно встановити потужні мотори, які допоможуть дрону набирати велику швидкість. Також потрібно встановити відповідне програмне забезпечення.

Після зіткнення з шахедом електричне поле замкнеться та відбудиться детонація вибухового зарду.

Першим українським реактивним перехоплювачем дронів є Alexa Spatium - це швидкісний реактивний безпілотний літак, розроблений українськими інженерами спеціально для знищення малорозмірних повітряних, наземних та надводних цілей у реальних бойових умовах.

Під час випробувань було підтверджено заявлені виробником тактико-технічні характеристики. Безпілотний літак має низку особливостей:

-потужний турбореактивний двигун;

-висока стеля польоту;

-значний бойовий радіус дії;

-широкий діапазон польоту - від низьких до середніх ешелонів;

-гнучка тактика бойового застосування – за заздалегідь заданими координатами або в режимі прямого наведення;

-варіативність бойових частин - уламково-фугасна, кумулятивна, термобарична;

-висока маневреність під час польоту;

-повна дистанційна підготовка і пуск;

-висока максимальна і низька мінімальна швидкість для збереження палива;

-наявність ефективних пошуково-прицільних систем.

Крім того, Alexa Spatium має надійні системи управління та відеопередачі.

Розвиток безпілотників - це яскравий приклад постійних перегонів озброєнь, де на кожен новий крок однієї сторони інша одразу шукає відповідь.

Після підвищення ефективності цієї системи протидії з'явилися реактивні шахеди. Висока швидкість зробила їх недосяжними для звичайних перехоплювачів. У відповідь було розроблено реактивні перехоплювачі, здатні оперативно підніматися в повітря та наздоганяти швидкісні цілі.

Цей процес працює як безперервний цикл, де вдосконалення нападу одразу змушує змінювати засоби протидії. Кожен новий виток перегонів озброєнь піднімає планку швидкості, маневреності та технологічності безпілотників. У цій тривалій дуелі вирішальну роль відіграє не просто наявність нових розробок, а здатність найшвидше запускати їх у масове виробництво. Перемагає той, хто створює економічно доцільні рішення та випереджає супротивника у швидкості адаптації до нових загроз.

СЕКЦІЯ 4
Космічна підтримка дій військ (сил)

Болобан С. І., канд. техн. наук, ст. наук. співроб.
Мельничук М. В., слухач
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА ДЕШИФРУВАННЯ НАФТОХІМІЧНИХ ПІДПРИЄМСТВ ЗА ДАНИМИ КОСМІЧНОГО ЗНІМАННЯ

В роботі запропоновано методику візуального дешифрування нафтохімічних підприємств як інструмент дистанційного аналізу структури та технологічних процесів. Методика включає набір етапів і процедур, що дозволяють ідентифікувати основні складові елементи об'єкту та оцінити їх взаємозв'язки. Паливно-мастильні матеріали становлять стратегічний ресурс, що визначає спроможність ведення бойових дій: вони забезпечують мобільність наземних сил і важкої техніки, експлуатаційну готовність авіаційних та морських компонентів, функціонування безпілотних систем і безперервність логістичних маршрутів. Актуальність роботи зростає в умовах збройної агресії росії проти України, коли особливої важливості набувають питання виявлення, ідентифікації та аналізу критичних об'єктів противника.

Методика включає три етапи: підготовка даних, ідентифікація ключових елементів, просторово-технологічний аналіз.

1. Підготовка даних полягає в обранні космічних знімків різного просторового розрізнення та часу знімання. Ці дані мають задовольняти ряду визначених в роботі критеріям відбору. Також цей етап включає, за необхідністю, проведення радіометричного калібрування знімків та їх георефернціювання.

2. Етап ідентифікації ключових елементів визначає послідовність дій для виявлення та розпізнавання основних складових підприємства на базі сформованої в роботі класифікації та бази даних елементів нафтохімічного заводу.

3. Просторово-технологічний аналіз будує на основі ідентифікованих елементів схеми можливих технологічних потоків і логістичних зв'язків між ключовими ділянками підприємства. Аналіз дозволяє виявити основні напрямки руху сировини та продуктів, ключові елементи інфраструктури.

Сформована методика може бути застосована для оперативного аналізу промислових об’єктів, зокрема для:

оцінки ступеня стійкості технологічних елементів нафтохімічного підприємства;

визначення критичних елементів у технологічних процесах;

моделювання наслідків руйнувань та пошкоджень.

Розроблена методика є науково-практичним інструментом, що базується на системному підході до візуального дешифрування. Вона дозволяє ефективно аналізувати структуру та технологічні процеси нафтохімічних підприємств.

Болобан С. І., канд. техн. наук, ст. наук. співроб.
Портовой М. І., слухач
Житомирський військовий інститут імені С. П. Корольова

ВИЯВЛЕННЯ РУЙНУВАНЬ ОБ’ЄКТІВ ЗА ДАНИМИ КОСМІЧНОГО ЗНІМАННЯ СЕРЕДНЬОГО ТА МАЛОГО ПРОСТОРОВОГО РОЗРІЗНЕННЯ

Використання космічних знімків має велике значення у військовій справі. Завдяки даним, отриманим з космічних апаратів, можна оцінювати стан місцевості, споруд або техніки, наявність руйнувань тощо. Для вирішення таких задач найчастіше застосовуються знімки з надвисоким просторовим розрізненням, які є не завжди доступними. Тому виникає потреба формування методичного апарату для підтвердження пошкоджень та руйнувань на основі більш доступних знімків середнього та малого розрізнення, що забезпечують частіше оновлення інформації на великих територіях.

Складність визначеної науково-практичної задачі полягає в тому, що зображення середнього та малого розрізнення не дають детальної інформації про об’єкти та зміни в них. Також ускладнюють вирішення задачі умови знімання, а саме освітлення, кут знімання, наявність хмарності тощо. Додатковою проблемою є потреба визначення можливості отримання даних, що пов’язана з періодичністю прольоту космічних апаратів (КА).

Пропонований підхід включає два комплекси робіт – аналітичний та практичний. Перший комплекс спрямований на визначення КА середнього та малого просторового розрізнення, що здійснюють оптико-електронне знімання

у визначений момент часу. Це процес базується на створений в роботі базі даних КА та дає змогу визначити, які апарати є найдоцільнішими для моніторингу визначених зон.

Другий комплекс включає безпосередньо методику виявлення руйнувань за знімками середнього та малого просторового розрізнення, що дозволяє оперативно й з прийнятною точністю виявляти наслідки руйнувань об'єктів. В складі методики передбачено попередню підготовку матеріалів і подальше визначення стану території. Для вирішення задачі застосовано методи виявлення змін – за відтінками, за формою, за відбивними властивостями тощо.

Пропонований підхід є важливим для розвитку методичного апарату обробки даних космічного знімання. Його впровадження підвищить ефективність підтвердження змін на об'єктах, зменшить вплив людського чинника та сприятиме більш якісному плануванню подальших дій.

Гордієнко Ю. О.
Лобода В. В.
Житомирський військовий інститут імені С. П. Корольова

МОНІТОРИНГ ІНОЗЕМНИХ ЯДЕРНИХ ВИПРОБУВАЛЬНИХ ПОЛІГОНІВ ЗАСОБАМИ СЕЙСМІЧНОГО ГРУПУВАННЯ З УРАХУВАННЯМ ФОРМИ ОЧІКУВАНОГО СИГНАЛУ

Вихід рф з Договору про всеосяжну заборону ядерних випробувань та активізація робіт щодо модернізації інфраструктури ядерного полігону "Нова Земля" свідчать про ймовірність підготовки до проведення таких випробувань. Також не виключається, як одного з видів розрахунків за постачання зброї та активну участь підрозділів ЗС кндр на боці московії у агресії проти України, передача рф технологій військового характеру, у тому числі з модернізації ядерної зброї, та подальше їх сумісне випробування. Тому питання моніторингу ядерних випробувальних полігонів (ВП) залишається актуальним.

В Україні завдання контролю за випробуванням ядерної зброї покладено на Головний центр спеціального контролю (ГЦСК) Державного космічного агентства (ДКА) України. Для моніторингу районів Земної кулі у дальній зоні найбільш ефективним елементом мережі сейсмічних спостережень ГЦСК є

система сейсмічного групування (ССГ), яка увійшла до Міжнародної системи моніторингу як станцій PS45.

Реалізовані методи оброблення вимірювальних даних ССГ (метод регульованого спрямованого прийому та метод кроскореляції) потребують значних обчислювальних затрат, як для пошуку району для якого перевищено значення порогу, так і для пошуку ділянки в межах району для якого вирішальна функція приймає максимальне значення. Крім того, існуючи методи оброблення вимірювальних даних ССГ не дозволяють реалізувати безперервний моніторингу певного району Земної кулі, оскільки повністю не виключають вплив сейсмічних сигналів від подій за межами району моніторингу.

В доповіді запропонований підхід щодо обробки вимірювальних даних ССГ, який дозволяє реалізувати безперервний моніторингу ядерних випробувань на ВП без попередньої оцінки належності сигналу сейсмічними джерелам інших районів Земної кулі. Виявлення сейсмічного сигналу від ядерних вибухів на ВП реалізовано шляхом визначення ступеня відповідності отриманої вибірки вимірювальних даних на виході ССГ, після формування максимуму діаграми спрямованості ССГ на відповідний ВП, та раніш зареєстрованим сигналом від ядерних вибухів на даному ВП. Приведено результати тестування запропонованого підходу для сейсмічних сигналів від землетрусів з різних районів Земної кулі та ядерних вибухів на Північно-Корейському випробувальному полігоні.

Якименко В. С.
Андрющенко К. О., курсант
Житомирський військовий інститут імені С. П. Корольова

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ СУПУТНИКОВОГО ЗВ’ЯЗКУ

Для підрозділів тактичної ланки управління основним видом зв’язку є радіозв’язок. Кожен підрозділ використовує електромагнітний простір для обміну інформацією. Засоби радіоелектронної боротьби (РЕБ) та радіоелектронної розвідки (РЕР) постійно здійснюють моніторинг електромагнітного середовища, у разі виявлення ретрансляторів,

радіопередавачів, здійснюється придушення. Артилерія не дозволяє забезпечити існування проводових систем зв'язку. За таких умов система супутникового зв'язку (СЗ) у тактичній ланці управління ("командир бригади — батальйон — рота — окремий БПЛА/Екіпаж") перетворилася з допоміжного каналу на основу для забезпечення ситуаційної обізнаності, швидкісного обміну даними та безперервного відеострімінгу у режимі реального часу.

Систем супутникового зв'язку підрозділів Збройних Сил України.

В Збройних Силах України використовують гібридну модель супутникового зв'язку, поєднуючи цивільні низькоорбітальні (LEO), геостаціонарні (GEO) та середньоорбітальні (MEO) системи.

Starlink (SpaceX):

основні характеристики системи це низька затримка (Latency 20–40 мс), висока швидкість (до 500 Мбіт/с), компактність, відносна стійкість до завад РЕБ через спрямованість вузького променю (beamforming) та високу динаміку LEO-супутників.

Проте має ризики геофенсингу, політика компанії щодо заборони безпосереднього використання терміналів на ударних БПЛА, активне використання противником сірого імпорту, політична складова в рішеннях компанії SpaceX.

OneWeb:

альтернатива та резервний канал для Starlink на рівні штабів батальйонів/бригад. Термінали OneWeb відрізняються високою стійкістю та більшим фокусом на урядовий сектор.

iDirect та Tooway (Геостаціонарні системи GEO):

застосовується переважно на пунктах управління (ПУ) вищого та середнього рівня для створення IP-каналів. Забезпечує середній рівень швидкості (до 50 Мб/с завантаження та до 5 Мб/с передача), при цьому має затримки до 600–800 мс що критично в деяких системах.

Satcom (Військові супутники NATO):

використовує захищені термінали UHF/SHF/K-діапазонів для зв'язку. Забезпечує максимальний захист від РЕБ, шифрування за стандартами NATO, проте мають суворо обмежену смугу пропускання (пріоритет — захищена голос/телеметрія), без ліцензії передача відбувається в відкритому режимі.

Супутниковий зв'язок ЗС рф.

Російська федерація у зв'язку з застарілим супутниковим угрупованням зіштовхується з системним дефіцитом сучасних високошвидкісних тактичних каналів високошвидкісного супутникового зв'язку.

Військовий супутниковий зв’язок рф:

базується на супутниках “Меридиан-М”, “Радуга-1М”, “Експрес” та “Ямал”;

основні термінали в підрозділах — станції серії “Центавр”, “Аурига”, “Ливень”, Р-444-ПТ (“Ладья”);

системи характеризуються громіздкістю, малою пропускною спроможністю, високою чутливістю до РЕБ та значні затримки геостаціонарних орбіт.

Використання сірого імпорту Starlink:

з метою отримання сучасного супутникового зв’язку, підрозділи ЗС рф масово застосовують термінали Starlink, закуплені через треті країни, що створює постійні виклики для їх верифікації та блокування.

Проєкт “Рассвет” (“Бюро 1440”):

російська приватна компанія “Бюро 1440” розгортає власну низькоорбітальну (LEO, орбіта ~500 км) супутникову систему “Рассвет”.

Станом на 2026 рік рф вивела на орбіту перші серійні супутники (понад 30 апаратів) та проведено перші успішні випробування із залученням терміналів 5G NTN та міжсупутникового лазерного зв'язку. Основні заявлені характеристики (швидкість прийому до 140Мб/с передачі – до 30Мб/с, затримка до 40мс, спроможність системи до 10Гб/с).

РФ планує використовувати “Рассвет” для прямої передачі даних на тактичні планшети, інтеграції в комплекси РЕБ/РЕР та створення системи супутникового управління ударними БПЛА далекого радіуса дії, що може позбавити ворога залежності від Starlink.

Програма Українського національного супутникового зв’язку

Залежність від приватних іноземних операторів створює ризики для підрозділів що потребують постійного якісного супутникового зв’язку. Випадки відключення системи StarLink на певний час, заборона використання в певних районах зумовило старт розробки суверенних супутникових спроможностей.

Розвиток суверенного угруповання:

в Україні реалізуються та готуються проєкти з розгортання власної супутникової мережі на низькій орбіті (зокрема, ініціативи UASAT / проєкт компанії Stetman із плановим розгортанням угруповання зі 360 супутників). На жовтень 2026 року виведено 1-й тестовий супутник. Орієнтовні характеристики (швидкість завантаження – 70-100Мб/с, передачі – 5-15Мб/с, затримка до 700мс).

1-й етап серійного запуску заплановано в 2027 році виведенням на орбіту перших 120 серійних супутників (угоди про бронювання місць на ракетах SpaceX вже укладено).

Повна конфігурація угруповання планується 2027–2029 роках, проєкт передбачає масштабування мережі до 360 супутників на висоті ~550 км для забезпечення постійного покриття та обслуговування до 100 000 військових і державних терміналів.

Перспективи розвитку тактичного СЗ ЗСУ:

Multi-Orbit & Multi-Vendor концепція: Одночасне використання терміналів, здатних переключатися між Starlink, OneWeb та майбутньою національною мережею в автоматичному режимі при придушенні одного з операторів засобами РЕБ противника.

Інтеграція з MESH-мережами (Sat-to-Mesh Gateways): Використання супутникового термінала як "вхідних воріт" (gateway) для локальних радіомереж (Silvus, TrellisWare, Meshtastic) на рівнях взводу/відділення.

Захищені Phased Array антени (ФАР/Flat Panel): Перехід на низькопрофільні плоскопаралельні антени для легкої та броньованої техніки, які забезпечують зв'язок у русі (SOTM — Satellite-on-the-Move) та мінімізують візуальну та теплову помітність.

Direct-to-Cell технології: Перспектива прямого підключення звичайних тактичних смартфонів та планшетів (системи Кропива, Дельта) до супутників LEO без проміжних габаритних тарілок.

Висновок: Супутниковий зв'язок став критичним фактором виживання та ефективності тактичної ланки управління. Україна наразі утримує якісну перевагу за рахунок інтеграції західних сузір'їв LEO (Starlink, OneWeb), проте активні кроки ворога у розгортанні власної системи "Рассвет" вимагають від України не лише впровадження засобів протидії супутниковим терміналам противника, а й прискорення створення власного захищеного супутникового ресурсу та масового впровадження терміналів типу SOTM для бойової техніки. Як альтернативу слід розглядати розгортання багато ієрархічну MESH систему для потреб Сил оборони України.

Самчишин О. В, канд. техн. наук., ст. досл.
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ ІЗ ДЕШИФРУВАННЯ МАТЕРІАЛІВ КОСМІЧНОЇ ВИДОВОЇ РОЗВІДКИ В УМОВАХ ВІЙНИ росії ПРОТИ УКРАЇНИ

З набуттям спроможностей Силами оборони України наносити далекобійні удари на стратегічну глибину, вимоги до підготовки військових фахівців з дешифрування матеріалів космічної видової розвідки значно зросли та посилились. Особливостями застосування далекобійних ударів Силами оборони України по території росії, окрім ураження класичних військових об’єктів (військово-морських баз, пунктів постійної дислокації, авіабаз, стартових майданчиків ракетних військ стратегічного призначення, баз зберігання озброєння та військової техніки), визначаються системні руйнування логістики, військово-промислового комплексу та економічного потенціалу ворога, здебільшого з використанням зброї власного виробництва. Удари наносяться не лише у прикордонних чи центральних областях (Курська, Самарська, Саратовська, Московська), а й на відстані понад 3 000 км від кордону (наприклад, об'єкти в Ямало-Ненецькому автономному окрузі). Проведення таких операції не можливе без врахування матеріалів космічної розвідки, як основного джерела інформації про визначені об’єкти.

Підготовка військових фахівців з дешифрування даних космічної розвідки (дистанційного зондування Землі) в умовах повномасштабної війни зазнала кардинальних змін. Основним центром підготовки таких спеціалістів в Україні є Житомирський військовий інститут імені С.П. Корольова, де функціонує спеціалізована Кафедра космічної розвідки, а також науково-дослідний відділ розвитку космічних систем та видової розвідки Науково-дослідного управління розвитку спеціальних систем та інновацій.

Через нестачу важкого ракетного озброєння та далекобійних БПЛА, вкрай важливо якісно, достовірно, точно та оперативно проводити дешифрування даних космічної розвідки законних воєнних цілей які забезпечують і підтримають ведення бойових збройними угрупуваннями росії. Наприклад:

нафтопереробні заводи та нафтобази: удари завдаються не просто по території, а по критичних елементах – установках первинної переробки нафти.

Послідовне виведення з ладу кількох таких ліній призводить до повної зупинки заводів (зокрема на Московському, Ільському та інших підприємствах).

хімічна промисловість: системне виведення з ладу підприємств хімічної галузі росії, які задіяні у виготовлені твердого палива для російських ракет, створює ланцюжкову проблему для всього виробництва засобів нападу росії.

Окрім нафтового сектору, цілями стають оптико-механічні заводи, підприємства з випуску компонентів для ракет, склади боєприпасів та великі логістичні вузли. Такий підхід підриває можливість росії забезпечувати безперебійне постачання окупаційного угруповання на фронті та фінансувати військові дії.

Ключові особливості підготовки фахівців-дешифрувальників в умовах сучасних бойових дій поділяються на кілька стратегічних напрямів:

1. Робота з різнорідними даними (Мультиспектральність).

Якщо раніше акцент робився переважно на оптичних знімках видимого спектра, то зараз фахівці навчаються аналізувати і розрізняти специфічні спотворення, шуми та текстури металевих об'єктів (техніки) на радіолокаційних знімках, виявляти замасковану техніку і сліди життєдіяльності за тепловим слідом (працюючі двигуни, генератори, вогнища) або визначати наслідки ударів в інфрачервоному та термальному діапазонах.

2. Впровадження штучного інтелекту та автоматизації.

Значне зростання обсягу супутникових даних, що надходить від комерційних сервісів Maxar, Planet Labs, ICEYE та засобів партнерів ускладнює оператору якісно і швидко переглянути терабайти зображень об’єктів розвідки. Тому військових аналітиків навчають взаємодіяти з нейромережами та алгоритмами комп'ютерного зору.

3. Комплексування даних.

Фахівців готують не просто дешифрувальниками а спеціалістами з геопросторової розвідки. Сучасна підготовка полягає у інтеграції супутникових даних із іншими джерелами розвідки (розвідувальних БПЛА, радіоелектронної розвідки, геопросторової інформації тощо) та комплексному аналізі цих даних. Результатом є опис, оцінка та візуалізація фізичних властивостей (характеристик) штучних та природних об’єктів, а також географічно співвіднесеної діяльності на земній поверхні для забезпечення максимально можливої повноти інформації по об’єктах розвідки. А робота з геоінформаційними системами та інтегрованими ситуаційними платформами

(на кшталт системи «Delta»), дає змогу результати дешифрування одразу наносити на цифрову карту.

4. Перехід на стандарти НАТО

Українська система підготовки повністю адаптується під стандарти Альянсу щодо обробки та розповсюдження розвідувальних зображень. В освітньому процесі застосовується методика отримання зображень військової техніки у видимому та інфрачервоному діапазонах для їх дешифрування на матеріалах аерокосмічного знімання на основі стандартів STANAG 4595, AEDP-20, AJP-2.6 та STANAG 4609, що спрощує спільне використання розвідданих із країнами-партнерами.

Таким чином, сучасні військові фахівці з дешифрування матеріалів космічної видової розвідки повинні не тільки досконало знати дешифрувальні ознаки озброєння і військової техніки збройних угрупувань росії, а й розуміти технологічні процеси, структуру військово-промислового комплексу та майстерно володіти сучасним спеціалізованим програмним забезпеченням і передовими технологіями ІТ-сфери для ефективної, оперативної та достовірної обробки даних космічної розвідки.

Бобай Ю. Ю.
Магалецький О. О.
Житомирський військовий інститут імені С. П. Корольова

ТРАНСФОРМАЦІЯ ВІЙСЬКОВОГО ЗАСТОСУВАННЯ КОСМІЧНИХ АПАРАТІВ ПІД ВПЛИВОМ ДОСВІДУ російсько-УКРАЇНСЬКОЇ ВІЙНИ 2014–2026 рр.

Російсько-українська війна стала одним із найбільш показових сучасних конфліктів, що докорінно змінили роль космічних систем у забезпеченні військових операцій. Починаючи з 2014 року, а особливо після початку повномасштабного вторгнення російської федерації у 2022 році, космічні апарати та пов’язані з ними наземні комплекси набули значення критичного елемента інформаційного забезпечення бойових дій. Сучасне військове застосування космічних систем охоплює широкий спектр завдань: супутниковий зв’язок, позиціонування, навігацію і синхронізацію, а також

розвідку, спостереження та рекогносцирування (включно з отриманням оптичних і радіолокаційних зображень).

Досвід збройного протистояння засвідчив, що космічний апарат недоцільно розглядати як ізольований технічний засіб. Він є лише складовою частиною цілісної космічної системи військового призначення. Її ефективність визначається узгодженою взаємодією орбітального сегмента, наземних комплексів управління та приймання інформації, каналів передачі даних, програмно-апаратних засобів опрацювання інформації та безпосередніх користувачів на тактичному та оперативному рівнях.

За оцінкою американської дослідницької організації RAND Corporation (назва утворена від Research And Development), найбільш вагомими для військових операцій у війні в Україні стали три ключові напрями використання космосу:

1. Супутниковий зв’язок (SATCOM, Satellite Communications) – забезпечення стабільного обміну даними за умов знищення наземних мереж.

2. Позиціонування, навігація і синхронізація (PNT, Positioning, Navigation and Timing) – прив’язка до глобальних навігаційних систем.

3. Розвідка, спостереження та рекогносцирування (ISR, Intelligence, Surveillance and Reconnaissance) – моніторинг переміщень противника та оцінка наслідків ударів.

На початковому етапі російської агресії у 2014 році Україна мала вкрай обмежені власні можливості використання космічних систем у військових цілях. Після початку бойових дій на сході країни виникла гостра потреба в забезпеченні підрозділів надійним зв'язком та розвідданими. Для цього почали активно залучатися комерційні супутникові сервіси, зокрема цивільні термінали Tooway, які масово закуповувалися волонтерами й стали одним із основних каналів комунікації для багатьох батальйонів.

Водночас, власна космічна інфраструктура України залишалася недостатньою для повноцінного задоволення потреб оборони. Запущений 13 січня 2022 року супутник «Січ-2-30» став першим новим українським космічним апаратом за десятиліття та важливим кроком до відновлення національної космічної діяльності. Проте, як зазначає RAND, його користь для виконання специфічних військових завдань залишилася обмеженою. Ресурс одного апарата не дозволяє сформувати повноцінне супутникове розвідувальне угруповання, здатне забезпечити необхідну періодичність спостереження,

оперативність та стійкість до зовнішнього впливу. Через це Україна до початку повномасштабного вторгнення не мала достатніх власних космічних спроможностей і спиралася на підтримку партнерів та приватного сектору.

Після початку повномасштабної агресії масштаб використання космічних можливостей зріс багаторазово. Комерційні супутникові системи почали обслуговувати не лише стратегічний рівень, а й безпосередньо бойові підрозділи на передовій. Оптичні та радіолокаційні знімки використовувалися для виявлення зосередження військ, відстеження переміщення техніки, моніторингу стану інфраструктурних об'єктів та оцінки ефективності вогневого ураження.

Особливим досягненням стало скорочення часу між отриманням космічної інформації та її передачею кінцевому користувачеві, що дозволило інтегрувати супутникові дані в реальний цикл прийняття військових рішень. Знімки компаній Maxar, Planet Labs та інших комерційних операторів забезпечили своєчасне попередження про дії противника та підвищили загальну ситуаційну обізнаність сил оборони.

Важливою особливістю сучасного конфлікту стало тісне поєднання державного та приватного секторів. Розвиток комерційного космічного ринку надав Україні доступ до передових технологій та ресурсів без необхідності самостійного тривалого та дорогого створення відповідної інфраструктури з нуля.

За даними Організації економічного співробітництва та розвитку (OECD, Organisation for Economic Cooperation and Development), під час війни комерційні сервіси масово застосовувалися для:

забезпечення стійкого супутникового зв'язку;

отримання високо деталізованих оптичних і радіолокаційних зображень;

регулярного моніторингу контрольованих та прифронтових територій.

Найпоказовішим прикладом інтеграції комерційної інфраструктури в систему військового управління стала мережа Starlink. Компанія SpaceX активувала термінали вже наприкінці лютого 2022 року, і за короткий час їхня кількість на лінії фронту сягнула десятків тисяч.

Starlink забезпечив безперебійний обмін даними між підрозділами, командними пунктами та засобами вогневого ураження незалежно від пошкодження традиційних наземних мереж зв'язку. Водночас цей досвід виявив і серйозну системну проблему — залежність критичних військових спроможностей від рішення приватного оператора. Відсутність формалізованих контрактів на початкових етапах

та потенційні розбіжності в пріоритетах підкреслили вразливість такої моделі та потребу в диверсифікації постачальників.

Кібератака на мережу Viasat KA-SAT у день повномасштабного вторгнення (24 лютого 2022 р.), яка вивела з ладу десятки тисяч модемів в Україні та Європі, продемонструвала, що вивести космічну систему з ладу можна не лише фізичним ударом по супутнику, а й через кібернетичний вплив на наземний сегмент та мережеву інфраструктуру. Це вимагає комплексного захисту всіх ланок інформаційного ланцюга.

Поряд з оптичними засобами дистанційного зондування Землі, критично важливого значення набули радіолокаційні системи із синтезованою апертурою (SAR, Synthetic Aperture Radar). На відміну від оптичних сенсорів, які залежать від рівня освітленості та погодних умов, супутники SAR (зокрема угруповання фінської компанії ICEYE) ведуть спостереження вночі, крізь хмарність та за умов задимлення.

За оцінками Міністерства оборони України та експертів RAND, використання даних SAR дозволило виявити тисячі місць розташування ворожої техніки та особового складу, значно підвищивши оперативність і точність розвідки.

Російська сторона активно застосовувала засоби радіоелектронного придушення проти глобальних навігаційних систем (CSIS, Center for Strategic and International Studies) та каналів супутникового зв'язку. Масовий вплив РЕБ призвів до суттєвого зниження ефективності окремих видів високоточних боєприпасів із GPS-навігацією (зокрема снарядів Excalibur).

Водночас українські сили навчилися використовувати комерційні супутникові датчики радіочастотної розвідки (наприклад, системи HawkEye 360) для геолокації джерел ворожих перешкод. Це актуалізувало завдання розробки завадостійких систем, багатосистемного позиціонування та резервних навігаційних технологій.

Головним висновком для України є необхідність подолання значної залежності від зовнішніх сервісів шляхом розвитку власних національних спроможностей та побудови диверсифікованої архітектури. Для цього пропонується реалізувати шість ключових напрямів:

1. Формування розподіленого національного угруповання супутників. Замість створення поодиноких дорогих апаратів доцільно орієнтуватися на

мережу малих і середніх супутників, що підвищує живучість системи у разі втрати окремих елементів.

2. Диверсифікація супутникового зв'язку. Паралельне використання кількох незалежних операторів та резервних каналів передачі даних для мінімізації ризиків монопольної залежності.

3. Розвиток системи космічної ситуаційної обізнаності (SSA/SDA, Space Situational Awareness / Space Domain Awareness). Створення національних можливостей для моніторингу космічних об'єктів, прогнозування загроз і виявлення аномальної активності в орбітальному просторі.

4. Захист наземного сегмента. Забезпечення кіберстійкості та фізичного захисту центрів приймання, обробки й розподілу інформації.

5. Інтеграція розвідувальних даних. Об'єднання космічної інформації з даними БПЛА, радіотехнічної розвідки та наземних сенсорів у єдиний інформаційний контур.

6. Автоматизація на основі штучного інтелекту (ШІ). Впровадження алгоритмів машинного навчання для автоматизованого детектування об'єктів, виявлення змін на знімках та прискорення циклу прийняття рішень (цикл OODA (спостереження, орієнтація, рішення, дія)).

Досвід російсько-української війни (2014–2026 рр.) довів, що військове застосування космосу зазнало якісної трансформації: космічні апарати перетворилися з допоміжного інструменту стратегічного планування на фундаментальний компонент тактичних і оперативних бойових дій.

Ефективність сучасних сил визначається не окремим супутником, а інтегрованою космічно-наземною екосистемою. Для забезпечення національної безпеки Україна має перейти від концепції використання окремих засобів до розбудови розподіленої, стійкої та захищеної національної космічної інфраструктури, що поєднує власні можливості, ресурси союзників і потенціал приватного сектору.

Болобан С. І., канд. техн. наук, ст. наук. співроб.
Шмуйло О. П.
Житомирський військовий інститут імені С. П. Корольова

ФАСЕТНА КЛАСИФІКАЦІЯ ШУМІВ ДАНИХ КОСМІЧНОГО ЗНІМАННЯ

Цифрові космічні знімки є одним із ключових джерел просторово-часової інформації про стан природного середовища та техногенно навантажених територій. Завдяки високим просторовому, радіометричному та спектральному розрізненням сучасні космічні оптико-електронні та радіолокаційні датчики дистанційного зондування Землі (ДЗЗ) забезпечують можливість отримання детальних даних, необхідних для геоінформаційного моделювання, моніторингу екосистем, картографування, аналізу землекористування та вирішення широкого кола задач у сфері безпеки і оборони. Ефективність використання таких даних істотно залежить від їх якості, яка може бути значно знижена через наявність в їх складі шумів.

Шуми на цифрових космічних знімках виникають унаслідок впливу великої кількості технічних, фізичних та інших факторів. До них належать: флуктуації в електронних компонентах датчиків, завади під час передачі сигналу, атмосферні явища тощо. Наявність шумів знижує інформативність зображення, погіршує точність просторових та спектральних вимірювань, ускладнює подальші етапи обробки, такі як візуальне дешифрування, інтерпретація, сегментація, тематична класифікація тощо.

В останні десятиріччя розроблено значну кількість методів боротьби з шумами на космічних знімках. Ефективне застосування таких методів вимагає наявності чіткої класифікації шумів, що є критично важливим для підготовки космічних знімків до попередньої та тематичної обробки. Коректне визначення природи та класу (типу) шуму дозволяє обрати найбільш ефективні методи його зменшення і забезпечити максимальне збереження корисної інформації. Помилки у класифікації шуму можуть призводити до спотворення ознак, зниження точності моделі розпізнавання та некоректних результатів щодо виявлення об’єктів, оцінки змін чи прогнозування процесів.

Існуючі підходи до класифікації шумів космічних знімків звичайно ґрунтуються на окремих його властивостях: статистичних характеристиках шуму,

його спектральних властивостях, структурних особливостях, етапах формування даних, фізичних джерелах виникнення тощо. У науково- прикладних дослідженнях звичайно виділяють декілька типів шумів, що найбільш часто зустрічаються на космічних знімках: гаусів шум, імпульсний шум, спекл-шум, дробовий шум тощо. Але, в більшості випадків не проводиться їх чітка класифікація, шуми об’єднуються в групи за різними ознаками (критеріями) або перелічуються без врахування їх природи, статистичних характеристик тощо.

Найбільш гнучким підходом до класифікації шумів космічних знімків є фасетний метод класифікації. Класична теорія фасетів виділяє п'ять основних універсальних категорій-фасетів (фундаментальна формула PMEST). Застосовуючи теорію фасетів до шумів космічних знімків можна отримати наступні групи класифікації та типи шумів.

1. P (Personality) – Особистість, індивідуальність: найспецифічніша ознака об'єкта. Те, як бачить оператор шум на зображенні. Цей фасет є відправним в аналізі шумів та дає можливість поєднати фасетний та морфологічний підходи, що дуже важливо з практичної точки зору. Дамо назву цьому фасету **«Морфологічний тип»**. В цієї групі можна виділити наступні типи шумів на космічних знімках: флуктуаційний шум на зображеннях отриманих пасивними (оптико-електронними) системами; флуктуаційний шум на зображеннях отриманих активними знімальним системами (радіолокаційними, лідарними датчиками); періодичний шум; шум смугастості; імпульсний шум; постерізація (бендінг); нерівномірна яскравість (плями на зображенні, шум «перлина» тощо); відблиски; димка; дефокусування тощо.

2. M (Matter) – Матерія: речовина об’єкту. Це фізична субстанція чи носій даних, у якому виникає визначений шум. Тобто, у нашому випадку, – в якому фізичному вигляді існують дані про сцену знімання в момент виникнення шуму. Назвемо цей фасет – **«Природа шуму»**. Класами шумів такого фасету будемо рахувати наступні: оптичні шуми, шуми радіодіапазону, шуми електроніки, цифрові шуми.

3. E (Energy) – Енергія: процеси, що призвели до появи об’єкту дослідження. Тобто, яка дія «активувала» проблему. У нашій трактовці: процес, при якому виникає шум. Надамо назву цьому фасету – **«Процес»**. В такому випадку класами шумів цього фасету є: *шуми процесів взаємодії та формування електромагнітного сигналу*; *шуми процесу експозиції*, *шуми процесу*

дискретизації та квантування, *шуми процесу передачі даних, шуми процесу запису даних на носіях, шуми процесу обробки*.

4. S (Space) – Місце, простір: локалізація місця проявлення об'єкту дослідження. У нашому випадку – де саме локалізований шум за простором на знімку (на скільки він розповсюджений по зображенню). Будемо називати цей фасет – «**Локалазація»**. В залежності від розповсюдження шуму по зображенню розрізняють глобальний та локальний шуми.

5. T (Time) – Час: період часу або стадії життєвого циклу об'єкту дослідження. У нашій класифікації – на скільки шум є стабільним за частотно-часовими характеристиками. Надамо назву цьому фасету – **«Частотно-часові характеристики»**. В залежності від частотно-часових характеристик шуму виділяють: систематичний, випадковий, білий, пофарбований, широкосмуговий, вузькосмуговий шуми тощо.

З часом перелік класичних фасетів поповнився низкою нових – **Instrument, Form, Prodact та Operation**. Адаптація цих фасетів дає наступні групи класифікації шумів.

6. I (Instrument) – Інструмент: конкретний пристрій або об'єкт, що сформував об'єкт дослідження. В нашому випадку обладнання або середовище, всередині якого виникає шум. Надамо назву цьому фасету – **«Пристрій».** До цього фасету включаються категорії шумів, що виникають в середовищах, через які проходить сигнал або окремих пристроях систем отримання та обробки даних космічного знімання: шуми атмосфери, шуми об'єктиву, шуми антени, шуми детектора, шуми аналого-цифрового перетворювача тощо. Наприклад, для оптико-електронних систем ДЗЗ характерні шуми, що формуються детектором оптичного випромінювання, що на зображені проявляються як флуктуаційні шуми. Для детекторів найбільш характерними є фотонний дробовий, темновий дробовий шуми, тепловий шум та шум зчитування.

7. F (Form of presentation) – Форма представлення об'єкту дослідженняя: те, яким чином можна описати шум математично. Це найглибша характеристика шуму – тип взаємодії шуму і зображення. Будемо називати цей фасет – «**Математичняна модель»**. Це «ДНК» шуму. Ця характеристика не змінюється, навіть якщо шум виник у різний час, на різних етапах формування та обробки зображення, у різних сенсорах тощо. Відповідно до моделі шуму будемо виділяти: адитивний, мультиплікативний та винищувальний шуми. Дуже часто поняття

винищувального шуму замінюють морфологічним типом – імпульсний шум, що близько по суті щодо взаємодії такого шуму з зображенням, але не охоплює інші шуми з подібною моделлю (наприклад, відблиски). *Винищувальний шум* проявляється у повній втраті корисного сигналу та його заміні на випадкову або мінімальну (максимальну) величину з динамічного діапазону сигналу. Модель винищувального шуму може бути описана виразом:

$$F(j, k)=(1-p)F_0(j, k)+ p\cdot\varepsilon(j, k)$$

де p – двійковий параметр, який може приймати лише значення 0 (винищувальний шум присутній) або 1 (шум відсутній); $\varepsilon(j, k)= \varepsilon_{m0}(j,k)$ – у випадку випадкового винищувального шуму; $\varepsilon(j, k)= F_{max}$ або F_{min} – у випадку заміни пікселя на мінімальну (максимальну) величину з динамічного діапазону сигналу.

8. **Pr (Prodact)** – Продукт, результат: те, що є кінцевим результатом дії об'єкту дослідження. Цей фасет класифікує шуми в залежності від того, до яких наслідків призводить наявність шуму (оцінка ризиків): шум, що призводить до втрати радіометричної точності, неможливості дешифрування, помилок у вимірах тощо. Назвемо це фасет – **«Ризик».** Оцінка ризиків це критичний міст між теорією та реальною роботою оператора з обробки даних ДЗЗ. Цей фасет перетворює суху класифікацію на інструмент прийняття рішень при відповідях на питання: «Чи можна за цим знімком обраховувати спектральні індекси?», «Чи достатньо точні дані для розпізнавання типів об'єктів?» тощо.

9. O (Operation) – Операция: зовнішній вплив на об'єкт дослідження. В нашому випадку – метод «лікування» (метод зменшення) шуму. Цей фасет перетворює фасетну класифікацію шумів на повноцінний операційний регламент. Оператор може бачити не лише проблему та розуміти її суть, а й визначати шлях її вирішення. Фасет класифікує шуми в залежності від того якими методами він може буте зменшений (усунутий). Наприклад: шум, що зменшується лінійної локальної фільтрацією; шум, що усувається обробкою в частотні області тощо. Можливість зменшити шуми на зображенні це важлива практична складова пропонованої класифікації. Застосування обробки завжди призводить до зменшення інформаційної ємності зображення. Тому крім методів зменшення важливо знати негативні наслідки до яких вони можуть призвести. Цей фасет будемо називати **«Метод та ризик усунення».**

Аналіз типів шумів з точки зору фасетного підходу дозволяє сформувати діагностичні карти шумів зображень. Приклад діагностичної карти «спекл шуму» на ведений на рис. 1. Такі карти можуть складатися у зведені аналітичні таблиці за видом зображення (панхроматичне, кольорове, мультиспектальне, радіолокаційне тощо). Формування таких аналітичних таблиць є фінальним етапом побудови фасетної класифікації шумів.

Код	Назва фасету	Категорія шуму
P	«Морфологічний тип»	спекл-шум
M	«Природа шуму»	шум радіодіапазону
E	«Процес»	шум когерентної інтерференції
S	«Локалізація»	глобальний піксельний шум
T	«Частотно-часові характеристики»	широкосмуговий некорельований випадковий шум, що описується Гамма-розподілом, розподілом Релея або експоненційним законом
I	«Пристрій»	шум антени радіолокатора
F	«Математична модель»	мультиплікативний шум
Pr	«Ризик»	шум, що призводить до зниження радіометричного розрізнення, формує помилкові межі на зображенні
O	«Метод та ризик усунення»	шум, що зменшується операцією multilooking, адаптивними локальними просторовими фільтрами (Lee, Frost, Gamma-MAP тощо). Ризик усунення – зменшення просторового розрізнення, дефокусування, постеризація

Рис. 1 – Діагностична карта «спекл-шуму»

Таким чином, в роботі обґрунтовано та розроблено багатовимірну фасетну класифікацію шумів космічних знімків. Запропонований підхід забезпечує багатовимірний аналіз кожного морфологічного типу шуму.

Фасетна класифікація шумів космічних знімків по суті формує активний аналітичний інструмент обробки даних ДЗЗ та дозволяє:

формувати точні технічні завдання щодо обробки даних ДЗЗ;

мінімізувати час на попередню обробку космічних знімків;

автоматизувати процес відбраковування знімків щодо подальшої обробки;

формувати у фахівців з обробки даних ДЗЗ системного мислення та навчати фахівців з обробки космічних знімків системному розумінню фізики та математики ДЗЗ.

Універсальність та масштабованість розробленої класифікації полягає у відкритості системи, яка легко дозволяє доповнювати систему новими типами шумів без руйнування загальної логіки класифікації.

Корнієнко І. В.
Попов М. О., д-р техн.наук, проф.
Воєнна академія імені Євгенія Березняка
Андрощук Р. А., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

МОБІЛЬНА СЕЙСМІЧНА ГРУПА ДЛЯ ВИКОНАННЯ ЗАВДАНЬ РОЗВІДКИ

У сучасній практиці ведення технічної розвідки ефективність одержаних результатів критично залежить від архітектури побудови мережі моніторингу. Потреба у балансуванні між безперервністю глобального спостереження та оперативністю отримання розвідувальних даних зумовлює необхідність детального аналізу переваг і обмежень стаціонарних та мобільних засобів сейсмічної розвідки. Стаціонарні сейсмічні мережі функціонують з метою довгострокового моніторингу, забезпечуючи постійне надходження інформації з визначених пунктів спостереження. Перевагами їх застосування є:

1. Безперервність та системність – забезпечують безперервний збір та реєстрацію сейсмічних подій у режимі 24/7, що важливо для формування архіву даних.
2. Висока стабільність характеристик – стаціонарне розміщення датчиків на корінних породах мінімізує вплив антропогенних шумових завад.
3. Інфраструктурна інтеграція – надійні лінії зв’язку та стабільне енергопостачання дозволяють використовувати сучасні комплекси оброблення даних.
4. Доступ до даних міжнародних систем геофізичних спостережень, що дозволяє оперативно отримувати інформацію про сейсмічні події в межах всієї земної кулі.

Наведені переваги дозволяють виконувати розвідувальні завдання оперативно-стратегічного рівня нарівні із засобами космічної розвідки

(наприклад, визначення ступеня враження об’єктів противника на території рф). Проте, для застосування на оперативно-тактичному рівні сейсмічні мережі мають ряд недоліків та обмежень: жорсткість геометрії мережі, тобто базова конфігурація датчиків є незмінною, що призводить до погіршення просторової точності місцевизначення у разі виникнення подій поза зоною оптимального покриття мережі; вразливість до дестабілізуючих факторів – стаціонарні об'єкти легше виявити та вивести з ладу. Використання таких стаціонарних систем є ускладненим або неможливим в умовах ведення бойових дій, що вимагає адаптації їх місць розміщення, геометричних розмірів та розроблення відповідного математичного апарату оброблення даних.

Мобільні сейсмічні мережі призначені для оперативної зміни їх конфігурації, розгортання в районах інтересу та вирішення завдань детальної розвідки. Перевагами їх є гнучкість просторової геометрії, покращення співвідношення сигнал-шум та висока живучість. Недоліками та обмеженнями розгортання в польових умовах є залежність від автономних джерел живлення, необхідність часу на транспортування, створення умов для реєстрації, забезпечення синхронізації часу тощо.

В доповіді представлено підходи до розрахунку конфігурації мобільної сейсмічної групи, її лінійних розмірів, умов розгортання для виконання завдань на тактичному, оперативному та стратегічному рівнях. Це дозволить створити стійкий, пасивний та високоточний канал отримання розвідувальних даних на оперативно-тактичному рівні, забезпечивши підрозділи розвідки оперативними даними, що є критично важливим в умовах агресії рф проти України.

Николюк О. М., д-р економ. наук, проф.
Пивовар П. В., канд. економ. наук, доц.
Поліський національний університет

ВІЙНА ЯК ФАКТОР ТРАНСФОРМАЦІЇ ЗЕМНОГО ПОКРИВУ УКРАЇНИ

Ключові слова: земний покрив, війна, дистанційне зондування Землі, аграрна стійкість, національна безпека.

Воєнна агресія Російської Федерації спричиняє нерівномірні зміни земного покриву України через руйнування поверхні, обмеження доступу до земель і перерозподіл господарської активності. Зміни покриву відображають

порушення виробничих та екологічних функцій територій. Їх оцінювання потребує розмежування зон воєнного впливу, оскільки загальнонаціональні показники згладжують територіальні відмінності.

Мета дослідження. Виявити особливості трансформації земного покриву України у 2016–2025 роках та визначити їх значення для продовольчої, екологічної й територіальної безпеки та планування відновлення.

Матеріали та методи. Використано Google Dynamic World V1 на основі Sentinel-2 (10 м, дев’ять класів покриву). За щоденними оцінками Інституту вивчення війни (ISW) виділено чотири зони: окуповані території, контрольовані РФ понад половину днів року; прифронтові території, що сумарно понад 60 днів перебували в 40-кілометровому буфері лінії зіткнення; 20-кілометрове прикордоння з РФ і РБ поза активними прифронтовими територіями; решту контрольованих урядом умовно-безпечних територій. Щорічні растрові класифікації перетнуто з векторними шарами зон. Абсолютні площі зіставлено із частками класів, оскільки межі зон змінювалися в часі (Рис.1).

Для порівняння типів аграрного землекористування застосовано просторовий проксі-підхід: території в межах полігонів населених пунктів умовно віднесено до особистих селянських господарств (ОСГ), за їх межами – до сільськогосподарських підприємств (СГП). Таке розмежування характеризує просторові відмінності землекористування, проте не встановлює фактичного власника або користувача земельної ділянки.

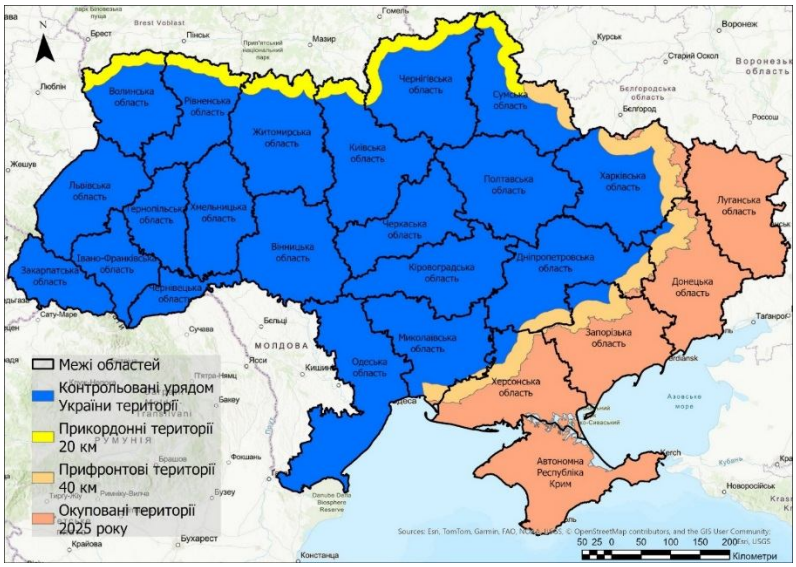


Рис. 1. Операційні зони просторового аналізу земного покриву України в умовах війни, станом на грудень 2025 року

Джерело: побудовано авторами на основі Institute for the Study of War (2026)

Результати дослідження. Найвиразніше порушення загальнонаціональної структури земного покриву зафіксовано у 2023 році. Площа культивованих угідь зменшилася з 349,2 тис. км² у 2022 році до 325,1 тис. км² у 2023 році, або на 6,9 %. Водночас площа відкритих ґрунтів зросла з 1 207 до 2 436 км². У 2025 році культивовані угіддя охоплювали 343,3 тис. км², що свідчить про часткове відновлення після спаду. Площа водних об'єктів скоротилася з 16,2 тис. км² у 2021 році до 13,5 тис. км² у 2025 році. Сукупність змін указує на перебудову аграрної та гідрологічної складових земного покриву (Рис. 2).

Найгостріші зміни локалізувалися у прифронтовій зоні. Частка культивованих угідь знизилася з 68 % у 2022 році до 54 % у 2023 році, а площа відкритих ґрунтів зросла приблизно з 43 до 842 км², майже у двадцять разів. Це узгоджується з інтенсивним фізичним порушенням поверхні внаслідок бойових дій. У 2025 році частка культивованих угідь становила близько 61 %, проте відновлення аграрного покриву поєднувалося зі збереженням порушених земель і рослинного покриву на ділянках обмеженого господарського використання.

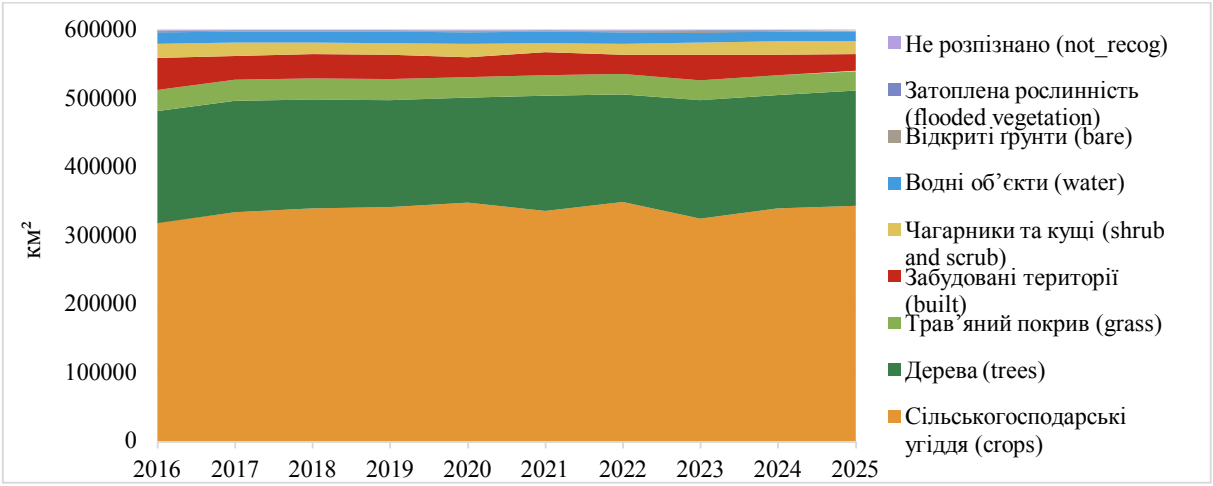


Рис. 3. Динаміка площ основних класів земного покриву України у 2016–2025 роках

Джерело: побудовано авторами на основі (Brown et al., 2022)

На окупованих територіях частка культивованих угідь зменшилася з 68 % у 2022 році до 60 % у 2023 році та знову досягла 68 % у 2025 році. Зростання їх абсолютної площі частково пов'язане з розширенням окупованої зони. Збереження аграрного покриву за таких умов сумісне з експлуатацією земель під окупаційним контролем і не є достатнім свідченням відновлення української

аграрної системи. Інтерпретація цих показників потребує врахування доступу населення до земель, стану інфраструктури та інституційних умов господарювання.

Прикордонна зона характеризувалася послідовним скороченням аграрної функції. У просторовій групі, умовно віднесеній до СГП, частка культивованих угідь зменшилася з 23 % у 2022 році до 13 % у 2025 році, а у групі ОСГ – з 13 % до 8 %. Така динаміка вказує на вразливість як великотоварного, так і домогосподарського землекористування в умовах тривалих безпекових обмежень. Втрата дрібного землекористування має значення для локальної продовольчої самозабезпеченості та життєздатності сільських громад.

Контрольовані урядом умовно-безпечні території зберігали відносно стабільну структуру покриву: частка культивованих угідь у 2021–2025 роках становила від 55 до 57 %. У 2025 році для просторової групи СГП цей показник дорівнював близько 60 %, для ОСГ – 26 %. Ці території залишалися основною базою підтримання аграрного виробництва та продовольчого забезпечення.

На окупованих територіях динаміка ОСГ є значно складнішою. Площа культивованих угідь у їхній структурі зросла з 353,7 км² у 2021 році до 2,1 тис. км² у 2022 році, а у 2025 році становила майже 2,0 тис. км². Однак це зростання передусім пов’язане з розширенням самої окупованої зони після 2022 року. Частка культивованих угідь у структурі ОСГ збільшилася з 9,4% у 2021 році до 24,7% у 2022 році, потім знизилася до 18,3% у 2023 році й стабілізувалася на рівні близько 22% у 2024–2025 роках (табл. 1). Проте навіть відносно стабільні показники не можуть розглядатися як доказ нормального селянського господарювання. ОСГ потребують фізичної присутності родин, безпечного доступу до ділянок, локальних ринків, транспортної доступності та мінімальної інституційної захищеності. Саме ці умови на окупованих територіях порушені найбільше.

Таблиця 1. Площа та частка сільськогосподарських угідь у структурі ОСГ за аналітичними зонами, 2016–2025, км² (%).

Зона	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**
Окуповані території	358 (10%)	497 (13%)	473 (13%)	459 (12%)	518 (14%)	354 (9%)	2131 (25%)	1588 (18%)	1936 (22%)	1962 (22%)
Прикордонна зона 20 км	–	–	–	–	–	–	183 (13%)	157 (12%)	153 (12%)	90 (8%)
Прифронтова зона 40 км	156 (11%)	194 (14%)	194 (14%)	184 (13%)	200 (14%)	151 (11%)	452 (27%)	260 (18%)	446 (22%)	516 (23%)
Контрольовані умовно-безпечні території	13308 (23%)	14624 (26%)	15223 (27%)	14858 (26%)	15220 (27%)	14599 (25%)	14282 (28%)	12514 (25%)	13430 (27%)	13142 (26%)

Джерело: побудовано авторами на основі (Brown et al., 2022)

Отримані результати узгоджується з опублікованими зовнішніми незалежними оцінками. EUSPA, ґрунтуючись на Copernicus Sentinel-1 і Sentinel-2, фіксує скорочення загальної площі культивованих угідь в Україні у 2022 році приблизно на 7% порівняно з середнім за 2017–2021 роки, причому для ключових культур зниження сягало близько 13%, а найсильніші зміни були зосереджені на сході та південному сході країни. Той самий документ посилається на дослідження Deininger et al., де лише 14% оцінених втрат урожайності безпосередньо приписано прямим ефектам війни, тоді як решта пов'язана з ширшим воєнно-економічним середовищем. Іншими словами, просторові зміни земного покриву є лише видимою частиною більшої системної кризи – логістичної, інституційної, демографічної, енергетичної. І саме тому їх слід включати до аналітики національної безпеки (EUSPA, 2023; Deininger et al., 2023).

Висновки. Війна формує просторову поляризацію землекористування України. Прифронтові території зазнають фізичного порушення поверхні, прикордонні – поступового згортання аграрної активності, окуповані – зміни режиму використання земель, тоді як контрольовані умовно-безпечні території підтримують відносну аграрну стійкість. Зміни земного покриву доцільно використовувати як просторові індикатори окремих складових національної безпеки. Регулярний супутниковий моніторинг у поєднанні з даними розмінування, ґрунтової діагностики та демографічної динаміки створює основу для визначення пріоритетів рекультивації, відновлення агровиробництва й підтримки сільських громад.

Топольницький П. П., канд .техн. наук, доц.
Ковальчук М. О., канд. пед. наук, доц.
Поліський національний університет

ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ГІС–ТЕХНОЛОГІЙ У НАВЧАЛЬНИЙ ПРОЦЕС

Сучасний фахівець дедалі частіше працює з інформацією, яка має просторову складову: земельні ресурси, екологічний стан територій, транспорт, інфраструктура, демографічні процеси, результати польових спостережень або дистанційного зондування Землі. Тому геоінформаційні системи доцільно розглядати не лише як спеціалізований інструмент картографів чи геодезистів,

а як універсальну технологію роботи з даними. Саме це стало вихідною ідеєю впровадження ГІС у навчальний процес. За сім років викладання накопичено досвід, який показує: найбільший ефект дає не вивчення окремих команд програмного забезпечення, а поступове формування у студентів просторового мислення і здатності використовувати карту як інструмент аналізу.

Навчання побудовано на прикладі *ArcGIS Pro*, однак головним об’єктом вивчення є не конкретний програмний продукт, а логіка роботи з геопросторовими даними. Студент має зрозуміти, що будь-яка ГІС поєднує карту, таблицю атрибутів і набір інструментів аналізу. Тому з перших занять важливо отримувати видимий практичний результат: створити власний просторовий об’єкт, нанести його на карту, виміряти площу або відстань, додати атрибутивну інформацію. Такий підхід зменшує психологічний бар’єр перед складним програмним середовищем і дає відчуття практичної корисності ГІС уже на початковому етапі.

Структура розробленого практикуму являє собою послідовність практичних етапів із поступовим ускладненням завдань. Після знайомства з інтерфейсом *ArcGIS Pro* студенти переходять до створення векторних шарів, систем координат і проекцій, роботи з атрибутивними таблицями, вибірок за атрибутами та просторовим розташуванням. Далі вивчаються засоби інфографіки, приєднання статистичних таблиць до просторових об’єктів, побудова тематичних карт і підготовка картографічних матеріалів. Важливо, що кожна нова тема спирається на попередню, а не існує як окремий набір функцій.

Наступний рівень навчання пов’язаний із растровими даними та дистанційним зондуванням Землі. Студенти виконують географічну прив’язку зображень, вирізання растрів за межами досліджуваної території, перетворення даних, працюють зі спектральними каналами, індексами рослинності та елементами класифікації знімків. Використання реальних супутникових матеріалів є особливо ефективним, оскільки дозволяє показати, що ГІС працює не лише з готовими картами, а й із первинними даними, з яких можна отримувати нову інформацію про стан території.

Окремий принцип нашого підходу – використання локальних і зрозумілих студентам об’єктів. Значна частина завдань виконується на прикладі Житомирської області, її населених пунктів, лісів, сільськогосподарських територій та інших реальних об’єктів. Коли студент бачить на екрані знайому

територію, навчальна вправа перестає бути абстрактною. Це дає можливість перейти від відповіді на запитання «яку кнопку натиснути?» до запитань «чому цей об’єкт розташований саме тут?», «що змінилося за певний період?» і «які дані потрібні, щоб це пояснити?». Саме в цей момент починає формуватися просторове мислення.

Важливою складовою навчання є перехід від окремих вправ до завершеного прикладного дослідження. У практикумі таким прикладом є аналіз трансформації сільських територій, де статистична інформація поєднується з матеріалами космічного знімання та результатами просторового аналізу. Для студентів це демонструє повний цикл роботи: від пошуку і підготовки даних до аналізу, візуалізації та формулювання висновків. У такому форматі ГІС стає не предметом вивчення, а середовищем для розв’язання реальної наукової або прикладної задачі.

Семирічний досвід показав декілька умов, які суттєво полегшують впровадження ГІС у навчальний процес. По-перше, складність завдань має зростати поступово. По-друге, студенту потрібні підготовлені вихідні дані та чітка логіка виконання роботи, особливо на початковому етапі. По-третє, бажано поєднувати короткі інструкції з елементами самостійного пошуку рішення. По-четверте, завершенням окремих навчальних блоків має бути невеликий власний проєкт, у якому студент сам обирає спосіб представлення результатів. Така організація дозволяє працювати з групами, у яких рівень цифрової підготовки студентів суттєво відрізняється.

Головний результат впровадження ГІС у навчання полягає не в тому, що кожен студент має стати професійним ГІС-фахівцем. Набагато важливіше сформувати здатність працювати з просторово прив’язаними даними, критично оцінювати їх джерела, бачити територіальні закономірності та аргументовано представляти результати за допомогою карт. Такі компетентності можуть бути корисними у природничих, аграрних, екологічних, економічних, управлінських, інженерних та комп’ютерних спеціальностях.

Отже, ГІС доцільно впроваджувати у закладах вищої освіти не лише у вигляді окремої спеціалізованої дисципліни, а й як наскрізний цифровий інструмент для виконання навчальних і дослідницьких завдань. *ArcGIS Pro* у цьому випадку є зручним середовищем, яке дозволяє пройти весь шлях від створення простих просторових об’єктів до комплексного аналізу даних і

підготовки готового інформаційного продукту. Практична спрямованість, робота з реальними даними та поступовий перехід до самостійних проєктів роблять ГІС не додатковою технологією, а дієвим засобом розвитку сучасних професійних компетентностей студентів.

Пивовар П. В., канд. економ. наук, доц.
Савчук А. В., канд. техн .наук, ст. наук. співроб.
Топольницький П. П., канд. техн. наук, доц.
Поліський національний університет
Франжі О. В.
Житомирський військовий інститут імені С. П. Корольова

ДВОДІАПАЗОННА СТАНЦІЯ ПРИЙМАННЯ НАУКОВОЇ ІНФОРМАЦІЇ З КОСМІЧНИХ АПАРАТІВ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ

Сучасні наземні комплекси приймання інформації з космічних апаратів дистанційного зондування Землі (ДЗЗ) мають забезпечувати роботу з різними радіолініями та цифровими потоками. Космічні апарати ДЗЗ відповідно до рекомендацій консультативного комітету з систем космічних даних (*Consultative Committee for Space Data Systems*) передають на Землю наукову інформацію у визначених діапазонах електромагнітних хвиль *L* (від 1 ГГц до 2 ГГц) або *X* (від 7,7 ГГц до 8,5 ГГц).

Відомі в Україні наземні станції, що містять антенну систему, високочастотний тракт, опорно-обертальний привід, систему управління, радіоприймальний пристрій і засоби оброблення даних, переважно забезпечують приймання лише в одному частотному діапазоні: *L* або *X*, залежно від встановленого опромінювача. Це обмежує функціональність наземного інформаційного комплексу та потребує застосування декількох окремих різних засобів приймання наукової інформації для різних діапазонів.

В доповіді представлено обґрунтування побудови дводіапазонної станції приймання наукової інформації в *L*- та *X*-діапазонах із використанням однієї антенної системи та спільної системи управління. Розглянуто технічне рішення щодо розроблення конструктивно об’єднаного *L*/*X*-опромінювача, до виходів

якого підключаються окремі високочастотні тракти. Запропоновано варіант кріплення опромінювача у фокусі антенної системи.

Застосування запропонованої дводіапазонної станції розширює можливості приймання наукової інформації від космічних апаратів ДЗЗ із різними частотними каналами, швидкостями передавання, шириною смуги, типами модуляції та структурами цифрових потоків без використання окремих спеціалізованих антенних постів. Очікуваним технічним результатом є підвищення коефіцієнта використання антенної системи, скорочення часу переналаштування при переході між космічними апаратами ДЗЗ, зменшення кількості дубльованого обладнання та підвищення експлуатаційної гнучкості наземного комплексу.

Завада А. А., канд. техн. наук, ст. наук. співроб.
Франжі О. В.
Беспалко І. А., канд. техн. наук, ст. досл.
Випорханюк Д. М.
Житомирський військовий інститут імені С. П. Корольова

АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ МАНЕВРІВ КОСМІЧНИХ АПАРАТІВ І ВІДОБРАЖЕННЯ ОРБІТАЛЬНОЇ ОБСТАНОВКИ НА ОСНОВІ ФОРМАТУ OMM В ІНТЕРЕСАХ СИЛ ОБОРОНИ УКРАЇНИ

Контроль космічної обстановки для Сил оборони України вже не є суто науковим завдання, а набув практичного значення як складова космічної підтримки дій військ (сил). Від нього залежить своєчасне оповіщення військ про прольоти іноземних космічних апаратів (КА) розвідки, а також виявлення змін їх орбіт. Водночас орбітальне середовище швидко ускладнюється: за даними CelesTrak, станом на 9 жовтня 2026 р. відкритий каталог Космічних сил США містить 35284 об’єкти на орбіті, з них 20267 – корисні навантаження. У доповіді представлено досвід створення автоматизованої системи моніторингу орбітальної обстановки, яка використовує формат OMM (Orbit Mean-elements Message), щодня оновлює локальний каталог, виявляє маневри КА та формує графічні продукти для оцінювання обстановки.

Головне обмеження традиційного формату TLE (Two-Line Elements) – п’ятизначне поле номера об’єкта в каталозі NORAD. Номери від 70 000 до 99999

зарезервовано для службових потреб, тому для звичайних об’єктів практична межа становила 69999. Її було досягнуто 11 липня 2026 р.: наступний каталогізований КА отримав номер 100000. Тимчасова схема Alpha-5, у якій першу цифру номера замінює літера, розширює діапазон до 339 999, але підтримується не всіма джерелами: зокрема, CelesTrak для об’єктів із шестизначними номерами дані у форматі TLE не формує взагалі. Інші обмеження TLE – дворозрядний рік епохи, жорстко фіксовані позиції символів і мінімум супровідних відомостей – ускладнюють автоматизовану обробку даних і ведення історії об’єктів.

Формат OMM, визначений стандартом CCSDS 502.0 “Orbit Data Messages”, ці обмеження знімає. Він подає середні елементи орбіти у структурованому вигляді (XML, JSON, KVN, CSV), допускає номери об’єктів до дев’яти цифр, повну дату епохи та опційну коваріаційну матрицю. Space-Track і CelesTrak поширюють дані у форматі OMM з 2020 р., а для нових об’єктів він фактично став єдиним повноцінним форматом. Слід підкреслити, що OMM не підвищує точності самих елементів: це ті самі середні елементи аналітичної моделі руху SGP4, що й у TLE. Перевага полягає в іншому – дані зручно зберігати в базі як часовий ряд параметрів кожного об’єкта і доповнювати відомостями каталогу (тип об’єкта, країна, дати запуску й сходження). Порівняння форматів наведено в табл. 1.

Таблиця 1 – Порівняння форматів TLE та OMM

Характеристика	**TLE**	**OMM**
Номер об’єкта	5 знаків: на практиці до 69999, з Alpha-5 – до 339999	до 9 цифр
Подання даних	2 рядки по 69 символів з фіксованими позиціями	XML, JSON, KVN, CSV
Рік епохи	дві цифри	повна дата і час
Точність елементів	середні елементи SGP4	ті самі середні елементи SGP4
Коваріаційна матриця	не передбачена	передбачена стандартом, у відкритих даних відсутня
Супровідні відомості	мінімальні	розширені (система відліку, шкала часу, модель руху тощо)
Об’єкти з номерами від 100000	лише Alpha-5 (Space-Track); CelesTrak не формує	доступні повністю

Система побудована за принципом локального зберігання: усі дані зберігаються й обробляються локально, а до зовнішніх джерел система звертається один раз на добу для планового оновлення. Елементи орбіт завантажуються з Space-Track у форматі OMM (клас даних GP, General Perturbations),

а відомості про пуски й сходження – з каталогу SATCAT двома окремими запитами: усі об'єкти, запущені в поточному році, та всі об'єкти, що зійшли з орбіти в поточному році. Другий запит обов'язковий, оскільки більшість сходжень припадає на об'єкти, запущені в попередні роки: досвід травня 2026 р. показав, що за самою лише першою вибіркою кількість сходжень занижувалася приблизно вдесятеро. Отримані дані об'єднуються в локальному каталозі зі збереженням історії змін.

Маневри КА виявляються порівнянням послідовних OMM-записів одного об'єкта у вікні від кількох годин до кількох діб. Ознакою маневру є перевищення порогових значень змін великої півосі Δa, ексцентриситету Δe та нахилу Δi. Пороги визначено емпірично за статистикою змін елементів на інтервалах без маневрів, тобто за рівнем власного шуму даних. Цей шум і обмежує чутливість методу: малі корекції орбіти можуть не перевищувати порогів. Виявлені маневри класифікуються за такими типами:

– підтримання орбітальної позиції (station-keeping) – малі регулярні корекції орбіти навколо номінальних значень;

– фазування (phasing) – зміщення КА вздовж орбіти за рахунок тимчасової зміни великої півосі;

– підняття або зниження орбіти (orbit raising/lowering) – значна одноразова зміна великої півосі;

– вивід з орбіти (deorbit) – серія односпрямованих знижень до висот близько 300 км, після чого атмосферне гальмування за кілька діб завершує сходження КА.

На рис. 1 наведено модельні приклади сигнатур трьох типів маневрів у часовому ряді середньої висоти орбіти h = a − R, де R – екваторіальний радіус Землі, обчисленому безпосередньо з послідовності OMM-записів. Супровід об'єкта в каталозі зазвичай припиняється на висотах близько 280 км.

Графічне відображення обстановки реалізовано мовою Python (бібліотеки matplotlib, Cartopy, Plotly). Система формує такі продукти: наземні траси КА з виділенням районів оперативного інтересу; тривимірні зображення орбіт та орбітальних угруповань; часові діаграми маневрів із зазначенням їхнього типу й величини; оцінки мінімальних відстаней зближення КА; прогноз сходження для об'єктів, у яких виявлено ознаки уводу з орбіти. Усі продукти формуються автоматично в щодобовому циклі й зберігаються в локальному архіві, тому залишаються доступними без підключення до зовнішніх ресурсів.

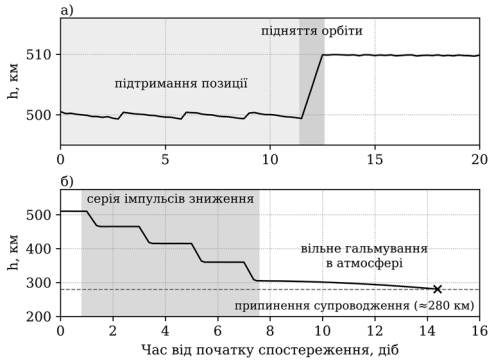


Рис. 1. Модельні сигнатури маневрів КА за середньою висотою орбіти: а – підтримання позиції та підняття орбіти; б – вивід з орбіти

Таким чином, розроблена система моніторингу орбітальної обстановки працює в штатному режимі з травня 2026 р. Вона щодня оновлює локальний каталог, веде таблиці пусків і сходжень для інформаційно-аналітичного бюлетеня, автоматично виявляє маневри КА за часовими рядами OMM-записів і формує графічні продукти для оцінювання обстановки. Перехід від TLE до OMM уже не є питанням вибору: з липня 2026 р. нові об’єкти каталогу у форматі TLE фактично недоступні. Подальший розвиток системи передбачає аналіз зближень з урахуванням коваріацій (за наявності відповідних даних), зіставлення орбітальних подій із даними радіоелектронної розвідки та уточнення графіків прольотів КА іноземної розвідки над районами дій військ.

Наумчак О. М., Ph. D.
Житомирський військовий інститут імені С. П. Корольова
Марцинкевич О. С.
Військова частина А2455

ШТУЧНИЙ ІНТЕЛЕКТ У ЖИТТЄВОМУ ЦИКЛІ КОСМІЧНИХ АПАРАТІВ: СВІТОВИЙ ДОСВІД І ПЕРСПЕКТИВИ ДЛЯ КОСМІЧНОЇ ПІДТРИМКИ ДІЙ ВІЙСЬК (СИЛ)

Війна рф проти України засвідчила, що космічна підтримка стала невід’ємною складовою дій військ (сил): засоби супутникового зв’язку, розвідки та навігації безпосередньо визначають швидкість ухвалення рішень і точність ураження. Водночас кількість космічних апаратів (КА) на орбіті стрімко зростає. До прикладу угруповання Starlink станом на вересень 2026 р. налічує понад 11 тис.

КА, а Космічні сили США в концепції Objective Force 2040 прогнозують, що до 2040 р. кількість урядових КА США перевищить 30 тис. Управляти такими угрупованнями та обробляти отримувані від них обсяги даних у ручному режимі неможливо. Тому штучний інтелект (ШІ) перетворюється з допоміжної технології на системоутворювальний чинник космічної підтримки.

Мета доповіді – узагальнити світовий досвід застосування ШІ на етапах життєвого циклу КА та визначити перспективні напрями його впровадження в інтересах Сил оборони України.

Розвиток ШІ став предметом стратегічного суперництва провідних держав. За оцінками колективної стратегії "A Transformative AI Strategy for Europe" (KIRA Center, 2026 р.), на США припадає близько 75 % світових обчислювальних потужностей для ШІ, на Китай – близько 15 %, на ЄС – менш ніж 5 %; автори допускають можливість появи трансформаційного ШІ до 2030 р. США у Плані дій у сфері ШІ (липень 2025 р.) та оборонній стратегії у сфері ШІ (січень 2026 р.) взяли курс на прискорене впровадження ШІ у військовій сфері. Китай, декларуючи на міжнародному рівні (Сяншаньський форум, вересень 2026 р.) необхідність регулювання військового ШІ та збереження людського контролю над системами озброєння, паралельно розгортає орбітальне обчислювальне угруповання «Три тіла» (заплановано 2800 КА) та мегаугруповання Guowang і Qianfan. рф в цій сфері суттєво відстає: з 32 КА низькоорбітального угруповання "Рассвет", запущених у 2026 р., станом на вересень лише один вийшов на робочу орбіту. Міжнародно-правове регулювання військового ШІ залишається обмеженим: декларацію саміту REAIM у 2026 р. підписали лише 35 із 85 держав-учасниць, а Регламент ЄС про ШІ не поширюється на системи військового призначення.

На етапі проєктування генеративні методи, які застосовує NASA, дають змогу за кілька годин отримувати конструктивні елементи, маса яких на величину до двох третин менша, ніж у спроєктованих вручну. Компанія Proteus Space у 2025 р. вивела на орбіту КА, який позиціонують як перший, спроєктований із наскрізним застосуванням ШІ; тривалість циклу від концепції до передстартової готовності становила 9 місяців. Великі мовні моделі впроваджуються в модельно-орієнтовану системну інженерію (MBSE) для генерування варіантів архітектури КА та забезпечення простежуваності вимог, а цифрові двійники застосовують для прогнозування технічного стану бортових систем.

На етапі експлуатації ключовою тенденцією є перенесення засобів ШІ безпосередньо на борт КА. Місія Європейського космічного агентства (ЄКА) PhiSat-2 (2024 р.) продемонструвала можливість оновлення прикладних моделей ШІ безпосередньо на орбіті; Лабораторія реактивного руху NASA на КА CogniSAT-6 (2025 р.) випробувала автономне перенацілювання знімальної апаратури з урахуванням хмарності, яке триває 60-90 с; на КА Pelican компанії Planet реалізовано бортове виявлення літаків на знімках. У 2025 р. на орбіту вперше виведено графічний процесор рівня центрів обробки даних, а компанія Google у межах проєкту Suncatcher готує орбітальні випробування тензорних процесорів. Для військ це означає отримання замість необроблених знімків готових відомостей про цілі, зменшення навантаження на радіоканали та скорочення часу доведення розвідувальних даних.

Під час управління КА ШІ забезпечує автономне виконання маневрів ухилення від зіткнень (КА Starlink протягом року виконали понад 355 тис. таких маневрів), виявлення аномалій у телеметричній інформації, автоматизоване планування цільового застосування та контроль космічної обстановки.

Найбільший ефект застосування ШІ забезпечує в ланцюзі “сенсор – стрілець”. Система Maven Національного агентства геопросторової розвідки США, яка інтегрує дані космічної та інших видів розвідки, за оцінками агентства, скоротила тривалість циклу цілевказання з годин до хвилин; кількість її користувачів перевищує 20 тис. У програмі протиракетної оборони Golden Dome передбачено інтеграцію ШІ в контур бойового управління, оскільки реагування в межах підльотного часу ракет неможливе без автоматизації.

Досвід України підтверджує ці тенденції: супутникові дані інтегровано в систему ситуаційної обізнаності Delta з модулем автоматичного виявлення військової техніки противника Avengers; Сили оборони України отримують радіолокаційні знімки ICEYE з надвисокою просторовою розрізненністю; запровадження у лютому 2026 р. “білого списку” терміналів Starlink позбавило противника можливості використовувати цей засіб зв’язку.

Застосування ШІ в космічних системах пов’язане з низкою ризиків: уразливістю нейронних мереж до змагальних атак (adversarial attacks: маскувальні покриття, хибні цілі); радіаційно-індукованими збоями бортових обчислювачів; кібератаками на агентні системи ШІ, унаслідок яких протиборство в кіберпросторі набуває характеру “ШІ проти ШІ”; складністю

верифікації рішень, ухвалених ШІ, та забезпечення людського контролю над застосуванням зброї. Для України окремим ризиком є залежність від іноземних постачальників космічних даних і послуг.

Отже, ШІ став наскрізною технологією, що охоплює всі етапи життєвого циклу КА – від проєктування до бойового застосування, а провідні держави розглядають його як основний засіб управління багатосупутниковими угрупованнями та скорочення циклу "сенсор – стрілець". Основний вектор розвитку – перенесення обробки даних на борт КА та в орбітальні обчислювальні центри, що змінює вимоги до каналів зв'язку і наземного сегмента.

Тому, для Сил оборони України доцільно:

– визначати бортову обробку даних із застосуванням ШІ як обов'язкову вимогу до розроблення перспективних вітчизняних КА та до комерційних космічних послуг, які закуповують;

– розробляти та вдосконалювати національні моделі розпізнавання об'єктів на космічних знімках, навчені на даних, отриманих під час війни;

– забезпечувати інтеграцію космічних даних у єдиний контур ситуаційної обізнаності з їх автоматизованою обробкою;

– диверсифікувати джерела отримання космічних даних і послуг та поглиблювати участь у програмах ЄС (IRIS², European Space Shield);

– забезпечувати збереження людини в контурі ухвалення рішень на ураження (принцип human-in-the-loop).

Перспективним напрямом подальших досліджень є розроблення методики оцінювання ефективності космічної підтримки дій військ (сил) з урахуванням застосування ШІ на борту КА і в наземному сегменті.

Рибачук О. І., канд. техн. наук, доц.
Борцова М. В.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ЕФЕКТИВНЕ ПЛАНУВАННЯ ЗАСТОСУВАННЯ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ ІЗ ЗАЛУЧЕННЯМ СПРОМОЖНОСТЕЙ КОСМІЧНИХ СИСТЕМ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ

Широке залучення безпілотних літальних апаратів (БпЛА) та наземних роботизованих комплексів (НРК) є головною відмінною рисою російсько-української війни, яку військові аналітики називають “війною дронів” або “першою технологічною війною нового покоління”. При цьому застосування НРК на передовій супроводжується низкою специфічних викликів, які роблять їхнє впровадження значно складнішим, ніж у випадку з БпЛА. У першу чергу це забезпечення прохідності в умовах бездоріжжя та ділянок маршруту із складним рельєфом. Навіть найсучасніша колісна чи гусенична платформа може застрягти у глибокому багні, снігу, завалах цегли у зруйнованих містах або перекинутися на крутому схилі. Тому є очевидним, що ефективність застосування НРК на передовій у значній мірі буде залежати від якості планування їх маршрутів руху при виконанні як логістичних, так і бойових завдань. При оцінюванні прохідності того або іншого маршруту має бути врахована низка характеристик та властивостей ґрунту і місцевості, серед них: тип ґрунту за класифікацією USCS (en: Unified Soil Classification System), його щільність, вологість, глибина промерзання (або температура на різних глибинах, за якою можна оцінити глибину промерзання), товщина снігового покриву, а також крутизна схилів, стан рослинності, наявність та стан доріг, мостів, бродів та інші. Найбільш популярними джерелами отримання властивостей ґрунтів є інтернет-ресурси: SoilGrids, OpenLandMap, SCMaP. Головна відмінність даних ресурсів полягає в тому, що SoilGrids і OpenLandMap надають користувачу готові карти властивостей ґрунту, які будуються за допомогою штучного інтелекту (ШІ) на основі багатьох глобальних та регіональних баз різнотипних даних, що об’єднують як польові вимірювання та верифіковані дослідження зі всього світу, так і дані дистанційного зондування

Землі (ДЗЗ), тоді як SCMaP – це спеціалізований процесор супутникових знімків космічних апаратів (КА) ДЗЗ Sentinel-2 й Landsat, що створює карти ґрунтів Європи без даних про рослинність. Необхідні для оцінювання прохідності значення вологості ґрунту, його глибини промерзання або температури можуть бути отримані за допомогою погодного сервісу Open-Meteo. Обмеженням такого підходу до отримання характеристик ґрунтів є те, що вищезазначені інтернет-ресурси призначені перш за все для вирішення завдань точного землеробства та геотехнічного аналізу й тому вони містять усереднені або інтерпольовані ШІ дані, точність яких у більшості практичних випадків невідома і змінюється в залежності від локації, а просторове розрізнення даних може досягати декількох кілометрів. За розміщеними на цих ресурсах даними часто неможливо точно класифікувати ґрунт за системою USCS, що є необхідною умовою застосування загальноприйнятних емпіричних моделей оцінювання номінального конусного індексу ґрунту. Крім того, за час бойових дій місцевість часто суттєво змінюється, й отримані оцінки прохідності маршрутів можуть швидко втратити актуальність. У таких умовах виглядає доцільним залучення на етапі планування логістичних операцій та бойових дій актуальних оптичних та радіолокаційних зображень заданого району для уточнення стану рослинності, доріг, мостів, бродів, а також таких динамічних характеристик ґрунту, як його вологості, глибини промерзання, товщини снігового покрову. Наприклад, технічні спроможності КА ICEYE з радіолокатором із синтезованою апертурою (РСА) у Х-діапазоні здатні забезпечити вимірювання вологості ґрунту із середньоквадратичною похибкою 0,06 м³/м³ та із значно кращим просторовим розрізненням у залежності від режиму зйомки – від 0,75 до 1,5 метри. Для уточнення глибини промерзання ґрунту та товщини снігового покрову можуть бути залучені дані з інших спеціалізованих КА з РСА у L-діапазоні, наприклад, КА NISAR. Точна класифікація ґрунтів за системою USCS неможлива без польових досліджень їх якостей, які виконуються силами підрозділів інженерної розвідки. Отримані карти з актуальними значеннями характеристик і типів ґрунтів мають бути інтегровані у автоматизовані системи бойового управління та інформаційні системи Збройних Сил України, такі як “Дзвін-АС” та “Delta” для оперативного та максимально достовірного оцінювання прохідності маршрутів при плануванні бойових дій та логістичних операцій, у тому числі з застосуванням НРК.

Беспалко І. А, канд. техн. наук, ст. наук. співроб.
Випорханюк Д. М.
Завада А. А., канд. техн. наук, ст. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова
Пекарєв Д. В., канд. техн. наук, ст. наук. співроб.
Секція прикладних проблем Президії НАН України

ПРОБЛЕМИ АКТУАЛІЗАЦІЇ ТЕРМІНОЛОГІЧНОЇ БАЗИ КОСМІЧНОЇ ПІДТРИМКИ ДІЙ ВІЙСЬК (СИЛ)

У грудні 2019 року космос визнано операційним доменом НАТО, а війна проти України продемонструвала залежність сучасних операцій від супутникового зв’язку, навігації, дистанційного зондування Землі, комерційних космічних послуг, а також від протидії їм засобами електромагнітної боротьби. Водночас термінологія, на якій ґрунтуються планування й управління космічною підтримкою, формувалася в різний час, за різними джерелами та різними авторськими колективами.

У НАТО базовим джерелом термінології космічних операцій є спільна доктрина повітряних і космічних операцій STANAG 3700 / AJP-3.3, що визначила космічне контролювання (space control) як область місій з поділом на наступальні та оборонні операції і прив’язує їх до забезпечення обізнаності про космічне середовище. Нова редакція операцій STANAG 3700 / AJP-3.3 станом на лютий 2026 р. переходить до операційних функцій обізнаності у космічному домені (SDA), операційної космічної підтримки (OSS) та координації у космічному домені (SDC).

У США система документів будується ієрархічно – серія доктринальних публікацій засвідчують:

перехід від поняття “обізнаність про космічну обстановку” (SSA) до “обізнаності про космічний домен” (SDA);

закріплення чіткої шкали впливу на космічні системи (disrupt – degrade – deny – destroy);

включення комерційних та союзних засобів у загальну картину обстановки;

уніфікацію документів за напрямами (ракетне попередження, електромагнітний спектр, планування).

Найбільшою перешкодою на шляху ефективного використання космічних спроможностей у діях військ (сил) на даний час є відсутність єдиного, узгодженого та актуального понятійного апарату космічної підтримки. Національна база формується військовими стандартами: ВСТ 01.048.001 (Космічна діяльність у сфері оборони), ВСТ 014.001:2024 (Космічна підтримка операцій), ВСТ 301.004:2023(01), що впроваджує AJP-3.3 Ed. B, а також встановленнями воєнної розвідки, електромагнітної й кіберборотьби та навігаційного забезпечення.

Комплексний аналіз цих джерел дозволив виявити низку системних розбіжностей, а додаткову складність створює те, що основні доктринальні документи НАТО зазнали змін. Таким чином термінологічна база космічної підтримки дій військ (сил) ЗС України потребує актуалізації, що доцільно здійснювати як системний процес, а не як разове виправлення окремих стандартів, а саме:

1. Сформувати єдиний глосарій космічної підтримки дій військ (сил) у форматі "український термін – англійський еквівалент – джерело – визначення – статус", щоб кожен термін мав одне правильне посилання на джерело та пункт.

2. Провести скоординований перегляд наявних військових стандартів, а не послідовно, щоб не відтворювати розбіжності між базовими та похідними документами.

3. Встановити, що у похідних документах терміни не перевизначають, а лише посилаються на базові; відхилення від еквівалента НАТО фіксують приміткою з обґрунтуванням.

4. Рішення щодо термінів приймати за критеріями: семантична точність (процес чи стан), узгодженість роду та відмінка, відповідність чинному правопису та можливість прямого співставлення з англійським терміном.

5. Запровадити постійний механізм моніторингу нових редакцій STANAG/AJP та доктринальних публікацій стратегічних партнерів з періодичним переглядом бази.

6. Уніфікувати графічну мову космічної підтримки: єдині познаки для моделі космічної обстановки та схеми оперативного стану космічних засобів (стан спроможностей, належність засобів, райони інтересу).

7. Ввести верифікацію термінів на навчаннях та штабних тренуваннях щодо розуміння термінів підрозділами космічної підтримки та споживачами космічної інформації.

Актуалізована термінологічна база космічної підтримки необхідна, перш за все, командирам (начальникам) і штабам всіх рівнів – від тактичного до стратегічного, які планують і проводять операції (бойові дії), а також офіцерам органів військового управління, що організовують космічну підтримку, обізнаність про космічний домен і оцінювання космічної обстановки.

Також вона потрібна підрозділам космічної розвідки, зв’язку, навігаційного забезпечення, ракетного попередження, електромагнітної та кіберборотьби, а також всім споживачам космічної інформації в родах військ збройних сил (розвідка, протиповітряна та протиракетна оборона, ракетні війська та артилерія, авіація, електронна боротьба), які мають однаково розуміти запити, продукти і попередження космічної підтримки.

Термінологічна база важлива для розробників нормативних та навчальних документів, викладачів і слухачів військових навчальних закладів, наукових організацій і розробників, що виконують науково-дослідні та дослідно-конструкторські роботи, організацій – виконавців космічної діяльності у сфері оборони та державних органів, залучених до реалізації державної політики в цій сфері, а також представникам військ стратегічних партнерів у рамках сумісних операцій, для яких термінологічна відповідність натовській доктрині є умовою взаємосумісності.

Стан термінологічної бази космічної підтримки дій військ (сил) у ЗСУ на даний час є базово узгодженим з доктринальними документами НАТО, але має низку внутрішніх розбіжностей та застарілі базові джерела. Актуалізація термінологічної бази має здійснюватись системно: через єдиний глосарій, скоординований перегляд базових та похідних стандартів, чіткі критерії вибору термінів, моніторинг змін у документах НАТО та національних документах, а також через уніфікацію графічної мови моделей і схем.

Sysoienko S. V., Cand. Sc. (Tech.), Ass. Prof.
Vovchanivska N.
State Scientific Research Institute of Armament and Military
Equipment Testing and Certification

INFORMATION AND ANALYTICAL PROVISION OF SPACE SUPPORT OF TROOPS IN CONDITIONS OF COUNTERACTION AND LIMITED ACCESS TO SPACE RESOURCES

Modern military conflicts are characterised by the growing dependence of troops on information obtained from space systems. At the same time, space environment is becoming increasingly competitive and vulnerable to radio-electronic interference, cyber influence, physical damage to individual components and restricted access to commercial or partner services. The relevance for Ukraine is determined not only by the need to increase its own space capabilities, but also by the need to ensure the continuity of obtaining information suitable for solving specific tasks under conditions of changing the accessibility of individual space resources. The practical value of the information obtained is determined by its timeliness, spatial characteristics, reliability, accessibility, resistance to external interference and ability to integrate with other information flows. In case of disruption of a separate source functioning, it becomes necessary to quickly select an alternative resource or integrate information from several sources. One of the tasks of information and analytical support consists not only in obtaining space data, but in ensuring their necessary quality, timeliness and continuity for a specific task of the troops. It is proposed to consider space support for military operations as a dynamic information and analytical environment, the functioning of which is based on the integration of heterogeneous state, partnership and commercial resources. This approach can be used when forming requirements for promising space support systems, designing the architecture for information interaction between state, military, international and commercial space resources, as well as substantiating the use of backup information channels. Future work should focus on developing a mathematical model of the integral indicator of information suitability, as well as an algorithm for dynamic selection and integration of space information resources depending on the requirements for a specific task of the troops.

Романчук М. П., канд. техн. наук., ст. досл.
Науково-дослідний інститут воєнної розвідки
Наумчак О. М., Ph. D.
Денисюк Ю. Р.
Житомирський військовий інститут імені С. П. Корольова

НАДІЙНІСНИЙ КРИТЕРІЙ ЯКОСТІ ЗОБРАЖЕННЯ ДЛЯ ПЛАНУВАННЯ ЗНІМАННЯ ОПТИКО-ЕЛЕКТРОННИМ КОСМІЧНИМ АПАРАТОМ

Під час планування зйомки оптико-електронним (ОЕ) космічним апаратом (КА) рівень інтерпретованості знімка прогнозують за шкалою NIIRS з використанням рівняння якості зображення GIQE5. Для врахування метеорологічних умов застосовують інтегральний показник:

$$NIIRS_{int} = PLOS \cdot NIIRS_{hw}, \quad (1)$$

де $NIIRS_{hw}$ – бал, прогнозований за GIQE5; $PLOS$ – імовірність вільної лінії візування. Цей показник трактується як математичне сподівання оперативної цінності вікна зйомки.

У чинних формулюваннях аерозольне послаблення враховано двічі. Ефективне відношення сигнал/шум $SNR_{eff} = SNR_0 \cdot F_{SEA} \cdot F_{AOD} \cdot k_{sh}^{S}$, що входить до GIQE5, містить множник $F_{AOD} = \exp\left[-\tau\left(1/\sin SEA - 1/\sin SEA_{ref}\right)\right]$, в якому τ – оптична товща аерозолів; SEA – кут піднесення Сонця; SEA_{ref} – його опорне значення. Водночас імовірність вільної лінії візування подають як:

$$\mathrm{PLOS} = (1 - P_{cloud}) \cdot \exp(-\tau/\sin SEA), \quad (2)$$

де P_{cloud} – імовірність перекриття лінії візування хмарністю. Другий множник відрізняється лише сталим коефіцієнтом $exp(-\tau/\sin SEA_{ref})$, тобто одна й та ж оптична товща аерозолів входить у модель двічі. Внески цих двох каналів непорівнянні: для типових умов (SEA = 38°, τ = 0,18) через SNR_{eff} аерозолі знижують прогноз на 0,0014 бала, а через $PLOS$ – на 1,374 бала, тобто приблизно на 3 порядки більше. Фізично мізерний радіометричний ефект набуває вирішального значення лише тому, що його вміщено в імовірнісний множник.

Причина суперечності – змішування величин різної природи. Множники зниження яскравості сцени F_{SEA} та атмосферного послаблення F_{AOD} описують детерміноване послаблення сигналу і впливають на якість через SNR_{eff} поступово

та з насиченням. Натомість $PLOS$ є ймовірністю бінарної події: хмара або перекриває лінію візування, або ні. Пропускання атмосфери ймовірністю не є, тому імовірнісний множник має містити лише хмарність:

$$PLOS = 1 - P_{cloud}, \quad (3)$$

а все атмосферне послаблення – залишатися у складі SNR_{eff}. Водночас доцільно врахувати відрізок оптичного шляху "ціль – сенсор":

$$F_{AOD} = \exp\left[-\tau\left(m(SEA,\psi) - m_{ref}\right)\right], \quad m(SEA,\psi) = \frac{1}{\sin SEA} + \frac{1}{\cos\psi}, \quad (4)$$

де ψ – кут відхилення лінії візування від надиру; $m_{ref} = 2{,}414$ – повітряна маса за умов $SEA_{ref} = 45°$, зйомка в надир. Нехтування відрізком "ціль – сенсор" завищує пропускання атмосфери на 19,7–23,1 % для $\psi = 0 \ldots 30°$.

Розмежування (3)–(4) є необхідною умовою коректності показника $NIIRS_{int}$. Якщо оперативна корисність кадру $U = NIIRS_{hw}$ у разі настання події W "лінія візування вільна, кадр отримано" та нулю в іншому разі, то:

$$NIIRS_{int} = E[U] = P(W) \cdot NIIRS_{hw} = PLOS \cdot NIIRS_{hw}, \quad (5)$$

Перехід до добутку в (5) правомірний лише тоді, коли $PLOS$ є ймовірністю події W, тобто лише за формулювання (3). Звідси випливає розмежування ролей: вимогу до якості перевіряється за $NIIRS_{hw}$, а $NIIRS_{int}$, що має розмірність "бал × імовірність", слугує цільовою функцією ранжування вікон. Пряме порівняння $NIIRS_{int}$ з вимогою $NIIRS_{req}$ некоректне: воно відхиляє вікна, у яких якість зйомки достатня, а недостатньою є лише ймовірність її здійснення.

Другий недолік чинного підходу – детермінована перевірка вимоги $NIIRS_{hw} \geq NIIRS_{req}$, хоча похибка прогнозу за GIQE5 характеризується середньоквадратичним відхиленням $\sigma_G \approx 0{,}3$ бала [3]. За такого критерію вікно з прогнозом 5,02 за вимоги $NIIRS_{req} = 5$ формально приймається, хоча ймовірність досягнення потрібного рівня становить лише 0,53. Пропонується надійнісний критерій $P(NIIRS_{true} \geq NIIRS_{req}) \geq \gamma$, який за нормального розподілу похибки прогнозу зводиться до перевірки зі зміщеним порогом:

$$NIIRS_{hw} \geq NIIRS_{thr} = NIIRS_{req} + z_\gamma \sigma_G, \quad (6)$$

де z_γ – квантиль стандартного нормального розподілу рівня γ. Для $\gamma = 0{,}90$ надійнісний запас становить 0,384 бала, що за оберненими співвідношеннями GIQE5 еквівалентно зменшенню наземного розміру пікселя на 23,4 % незалежно від рівня шкали. Тим самим ціну врахування похибки прогнозу виражено в термінах тактико-технічних вимог до сенсора (рис. 1).

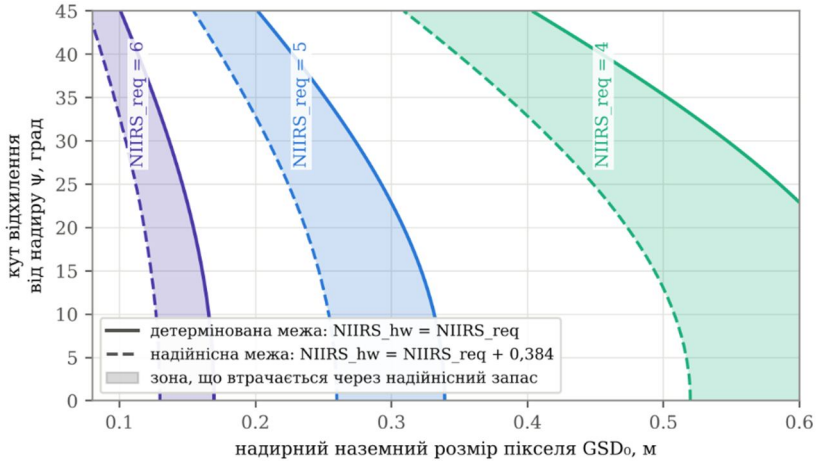


Рис. 1. Детермінована та надійнісна межі області допустимих режимів зйомки ($RER_{GM} = 0{,}80;\ G = 1{,}6;\ SNR_0 = 110$)

Для вікна зйомки позиції зенітного ракетного комплексу ($NIIRS_{req} = 5;\ GSD_0 = 0{,}24$ м; $SEA = 38°;\ P_{cloud} = 0{,}15;\ \tau = 0{,}18$) розмежування множників змінює прогнозований бал $NIIRS_{hw}$ лише на 0,0002, тоді як інтегральний показник $NIIRS_{int}$ за $\psi = 15°$ зростає з 3,44 до 4,61, тобто на 34 %. Отже, йдеться не про уточнення радіометричної моделі, а про усунення помилки в структурі показника. Надійнісний критерій змінює й рішення щодо вікна: за $\psi = 22°$ прогноз 5,331 не досягає порогу 5,384 (імовірність виконання вимоги 0,865 < 0,90), хоча детермінований критерій це вікно прийняв би; вимогу виконано за $\psi \leq 18{,}1°$.

Отже, у чинних методиках планування зйомки ОЕ КА оптична товща аерозолів ураховується двічі – у складі SNR_{eff} і в імовірності $PLOS$, причому внесок другого каналу приблизно на три порядки перевищує внесок першого. Розмежування множників за їхньою природою ($PLOS = 1 - P_{cloud}$, атмосферне послаблення – лише у складі SNR_{eff}) усуває подвійне врахування і є необхідною умовою того, щоб $NIIRS_{int}$ був математичним сподіванням корисності. При цьому $NIIRS_{hw}$ слугує критерієм якості, а $NIIRS_{int}$ – цільовою функцією ранжування вікон зйомки. Надійнісний критерій $NIIRS_{hw} \geq NIIRS_{req} + z_\gamma \sigma_G$ ураховує похибку прогнозу за GIQE5; для $\gamma = 0{,}90$ він еквівалентний вимозі зменшити наземний розмір пікселя на 23,4 %. Напрямом подальших досліджень є емпіричне оцінювання σ_G для конкретних космічних платформ, оскільки саме ця величина визначає надійнісний запас.

Лящук О. І., канд. фіз.-мат. наук, ст. досл.
Андрущенко Ю. А., канд. геол. наук
Осадчий В. І.
Головний центр спеціального контролю
Національного центру управління та випробувань
Державного космічного агентства України

КОМПЛЕКСНИЙ ГЕОІНФОРМАЦІЙНИЙ МОНІТОРИНГ ВИСОКОЕНЕРГЕТИЧНИХ ВИБУХОВИХ ПОДІЙ

У сучасних умовах, коли високоенергетичні вибухові події можуть мати значний вплив на безпеку та інфраструктуру, особливого значення набуває розвиток комплексних систем моніторингу. Одним з перспективніших напрямків у цій галузі є поєднання даних сейсмічних, інфразвукових наземних сенсорних мереж та дистанційного зондування Землі. Такий комплексний підхід дозволяє не лише оперативно виявляти події, але й забезпечувати їх локалізацію, визначення характеристик джерела та об’єктивну оцінку наслідків.

В такій системі сейсмічні спостереження надають первинну інформацію про подію вже через одиниці-десятки хвилин, тоді як інфразвукові методи потребують більше часу, але доповнюють картину, особливо в умовах, коли сейсмічні сигнали можуть бути обмежені. Супутникові дані забезпечують візуальне підтвердження наслідків події, таких як зміни поверхні, руйнування об’єктів, пожежі тощо.

Головною перевагою комплексного геоінформаційного моніторингу є здатність подолати обмеження окремих методів. Поєднання сейсмічних, інфразвукових та супутникових даних дозволяє отримувати більш повну та об’єктивну картину події. Автоматизована обробка даних, отриманих з різних джерел, дозволяє оперативно формувати аналітичні звіти, які можуть бути використані для прийняття рішень.

Практичне застосування комплексного моніторингу вже продемонструвало свою ефективність у різних сценаріях. Особлива увага - об’єктивний дистанційний контроль застосування засобів ураження Сил оборони. Основна надана інформація – час, місце та потужність кожного виявленого вибуху. Отримана інформація є суттєвим доповненням до космічних та інших розвідувальних даних. Також при несприятливих

метеорологічних умовах, геофізична інформація може стати єдиним джерелом про ефективність застосування засобів ураження. Тож, комплексування сейсмічних, акустичних та супутникових методів моніторингу є важливим кроком у забезпеченні оперативного, точного та об’єктивного контролю високоенергетичних подій.

Лящук О. І., канд. фіз.-мат. наук, ст. досл.
Парновський О. С., канд. фіз.-мат. наук, ст. наук. співроб.
Андрущенко Ю. А., канд. геол. наук
Осадча Н. Ю.
Довбиш С. В.
Головний центр спеціального контролю
Національного центру управління та випробувань
Державного космічного агентства України

ОРГАНІЗАЦІЯ ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО КОСМІЧНУ ПОГОДУ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Сучасна військова діяльність значною мірою залежить від стабільності каналів зв’язку, точності навігаційних даних, функціонування супутникових систем та надійності електронного обладнання. На роботу окремих із цих систем можуть впливати не лише техногенні чинники та навмисні дії противника, а й природні процеси в навколоземному космічному середовищі. Тому інформація про космічну погоду може розглядатися як додаткове джерело даних для оцінювання умов виконання завдань, аналізу технічних порушень і завчасної підготовки до можливих несприятливих явищ.

Під космічною погодою розуміють сукупність змін у навколоземному космічному середовищі, зумовлених сонячною активністю та взаємодією сонячного вітру з магнітосферою Землі. До основних явищ належать сонячні спалахи, корональні викиди маси, потоки сонячних енергетичних частинок, геомагнітні бурі та збурення іоносфери. Їхній вплив залежить від інтенсивності явища, його тривалості, місця й часу спостереження, а також від технічних характеристик конкретної системи.

Одним із найбільш чутливих до стану іоносфери засобів є радіозв’язок у короткохвильовому діапазоні (HF, 3–30 МГц), поширення радіохвиль у якому

значною мірою визначається властивостями іоносфери. Під час сильних сонячних спалахів посилення поглинання радіохвиль у нижніх шарах іоносфери може призводити до погіршення або тимчасової втрати зв'язку на освітленому боці Землі. Іоносферні збурення також можуть впливати на точність супутникової навігації, зокрема через зміни затримки сигналів під час їх проходження крізь іоносферу. Водночас характер і ступінь впливу на інші діапазони радіозв'язку, радіолокаційні засоби та електронне обладнання потребують окремого оцінювання з урахуванням особливостей відповідних систем.

Показовим прикладом масштабного прояву космічної погоди стала геомагнітна буря 10–11 травня 2024 року, яка досягла найвищого рівня G5 за шкалою NOAA. Ця подія супроводжувалася значними збуреннями магнітосфери та іоносфери й продемонструвала актуальність урахування космічної погоди для операторів навігаційних, радіотехнічних і супутникових систем. У той самий період на Харківському напрямку розпочався російський наступ. За повідомленнями, що надходили від військових, спостерігалися проблеми зі зв'язком, які могли пов'язуватися з дією засобів радіоелектронної боротьби противника. Водночас фахівці інформували про сильну геомагнітну бурю.

Збіг цих подій у часі сам по собі не доводить причинного зв'язку між геомагнітною бурею та конкретними порушеннями зв'язку або перебігом бойових дій. Проте цей приклад засвідчує важливість комплексного аналізу можливих причин технічних збоїв. Наявність оперативної інформації про космічну погоду могла б бути одним із чинників, які враховуються під час оцінювання ситуації поряд з аналізом технічного стану обладнання, умов поширення радіохвиль і можливого впливу противника.

В Україні вже існує інституційна основа для розвитку такого напряму. Головний центр спеціального контролю (ГЦСК) здійснює цілодобовий моніторинг геофізичних явищ і має технічні засоби, зокрема магнітометричні комплекси, станції моніторингу радіотрас у наднизькочастотному діапазоні та доступ до RTK-систем НЦУВКЗ. Водночас наявність вимірювальних засобів і можливість спостерігати поточний стан середовища не означають автоматичної наявності повного циклу прогнозування та оцінювання впливу космічної погоди на конкретні технічні системи.

Для розвитку відповідної спроможності доцільно поєднувати дані власних спостережень із прогнозами, попередженнями та аналітичними продуктами міжнародних служб, насамперед Центру прогнозування космічної погоди

Національного управління океанічних і атмосферних досліджень США (NOAA SWPC) та сервісів Європейського космічного агентства (ESA). Такий підхід дає змогу використовувати наявні міжнародні інформаційні ресурси, одночасно накопичуючи досвід їх інтерпретації та оцінюючи потребу в подальшому розвитку національних спроможностей.

Важливим завданням є перетворення наукових даних і спеціалізованих прогнозів на зрозумілу для органів військового управління інформацію. Значення індексів геомагнітної активності, повідомлення про сонячні спалахи або іоносферні збурення не завжди безпосередньо вказують на можливі наслідки для конкретного обладнання. Тому доцільно розробити стандартизовані інформаційні повідомлення, у яких зазначатимуться характер очікуваного явища, прогнозований період його впливу, рівень невизначеності, потенційно чутливі категорії технічних систем та рекомендовані загальні заходи перевірки їхньої готовності. Такі повідомлення мають доповнювати, а не замінювати технічну діагностику та інші джерела ситуаційної інформації.

Організаційною основою цієї роботи може стати взаємодія ГЦСК, наукових установ Національної академії наук України та визначених представників органів військового управління. ГЦСК доцільно розглядати як потенційний координаційний центр оперативного отримання, узагальнення та поширення відповідної інформації. Наукові установи могли б забезпечувати наукове обґрунтування методик, перевірку інтерпретацій, аналіз даних і розроблення підходів до оцінювання впливу космічної погоди. Представники військових органів управління, зі свого боку, визначали б практичні інформаційні потреби, вимоги до форми повідомлень та критерії їхньої корисності для підтримки рішень.

У цьому контексті варто враховувати досвід США, де забезпечення військової діяльності метеорологічною та космічною інформацією ґрунтується на поєднанні спеціалізованих державних спроможностей, профільної експертизи та доведення інформації до її практичних користувачів. Для України цінним є насамперед організаційний принцип: розвиток нової функції не обов’язково має передбачати створення окремого великого підрозділу. На початковому етапі можна розглянути можливість визначення відповідальних посадових осіб у вже наявних органах управління, які забезпечуватимуть взаємодію з ГЦСК та науковими установами. Конкретна модель і розподіл

обов'язків мають визначатися за результатами оцінювання потреб, наявних ресурсів і досвіду практичного застосування. Такий підхід дає змогу перевірити доцільність нової функції без передчасного ускладнення організаційної структури.

Для визначення практичної цінності запропонованої моделі доцільно розпочати з пілотного проєкту за участю зацікавлених підрозділів і фахівців, зокрема тих, чия діяльність залежить від стабільності зв'язку та функціонування безпілотних систем. На першому етапі необхідно встановити порядок отримання й передавання інформації, погодити формат попереджень і визначити критерії оцінювання результатів. Серед таких критеріїв можуть бути своєчасність і зрозумілість повідомлень, їхня відповідність фактичним умовам, практична корисність для користувачів, а також можливість точніше розрізняти природні чинники порушень і ймовірний вплив засобів радіоелектронної боротьби. Важливо також документувати випадки, коли прогнозована подія не супроводжувалася помітним впливом на обладнання, щоб уникати необґрунтованого приписування космічній погоді будь-яких технічних несправностей.

Окремим напрямом має стати підготовка інформаційно-методичних матеріалів для військовослужбовців. Короткі пам'ятки та буклети можуть містити базові відомості про явища космічної погоди, можливі прояви їхнього впливу, способи отримання офіційних попереджень і принципи коректного використання такої інформації під час оцінювання технічної ситуації. Для формування кадрового потенціалу доцільно також розглянути запровадження короткого навчального модуля або циклу лекцій у профільному закладі вищої військової освіти, зокрема в Житомирському військовому інституті імені С. П. Корольова. Це сприятиме формуванню спільного понятійного апарату серед військових фахівців і створить основу для подальшого розвитку прикладних досліджень.

Отже, використання інформації про космічну погоду може стати додатковим елементом інформаційного забезпечення військової діяльності України. Практичний шлях розвитку цього напряму полягає в поєднанні можливостей ГЦСК, міжнародних сервісів прогнозування та наукової експертизи НАН України з потребами органів військового управління. Початковим кроком має бути не обов'язкове запровадження нової системи в усіх підрозділах, а апробація відповідних інформаційних продуктів у межах пілотного проєкту, підготовка методичних матеріалів і навчання персоналу. Результати апробації дадуть змогу оцінити реальну користь такого підходу, уточнити розподіл функцій і визначити подальші напрями розвитку національних спроможностей у сфері космічної погоди.

Миклуха В. А., Ph. D.
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНФРАЧЕРВОНИХ КОСМІЧНИХ ЗНІМКІВ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ОБ’ЄКТІВ

Розвиток технологій дистанційного зондування Землі (ДЗЗ) створює нові можливості для виявлення та ідентифікації об’єктів, які складно розпізнати за матеріалами знімання у видимому діапазоні електромагнітного спектра. Особливого значення набуває використання інфрачервоних (ІЧ) даних, що дають змогу досліджувати особливості теплового випромінювання земної поверхні та відмінності температурних характеристик природних і штучних об’єктів. Актуальність дослідження зумовлена необхідністю вдосконалення методів оброблення й інтерпретації космічних знімків для підвищення інформативності дистанційного моніторингу територій у складних природних умовах.

Мета роботи – обґрунтувати методичний підхід до виявлення та ідентифікації прихованих об’єктів за матеріалами інфрачервоного дистанційного зондування Землі з урахуванням особливостей формування ІЧ-зображень і впливу характеристик підстильної поверхні на результати їх інтерпретації.

Інфрачервоні зображення містять інформацію про енергетичні характеристики земної поверхні, які залежать від температури об’єктів, їхньої випромінювальної здатності, властивостей матеріалів та умов знімання. Відмінності теплових характеристик об’єктів і навколишнього середовища можуть створювати передумови для виявлення ознак, недостатньо виражених на знімках у видимому діапазоні. Водночас достовірність інтерпретації залежить від просторової та радіометричної роздільної здатності даних, часу знімання, метеорологічних умов, особливостей рослинного покриву й неоднорідності земної поверхні.

Методичний підхід до аналізу ІЧ-знімків передбачає послідовне виконання взаємопов’язаних етапів: отримання та перевірку вихідних даних; попереднє оброблення й радіометричну корекцію знімків; вибір відповідних інфрачервоних каналів; аналіз спектральних і температурних характеристик; дешифрування зображень; перевірку виявлених ознак та оцінювання достовірності результатів. На завершальному етапі здійснюється узагальнення

отриманих даних і формування інформаційного звіту для подальшого використання.

Практичне застосування такого підходу можливе під час моніторингу територій із розвиненим рослинним покривом, урбанізованих зон, промислових майданчиків та інших техногенних об’єктів. Порівняння інфрачервоних даних з інформацією у видимому діапазоні, за наявності відповідних матеріалів, дає змогу комплексніше оцінювати особливості досліджуваної території. При цьому теплова аномалія або спектральна відмінність не є самостійним доказом наявності конкретного об’єкта, тому результати потребують перевірки з урахуванням просторового контексту та можливих альтернативних пояснень.

Висновки. Використання інфрачервоних даних дистанційного зондування Землі є перспективним напрямом удосконалення методів виявлення та аналізу прихованих об’єктів. Запропонований методичний підхід систематизує основні етапи оброблення й інтерпретації ІЧ-зображень та створює передумови для підвищення обґрунтованості результатів дистанційного моніторингу. Подальші дослідження доцільно спрямувати на експериментальну перевірку методики, визначення кількісних показників точності виявлення та оцінювання впливу умов знімання на достовірність результатів. Отримані напрацювання можуть бути використані в екологічному моніторингу, цивільній безпеці, контролі стану техногенних об’єктів та інших сферах застосування ДЗЗ.

СЕКЦІЯ 5
Радіоелектронна розвідка

Єгоров В. О., Ph. D.
Запорожченко Ю. І.
Житомирський військовий інститут імені С. П. Корольова

РАДІОЧАСТОТНІ ВІДБИТКИ ЯК ІНСТРУМЕНТ ІДЕНТИФІКАЦІЇ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ У СИСТЕМАХ РАДІОТЕХНІЧНОЇ РОЗВІДКИ

Сучасний розвиток радіоелектронних систем, широке застосування цифрових засобів зв’язку, програмно визначених радіосистем та адаптивних технологій передачі інформації призводять до суттєвого ускладнення електромагнітної обстановки. У цих умовах одним із актуальних завдань радіотехнічної розвідки є не лише виявлення факту наявності радіовипромінювання, а й визначення належності сигналу конкретному радіоелектронному засобу. Традиційні методи, що базуються на аналізі частотних, енергетичних та модуляційних характеристик сигналів, мають обмежені можливості у випадках використання однотипних засобів зв’язку, однакових протоколів передачі або змінних режимів роботи.

Одним із перспективних напрямів підвищення ефективності систем РТР є використання технології радіочастотних відбитків (Radio Frequency Fingerprinting, RFF), яка дозволяє здійснювати індивідуальну ідентифікацію джерел радіовипромінювання за особливостями фізичного рівня сигналу. На відміну від програмних ідентифікаторів, які можуть бути змінені або скопійовані, радіочастотний відбиток формується сукупністю апаратних особливостей конкретного передавача. До таких особливостей належать нелінійності підсилювальних каскадів, нестабільність частоти генераторів, фазові шуми, амплітудно-фазовий дисбаланс I/Q-модулятора та характеристики аналогових фільтрів. Саме ці відмінності формують індивідуальний радіочастотний відбиток кожного засобу та створюють можливість реалізації задачі поекземплярного розпізнавання навіть для однотипних пристроїв з однаковими параметрами передачів.

Основна ідея застосування RFF у системах радіотехнічної розвідки полягає у переході від аналізу інформаційного вмісту сигналу до аналізу його

фізичних властивостей. При цьому сигнал розглядається як сукупність корисної інформації та апаратних спотворень, які несуть відомості про конкретний передавач. Практична складність полягає у необхідності відокремлення стабільних характеристик радіоелектронного засобу від впливу випадкових факторів — шумів, завад, багатопроменевого поширення, зміни умов прийому та характеристик приймачів.

Перші підходи до ідентифікації радіовипромінювачів базувалися на методах ручного виділення експертних ознак. Аналізувалися спектральна щільність потужності, фазові характеристики, статистичні параметри сигналу, частотні похідні та особливості перехідних процесів увімкнення передавача. Перевагою таких методів була можливість фізичної інтерпретації отриманих результатів, однак їх ефективність значною мірою залежала від умов функціонування системи. Зміна рівня сигналу, параметрів каналу або вплив зовнішніх завад могли призводити до суттєвого зниження точності ідентифікації.

Сучасний етап розвитку технологій RFF пов’язаний із широким використанням методів штучного інтелекту та глибокого навчання. На відміну від класичних підходів, нейромережеві моделі здатні автоматично знаходити приховані закономірності без попереднього ручного формування набору ознак.

Особливого поширення набули згорткові нейронні мережі (CNN), які дозволяють аналізувати сирі синфазні та квадратурні (I/Q) дані радіосигналів і визначати характерні особливості спектральних компонент, фазових переходів та нелінійних спотворень.

Для підвищення ефективності ідентифікації також застосовуються глибокі залишкові мережі (ResNet) та генеративно-змагальні моделі (GAN). ResNet-архітектури забезпечують аналіз складних часових залежностей у сигналах, а GAN дозволяють формувати додаткові навчальні дані у випадках обмеженої кількості реальних вибірок. Використання таких моделей дозволяє підвищувати стійкість систем розпізнавання та адаптувати їх до роботи у складних умовах радіоефіру.

У системах радіотехнічної розвідки технологія RFF може використовуватися для створення автоматизованих засобів класифікації та ідентифікації радіоелектронних засобів різного призначення. Перспективним напрямом є формування бібліотек радіочастотних портретів, які містять еталонні характеристики відомих джерел випромінювання та дозволяють

автоматично порівнювати отримані сигнали з наявними зразками. Це створює можливість переходу від загального аналізу параметрів сигналу до встановлення індивідуальної належності конкретного випромінювача.

Разом із високими потенційними можливостями практичне використання RFF у системах РТР має низку складних науково-технічних проблем. Однією з основних є недостатня відповідність між навчальними наборами даних та реальними умовами експлуатації. Синтетичні сигнали, які широко застосовуються для навчання моделей машинного навчання, не завжди можуть повністю відтворити багатопроменеве поширення, відбиття сигналів, часові зміни каналу та випадкові апаратні фактори.

Наукова новизна застосування RFF у системах радіотехнічної розвідки полягає у використанні фізичних характеристик радіосигналу як додаткового джерела інформації про належність випромінювача. Подальший розвиток цього напряму пов’язаний із розробкою адаптивних моделей глибокого навчання, використанням методів перенесення навчання для нових класів радіоелектронних засобів, створенням масштабних баз радіочастотних портретів та інтеграцією RFF із комплексними системами радіомоніторингу.

Таким чином, технологія радіочастотних відбитків є перспективним інструментом підвищення ефективності сучасних систем радіотехнічної розвідки. Вона дозволяє перейти від традиційного аналізу параметрів сигналу до інтелектуальної ідентифікації конкретних джерел радіовипромінювання за їхніми фізичними характеристиками. Подальше вдосконалення алгоритмів машинного навчання та розвиток методів обробки I/Q-сигналів створюють передумови для формування нових поколінь автоматизованих систем радіотехнічного аналізу.

Єгоров В. О., Ph. D.
Андрущенко І. С.
Житомирський військовий інститут імені С. П. Корольова

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ТА ПЕРСПЕКТИВНІ НАПРЯМИ РОЗВИТКУ СИСТЕМ РАДІОТЕХНІЧНОЇ РОЗВІДКИ: КОГНІТИВНІ, РОЗПОДІЛЕНІ ТА КВАНТОВІ ПІДХОДИ

Сучасний розвиток радіолокаційних систем із програмно-визначеною архітектурою (SDR), використання складних видів модуляції та режимів низької ймовірності перехоплення суттєво ускладнює функціонування традиційних систем радіотехнічної розвідки. Зростання щільності та динамічності електромагнітного середовища потребує переходу від класичних методів параметричного аналізу до інтелектуальних методів обробки сигналів.

Одним із перспективних напрямів є специфічна ідентифікація джерел радіовипромінювання, яка базується на формуванні унікального радіочастотного відбитка (RF Fingerprinting) за рахунок аналізу апаратних мікроознак передавача. Для виділення таких ознак використовуються характеристики ненавмисної внутрішньоімпульсної модуляції (UMOP), фазові та амплітудні шуми генераторів, а також перехідні процеси роботи радіочастотних трактів. Ефективність аналізу підвищується шляхом застосування частотно-часових методів обробки сигналів, зокрема вейвлет-перетворення, розподілу Вігнера–Вілля та варіаційної модової декомпозиції, у поєднанні з алгоритмами машинного навчання.

Важливим напрямом розвитку є створення когнітивних систем радіотехнічної розвідки (Cognitive ESM), здатних адаптивно аналізувати нові типи сигналів без повної попередньої апріорної інформації. Використання методів некерованого навчання та моделей глибинного навчання дозволяє підвищити ефективність розв’язання задач деінтерлівінгу у складних сигнальних середовищах із високою щільністю імпульсних потоків.

Подальший розвиток пов’язаний із переходом до розподілених сенсорних мереж та багатопозиційних систем радіомоніторингу. Спільна обробка даних від просторово рознесених приймачів та систем із використанням методів різниці часу приходу сигналу (TDOA) та різниці частот Доплера (FDOA) забезпечує підвищення точності локалізації джерел радіовипромінювання.

Перспективними апаратними рішеннями є застосування радіофотоніки, оптичних аналого-цифрових перетворювачів та методів компресійного зондування, що забезпечують ефективну обробку надширокосмугових сигналів. Окремий напрям становлять квантові радіочастотні сенсори на основі атомів Рідберга, які відкривають можливості створення високочутливих систем вимірювання електромагнітних полів у широкому частотному діапазоні.

Таким чином, перспективні системи радіотехнічної розвідки формуються на основі комплексної інтеграції методів машинного навчання, когнітивної обробки сигналів, розподіленої сенсорики та нових фізичних принципів вимірювання. Поєднання зазначених технологій створює передумови для розроблення інтелектуальних систем радіомоніторингу, здатних функціонувати в умовах складного електромагнітного середовища.

Тимчук С. В., канд. техн. наук
Тарасенко В. О.
Житомирський військовий інститут імені С. П. Корольова

ОЦІНЮВАННЯ МЕЖ ЗАСТОСОВНОСТІ ПІВТОНОВОГО ТЕНЗОРНОГО ПОДАННЯ СПЕКТРОГРАМ У ХОДІ РОЗПІЗНАВАННЯ ВУЗЬКОСМУГОВИХ РАДІОСИГНАЛІВ

Автоматизація класифікації короткохвильових радіосигналів за зображеннями спектрограм є актуальною для систем радіомоніторингу, у яких відсутній прямий доступ до первинних квадратурних IQ-відліків. У таких умовах джерелом інформації для алгоритму може бути візуалізований частотно-часовий «водоспад», що дає змогу застосовувати методи комп’ютерного зору. Водночас перетворення фізичного сигналу у графічне представлення неминуче супроводжується втратою частини інформації. Тому важливим є не лише підвищення інтегральної точності класифікації, а й визначення меж застосовності конкретного способу тензорного подання та аналіз структури помилок для окремих класів сигналів.

У попередньому дослідженні було сформовано одноканальне півтонове подання спектрограм, яке усуває залежність нейромережі від псевдокольорової палітри SDR-інтерфейсу та допускає роботу з довільною просторовою

розмірністю входу. Частотно-часове представлення формувалося за допомогою короткочасного перетворення Фур'є з вікном Хеммінга довжиною 1024 відліки. Лінійні рівні спектральної густини потужності переводилися у 8-бітові значення інтенсивності пікселів, після чого зображення подавалося на повнозгорткову модель із паралельними гілками MaxPooling та AveragePooling, механізмом Squeeze-and-Excitation і глобальним усередненим пулінгом. Така схема забезпечила загальну точність 77,50 % на незалежній тестовій вибірці, проте результати різних класів істотно відрізнялися.

Метою цієї роботи є оцінювання меж застосовності півтонового тензорного подання спектрограм для розпізнавання структурно подібних вузькосмугових радіосигналів та визначення інформаційних ознак, втрата яких найбільше впливає на помилки класифікації. На відміну від акценту на механізмі динамічної уваги, основну увагу зосереджено на аналізі матриці помилок, показників повноти та F1-міри, а також на фізичних причинах змішування класів після перетворення сигналів у 8-бітове півтонове зображення.

Експериментальна перевірка виконувалася для п'яти класів: Chayka N, Chayka P, Noise, RTTY та Stanag 4285. Для навчання і валідації було використано 5000 тензорів: по 900 навчальних та 100 валідаційних реалізацій кожного класу. Незалежна тестова вибірка містила 600 реалізацій, по 120 для кожного класу. За таких умов F1-міра становила 0,92 для Chayka N, 0,83 для Chayka P, 0,78 для Stanag 4285, 0,75 для Noise та лише 0,54 для RTTY. Саме клас RTTY продемонстрував найбільше зниження якості та став показовим для аналізу обмежень графічного представлення.

Матриця помилок показала, що з 120 тестових реалізацій RTTY правильно класифіковано 51. При цьому 50 реалізацій було віднесено до Chayka P, 12 – до Noise, 6 – до Stanag 4285 та 1 – до Chayka N. Повнота класу RTTY становила 0,43, тобто модель втрачала більше половини реальних зразків цього типу. Водночас для Chayka P усі 120 тестових реалізацій були правильно віднесені до свого класу. Така асиметрія свідчить, що помилка не має випадкового характеру: після півтонового перетворення частина RTTY набуває ознак, які в просторі згорткової моделі стають близькими до ознак Chayka P.

Фізичною причиною такого ефекту є свідоме виключення фазової інформації. Після обчислення спектральної густини потужності та квантування її рівнів до 8-бітової шкали модель працює лише з амплітудно-частотним

рельєфом. Для класів, між якими існують виразні відмінності за енергетичною структурою, цього представлення достатньо для стійкого розпізнавання. Однак для вузькосмугових сигналів із частотною маніпуляцією мікроструктурні відмінності можуть бути пов’язані не тільки з абсолютним рівнем енергії, а й із часовою послідовністю переходів, фазовою поведінкою та тонкими відмінностями спектральних компонентів. Після редукції до одноканального зображення ці ознаки частково або повністю втрачаються.

Додатковим фактором є обмеження динамічного діапазону. Перетворення у 8-бітову шкалу інтенсивностей залишає 256 можливих рівнів представлення спектральної енергії. Це спрощує вхідний тензор, зменшує залежність від конкретної візуалізації та полегшує навчання моделі, але одночасно стискає слабкі відмінності між близькими за амплітудно-частотним рельєфом сигналами. У результаті згортковий екстрактор ознак може коректно виділяти енергетичні максимуми та локальні просторові структури, але не відновлює інформацію, яка була втрачена ще до подання даних на вхід мережі.

Отримані результати також дають змогу уточнити роль механізму Squeeze-and-Excitation. Канал-залежне зважування є ефективним тоді, коли необхідна інформація вже присутня у сформованих картах ознак і потрібно адаптивно послабити неінформативні канали. Воно не може компенсувати відсутність фазової або часової інформації у початковому тензорі. Тому подальше ускладнення лише просторової архітектури без зміни складу вхідних даних має обмежений потенціал для класів, які стають структурно подібними після півтонового перетворення.

З позиції побудови системи радіомоніторингу це означає, що одноканальне півтонове представлення доцільно розглядати як спеціалізований режим для умов, коли доступним джерелом є лише графічний «водоспад». Його перевагами є відсутність залежності від кольорової палітри, можливість обробляти спектрограми різної просторової розмірності та достатньо висока ефективність для класів із вираженими просторово-енергетичними ознаками. Водночас для сигналів, розрізнення яких потребує збереження фази або детальної часової структури, таке подання не повинно розглядатися як інформаційно повне.

Логічним напрямом подальшого розвитку є гібридизація вхідного представлення. У межах наявної архітектури доцільно поєднати візуальну гілку,

яка обробляє півтонову спектрограму, з додатковим джерелом ознак, що зберігає фазову або часову інформацію. У попередньому дослідженні як перспективні варіанти визначено комплексні спектрограми та безпосередні IQ-вибірки. Таке поєднання має не замінювати переваги візуального аналізу, а доповнити його інформацією, втраченою під час переходу до спектральної густини потужності та 8-бітового графічного представлення.

Таким чином, аналіз клас-специфічних результатів показує, що загальна точність моделі не є достатнім критерієм для визначення придатності тензорного подання до всіх типів радіосигналів. Півтонове представлення ефективно виконує задачу нормалізації графічної форми спектрограми та знижує ризик залежності від особливостей SDR-інтерфейсу, однак має принципову межу, пов’язану з відсутністю фазової інформації та 8-бітовим обмеженням динамічного діапазону. Найвиразніше ця межа проявляється для RTTY, де F1-міра становить 0,54, а значна частина реалізацій змішується з Chayka P. Отже, подальше підвищення достовірності розпізнавання структурно подібних вузькосмугових сигналів доцільно пов’язувати не лише з удосконаленням механізмів виділення ознак, а насамперед із розширенням інформаційної повноти вхідного тензора.

Тарасенко В. О.
Шишкін Ю. Д.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РАДІОЕЛЕКТРОННІЙ РОЗВІДЦІ: МОЖЛИВОСТІ АВТОМАТИЗАЦІЇ ТА РОЛЬ ОПЕРАТОРА-АНАЛІТИКА

Сучасна радіоелектронна розвідка (РЕР) функціонує в умовах постійного зростання обсягів даних, ускладнення структури сигналів та скорочення часу, доступного для їх аналізу. За таких умов перспективним напрямом розвитку є застосування штучного інтелекту (ШІ), здатного автоматизувати рутинні операції, виявляти закономірності у великих масивах інформації та надавати оператору-аналітику інформаційну підтримку. Водночас ефективність таких систем визначається не лише точністю алгоритмів, а й правильною організацією взаємодії людини та машинних засобів аналізу.

Однією з основних можливостей ШІ у РЕР є автоматизація первинного оброблення інформації. Алгоритми машинного навчання можуть здійснювати попередню фільтрацію даних, виділення характерних ознак, групування подібних об'єктів та визначення фрагментів, які потребують першочергової уваги. Це дозволяє зменшити обсяг інформації, що безпосередньо переглядається людиною, та знизити ризик пропуску важливої події в умовах значного інформаційного навантаження.

Окремим напрямом є автоматизоване розпізнавання і класифікація сигналів. На відміну від систем, побудованих лише на фіксованих правилах і порогових значеннях, моделі машинного навчання можуть виявляти складні взаємозв'язки між ознаками та використовувати накопичені дані для розпізнавання типових об'єктів. Практичне значення має також виявлення аномалій, коли система визначає відхилення від характерної поведінки або появу нетипової інформації, яка не відповідає відомим класам. У такому випадку ШІ може швидко привернути увагу оператора до потенційно значущої зміни обстановки.

Перспективним є використання ШІ для узагальнення інформації, отриманої у різні моменти часу або з різних джерел. Автоматичне порівняння поточних і накопичених даних дає змогу знаходити повторювані ознаки, фіксувати зміни та формувати структуроване подання інформації. У результаті оператор отримує не суцільний потік первинних даних, а попередньо впорядкований інформаційний масив, що спрощує подальший аналіз і скорочує час реагування.

Разом із перевагами застосування ШІ має низку обмежень. Результати роботи моделі залежать від якості та репрезентативності навчальних даних. За появи нових або рідкісних типів сигналів точність класифікації може знижуватися. Також можливі хибнопозитивні та хибнонегативні результати, тому автоматично сформований висновок не повинен сприйматися як безумовно правильний. Важливими вимогами до таких систем є відображення рівня впевненості моделі та можливість перевірити підстави, за якими інформацію було віднесено до певного класу або визначено як аномальну.

У зв'язку з цим найбільш доцільною є концепція взаємодії «людина - ШІ», у якій машинні алгоритми виконують швидке сортування, класифікацію, пошук закономірностей і виділення пріоритетної інформації, а оператор-аналітик

здійснює перевірку та контекстну інтерпретацію результатів. Людина здатна враховувати чинники, які не були представлені в навчальних даних, зіставляти суперечливу інформацію та оцінювати нестандартні ситуації. Тому впровадження ШІ не усуває роль оператора, а змінює її від виконання рутинних операцій до аналітичного контролю та формування обґрунтованого висновку.

Особливо важливо запобігати автоматизаційному упередженню, коли користувач схильний некритично погоджуватися з рекомендацією системи. Оператор повинен розуміти можливості та обмеження застосованої моделі, вміти оцінювати рівень її впевненості й визначати випадки, що потребують додаткової перевірки. Корисним є і зворотний зв'язок: результати експертної оцінки можуть використовуватися для уточнення моделей та актуалізації навчальних даних.

Важливим чинником практичної ефективності є також організація інтерфейсу та підготовка персоналу. Інтелектуальна система має подавати результати у формі, що дає змогу швидко визначити пріоритет інформації, оцінити ступінь упевненості алгоритму та перейти до перевірки вихідних даних. Підготовка оператора повинна поєднувати професійні знання у сфері РЕР із базовим розумінням принципів машинного навчання, характерних помилок моделей і способів їх виявлення. Такий підхід зменшує ризик некритичного використання автоматизованих висновків та підвищує стійкість аналітичної роботи в умовах зміни інформаційної обстановки.

Отже, застосування ШІ в РЕР створює можливості для автоматизації оброблення великих обсягів інформації, розпізнавання сигналів, виявлення аномалій та зменшення когнітивного навантаження на персонал. Водночас найбільш ефективною є не повна заміна людини, а поєднання швидкості машинного аналізу з професійним досвідом, критичним мисленням і контекстною оцінкою оператора-аналітика. Подальший розвиток таких систем доцільно спрямовувати на підвищення точності та пояснюваності алгоритмів, удосконалення людино-машинної взаємодії й збереження обов'язкового людського контролю над кінцевими аналітичними висновками.

Єгоров В. О., Ph. D.
Гайка Ю. А.
Житомирський військовий інститут імен С. П. Корольова

ЗАСТОСУВАННЯ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ КЛАСИФІКАЦІЇ РАДІОЛОКАЦІЙНИХ СИГНАЛІВ В УМОВАХ ІНТЕНСИВНИХ ЗАВАД ТА НИЗЬКОГО ВІДНОШЕННЯ СИГНАЛ / ШУМ

Зростання щільності електромагнітного середовища, ускладнення структури радіолокаційних сигналів та широке застосування різних типів внутрішньоімпульсної модуляції зумовлюють необхідність удосконалення методів їх автоматичного розпізнавання. Особливо складною є задача класифікації сигналів за низького відношення сигнал/шум, коли інформативні ознаки частково маскуються шумом, нестаціонарними перешкодами та спотвореннями каналу поширення. За таких умов традиційні методи, засновані на спектральному, кореляційному та статистичному аналізі, демонструють зниження ефективності через високу залежність від якості виявлення, точності оцінювання параметрів сигналу та коректності сформованого набору ознак.

Перспективним напрямом вирішення зазначеної задачі є використання методів глибокого навчання, зокрема згорткових нейронних мереж, здатних автоматично формувати багаторівневі ознаки без необхідності їх ручного визначення. На відміну від класичних алгоритмів, згорткові нейронні мережі забезпечують можливість виявлення локальних і глобальних закономірностей у структурі сигналу та можуть адаптуватися до варіативності його параметрів, рівня шуму і характеру спотворень. Особливо доцільним є застосування таких моделей до частотно-часових представлень, у яких ознаки внутрішньоімпульсної модуляції відображаються у вигляді просторово організованих структур.

Для обробки радіолокаційних сигналів пропонується підхід автоматичної класифікації сигналів на основі перетворення комплексних I/Q-відліків у двовимірне частотно-часове представлення з подальшою обробкою згортковою нейронною мережею. Як базові способи формування ознак можуть використовуватися спектрограми короткочасного перетворення Фур’є та розподіл Чоя–Вільямса. Перший метод характеризується відносно невеликою обчислювальною складністю та придатністю до потокової обробки, тоді як

другий забезпечує кращу концентрацію енергії у частотно-часовій області та дає можливість детальніше відобразити складні закони зміни миттєвої частоти і фази. Використання таких представлень дає змогу сформувати вхідні дані у вигляді структурованих зображень, що є зручним для подальшої обробки двовимірними згортковими нейронними мережами.

Як основну архітектуру класифікатора доцільно використати модифіковану ResNet18, адаптовану до одноканальних частотно-часових зображень. Застосування залишкових зв'язків забезпечує навчання мережі та дозволяє формувати ознаки різного рівня складності без істотного погіршення передачі градієнта. На початкових рівнях мережа виділяє локальні частотно-часові структури, а на глибших — узагальнені ознаки, пов'язані з характером модуляції, законом зміни частоти, фазовими переходами та часовою структурою імпульсу. Для підвищення узагальнювальної здатності моделі передбачається застосування нормалізації, регуляризації, Dropout та аугментації навчальних даних.

До множини класифікованих сигналів можуть бути включені немодульовані радіоімпульси, сигнали з лінійною частотною модуляцією, фазокодовані сигнали з кодами Баркера, поліфазні сигнали, а також багаточастотні сигнали типу Costas. Через обмежену доступність репрезентативних реальних записів доцільним є формування синтетичного набору даних із випадковою зміною параметрів сигналів у визначених межах. Для кожного класу необхідно генерувати незалежні реалізації з варіацією тривалості, смуги частот, початкової фази та інших характеристик. Такий підхід дозволяє зменшити ризик перенавчання на фіксованих шаблонах і краще оцінити здатність моделі до узагальнення.

Особливу увагу слід приділити моделюванню шумового та завадового середовища. Крім адитивного білого гаусівського шуму, доцільно враховувати імпульсні, широкосмугові та частково-смугові завади, а також завмирання і багатопроменеве поширення. Рівень сигнал/шум доцільно варіювати в широкому діапазоні, зокрема від −20 до +20 дБ, що дозволяє дослідити поведінку алгоритму як у сприятливих, так і в критично складних умовах. При цьому навчальна, валідаційна та тестова вибірки повинні формуватися з незалежних реалізацій сигналів.

Для об'єктивного оцінювання ефективності запропонованого підходу його доцільно порівнювати з традиційним класифікатором методу опорних

векторів, одновимірною згортковою нейронною мережею, що працює безпосередньо з I/Q- відліками, та базовою двовимірною згортковою мережею. Основними показниками якості є загальна точність класифікації, Precision, Recall, Macro-F1 та матриця помилок. Найбільш інформативною характеристикою стійкості є залежність точності класифікації від рівня сигнал/шум. Окремого аналізу потребують результати у діапазоні від −5 до −10 дБ, де вплив шуму стає критичним і найбільш виразно проявляються переваги або обмеження різних методів.

Наукова новизна запропонованого підходу полягає у комплексному використанні частотно-часового представлення, залишкової згорткової нейронної мережі та розширеної моделі шумів і завад для оцінювання стійкості автоматичної класифікації радіолокаційних сигналів. На відміну від спрощених постановок, орієнтованих переважно на адитивний білий гаусівський шум, запропонована методика передбачає тестування алгоритму в умовах статистично різних спотворень та на незалежних реалізаціях сигналів. Це дозволяє більш об’єктивно оцінити здатність нейронної мережі до узагальнення та уникнути необґрунтованого завищення результатів.

Водночас кількісні показники ефективності повинні визначатися виключно за результатами фактичного експерименту на незалежній тестовій вибірці. Це особливо важливо для значень відношення сигнал/шум нижче 0 дБ, де абсолютна точність істотно залежить від кількості класів, способу формування датасету, моделі каналу та типів завад.

Таким чином, використання глибоких згорткових нейронних мереж у поєднанні з частотно-часовими представленнями є перспективним напрямом підвищення ефективності автоматичної класифікації радіолокаційних сигналів у складній електромагнітній обстановці. Подальші дослідження доцільно спрямувати на експериментальне порівняння різних типів частотно-часових перетворень, оптимізацію архітектури мережі, зменшення її обчислювальної складності, а також перевірку запропонованого підходу на реальних радіосигналах і даних, параметри яких не використовувалися під час навчання.

Бугайов М. В., канд. техн. наук, ст. досл.
Житомирський військовий інститут імені С. П. Корольова

ТОПОЛОГІЯ СИСТЕМИ РАДІОМОНІТОРИНГУ З ВИКОРИСТАННЯМ ГРУПИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Передумовами застосування безпілотних літальних апаратів (БпЛА) для ведення радіомоніторингу (РМ) є стрімкий розвиток як самих апаратів так і апаратури приймання та оброблення радіосигналів. Концепція ведення РМ з використанням групи БпЛА полягає у переході від статичного РМ до динамічного просторово-адаптивного РМ шляхом поєднання моделей багатопроменевого поширення радіохвиль із математичними моделями руху самих БпЛА. Це дозволяє перетворити недолік, пов’язаний із переміщенням приймача на БпЛА, що створює динамічні завмирання радіосигналів, на перевагу шляхом статистичного оброблення мінливостей прийнятих сигналів.

Під топологією системи РМ із використанням групи БпЛА будемо розуміти способи розміщення та взаємодії наземної станції керування та контролю (СКК) та БпЛА у групі між собою. Оскільки БпЛА повинні практично постійно переміщуватися, то головними вимогами до такої системи є гнучкість маршрутів польоту БпЛА, висока швидкість передачі даних, стійкість зв’язку та перехід до автономної роботи у разі його втрати.

Розглянемо три види топологій, із використанням яких може бути побудована система РМ: централізовану, мережеву та кластерну.

Для централізованої системи кожен БпЛА незалежно від інших виконує завдання з пошуку та локалізації джерел радіовипромінювання (ДРВ) під управлінням наземної СКК і передає на неї дані, отримані в результаті виконання завдань РМ, та телеметрію. Дальність дії такої системи обмежена дальністю каналу управління та передавання даних. Проте для неї досить просто забезпечити синхронну роботу усіх БпЛА. Дані з БпЛА при цьому можуть як передаватися на СКК, так і записуватися на носій на борту.

Для мережевої (повнозв’язної) топології (FANET, Flying Ad-hoc Network) усі БпЛА в повітрі можуть працювати одночасно як засоби РМ і як ретранслятори. Дана топологія від централізованої відрізняється наявністю додаткового радіоканалу між усіма БпЛА групи. Для реалізації такої схеми необхідні відповідні алгоритми для розрахунку оптимального маршруту

передавання даних та здійснення управління БпЛА. За відсутності зв’язку з наземною СКК дана система стає автономною. Дані про результати РМ з БпЛА можуть передаватися на СКК або записуватися на носій.

Кластерна топологія передбачає поділ усіх БпЛА групи на кластери. В кожному кластері один БпЛА виконує роль головного – повітряної станції управління та збору інформації, на яку передаються результати РМ інших БпЛА кластера. Повітряні станції управління обмінюються даними між собою та передають їх на наземну СКК. Кожен БпЛА у кластері може виконувати функції повітряної станції. Ним стає той, що має найкращий зв’язок з рештою БпЛА кластера та наземною СКК. Усі БпЛА кластера здійснюють обмін інформацією між собою. Інформація передається пакетами. Кожен пакет містить поточні координати БпЛА, вектор руху та параметри виявлених сигналів і пеленг на ДРВ.

Кластерна топологія системи РМ утворюється із мережевої топології. У разі виявлення одним БпЛА сигналу ДРВ він передає дані про його параметри та пеленг на ДРВ сусіднім БпЛА. Найближчі 3-4 БпЛА налаштовують апаратуру РМ на вказану частоту і формують відповідну базу пелентування для зменшення помилки оцінювання місцеположення ДРВ. На головному БпЛА кластера розраховуються уточнені оцінки параметрів сигналу виявленого ДРВ та його координати.

Незалежно від виду топології системи РМ БпЛА у групі чи кластері повинні бути рознесені в просторі відносно ДРВ таким чином, щоб пеленги на нього перетиналися під кутом, близьким до 90°. Це досягається шляхом обміну інформацією між БпЛА і СКК для централізованої топології або між окремими БпЛА групи для мережевої топології чи кластера для кластерної.

Данилюк І. А., канд. техн. наук, доц.
Куцаєв В. В.
Матвієнко В. М.
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

ВИЗНАЧЕННЯ ПОЗИЦІЙНИХ РАЙОНІВ РОЗГОРТАННЯ ОПЕРАТИВНО-ТАКТИЧНОГО РАКЕТНОГО КОМПЛЕКСУ “ІСКАНДЕР” ЗА ДАНИМИ БАГАТОКАНАЛЬНОЇ РАДІОТЕХНІЧНОЇ РОЗВІДКИ

Оперативно-тактичний ракетний комплекс (ОТРК) “Іскандер” характеризується високою оперативністю передислокації, короткотривалим

розгортанням на позиції та застосуванням заходів маскування і зниженням демаскувальних ознак, що ускладнює своєчасне виявлення та ідентифікацію засобу: часовий інтервал між виявленням факту пуску та безпосереднім впливом на об'єкти, як правило, недостатній для протидії загрозі. У зв'язку з цим актуальним є завчасне визначення ймовірних районів розгортання ракетних засобів до моменту їх фактичного зайняття позицій.

Тому науковою задачею стає завчасне (упереджене) визначення ймовірних районів розгортання ОТРК противника ще до початку його фізичного розгортання.

Мета – раннє попередження про загрозу застосування та ухвалення рішень щодо захисту об'єктів, що охороняються: укриття, евакуації, обмеження маршрутів і режимів діяльності військового й цивільного населення. Основою даних слугують непрямі ознаки підготовки, що передують розгортанню та фіксуються переважно радіотехнічною, оптичною й тепловою розвідкою. Актуальність напряму зумовлена потребою удосконалення форм і способів ведення радіоелектронної розвідки відповідних підрозділів Сил оборони України — від виявлення наявних засобів випромінювання до прогнозування підготовки до їхнього застосування.

1. Термінологічний апарат основних понять.

1) Загрозлива подія – швидкоплинна високоенергетична дія (ракетний пуск, вибух, розгортання техніки), що супроводжується комплексом взаємопов'язаних змін стану навколишнього середовища.

2) Прогнозне виявлення – встановлення факту та параметрів підготовки до загрозливої події за сукупністю непрямих просторово-часових ознак.

3) Об'єкт виявлення – позиційний район (ділянка місцевості), ознаки підготовки до розгортання на якій спостерігаються; об'єктом є не сам комплекс.

4) Позиційний район розгортання – придатна для розміщення засобу ураження ділянка місцевості за оцінкою сукупних просторових, логістичних, транспортних, інженерних, радіочастотних, теплових і поведінкових ознак.

5) Ознаки підготовки – непрямі прояви діяльності з підготовки до застосування: підвезення техніки й боєприпасів, розчищення ділянки, поява маскувальних конструкцій, активізація засобів зв'язку, режим “прибуття – розгортання – активність – тиша”.

6) Фоновий стан середовища – статистично усталена сукупність параметрів сенсорних каналів за відсутності підготовки до загрозливої дії.

7) Інформаційна достатність – принцип, за яким ступінь категоричності висновку не може перевищувати забезпечення фактично отриманих вимірювань.

8) Рівень категоричності висновку – дискретна шкала достовірності висновку, що розрізняє стани “немає ознак підготовки”, “ознаки не підтверджені”, “ознаки підтверджено”, “розгортання зафіксовано”. Кожному рівню відповідає власна межа невизначеності оцінки.

9) Упереджене визначення позиційних районів розгортання – формування їх переліку до початку фізичного розгортання засобу, що забезпечує виграш часу, потрібний для попередження про загрозу застосування та ухвалення рішень щодо захисту об'єктів, що охороняються.

10) Коридор потенційної загрози – область простору, у якій із заданою імовірністю може розвиватися траєкторія засобу ураження після початку події, який звужується в міру надходження спостережень. Термін “коридор” вжито тому, що траєкторія має вигляд протяжної смуги простору, на відміну від кутового “сектору”, поверхневої “зони” (області розсіювання) та адміністративного “району”.

11) Сектор потенційної загрози – кутова частина простору, у межах якої траєкторія реалізується за напрямом, визначеним на момент підтвердження пускової події.

12) Ймовірна площа спостереження (ЙПС) – підобласть контрольованої території, для якої задано апріорну та поточну імовірність появи і підготовки засобу ураження та оцінку очікуваної інформативності покриття; вона є одиницею розподілу обмежених ресурсів спостереження.

2. Загальна постановка наукової задачі.

Сутність задачі полягає у визначенні переліку ймовірних позиційних районів розгортання ОТРК – від складних (районів базування та позицій комплексу) до простих (окремих стартових позицій) заздалегідь, до фактичного розгортання, на підставі безперервного спостереження за середовищем та оцінювання переходів між його функціональними станами, для своєчасного попередження про загрозу та ухвалення рішень щодо захисту об'єктів, що охороняються.

Формалізовано: $\{X_d : P(D_d) \geq p_{пор}\}$ та $\{T_{вп} - T_{фіз} \geq T_{реаг}\}$, де X_d – множина позиційних районів розгортання; D_d – подія підготовки до розгортання в районі

d; $p_{пор}$ – допустимий поріг імовірності; $T_{вп}$ і $T_{фіз}$ – моменти встановлення ознак підготовки та фактичного розгортання; $T_{реаг}$ – мінімально необхідний час реагування. Перша умова задає множину придатних районів, друга – вимогу щодо випередження.

Розв'язання задачі передбачає вирішення підзадач:

1) формування й супровід карти потенційно придатних районів розгортання, що на відміну від карти виявлених і підтверджених позицій містить також райони з підвищеною імовірністю підготовки, де доцільно сконцентрувати обмежені ресурси спостереження;

2) виявлення ознак підготовки та їхньої просторово-часової узгодженості;

3) розпізнавання переходів між станами “очікування – підготовка – здійснення дії – згортання”;

4) прогнозування сектору та коридору потенційної загрози (пункти 10, 11 термінології) після підтвердження пускової події;

5) контроль інформаційної достатності кожного рівня висновку.

Особливостями задачі є ненадійність окремої ознаки, потреба у багатоканальному узгодженні та тривалому автономному спостереженні, обмеженість ресурсів. Висновком системи має бути не категоричне твердження “комплекс знайдено”, а ймовірнісна оцінка готовності ділянки з рівнем упевненості (підпункти 7, 8 термінології) та межею власного знання про середовище.

3. Пропонований підхід до формалізації виявлення.

Базовим елементом запропонованого підходу є ідея ймовірних площ спостереження (ЙПС) (підпункт 12 термінології). Замість суцільного покриття контрольованого району X, що потребує нерозмірних ресурсів, територія розбивається на ЙПС з різною апріорною та поточною імовірністю появи засобу і різною оцінкою очікуваної інформативності. Це дає змогу сконцентрувати обмежену кількість сенсорів там, де вони дають максимум інформації. Розподіл ресурсів переглядається за накопиченням даних, що дозволяє адаптувати схему спостереження без перебудови системи.

Відносно підзадачі 1 процедура формалізації така: для кожної ЙПС оцінюється поточна невизначеність оцінки стану та її відповідність рівню категоричності висновку, який можна обґрунтувати наявними даними. Район, для якого невизначеність перевищує допустиму для обраного рівня, до переліку не вноситься або вноситься з позначкою низької впевненості. Механізм

переводить карту потенційної готовності з евристичної у формалізовану: вона відображає не факт наявності установки, а встановлену ймовірність підготовки.

Контроль інформаційної достатності (підзадача 5) реалізується зіставленням поточної невизначеності оцінки із заданим порогом, що визначає максимально допустиму категоричність висновку на кожному рівні. Отже, зазначена підзадача є контрольною вимогою до висновку, а зіставлення – способом її виконання.

Формалізація ознак підготовки (підзадача 2) передбачає їх поділ на просторові (радіочастотні, теплові, візуальні) та поведінкові (режим прибуття, тривалість активності, періодичність); для кожної ознаки вводяться тривалість і просторово-часова узгодженість. Через ненадійність окремої ознаки висновок формується лише за узгодженою сукупністю ознак різних каналів: поодиноке спрацювання каналу не є підставою для підвищення рівня висновку. Роль радіотехнічної розвідки тут визначальна, оскільки вона забезпечує найбільш ранній потік даних про активізацію засобів зв'язку, перемикання режимів роботи та зміну електромагнітного обліку об'єкта.

Розпізнавання переходів між станами (підзадача 3) формалізується як послідовність “фоновий стан – поява ознак підготовки – їх просторово-часове накопичення – інтенсифікація діяльності – пускова подія – згортання”, де кожному переходу відповідає власний набір очікуваних ознак і рівень категоричності висновку. Такий опис пов'язує часовий бюджет задачі з конкретними стадіями, тобто якщо перехід до пускової події встановлено із випередженням $T_{реаг}$, то вимога достатності інформації (пункт 7 термінології) виконана. Після реєстрації пускової події межі сектору та коридору потенційної загрози уточнюються пропорційно надійності каналу.

4. Висновки.

Таким чином, авторами:

1) сформульовано та узгоджено термінологічний апарат прогнозного виявлення швидкоплинних загрозливих подій: визначено об'єкт виявлення, рівні категорічності висновку, сектор і коридор потенційної загрози, одиницю розподілу ресурсів спостереження;

2) виконано загальну постановку наукової задачі упередженого визначення позиційних районів розгортання ОТРК “Іскандер” для своєчасного попередження про загрозу застосування;

3) запропоновано підхід до формалізації виявлення, що ґрунтується на розбитті території на ймовірні площі спостереження, пороговому зіставленні невизначеності оцінки з допустимою категоричністю висновку та просторово-часовій узгодженості ознак.

На даному етапі розв'язано лише завдання формалізації виявлення: узгоджено термінологічний апарат, формалізовано об'єкт виявлення, ознаки підготовки та механізм контролю інформаційної достатності; емпіричне оцінювання запропонованого підходу на реальних даних не проводилося.

Напрямки подальших наукових досліджень: 1) накопичення емпіричних даних про просторово-часові ознаки підготовки за матеріалами радіотехнічної, оптичної й теплової розвідки; 2) розвиток ймовірнісної моделі станів середовища; 3) розроблення критеріїв достатності інформації та їх прив'язки до типів захищуваних об'єктів; 4) оптимізація розподілу ресурсів спостереження між ЙПС; 5) дослідження стійкості методів до втрати й підміни каналів; 6) експериментальна апробація методів з оцінюванням часу випередження та хибних спрацювань.

Дзігора О. М.
Яровий С. В., канд. техн. наук, доц.
Красношапка І. В., канд. техн. наук, доц.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ТЕХНОЛОГІЧНІ МОЖЛИВОСТІ КОНСТРУЮВАННЯ ТВЕРДОТІЛЬНОГО ПІДСИЛЮВАЧА ПОТУЖНОСТІ РАДІОЛОКАЦІЙНОГО ПРИЗНАЧЕННЯ S-ДІАПАЗОНУ

Постановка проблеми. Технологія твердотільних підсилювачів потужності НВЧ діапазону поступово займає своє місце на ринку військових і космічних систем. Останні роки у світі чітко сформувалась тенденція переходу від підсилювачів на основі GaAs-структур до технології на основі нітріда галія GaN. Іноземна високотехнологічна продукція зв'язкового, супутникового і військового призначення широко використовує її для підсилення сигналів у L-, S-, C-, і навіть X- і Ku- діапазонах.

Перехід на твердотільну технологію обумовлений необхідністю підвищення надійності, зменшення масо-габаритних характеристик, спрощення технічного обслуговування та забезпечення високої стабільності амплітудно-фазових параметрів сигналу. У сучасних радіолокаційних системах саме стабільність параметрів зондувального сигналу визначає можливості застосування складних видів внутрішньоімпульсної модуляції, цифрової та когерентної обробки з поєднанням придушення активних і пасивних завад з високою ефективністю.

Незважаючи на очевидні переваги твердотільних рішень, абсолютна більшість існуючих вітчизняних РЛС S-діапазону досі використовують електровакуумні генератори та підсилювачі. Відомо, що такі електровакуумні прилади (ЕВП) мають низку суттєвих недоліків: обмежену смугу робочих частот, високовольтне живлення, значний час прогріву, що впливає на боєготовність радара, деградацію параметрів у процесі експлуатації, низький ресурс та дуже високу вартість.

Окремо серед електровакуумних приборів виділяється клістрон, він, хоча і забезпечує припустиму когерентність сигналів у підсилювачах потужності, має низьку суттєвих недоліків – складність конструкції і громіздкість підсилювачів у S-діапазоні, значний час готовності до бойової роботи, достатньо обмежений робочий частотний діапазон і малий коефіцієнт перестроювання по частоті, складність реалізації частотної маневреності та використання широкосмугових складномодульованих сигналів необхідних для сучасної завадозахищеної радіолокації. А, головне на сьогодні, малий час напрацювання на відмову – до 1000 год при дуже високій його вартості. На сучасному етапі вартість за одиницю прибора настільки висока, що може сягнути собівартості повністю закінченої (зконструйованої) шафи твердотільного підсилювача потужності, який потенційно забезпечить час напрацювання до відмови до 1 млн годин. І це не враховуючи вартості схемної обв’язки клістрона – шафи модулятора, шафи попереднього підсилювача, шафи високовольтного стабілізованого випрямляча, соленоїда та системи рідинного охолодження.

При цьому, очевидним фактом є майже 100%-ва твердотільна реалізація сучасних радарів іноземного виробництва у сантиметровому діапазоні хвиль. Однак, характерною особливістю цих радарів є реалізація методу просторового

складання енергії сигналу за допомогою активної фазованої антенної решітки (AESA) і майже відсутні реалізації твердотільних потужних підсилювачів для радарів із дзеркальними антенами та пасивними антенними решітками (PESA).

В цілому наукові дослідження в області підсилення потужності у НВЧ діапазоні з використанням окремих монолітних інтегральних схем надвисоких частот (MMIC) або дискретних GaN-транзисторів мають на меті розробку підсилювачів із піковою потужністю до 40–45 dBm, у той же час недостатньо опрацьованим є більш потужні імпульсні підсилювачі рівня 70–73 dBm, які дозволять заживити пасивні антенні решітки й дзеркальні антени радарів S-діапазону.

Опубліковані дослідження доказують, що GaN технологія є найбільш перспективною для побудови імпульсних НВЧ підсилювачів радіолокаційного призначення завдяки високій питомій потужності, великій пробивній напрузі, високому ККД, добрій теплопровідності та значному часу напрацювання на відмову (MTTF).

Виклад основного матеріалу. Застосування твердотільних передавачів на перевагу від лампових обумовлене:

1) значним спрощенням експлуатаційних, сервісних та технічних вимог, оскільки передавач працює на набагато нижчих напругах;

2) немає потреби в гарячих катодах, потужних модуляторах та інших складних потужних елементах;

3) можливістю використовувати лише повітряне охолодження;

4) виключається ризик небезпечного рентгенівського випромінювання та ураження електричним струмом;

5) безпотрібністю імпульсного модулятора, оскільки твердотільні мікрохвильові пристрої зазвичай є самоімпульсними;

6) широкою смугою пропускання (до 50 % порівняно з 5–20 % у лампах);

7) тривалиим безвідмовним терміном служби та поступовим зниженням продуктивності системи, оскільки система зазвичай складається з великої кількості модулів;

8) вдосконаленістю та компактністю технології (наприклад, використання активних приймально-передавальних модулів для фазованих радіолокаційних решітчастих ґраток), що дозволяє розробляти недорогі, компактні, легкі та надійні повністю твердотільні радари, які можуть працювати без участі персоналу.

Для проектування підсилювача потужності з необхідним рівнем потужності до 70–73 dBm доцільне використання схеми із комбінованою

паралельно-послідовною структурою (для дзеркальних систем) або гібридної схеми (для PESA).

Розвиток технології GaN HEMT протягом останніх двох десятиліть відбувався поетапно – від першого до п’ятого покоління, де кожне наступне покоління вирішувало специфічні фізико-технічні проблеми та розширювало частотний і потужнісний потенціал приладів.

Сучасний п’ятий етап розвитку (2025–2026 роки) характеризується технологічним переходом на епітаксіальне вирощування структур GaN-on-SiC на пластинах діаметром 300 мм. Це забезпечує безпрецедентне зниження собівартості приладів за збереження високої якості кристалічної ґратки. Надважливою інновацією п'ятого покоління (Gen 5) є застосування технологій послідовного каскодного з'єднання кристалів (stacking), що дозволяє транзисторам працювати під напругою до 150 В і досягати рекордної питомої потужності на рівні 29 Вт/мм. В результаті дискретні транзистори відомих світових виробників (Ampleon, Integra Technologies, Qorvo, MACOM, Wolfspeed, Sumitomo Electric Device Innovations) забезпечують вихідну імпульсну потужність в межах 500–2000 Вт у діапазоні 2,7–3,1 ГГц зі шпаруватістю 10 % і високим коефіцієнтом корисної дії до 60 %. При цьому стоково-істокова напруга живлення складає всього 50–150 В. Названі вище компанії також пропонують НВЧ-вироби у вигляді інтегрованих підсилювальних палет та модулів, виконаних за технологією GaN-on-SiC, які є повністю узгодженими до стандартного імпедансу 50 Ом. Їх пікова потужність досягає величини до 4 кВт на палету при майже 20 %-й шпаруватості імпульсної послідовності.

Аналіз параметрів як дискретних транзисторів так і підсилювальних палет дозволив стверджувати про можливість їх застосування для проектування когерентних передавальних пристроїв сучасних радарів сантиметрового діапазону із дзеркальними антенами та пасивними антенними решітками. Однак узгодженість таких параметрів як пікова потужність – шпаруватість пристроїв вимагає використання для дальньої радіолокації в якості зондувальних довготривалих складномодульованих радіоімпульсів тривалістю сотні мікросекунд с базою 150–200.

Висновки і перспективи подальших досліджень. Платформа GaN-on-SiC HEMT на сьогодняшній день залишається домінуючим та безальтернативним рішенням для потужних радарних систем S-діапазону за

рахунок неперевершеної густини потужності та теплопровідності, що дозволяє створювати компактні модулі. Сучасні підсилювальні палети та модулі на базі GaN-on-SiC досягли рівня технологічної готовності, яка забезпечує пікову потужність до 2,8–4,0 кВт в одному модулі із ККД понад 40–60 %. Це робить їх повністю придатними для побудови потужних радіолокаційних передавачів. Принцип комплектування потужних трактів підсилення негерметизованими модулями SSPA типу Pallet (у складі загального герметизованого обсягу) дозволяє досягти максимальної експлуатаційної ефективності та надійності апаратури, а також зменшення її масо-габаритних характеристик та терміну розробки. В умовах серійного виробництва РЛС використання таких модулів як закінчених електронних компонентів з гарантованими параметрами дозволяє суттєво зменшити витрати на технічне обслуговування та ремонт апаратури у процесі її експлуатації.

Радушинський О. П.
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ ВИЯВЛЕННЯ ТА СПЕКТРАЛЬНОГО АНАЛІЗУ РАДІОВИПРОМІНЮВАНЬ MESH / MANET-МЕРЕЖ У ЗАВДАННЯХ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ

Сучасна радіоелектронна розвідка (РЕР) є важливою складовою моніторингу електромагнітного середовища та ситуаційної обізнаності. Одним із основних її завдань є своєчасне виявлення, класифікація та локалізація радіовипромінювань, пов'язаних із засобами зв'язку, передачі даних та управління. Однак розвиток цифрових радіосистем суттєво змінює характер радіоелектронної обстановки та створює нові вимоги до засобів радіомоніторингу.

Однією з важливих тенденцій є поширення самоорганізованих мереж типу Mesh та MANET (Mobile Ad Hoc Network). У таких системах окремі вузли можуть виконувати функції кінцевих абонентів, маршрутизаторів або ретрансляторів, а структура мережі здатна динамічно змінюватися залежно від стану вузлів та умов радіоканалу. При цьому Mesh/MANET визначає передусім принцип організації мережевої взаємодії, тоді як конкретні характеристики

радіосигналу — ширина смуги, тип модуляції, метод розширення спектра, швидкість передачі та механізми перебудови частоти — залежать від реалізації фізичного та канального рівнів.

Для засобів РЕР особливу складність становлять широкосмугові цифрові сигнали та пакетний характер передачі. Використання технологій розширення спектра, багатонесучих сигналів, частотно-часової адаптації та інших методів формування радіосигналу може призводити до зниження його спектральної щільності потужності та ускладнювати виявлення на фоні шумів. Водночас такий сигнал не слід вважати принципово невидимим. Факт його наявності може бути виявлений за відповідного співвідношення сигнал/шум і використання відповідних методів цифрового аналізу. Значно складнішими можуть бути подальші завдання — визначення типу сигналу, його синхронізація, класифікація та декодування.

Додатковою проблемою є короткочасний характер пакетних передач. Якщо тривалість окремого радіопакета є малою порівняно з часом послідовного перебування приймача на певній частоті, традиційне сканування може мати низьку ймовірність перехоплення такого сигналу. Особливо це проявляється при одночасному контролі широкого діапазону частот. У зв'язку з цим перспективним напрямом є використання аналізаторів спектра в реальному часі (RTSA) та широкосмугових SDR-приймальних систем, які забезпечують одночасне спостереження значної частини спектра та фіксацію короткочасних радіоподій.

Аналіз радіовипромінювань доцільно розглядати як послідовність декількох завдань: виявлення сигналу, оцінювання його параметрів, класифікація, локалізація джерела та, за наявності відповідних можливостей, подальший аналіз його структури. Ускладнення одного з цих етапів не означає неможливості виконання інших. Наприклад, широкосмугове випромінювання може бути виявлене за енергетичними або статистичними ознаками навіть без знання його внутрішньої структури, тоді як його детальна класифікація потребуватиме аналізу часових, частотних та інших характеристик.

Суттєвий вплив на ефективність РЕР має просторова структура Mesh/MANET-мережі. Наявність декількох вузлів, їхня мобільність, зміна маршрутів та різна інтенсивність випромінювання формують динамічну картину радіообстановки. Один приймальний пункт при цьому може спостерігати лише частину активних джерел. З іншого боку, децентралізована

структура не робить локалізацію випромінювань принципово неможливою. Навпаки, використання просторово розподілених синхронізованих приймальних вузлів дає можливість застосовувати багатопозиційні методи, зокрема оцінювання кута приходу сигналу (AOA) та різниці часу приходу (TDOA), а за відповідних умов — різниці частоти приходу (FDOA).

Ефективність просторової локалізації залежить від геометрії системи спостереження, точності часової та частотної синхронізації, характеристик антен, калібрування приймальних трактів і умов поширення радіохвиль. Особливу проблему створюють міська забудова та складний рельєф, де відбиття, затінення та багатопроменеве поширення можуть викликати амплітудні та фазові спотворення. Унаслідок цього для підвищення достовірності локалізації доцільно використовувати сукупність просторових, часових і частотних ознак.

Ще одним фактором є адаптивність сучасних цифрових радіосистем. Залежно від конкретної реалізації може здійснюватися зміна режимів модуляції та кодування, швидкості передачі, ширини займаної смуги, робочої частоти та інших параметрів. Застосування псевдовипадкової перебудови частоти або інших частотно-часових механізмів додатково ускладнює тривале спостереження за окремим випромінювачем. Водночас такі механізми не є обов'язковими властивостями Mesh/MANET і визначаються конкретною технологією радіоканалу.

Для роботи з такими сигналами перспективною є SDR-архітектура, яка забезпечує перенесення значної частини функцій обробки сигналів із апаратного рівня у програмну область. Це дозволяє адаптувати алгоритми приймання та аналізу до різних типів радіосигналів, виконувати потокову спектральну обробку, детектування короткочасних подій, побудову спектрограм і водоспадних діаграм, а також виділення інформативних фрагментів I/Q-даних.

Одночасно широкосмугове оцифрування створює проблему значного обсягу даних. Потік I/Q-вибірок залежить від ширини смуги спостереження, частоти дискретизації, розрядності аналого-цифрового перетворювача та кількості паралельних каналів. Тому передавання і зберігання необробленого потоку може бути ресурсомістким. Одним із способів зменшення навантаження є виконання частини первинної обробки безпосередньо на приймальному вузлі:

детектування сигналів, фільтрація, виділення ознак та збереження лише інформаційно значущих фрагментів. Для високопродуктивної обробки можуть застосовуватися FPGA, GPU, CPU та спеціалізовані апаратні прискорювачі.

Окремим перспективним напрямом є використання методів машинного навчання та штучного інтелекту для автоматизації аналізу радіоелектронної обстановки. AI/ML-алгоритми можуть застосовуватися для автоматичного виявлення сигналів, кластеризації випромінювань, класифікації їхніх типів, пошуку аномальних патернів та аналізу зміни активності джерел у часі. Особливо перспективними є системи, які поєднують спектральні, часові та просторові ознаки замість аналізу окремої спектрограми.

Таким чином, розвиток широкосмугових пакетних Mesh/MANET-мереж зміщує завдання РЕР від традиційного послідовного радіомоніторингу до комплексного аналізу просторово-часової та спектральної структури радіоелектронної обстановки. Основними проблемами стають виявлення короткочасних передач, одночасне спостереження широких ділянок спектра, нестабільність параметрів випромінювачів, багатопроменеве поширення та необхідність обробки значних потоків цифрових даних.

Сучасні пакетні Mesh/MANET-мережі створюють новий клас задач для радіоелектронної розвідки, пов'язаний із необхідністю виявлення та аналізу динамічних широкосмугових випромінювань у складному електромагнітному середовищі. Основна складність полягає не в принциповій невидимості таких сигналів, а у зменшенні ймовірності їх своєчасного виявлення, короткочасності передач, динамічній зміні параметрів та необхідності одночасного аналізу великої кількості джерел.

Перспективним напрямом розвитку засобів РЕР є створення розподілених систем на основі SDR та RTSA із синхронізованими приймальними вузлами, здатними виконувати широкосмугове спостереження, цифрову обробку сигналів і багатопозиційну локалізацію. Додаткове застосування методів AI/ML дозволяє автоматизувати виявлення, класифікацію та кластеризацію радіовипромінювань, зменшуючи навантаження на оператора та підвищуючи оперативність аналізу радіоелектронної обстановки.

Отже, подальше вдосконалення систем РЕР доцільно пов'язувати з переходом від окремих засобів радіомоніторингу до розподілених інтелектуальних систем, які об'єднують широкосмугове приймання, високопродуктивну цифрову обробку, просторовий аналіз та автоматизоване машинне навчання.

Гайка Ю. А.
Єгоров В. О., Ph. D.
Житомирський військовий інститут імені С. П. Корольова

ОПТИМІЗАЦІЯ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ЗАСОБІВ РАДІОРОЗВІДКИ НА БАЗІ БЕЗПІЛОТНИХ АВІАЦІЙНИХ ПЛАТФОРМ

Сучасний етап розвитку військового мистецтва характеризується стрімкою трансформацією форм і способів ведення збройної боротьби, де ключову роль відіграє інформаційна перевага на полі бою. Досвід сучасних інтенсивних збройних конфліктів та локальних бойових дій довів, що традиційні підходи до виявлення та ураження сил противника втрачають свою ефективність без суцільного, безперервного та високоточної розвідувального забезпечення. Ключовим каталізатором цієї технологічної революції стало масове та системне впровадження безпілотних літальних апаратів (БпЛА) різного класу в загальну систему розвідки та управління військами.

У загальному контурі збору оперативної та тактичної інформації особливе стратегічне значення належить радіорозвідці (РР). За умов масового застосування противником засобів радіоелектронної боротьби (РЕБ), замаскованих командних пунктів, автоматизованих систем управління та безпілотних комплексів, саме радіовипромінювання часто залишається єдиним демаскувальним фактором об'єктів ворога. Радіорозвідка є критично важливим інструментом для оперативної виявлення, ідентифікації, класифікації та точної локалізації (визначення координат) джерел радіовипромінювання (ДРВ) потенційного противника у режимі реального часу.

Актуальність дослідження напряму зумовлена специфікою та викликами сучасного високодинамічного бою:

Традиційні комплекси радіорозвідки, що базуються на стаціонарних наземних платформах або важкій колісній та гусеничній техніці, стикаються з критичними обмеженнями. Вони мають низьку мобільність, потребують тривалого часу для розгортання та є першочерговими цілями для високоточної зброї противника. Крім того, наземні комплекси суттєво залежать від рельєфу місцевості, щільності забудови та лісових масивів, які утворюють численні “сліпі зони” та унеможливлюють пеленгацію малопотужних сигналів.

Сучасна тактика передбачає широке використання малопотужних цифрових радіостанцій з псевдовипадковим перелаштуванням робочої частоти

(ППРЧ), а також каналів управління дронами. Виявлення таких сигналів із землі на безпечній відстані є майже неможливим через швидке згасання радіохвиль біля поверхні землі. Інтеграція апаратури РР на авіаційні платформи дає змогу підняти приймальні антени на необхідну висоту та подолати фізичні обмеження наземної розвідки.

Розвиток технологій програмно-конфігурованого радіо (Software-Defined Radio — SDR) створив технологічне підґрунтя для кардинального зменшення масогабаритних показників розвідувального обладнання. Це робить можливим встановлення повноцінних радіоприймальних та пеленгаційних модулів на доступні, відносно недорогі малі та середні БПЛА, що суттєво знижує вартість виконання розвідувальних завдань.

Таким чином, актуальність даного дослідження полягає у необхідності теоретичного обґрунтування та практичного вирішення завдань підвищення ефективності радіорозвідки шляхом створення та інтеграції малогабаритних радіоелектронних комплексів на безпілотні авіаційні платформи.

Розміщення радіорозвідувальних модулів на борту безпілотних літальних апаратів дозволяє успішно розв'язати низку критичних проблем, які є нерозв'язними для наземних аналогів:

1. Суттєве збільшення дальності прямої радіовидимості: підняття антено-фідерних систем на значну висоту над поверхнею землі суттєво розширює радіообрій. Це дає змогу повністю нівелювати затіняючий вплив складного рельєфу — гірських масивів, складних елементів ландшафту, щільної міської забудови та лісових масивів. Крім того, це відкриває можливість упевненого перехоплення сигналів малопотужних радіостанцій тактичної ланки управління (наприклад, портативних радіостанцій та засобів зв'язку низької потужності), які раніше були абсолютно недоступні для фіксації наземними пунктами спостереження через згасання сигналу на малих висотах.

2. Підвищення мобільності та мінімізація ризиків для особового складу: динамічність БпЛА дозволяє здійснювати оперативне передислокування розвідувальних потужностей у призначені зони в найкоротші терміни. Це забезпечує можливість постійного супроводу передових підрозділів без необхідності розгортання громіздких наземних антенних систем. Найважливішим аспектом є дистанційне керування комплексом, що повністю виключає загрозу життю та здоров'ю розвідувального екіпажу в умовах активного вогневого впливу ворога.

3. Технологічна мініатюризація на основі SDR-архітектури: стрімкий прогрес у галузі мікроелектроніки уможливив створення високоефективних та компактних модулів РР, побудованих за принципом програмно-конфігурованого радіо. Такі блоки мають незначну масу, мінімальні габаритні розміри та низький рівень енергоспоживання. Завдяки цьому стало можливим оснащувати засобами радіорозвідки навіть малі БпЛА тактичного рівня, розширюючи їх функціонал від суто оптико-електронної спостережності до повноцінного радіоелектронного

Аналіз тенденцій розвитку військово-технічної сфери дозволяє виділити три основні вектори вдосконалення апаратури радіорозвідки на БпЛА:

Побудова багатопозиційних розвідувальних систем: перехід від поодиноких носіїв до застосування груп або “роїв” БпЛА, які функціонують у єдиному синхронізованому інформаційному просторі. Завдяки високій точності часової синхронізації це дозволяє реалізувати складності різницево-дальномірних (TDOA) та амплітудно-фазових методів пеленгації. Результатом є забезпечення високої точності визначення просторових координат ДРВ у режимі реального часу.

Інтеграція інтелектуальних систем обробки сигналів: впровадження алгоритмів штучного інтелекту (ШІ) та машинного навчання (ML) безпосередньо в обчислювальні потужності бортового комп'ютера БпЛА (Edge AI). Це дає можливість здійснювати первинну автоматичну класифікацію типів сигналів, ідентифікувати протоколи зв'язку противника, селектувати корисні сигнали на тлі інтенсивного радіоелектронного шуму та фільтрувати активні завади без залучення оператора.

Автоматизація контуру “розвідка — ураження”: Максимальне скорочення часу від моменту виявлення радіоцілі до її знищення шляхом автоматичної передачі отриманих координат на засоби вогневого ураження (артилерію, ракетні комплекси) або безпосередньо на ударні безпілотні апарати в межах єдиної розвідувально-ударної мережі.

Попри очевидні переваги, масове впровадження засобів радіорозвідки на безпілотних платформах стримується низкою складних інженерно-технічних проблем:

Обмеження по масогабаритних та енергетичних показниках: малі та середні БпЛА мають суворо обмежену корисну вантажопідйомність та ємність акумуляторних батарей (або запас палива), що лімітує тривалість їх перебування у повітрі під час роботи бортового обладнання РР.

Захищеність ліній передачі даних: необхідність передачі великих обсягів первинних розвідувальних даних у реальному часі вимагає створення високошвидкісних, завадостійких та шифрованих каналів зв'язку, які важко придушити засобами РЕБ противника.

Проблема електромагнітної сумісності (ЕМС): близьке розташування чутливих приймачів радіорозвідки до бортових систем телеметрії, передавачів відеосигналу, систем навігації та електродвигунів БпЛА викликає високий рівень внутрішніх завад, що потребує складного екранування та спеціальної фільтрації.

Таким чином, застосування засобів радіорозвідки на базі безпілотних літальних апаратів є ключовим фактором підвищення ефективності збору даних про радіоелектронну обстановку на сучасному театрі бойових дій. Основні перспективи розвитку даної галузі полягають у подальшій мініатюризації радіоелектронного обладнання, автономізації процесів аналізу сигналів безпосередньо на борту носія за допомогою штучного інтелекту, а також у глибшій інтеграції БпЛА-РР у мережецентричні розвідувально-ударні комплекси.

Сидорчук О. Л., канд. техн. наук, доц.
Залевський В. Й.
Житомирський військовий інститут імені С. П. Корольова

ДОСЛІДЖЕННЯ КОЕФІЦІЄНТІВ ВІДБИТТЯ ЕЛЕКТРОМАНІТНИХ ХВИЛЬ ВІД ПОЗАМЕЖНИХ ПЕРЕРІЗІВ ОПРОМІНЮВАЧІВ ФАЗОВАНИХ АНТЕННИХ РЕШІТОК

Сучасні зразки озброєння та військової техніки (ОВТ) протиповітряної оборони (ППО) у своєму складі налічують значну кількість антен. Для їх удосконалення і покращення тактико-технічних характеристик (ТТХ) найчастіше проводять заміну звичайних антен на більш досконалі, шляхом впровадження фазованих антенних решіток (ФАР). Це дозволить підвищити коефіцієнт підсилення, а відповідно і дальність дії, збільшити кількість цілей (об'єктів пеленгації) тощо. Більшість останніх досліджень спрямовано на заміну їх антенами MIMO, проте залежно від задачі залишається проблема покращення ТТХ саме рупорних антен у складі ФАР.

З’ясовано, що перевагою застосування рупорних антен у складі ФАР є висока спрямованість їх випромінювання, значний коефіцієнт корисної дії та

досить високий коефіцієнт підсилення. Проте їх основним недоліком є зворотне випромінювання (розсіювання) електромагнітних хвиль елементами конструкції антени. Це впливає на радіолокаційну помітність зразків ОВТ та їх електромагнітну сумісність.

Для усунення зазначених недоліків у доповіді проаналізовано характеристики діаграм зворотного розсіювання рупорних опромінювачів, що входять до складу ФАР з урахуванням коефіцієнтів відбиття від їх позамежних перерізів.

Авторами запропоновано вдосконалений математичний апарат розрахунку електромагнітного поля, перевипроміненого антенною решіткою, що складається з рупорних опромінювачів пірамідальної форми для випадку нормальної поляризації електромагнтної хвилі до площини її падіння. Новизною є врахуванням коефіцієнтів відбиття від позамежних перерізів рупорних опромінювачів, що входять до складу ФАР. Аналогічно двом наведеним у доповіді прикладам знаходження ЕПР рупора лінійної поляризації можна розрахувати ЕПР рупорного опромінювача колової поляризації. Різними будуть лише коефіцієнти відбиття від внутрішніх неоднорідностей.

У доповіді запропоновано розрахункові формули дослідження поля, відбитого розкривом одного або n-го випромінювача антенної решітки, у разі падіння на неї нормально поляризованої хвилі, асимптотичними методами із застосуванням леми Лоренца.

Визначено коефіцієнти відбиття для хвиль електричного і магнітного типу від розкриву за умови узгодження з хвильовим опором вільного простору. Виведено вираз для розсіяного поля від розкриву без урахування внеску «паразитних» хвиль та з урахуванням такого внеску.

Із отриманих математичних моделей добре видно, що коефіцієнти відбиття, наприклад хвилі Н типу, у зворотному напрямку від внутрішніх неоднорідностей залежатимуть від співвідношення розмірів рупора й довжини падаючої на розкрив хвилі. У доповіді наведено можливі варіанти таких співвідношень та варіанти її відбиття

Для перевірки виведених математичних моделей для розрахунку ЕПР рупора у складі ФАР було досліджено внесок відбитого сигналу від апертури антени у її сумарну (інтегральну) ЕПР. Для цього було проведено натурний експеримент. Вимірювання ЕПР антени проводились при її підключенні до узгодженого навантаження, закороченому виході і розімкненому фідері.

Дослідження проводилось у діапазоні частот 10–15ГГц та за нормальної поляризації електромагнітної хвилі, що падає на антену до площини її падіння.

Новизною є те, що було отримано формули саме для випадку нормальної поляризації падаючої електромагнітної хвилі до площини її падіння а також враховано коефіцієнти відбиття для хвиль вищих типів від неоднорідностей прямокутного хвилеводу та його поперечних перерізів.

Таким чином вдалось покращити математичну модель дослідження перевипроміненої від ФАР електромагнітної енергії з визначенням усіх коефіцієнтів відбиття від рупорних опромінювачів та врахуванням коефіцієнтів відбиття від їх позамежних перерізів задля його зменшення. Це дозволить зменшити коефіцієнт стоячої хвилі за напругою та рівень бічних пелюсток. Отже, до зондуючої радіолокаційної станції надійде зменшений рівень відбитого сигналу, що дозволить покращити розвідзахищеність ОВТ ППО та інших зразків, до складу яких входить рупор як окрема антена або в складі ФАР.

Мельник С. В.
Житомирський військовий інститут імені С. П. Корольова

СУЧАСНИЙ СТАН ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛАМИ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ

Під час ведення бойових дій (операцій) в умовах динамічної зміни оперативної обстановки надзвичайно важливим для прийняття раціональних рішень є якісне та своєчасне розвідувально-інформаційне забезпечення керівного складу. Виконання даної умови потребує ефективної організації інформаційно-аналітичної діяльності, критичним аспектом якої є інформаційна взаємодія (взаємний обмін, передавання, отримання та спільне використання розвідувальної інформації між розвідувальними органами та органами військового управління). Саме тому одним з головних факторів щодо забезпечення доступності інформації стало впровадження та використання інформаційно-комунікаційних систем (ІКС).

Однією з основних ІКС, яка використовується підрозділами Збройних Сил України є система ситуаційної обізнаності “Delta”, яка дозволяє відстежувати

зміни в наявній оперативній обстановці в режимі часу близькому до реального з відображенням об’єктів противника, що викриваються органами розвідки. Використання такого підходу дає змогу проаналізувати розміщення підрозділів противника, його пунктів управління, складів боєприпасів та інших об’єктів з метою подальшого нанесення вогневого ураження. Проте наявний функціонал даної системи не дозволяє забезпечити потреб щодо обробки інформаційного потоку, що виникають у підрозділів радіоелектронної розвідки під час виконання ними завдань за призначенням.

Враховуючи суттєве збільшення обсягу розвідувальної інформації, яке відмічається з початку повномасштабної збройної агресії рф проти України, виникла необхідність розробки та впровадження нових ІКС, які дозволяють підвищити оперативність виконання комплексу заходів і дій з добування розвідувальної інформації, спрямованих на викриття функціонування радіоелектронних засобів і систем, які застосовуються для управління військами (силами) та зброєю, збору, обробки, аналізу та доведення цієї розвідувальної інформації визначеним споживачам у встановлені терміни. Саме виникнення даної необхідності зумовило створення в Україні нового сегменту спеціалізованого програмного забезпечення, яке стало вагомим допоміжним інструментом в ході виконання завдань за призначенням добувними, інформаційними та інформаційно-аналітичними підрозділами.

Варто відмітити, що на даний час існує декілька основних ІКС нового сегменту, які активно використовуються підрозділами радіоелектронної розвідки. Дані системи мають різний інтерфейс, функціональні можливості та структуру, але призначені для виконання подібних завдань. Одними із ключових проблемних питань є відсутність кодифікації зазначених систем та їх офіційного прийняття на озброєння. Саме тому процес вибору та впровадження систем в конкретному підрозділі є несистематизованим та здійснюється відповідно до рішення розвідувальних органів на місцях. З урахуванням цього виникає необхідність аналізу можливостей даних систем, їх слабких та сильних сторін, та створення на основі результатів проведеного аналізу єдиного системного рішення, здатного в подальшому забезпечити виконання відповідних функцій в одному інформаційному середовищі.

Остапчук О. М.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ АВТОМАТИЗОВАНОЇ КЛАСИФІКАЦІЇ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ В СУЧАСНИХ КОМПЛЕКСАХ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ

Електромагнітне середовище сучасного поля бою характеризується високою щільністю різнорідних випромінювань та широким використанням складних алгоритмів формування й обробки сигналів. Серед них особливе місце займають системи зі стрибкоподібною перебудовою робочої частоти (Frequency Hopping Spread Spectrum — FHSS), сигнали з низькою ймовірністю перехоплення (Low Probability of Intercept — LPI), а також різноманітні види внутрішньоімпульсної модуляції. У таких умовах комплекси радіоелектронної розвідки (РЕР) функціонують в умовах значної зашумленості, великої кількості перешкод та значних потоків радіочастотних даних.

Традиційні підходи до виявлення, пеленгування та класифікації джерел радіовипромінювання (ДРВ) ґрунтуються переважно на детермінованих алгоритмах, пороговій обробці та аналізі заздалегідь визначених параметрів сигналів: тривалості імпульсу (Pulse Width), періоду повторення імпульсів (Pulse Repetition Interval), несучої частоти та інших характеристик. Їх ефективність знижується за низького співвідношення сигнал/шум (SNR), перекриття сигналів, складних сигнальних форматів і нестабільних умов поширення радіохвиль. Додатковим обмеженням є необхідність ручного або напівавтоматичного аналізу значних масивів часової та спектральної інформації, що збільшує час прийняття рішень. Це зумовлює необхідність переходу до адаптивних методів на основі штучного інтелекту (ШІ) та машинного навчання.

Однією з ключових проблем є робота комплексів РЕР в умовах високої електромагнітної зашумленості та низького SNR. Радіосигнали зазнають затухання, багатопроменевого поширення та впливу природних і штучних перешкод, унаслідок чого традиційні статистичні, кореляційні та порогові методи можуть втрачати стійкість. Перспективним напрямом є поєднання

нейромережевих класифікаторів із попередньою цифровою обробкою, шумозаглушенням, автоенкодерами та спеціалізованими архітектурами, стійкими до спотворень вхідних даних. Водночас ефективність моделей машинного навчання залежить від наявності репрезентативних маркованих вибірок. Дефіцит RAW-даних для нових або модифікованих типів сигналів і дисбаланс між поширеними та рідкісними класами можуть призводити до перенавчання моделей. Для подолання цієї проблеми доцільно використовувати трансферне та напівконтрольоване навчання, аугментацію й балансування даних.

Важливим фактором є також обмеження мобільних і бортових платформ РЕР за габаритами, масою, енергоспоживанням та обчислювальними ресурсами. Глибокі нейронні мережі потребують значної обчислювальної потужності, тоді як результати аналізу мають формуватися із мінімальною затримкою. Тому перспективним є застосування концепції Edge AI, за якої інтелектуальна обробка виконується безпосередньо на периферійній платформі. Для зменшення обчислювальної складності використовуються квантування (Quantization), прунінг (Pruning), дистиляція знань (Knowledge Distillation) та спеціалізовані апаратні прискорювачі. Такий підхід створює можливість інтеграції алгоритмів ШІ з SDR-приймальними системами, FPGA та іншими вбудованими платформами.

Для автоматизованого розпізнавання складних радіосигналів перспективним є застосування згорткових нейронних мереж (CNN) для аналізу часо-частотних представлень. Сирі I/Q-дані можуть перетворюватися на спектрограми за допомогою короткочасового перетворення Фур'є (STFT), розподіли Вігнера–Вілла або вейвлет-коефіцієнти. Такі представлення дають змогу одночасно враховувати часові та частотні характеристики сигналу. CNN здатні автоматично виділяти характерні ознаки, а гібридні моделі — поєднувати аналіз I/Q-послідовностей і спектральних характеристик. Для аналізу послідовностей імпульсів та їх часових залежностей можуть застосовуватися рекурентні нейронні мережі RNN, LSTM і GRU. Їх використання дає змогу враховувати послідовність подій, часові інтервали та зміни параметрів сигналу. Поєднання таких мереж із механізмами уваги розширює можливості аналізу довгих послідовностей.

Окремим завданням є виявлення нових або раніше невідомих типів радіовипромінювання, відсутніх у наявних базах даних. Класифікатори з

фіксованим набором класів у такій ситуації можуть неправильно відносити нові сигнали до вже відомих категорій. Для вирішення цієї проблеми перспективним є застосування неконтрольованого та напівконтрольованого навчання, а також алгоритмів виявлення аномалій. Автоенкодери та варіаційні автоенкодери (VAE) можуть навчатися на даних відомого радіоелектронного середовища. Якщо структура нового сигналу істотно відрізняється від навчальної вибірки, зростання помилки реконструкції може бути використано як критерій виявлення аномалії та привернення уваги оператора.

Таким чином, поєднання CNN, RNN/LSTM/GRU, механізмів уваги та моделей виявлення аномалій дозволяє сформувати багаторівневу архітектуру інтелектуального аналізу радіосигналів: від виявлення та попередньої обробки до виділення ознак, класифікації відомих типів і виявлення невідомих сигналів. Інтеграція ШІ та МН підвищує рівень автоматизації, скорочує час аналізу та зменшує когнітивне навантаження на операторів. Водночас необхідно враховувати можливість зловмисних збурень, здатних негативно впливати на результати класифікації, що зумовлює необхідність підвищення стійкості моделей за допомогою захисного навчання, контролю якості вхідних даних та оцінювання достовірності результатів.

Подальший розвиток інтелектуальних комплексів РЕР пов'язаний із поєднанням ШІ, цифрової обробки сигналів, SDR та Edge AI. Оптимізовані нейромережеві моделі, інтегровані з периферійними обчислювальними платформами та апаратними прискорювачами, створюють передумови для автоматизованого виявлення, виділення ознак, класифікації та первинного аналізу ДРВ. У результаті комплекси РЕР можуть трансформуватися від переважно реєстраційних систем у адаптивні інтелектуальні аналітичні комплекси, здатні оперативно обробляти великі потоки радіочастотної інформації, виявляти нові закономірності та надавати оператору структуровані результати аналізу.

Красношапка І. В., канд. техн. наук, доц.
Садовий К. В., канд. техн. наук, доц.
Чепурний В. П.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ОБҐРУНТУВАННЯ СТРУКТУРИ АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ ПАСИВНОГО ВИЯВЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ НА ОСНОВІ SDR-ТЕХНОЛОГІЙ

Інтенсивний розвиток безпілотних літальних апаратів істотно змінив характер ведення сучасних бойових дій. Широке використання БпЛА для повітряної розвідки, коригування вогню та завдання ударів актуалізує потребу в розробленні ефективних засобів їх своєчасного виявлення. Водночас традиційні радіолокаційні системи часто демонструють недостатню ефективність під час виявлення малорозмірних цілей із низькою ефективною площею розсіювання.

Метою дослідження є розроблення апаратно-програмного комплексу пасивного виявлення безпілотних літальних апаратів на основі SDR-технології, призначеного для виявлення та класифікації повітряних цілей за сукупністю характеристик їхнього радіочастотного випромінювання.

У роботі здійснено аналіз сучасних типів безпілотних літальних апаратів та встановлено, що інформаційний обмін у процесі їх функціонування реалізується із застосуванням складних протоколів передавання даних. Визначено, що основними джерелами радіочастотного випромінювання БпЛА є канали керування, телеметрії та передавання відеоінформації.

Аналіз наявних методів виявлення засвідчив, що найвищу ефективність забезпечує їх комплексне застосування. Водночас у роботі основну увагу зосереджено на пасивних радіотехнічних методах. Для формування так званого «радіочастотного почерку» БпЛА запропоновано здійснювати спектральний аналіз сигналів. Визначено характерні ознаки випромінювання різних типів безпілотних літальних апаратів:

Сформовано структуру апаратної складової комплексу, до якої входять антено-фідерна система, SDR-приймач із широкою смугою огляду та малошумлячий підсилювач, призначений для підвищення чутливості приймального тракту.

Функціонування програмної складової комплексу ґрунтується на обробленні спектрограм і відображенні «водоспаду» сигналів у режимі реального часу. Запропоновано створення бібліотеки сигнатур БПЛА та алгоритмів їх автоматичного розпізнавання. Проведено математичне моделювання роботи апаратно-програмного комплексу та розраховано потенційну дальність виявлення БПЛА.

За результатами дослідження доведено доцільність використання SDR-технологій у поєднанні з методами цифрової обробки сигналів для побудови ефективних, мобільних і порівняно недорогих систем виявлення БпЛА.

Гребенюк О. О., Ph. D.
Гребенюк О. П., канд. тех. наук
Житомирський військовий інститут імені С. П. Корольова

ОБҐРУНТУВАННЯ ВИБОРУ МАТЕМАТИЧНОЇ МОДЕЛІ ДЛЯ РОЗПІЗНАВАННЯ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ В УМОВАХ СКЛАДНОЇ РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ

Сучасні умови застосування засобів радіоелектронної розвідки (РЕР) в ході широкомасштабних бойових дій росії проти України характеризуються високою динамічністю зміни радіоелектронної обстановки (РЕО), інтенсивним застосуванням противником засобів радіоелектронної боротьби, а також динамічною зміною режимів функціонування джерел радіовипромінювання (ДРВп). За таких обставин, особливого значення набуває забезпечення своєчасного виявлення та достовірного розпізнавання ДРВп, насамперед у багатосигнальному середовищі за наявності перешкод та умов часткової апріорної невизначеності. Ефективність виконання завдань РЕР значною мірою визначається спроможністю засобів своєчасно розпізнавати ДРВп за сукупністю їхніх інформаційних ознак. У зв’язку з цим, важливим науково-практичним завданням є обґрунтований вибір математичної моделі, здатної забезпечити необхідний рівень достовірності розпізнавання за умови збереження оптимальної обчислювальної складності та оперативності функціонування засобів і комплексів РЕР.

Завдання розпізнавання сигналів ДРВп належить до класу задач теорії розпізнавання образів і передбачає формування рішення на основі аналізу множини параметрів досліджуваного об’єкта. Для її розв’язання можуть застосовуватися статистичні, метричні, евристичні та комбіновані підходи, результативність яких визначається структурою вхідних даних і конкретними умовами функціонування системи. Вибір математичної моделі залежить від повноти навчальних вибірок, обсягу апріорної інформації, кількості та інформативності ознак, рівня завад, а також доступних обчислювальних ресурсів. Зазначені чинники безпосередньо впливають на достовірність розпізнавання та тривалість формування кінцевого рішення. Водночас, застосування лише одного підходу не в усіх випадках забезпечує необхідні показники ефективності, що зумовлює доцільність використання комбінованих моделей, здатних адаптуватися до змін параметрів радіоелектронної обстановки.

Досліджено ймовірнісні, метричні та евристичні підходи до розпізнавання сигналів із використанням модернізованого байєсівського методу, зваженої евклідової відстані та евристичної класифікації. Моделювання виконано з урахуванням особливостей функціонування алгоритмів на імітаційних і реальних експериментальних даних, що дало змогу оцінити їхню ефективність за різних рівнів інформаційної визначеності. Встановлено, що вибір математичної моделі розпізнавання доцільно здійснювати на основі співвідношення між вимогами до оперативності прийняття рішення та необхідною достовірністю отриманого результату. Ймовірнісний підхід забезпечує високу достовірність розпізнавання за наявності достатньо повних і репрезентативних баз даних, а також достовірної статистичної інформації про характерні ознаки джерел радіовипромінювання. Метричний підхід є менш залежним від обсягу апріорних відомостей та забезпечує можливість розпізнавання за обмеженої або частково невизначеної сукупності вхідних параметрів шляхом оцінювання ступеня близькості отриманих ознак до еталонних значень. Евристичний підхід ґрунтується на використанні попередньо сформованих правил, експертних оцінок та характерних поєднань ознак, що забезпечує високу оперативність прийняття рішення і можливість його застосування за відсутності достатнього обсягу статистичних даних. Водночас його результативність значною мірою визначається повнотою та обґрунтованістю сформованої системи оцінювання.

Отримані результати свідчать, що жодна із зазначених моделей не є універсальною для всіх можливих умов РЕО. Раціональний вибір підходу має здійснюватися залежно від рівня апріорної визначеності, повноти та достовірності вхідних параметрів, наявності еталонних і статистичних даних, а також установлених вимог до швидкодії та достовірності розпізнавання. За умов достатнього статистичного забезпечення доцільним є застосування ймовірнісної моделі, за неповних або частково визначених даних – метричної, а за необхідності оперативного прийняття рішення на основі заздалегідь визначених ознак – евристичної. Перспективним напрямом є комплексне використання трьох зазначених підходів, що дає змогу підвищити достовірність розпізнавання ДРВп в умовах складної та динамічної РЕО.

Андрущенко І. С.
Єгоров В. О., Ph. D.
Житомирський військовий інститут імені С. П. Корольова

МЕТОД ЦИКЛОСТАЦІОНАРНОГО АНАЛІЗУ СИГНАЛІВ У ЗАВДАННЯХ РАДІОМОНІТОРИНГУ

Сучасний стан розвитку засобів і систем радіозв’язку характеризується суттєвим ускладненням сигнально-завадової обстановки. Широке впровадження складних цифрових видів модуляції, технологій розширення спектра та адаптивного регулювання потужності призводить до того, що рівень радіосигналів у точці приймання може бути нижчим за рівень фонового шуму та інших завад. У таких складних і динамічних умовах традиційні енергетичні та спектральні методи виявлення і розпізнавання сигналів у засобах радіомоніторингу можуть втрачати ефективність, оскільки не забезпечують надійного відокремлення корисного сигналу від шуму за низьких значень відношення сигнал/шум. Це зумовлює актуальність розроблення та впровадження методів, орієнтованих на використання циклостаціонарних властивостей радіосигналів.

Багато сучасних інформаційних радіосигналів за своєю природою можуть розглядатися як циклостаціонарні випадкові процеси. Ця властивість зумовлена наявністю періодичних або квазіперіодичних структур, пов’язаних із

функціонуванням систем зв'язку, зокрема цикловою та символьною синхронізацією, періодичністю тактових інтервалів, структурою кадрів, маніпуляцією несучої частоти, а в окремих системах — використанням циклічного префікса. На відміну від стаціонарного шуму, статистичні характеристики циклостаціонарного сигналу змінюються періодично або мають періодичні складові. Зокрема, його автокореляційна функція може бути представлена як функція, що має періодичну складову в часі та розкладається в гармонійний ряд за циклічними частотами.

Однією з основних характеристик циклостаціонарного процесу є функція циклічної спектральної кореляції (циклічний спектр), яка характеризує статистичний взаємозв'язок між спектральними компонентами сигналу, рознесеними за частотою на величину, що відповідає певній циклічній частоті. Наявність виражених спектрально-кореляційних компонент на ненульових циклічних частотах є характерною ознакою багатьох інформаційних сигналів і практично не властива ідеальному стаціонарному білому шуму. Тому аналіз площини «частота — циклічна частота» дає змогу виявляти та селектувати корисні сигнали навіть за низьких значень відношення сигнал/шум.

Запропонований метод циклостаціонарного аналізу передбачає виконання таких основних етапів:

– цифрове фільтрування та квадратурне оцифрування вхідного аналогового радіосигналу з формуванням послідовності комплексних відліків;

– сегментацію часової послідовності на перекривні інтервали та обчислення локальних спектрів за допомогою швидкого перетворення Фур'є;

– формування спектральних добутків між компонентами сигналу, частотно рознесеними відповідно до заданих значень циклічної частоти;

– усереднення отриманих спектральних оцінок за інтервалом спостереження для зменшення впливу випадкових складових та підвищення достовірності виявлення циклостаціонарних ознак;

– формування двовимірного циклічного спектрального портрета сигналу у площині «частота — циклічна частота»;

– автоматизований пошук локальних максимумів на циклічному спектрі та їх порівняння з еталонними ознаками, що містяться в базі даних системи розпізнавання сигналів.

Застосування запропонованого підходу дає змогу підвищити стійкість виявлення радіосигналів до впливу шумів і завад різної природи. За

результатами комп’ютерного моделювання встановлено, що використання циклостаціонарних ознак може забезпечувати виявлення інформаційних сигналів за відношень сигнал/шум, за яких традиційні енергетичні методи виявлення втрачають ефективність. При цьому конкретне граничне значення відношення сигнал/шум залежить від виду сигналу, тривалості спостереження, параметрів оцінювача циклічного спектра, характеристик завад та обчислювальних ресурсів системи.

Окрім виявлення факту наявності радіовипромінювання, циклостаціонарний аналіз може використовуватися для оцінювання його основних параметрів без виконання повної процедури демодуляції. Зокрема, за характером і розташуванням максимумів циклічної спектральної кореляції можна отримувати інформацію про несучу частоту, символьну або тактову швидкість, структуру сигналу та, за наявності достатньо виражених і характерних ознак, здійснювати класифікацію виду модуляції. Таким чином, циклостаціонарні ознаки можуть бути використані як інформативні параметри для автоматизованого розпізнавання радіовипромінювань.

Практична реалізація запропонованого методу є доцільною у програмно-конфігурованих радіосистемах (SDR), автоматизованих комплексах радіомоніторингу та системах технічного аналізу радіовипромінювань. Використання цифрової обробки сигналів дає змогу реалізувати адаптивний вибір діапазону частот, тривалості спостереження, роздільної здатності за частотою та циклічною частотою, а також забезпечити автоматизоване формування і порівняння циклостаціонарних ознак із відповідними еталонами.

Отже, використання методів циклостаціонарного аналізу в засобах радіомоніторингу дає змогу підвищити достовірність виявлення та розпізнавання радіовипромінювань у складних сигнально-завадових умовах. На відміну від суто енергетичних методів, циклостаціонарний підхід використовує не лише енергетичні характеристики сигналу, а й притаманні йому статистичні та структурні ознаки. Це робить його перспективним інструментом для побудови сучасних автоматизованих систем радіомоніторингу, особливо на основі SDR-технологій.

Козюра І. В.
Житомирський військовий інститут імені С. П. Корольова

ОБҐРУНТУВАННЯ МЕТОДИКИ ПЕРЕВІРКИ ДОСТОВІРНОСТІ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ В УМОВАХ СКЛАДНОЇ ОПЕРАТИВНОЇ ОБСТАНОВКИ

В сучасній оперативній обстановці великий обсяг інформації, що циркулює в сучасному інформаційному просторі, обмежує можливість використання наявних ресурсів для своєчасного фокусування їх у відповідних сферах.

На процеси добування та обробки розвідувальної інформації впливають такі фактори:

обмеження у часі – будь яка розвідувальна інформація з часом втрачає свою цінність та актуальність, залежно від її характеру мова може йти про декілька днів, годин чи навіть лічені хвилини;

обмеження у силах та засобах – кількості та якості апаратури розвідки ніколи не достатньо для того щоб здобути 100% можливої інформації; спеціалістів, які працюють над добуванням та обробкою розвідувальною інформації ніколи не буває достатньо, а якість їх роботи не буває абсолютно ідеальною.

Таким чином, слід враховувати, що і розвідувальна інформація ніколи не буде ідеальною. Вона, як правило, містить певні вади. Вони можуть виникнути як в процесі добування розвідувальної інформації, так і на всіх етапах її обробки. Очевидно, що ступінь їх впливу на оцінювання обстановки та прийняття рішення може суттєво відрізнятися: не впливати взагалі, впливати певною мірою або критично впливати.

Особливу небезпеку становлять неточності в числових характеристиках (координати, номери військових частин чи з’єднань, кількісні показники тощо), а також в назвах географічних об’єктів.

Повністю уникнути спотворень розвідувальної інформації ніколи не вдасться, однак мінімізувати такі ризики можливо, а отже працювати над цим треба. Для цього розроблені та надані рекомендації щодо уникнення ризиків подання хибної розвідувальної інформації.

Повідомлення зіставляються:

з іншими повідомленнями про той же об’єкт;

із загальними уявленнями щодо об’єктів того типу, до якого відносять той, що описується;

з характеристикою джерела.

Отримані результати свідчать, що отримані повідомлення необхідно зіставляти:

з іншими повідомленнями про той же об’єкт;

із загальними уявленнями щодо об’єктів того типу, до якого відносять той, що описується;

з характеристикою джерела.

Інформація від різних видів (органів) розвідки може підтверджувати, доповнювати, частково або повністю спростовувати одна одну. Надмірна схожість двох повідомлень із різних джерел може бути таким же підґрунтям для особливої підозри, як і надмірне розходження. В такому випадку інформація підлягає перевірці. Аналітик повинен запросити підтверджуючі матеріали, ініціювати (організувати) добування та збір додаткової інформації. Також аналітик також має чітко уявляти з якого джерела надійшла розвідувальна інформація і наскільки їй можна довіряти.

Основними напрямками підвищення ефективності роботи аналітиків визначено використання спеціального програмного забезпечення в процесі обробки інформації, ведення на постах добування та обробки електронних баз даних, постійне удосконалення знань та практичних навичок аналітиків, а також забезпечення комфортних умов для їх роботи.

Любиченко В. П.
Житомирський військовий інститут імені С. П. Корольова

ОЦІНЮВАННЯ СТАНУ ГРУПОВИХ ОБ’ЄКТІВ СПОСТЕРЕЖЕННЯ В УМОВАХ ОБМЕЖЕНОЇ АПРІОРНОЇ ІНФОРМАЦІЇ

Сучасні умови функціонування систем спостереження характеризуються значною невизначеністю, неповнотою та неоднорідністю інформації про об’єкти, що підлягають оцінюванню. Особливої складності набуває визначення стану групового об’єкта, структура якого може бути відома лише частково, а окремі його складові можуть не проявлятися на різних етапах в процесі

спостереження. В умовах непрояву окремої складової групового об’єкта неможливо однозначно визначити, чи зумовлено це її фактичною відсутністю, чи відсутністю відповідного спостережуваного прояву, що потребує врахування невизначеності під час формування узагальненої оцінки стану групового об’єкта.

Пропонується підхід до оцінювання стану групового об’єкта, що ґрунтується на комплексному використанні доступної інформації про його складові, їхні ознаки та характер зміни в часі. Груповий об’єкт розглядається як складна система, стан якої визначається не тільки станом окремих складових, а й характером їх взаємозв’язків та загальною структурою об’єкта. При цьому оцінювання здійснюється за умов, коли частина складових може бути безпосередньо викритою, частина — тимчасово не проявлятися, а щодо окремих складових інформація може бути недостатньою.

В основу підходу покладається формування узагальненої оцінки стану групового об’єкта на основі сукупності доступних ознак із одночасним урахуванням як отриманої, так і відсутньої інформації. При цьому особливого значення набуває розмежування понять «не виявлено» та «не провився», що дозволяє уникнути неправильного визначення стану об’єкта за умов неповного спостереження.

Для підвищення обґрунтованості оцінювання пропонується враховувати попередні результати спостереження та динаміку зміни ознак. Це дає можливість визначати не лише поточний стан групового об’єкта, але й тенденцію його зміни та можливий характер подальшої діяльності. Одночасно результат оцінювання має характеризуватися певним рівнем невизначеності, який залежить від повноти, достовірності та актуальності доступної інформації.

Запропонований підхід передбачає формування комплексного висновку про стан групового об’єкта, який включає його поточну оцінку, ступінь невизначеності та тенденцію зміни стану. Він може бути використаний для інформаційно-аналітичної підтримки прийняття рішень у системах військового управління.

Пінчук О. А.
Тимчук С. В., канд. техн. наук
Житомирський військовий інститут імені С. П. Корольова

МАТЕМАТИЧНІ МОДЕЛІ ПОВЕДІНКИ РАДІОМЕРЕЖ ДЛЯ ПРОГНОЗУВАННЯ ДІЙ ПІДРОЗДІЛІВ ПРОТИВНИКА

Надшвидкі темпи розробки та розповсюдження радіоелектронних засобів в збройних силах держав світу й триваючий технічний прогрес у створенні завадозахищених засобів і систем радіозв’язку, що функціонують з використанням алгоритмів застосування сигналів із складними видами дискретної модуляції, кодуванням та шифруванням, зокрема використання симетричних алгоритмів шифрування типу AES-256 (Advanced Encryption Standard 256-bit), приводять до значного ускладнення радіоелектронної обстановки з великим завантаженням робочих діапазонів частот, високою динамікою їхньої зміни в просторі та часі і зниженням можливості виокремлення інформаційної складової матеріалів радіоперехоплень.

Актуальність теми зумовлена необхідністю виявлення прихованої підготовки військ противника до дій в умовах динамічних змін поля бою та зниженням можливості виокремлення інформаційної складової матеріалів радіоперехоплень. У даній ситуації головним джерелом інформації може стати аналіз метаданих: структури мереж, інтенсивності трафіку, координат та часових параметрів.

Основною метою слід виокремити використання комплексу математичних моделей, який дозволить опрацьовувати метадані радіообміну з мінімальним часовим запізненням.

Досягнення мети можливе з використанням наступних підходів:

Приховані Марковські моделі – для розрахунку ймовірностей зміни поточного стану підрозділу, де справжні наміри противника є прихованими станами; метадані радіообміну є спостережуваними сигналами. З використанням алгоритму Вітербі можливо з високою точністю зробити висновки на основі розрахунків щодо ймовірного наступного кроку противника.

Теоретико-графові моделі – для розкриття системи управління противника без необхідності дешифрування змісту повідомлень. Прогнозування дій підрозділів противника здійснюється шляхом моніторингу еволюції графа у часі.

Поєднання даних методів дозволить збільшити точність прогнозування дій противника без виокремлення інформаційної складової матеріалів радіоперехоплень.

Поєднання наведених вище математичних моделей забезпечує створення автоматизованого аналізу поведінки підрозділів противника в режимі реального часу. Практичне впровадження математичних моделей надасть змогу випереджати дії противника за часом та викривати його дезінформаційні радіомережі без необхідності витрати ресурсів на виокремлення інформаційної складової матеріалів радіоперехоплень в умовах динамічних змін поля бою.

Нікітін А. І.
Площик А. С.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ПЕРСПЕКТИВИ СТВОРЕННЯ ПОСТІВ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ З ЕЛЕМЕНТАМИ ШТУЧНОГО ІНТЕЛЕКТУ В ПІДРОЗДІЛАХ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ УКРАЇНИ

Охорона державного кордону в сучасних умовах потребує використання не лише традиційних засобів спостереження, а й технологій, здатних завчасно виявляти ознаки підготовки можливих правопорушень. Одним із перспективних напрямів є застосування засобів радіоелектронної розвідки (РЕР), які можуть забезпечити постійний контроль радіоелектронної обстановки на визначених ділянках відповідальності прикордонних підрозділів.

Особливістю сучасних загроз є те, що підготовка до незаконного переміщення через державний кордон людей або товарів може супроводжуватися використанням безпілотних літальних апаратів, засобів дистанційного зв’язку та іншого радіоелектронного обладнання. При цьому візуальне спостереження не завжди дає змогу своєчасно виявити такі ознаки, особливо вночі, за складних погодних умов або на значній відстані. У зв’язку з цим доцільним є доповнення системи технічного спостереження підрозділів охорони державного кордону постами РЕР.

Перспективним рішенням може стати створення стаціонарних або напівмобільних постів РЕР, розміщених у межах відповідальності прикордонних підрозділів. Їх основним завданням має бути безперервний моніторинг радіоелектронної обстановки та виявлення змін, які можуть свідчити про появу або активізацію безпілотних систем та інших радіоелектронних засобів. Водночас ефективність такого підходу значною мірою залежатиме не лише від технічних характеристик приймального обладнання, а й від можливості оперативно обробляти значні обсяги отриманої інформації.

Саме тому перспективним є використання елементів штучного інтелекту для автоматизованого аналізу радіоелектронної обстановки. На відміну від оператора, який фізично не може безперервно аналізувати всі зафіксовані сигнали, програмний комплекс може працювати цілодобово, накопичувати інформацію про характерну для конкретної ділянки радіоелектронну обстановку та визначати відхилення від її звичайного стану. У результаті оператор отримуватиме не весь масив необроблених даних, а інформацію про виявлені зміни, які потребують додаткової перевірки.

Особливу увагу доцільно приділити виявленню ознак активності безпілотних літальних апаратів. Запропонована система не повинна обмежуватися простим визначенням наявності сигналу. Її завданням має бути встановлення характеру радіоелектронної активності, порівняння її з попередньо накопиченими даними та формування повідомлення про потенційно нетипову ситуацію. Це дозволить перейти від пасивної фіксації радіосигналів до постійного аналізу змін радіоелектронної обстановки.

Практичний результат такого підходу полягає у створенні додаткового рівня раннього попередження для прикордонного підрозділу. Наприклад, у разі виявлення нетипової радіоелектронної активності система може автоматично сформувати повідомлення для відповідального оператора із зазначенням часу та району виявлення активності. Отримана інформація може бути використана як підстава для посилення спостереження відповідної ділянки, перевірки її іншими технічними засобами або спрямування прикордонного наряду для уточнення обстановки.

Важливо, що РЕР у такій системі не повинна розглядатися як самостійний засіб встановлення факту правопорушення. Виявлення радіоелектронної активності може бути лише одним з інформаційних показників, який потребує підтвердження іншими засобами. Саме поєднання даних РЕР, технічного спостереження та інформації від прикордонних нарядів може забезпечити більш обґрунтовану оцінку ситуації.

Перспективним також є об'єднання декількох постів РЕР у розподілену систему. У такому випадку інформація з різних ділянок може надходити до єдиного інформаційного середовища, що дозволить порівнювати радіоелектронну активність у просторі та часі. Це створює передумови для виявлення не лише окремих сигналів, а й певних закономірностей, які можуть мати значення для оцінки обстановки на державному кордоні.

Таким чином, створення постів РЕР з елементами штучного інтелекту може стати перспективним напрямом удосконалення технічної складової охорони державного кордону. Основна перевага запропонованого підходу полягає у переході від епізодичного спостереження до постійного моніторингу радіоелектронної обстановки та автоматизованого виявлення її нетипових змін. У перспективі така система може використовуватися як додатковий інструмент раннього виявлення потенційної активності безпілотних систем і підвищення ситуаційної обізнаності прикордонних підрозділів щодо можливих спроб незаконного переміщення людей або товарів через державний кордон.

Вода Ю. Л.
Науково-дослідний центр ракетних військ і артилерії

АКТУАЛЬНІ ПИТАННЯ РОЗВИТКУ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ЯК ВИДУ АРТИЛЕРІЙСЬКОЇ РОЗВІДКИ В УМОВАХ СУЧАСНИХ ВИСОКОТЕХНОЛОГІЧНИХ КОНФЛІКТІВ

Еволюція засобів та способів ведення збройної боротьби в умовах сучасних високоінтенсивних конфліктів продемонструвала критичну залежність ефективності артилерійських підрозділів від точності, оперативності та своєчасності отримання розвідувальних даних. Традиційні види артилерійської розвідки – оптико-електронна (зокрема із застосуванням безпілотних літальних апаратів (БпЛА)), звукометрична та радіолокаційна – мають низку обмежень, зумовлених метеорологічними умовами, впливом рельєфу, застосуванням противником засобів маскування та систем радіоелектронної боротьби (РЕБ).

У цих умовах особливого значення набуває радіоелектронна розвідка (РЕР), яка функціонує як складова частина загальної системи артилерійської

розвідки. Вона забезпечує виявлення, ідентифікацію та визначення координат радіовипромінювальних засобів противника без прямого оптичного контакту, незалежно від часу доби та погодних умов. Розвиток РЕР як виду артилерійської розвідки потребує перегляду концептуальних підходів до її побудови, оснащення та інтеграції в автоматизовані системи управління вогнем (АСУВ).

Специфіка застосування РЕР в інтересах артилерії полягає у її орієнтації на виявлення вузького, але критично важливого спектра об’єктів противника. До основних об’єктів розвідки належать:

спостережні пункти та пункти управління вогнем артилерії, які виявляються за інтенсивністю та сигнатурою роботи засобів радіозв'язку та цифрових систем передачі даних;

радіолокаційні станції контрбатарейної боротьби, що розпізнаються за характерними параметрами імпульсного випромінювання та робочими частотами;

засоби РЕБ противника, які виявляються за потужним широкосмуговим або загороджувальним випромінюванням;

пункти управління та оператори БпЛА, що виявляються за радіолініями керування та передачі відеосигналу.

Отримання даних про ці об’єкти засобами РЕР дозволяє здійснювати ураження противника ще до того, як його артилерійські засоби відкриють вогонь або завершать розгортання в бойовий порядок.

Аналіз застосування засобів РЕР у сучасних бойових діях дозволяє виділити такі ключові проблемні питання:

ускладнення радіоелектронної обстановки та завадозахищеність цілей;

вимоги до точності визначення координат об’єктів для їх ураження;

вразливість розвідувальних засобів.

Для подолання вказаних викликів розвиток РЕР артилерії має здійснюватися за декількома основними напрямами:

перехід до розподілених мереж пеленгації;

інтеграція штучного інтелекту;

використання повітряних та мобільних носіїв;

зменшення часу між засічкою цілі і її ураженням артилерійськими засобами.

Для удосконалення РЕР артилерії необхідно:

уніфікація протоколів даних між засобами РЕР та артилерійськими АСУВ;

оснащення артилерійських підрозділів штатними малогабаритними засобами РЕР;

комплексування із засобами оптико-електронної та радіолокаційної розвідки.

Висновки

Трансформація радіоелектронної розвідки з допоміжного засобу в один із провідних видів артилерійської розвідки є об'єктивною вимогою сучасної високотехнологічної війни.

Основою перспективного розвитку РЕР артилерії є перехід від громіздких комплексів до розподілених, мобільних, безпілотних мереж, інтегрованих з інтелектуальними системами обробки даних та АСУВ. Впровадження таких підходів дозволить забезпечити високу оперативність розвідки, скоротити час від виявлення цілі до її ураження та забезпечити перевагу в контрбатарейній боротьбі.

Ставісюк Р. Л., канд. техн. наук, ст. досл.
Каменчук А. В.
Житомирський військовий інститут імені С. П. Корольова

ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ ПАРАМЕТРІВ СИГНАЛІВ ТЕХНОЛОГІЇ "НЕСУЧА - В - НЕСУЧІЙ"

Сучасний розвиток супутникових систем супроводжується великою кількістю застосуванням технологій. Однією з таких є технологія "несуча-в-несучій" (Carrier-in-Carrier). ЇЇ сутність полягає у суміщенні двох сигналів в одній і тій самій смузі частот. Практичний досвід фахівців радіоелектронної розвідки показує, що сформований за цією технологією композитний сигнал створює ефект прихованості. Досягається це за умови взаємного перекриття спектрів двох незалежних несучих, забезпечуючи "маскування" сигналу, при якому стандартні методи виявлення сприймають дане явище, як сигнал із завадами.

Чинниками, що визначають актуальність цього дослідження є: необхідність у розділенні композитного сигналу та підвищення швидкості та точності обробки. В умовах динамічної роботи, традиційні методи вимагають значних витрат у часі. Тому, оптимізація алгоритмів вимірювання параметрів із застосуванням циклостаціонарного аналізу та кумулянтних методів дозволяє проводити розпізнавання в режимі, що буде максимально наближений до реального часу.

Практичний досвід застосування засобів супутникового зв’язку під час російсько-української війни показав суттєві зміни у підходах до організації систем упраавління та передачі інформації. Саме, зростання потреби у використанні обмеженого супутникового ресурсу та забезпечення стійкості каналів зв’язку, призвело до активного застосування технологій, які передбачають спільне використання частотного діапазону двома сигналами, зокрема “несуча-в-несучій”.

Задіяння зазаначеного методу в супутникових лініях зв’язку пунктів управління оперативно-стратегічної та тактичної ланок управління противника створює складну радіоелектронну обстановку та формує нові завдання для систем радіоелектронної розвідки Сил Оборони України. Застосування вищевказаної технології дозволяє противнику не лише підвищити пропускну спроможність супутникового ресурсу, який використовується, а й суттєво ускладнити роботу наших підрозділів через ефект маскування сигналів.

Таким чином, аналіз реального досвіду бойових дій підтверджує, що розробка методів виявлення та оцінки параметрів композитних сигналів є необхідним завданням. Розв’язання цієї проблеми безпосередньо впливає на підвищення повноти, достовірності, ефективності та оперативності добування інформації для підрозділів радіоелектронної розвідки.

Бондаренко Д. М.
Стефанишин Я. І.
Липський О. А., канд. техн. наук, доц.
Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ПРОЄКТУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ НА FPGA

Зважаючи на зростання складності спеціальної техніки, систем оброблення сигналів, криптографічних модулів, мережевих акселераторів та інших спеціалізованих пристроїв, "класичні" методи їх проектування із застосуванням FPGA займають багато часу і потребують високої кваліфікації персоналу. Важливим фактором збільшення термінів циклу проєктування

криптографічних модулів на FPGA виступає також необхідність використання застарілих САПР для підтримки життєвого циклу застарілого обладнання.

Крім того, класичні інструменти синтезу та трасування при проєктуванні криптографічних модулів не завжди забезпечують оптимальне використання ресурсів FPGA.

Наведені чинники та багато інших для розроблення спеціальної техніки на FPGA вимагають використання штучного інтелекту (ШІ).

Відкриті моделі ШІ. Вагомим важелем використання відкритих моделей ШІ із онлайн доступом є доступність та прозорість алгоритмів, велика спільнота розробників, а також можливість швидкого оновлення та виправлення.

Разом з тим, поряд із перевагами цих моделей ШІ, присутні і певні проблеми, а саме:

безпека та конфіденційність (відкриті моделі ШІ часто потребують хмарних сервісів, що створює ризики витоку даних);

нестабільність якості (різні реалізації відкритих моделей ШІ можуть давати неоднакові результати);

відсутність гарантій продуктивності (open□source рішення не завжди оптимізовані для високонавантажених систем).

Локальні моделі ШІ. Локальні моделі ШІ (розміщені на локальних ресурсах) дають можливість забезпечити повний контроль над даними та процесами. Можлива також адаптація локальних моделей ШІ для виконання специфічних задач (наприклад, криптографічні модулі чи FPGA□оптимізація). Крім того, локальні моделі ШІ забезпечують вищу безпеку у критичних застосуваннях (військові, телекомунікаційні, фінансові системи).

До недоліків локальних моделей ШІ можна віднести:

високі вимоги до ресурсів;

значне енергоспоживання та висока вартість;

велика складність адміністрування;

складності при масштабуванні.

Використання ШІ для генерації коду апаратних описових мов (HDL). Моделі ШІ здатні швидко генерувати код, але вони не завжди пристосовані до специфіки апаратних описових мов (таких, як VHDL). Це призводить до синтаксично правильного, але семантично некоректного коду. Елементарні помилки в алгоритмах, навіть достатньо простих (наприклад, лічильники, регістри зсуву, FSM).

Відсутність оптимізації під FPGA. Код, згенерований ШІ, часто не враховує обмеження ресурсів FPGA (кількість LUT, FF, BRAM), що робить його неефективним для синтезу.

Ризик прихованих помилок. Код, згенерований ШІ, може компілюватися, але працювати неправильно.

Для перевірки (валідації) коду, згенерованого ШІ, необхідно застосовування процесу HDL lint. Це дає змогу перевірити чи всі сигнали оголошені, чи правильно використано типи, чи є синхронізація з clk.

Виявленні помилки виправляються вручну або через повторну генерацію ШІ.

Лише після lint□валідації коду можна переходити до симуляції (ModelSim, QuestaSim).

Висновок. Можливості штучного інтелекту значно перебільшені, зважаючи на його схильність до елементарних помилок у простих алгоритмах, але, він значно прискорює процес написання VHDL□коду. Тому критично важливо застосовувати валідацію та симуляцію отриманого коду.

Kononova O. A.
Ivan Kozhedub Kharkiv National Air Force University

APPLICATION OF RADIO FREQUENCY IDENTIFICATION SYSTEMS FOR TARGET IDENTIFICATION BY RADIO-TECHNICAL UNITS OF AIR DEFENCE OF THE AIR FORCE OF THE ARMED FORCES OF UKRAINE DURING ELECTRONIC RECONNAISSANCE

The quality of target identification by Radio-Technical Units of the Air Defence of the Air Force of the Armed Forces of Ukraine (RTU AD AF AFU) during electronic reconnaissance directly affects their combat readiness. Significant importance is attached to the use of Radio Frequency Identification (RFID) systems, which consist of an identifier - a device containing an object code - together with a transceiver antenna referred to as a transponder (TP), and a transceiver base station (BS) that interrogates the TP and decodes the return signal. Transponders are classified as active, which require a power source, and passive, which operate using energy received from the BS. Supplying power from an external source (for stationary objects) requires connecting each monitored object to an electrical supply, which is not always feasible due to operational and storage requirements. Passive transponders

are implemented based on solid-state retranslators using surface acoustic wave (SAW) technology, providing high resistance to ionizing radiation, elevated temperatures, and mechanical shock. RFID systems with SAW-based passive transponders offer superior reliability and ease of operation due to the absence of an internal power source. The development of identification and target monitoring systems based on supplementary sensor structures substantially impacts electronic reconnaissance as a whole, which determines the relevance of this applied research task.

The objective of this report is to assess the compatibility of identification and monitoring systems when an additional sensor structure is incorporated into the delay line containing the identification code. The report establishes that, to register discrete values of active non-standard factors, it is sufficient to supplement the standard reflectors in the delay line with the required number of additional reflectors connected to external sensors that open or close their contacts. The detection of discrete threshold values of active factors is determined by the presence or absence of the corresponding reflected pulses in the information signal, which is exploited in the transponder of the remote identification and monitoring system during electronic reconnaissance.

Іванов В. К., канд. техн. наук
ТОВ «Науково-виробничий центр «Інфозахист»»

БОЙОВА ЕФЕКТИВНІСТЬ ТА АРХІТЕКТУРНА ЖИВУЧІСТЬ АЕРОСТАТНОГО КОМПЛЕКСУ РАДІОТЕХНІЧНОЇ РОЗВІДКИ

Сучасний розвиток засобів радіотехнічної розвідки (РТР), безпілотних систем та інших засобів отримання розвідувальної інформації зумовлює необхідність перегляду традиційних підходів до оцінювання ефективності розподілених радіотехнічних систем. Тривалий час одним із основних критеріїв оцінювання комплексу РТР була точність визначення координат джерел радіовипромінювання (ДРВ). Такий підхід був природним за умов, коли радіолокаційні засоби тривалий час працювали в одному режимі, забезпечували накопичення значної кількості вимірювань, а основним завданням РТР було виявлення джерела випромінювання та визначення його координат.

Зміна характеру функціонування сучасних радіоелектронних систем, розвиток безпілотних і космічних засобів розвідки, скорочення часу роботи

окремих радіолокаційних засобів та підвищення їх адаптивності змінюють вимоги до систем РТР. За таких умов координата дедалі частіше перестає бути кінцевим продуктом розвідки та стає лише одним із елементів загального процесу отримання, уточнення й використання розвідувальної інформації. Тому поряд із точністю координатометрії необхідно враховувати своєчасність виявлення, достовірність отриманого результату, кількість валідних вимірювань та здатність комплексу функціонувати за умов деградації окремих компонентів.

Метою дослідження є формування системного підходу до оцінювання бойової ефективності та архітектурної живучості аеростатного комплексу РТР з урахуванням імовірності отримання результату, якості координатометрії, доступності вимірювальних каналів та стійкості архітектури до деградації окремих компонентів.

У сучасному розвідувальному контурі комплекс РТР може виконувати первинне виявлення та класифікацію радіовипромінювання, підтверджувати активність джерела та формувати інформацію для подальшої розвідки. Уточнення координат і підтвердження цілі можуть здійснюватися іншими сенсорними засобами. Таким чином, практична цінність комплексу визначається не тільки похибкою окремого координатного вимірювання, а насамперед здатністю своєчасно сформувати достатньо достовірний результат для подальшого використання.

Додатковий вплив на ефективність систем РТР має характер роботи сучасних радіолокаційних станцій, зокрема систем з активними фазованими антенними решітками. Вузькі діаграми спрямованості, швидка перебудова секторів роботи, адаптивний розподіл енергетики та одночасне виконання пошуку й супроводу можуть призводити до ситуацій, коли різні сенсори розподіленої системи отримують різний обсяг інформації про одне й те саме джерело. У таких умовах проблема полягає не лише в точності окремого вимірювання, а й у здатності комплексу отримати достатню кількість валідних вимірювань для формування достовірного рішення.

Для кількісного оцінювання запропоновано розглядати бойову ефективність як інтегральну характеристику здатності комплексу забезпечувати локалізацію ДРВ у заданих умовах застосування. Її доцільно характеризувати показниками імовірності отримання результату PLOP, якості отриманого координатного результату PCOORD та інтегральної ймовірності успішної

локалізації PLOC. Просторовий розподіл цих показників може бути представлений у вигляді карт бойової ефективності. Такий підхід дає змогу оцінювати не окрему характеристику вимірювального каналу, а реальну здатність системи забезпечувати необхідний результат у конкретних просторових і сигнальних умовах.

Для аеростатного комплексу РТР розміщення сенсорів на значній висоті створює передумови для розширення радіогоризонту та області спостереження. Водночас збільшення просторової області роботи підвищує вимоги до антенно-приймальної системи, системи часу та синхронізації, транспортної мережі, позиціонування й орієнтування, а також до обчислювальної інфраструктури.

Другим системним критерієм розвитку комплексу пропонується визначити архітектурну живучість. Під архітектурною живучістю розуміється здатність комплексу зберігати необхідний рівень функціональності та забезпечувати отримання корисного інформаційного результату за умов деградації окремих компонентів або погіршення умов функціонування. Така деградація може бути пов'язана з втратою частини сенсорів, погіршенням характеристик каналів зв'язку, порушенням синхронізації, впливом завад або частковою недоступністю вимірювальних каналів.

Архітектурна живучість повинна закладатися на рівні побудови всієї вимірювальної платформи. До її основних складових належать антенноприймальний тракт, високочастотна система, засоби цифрової обробки, FPGA, система часу та синхронізації, транспортна мережа, система позиціонування й орієнтування та обчислювальна інфраструктура. Взаємозв'язок цих компонентів визначає не лише поточні характеристики комплексу, а й можливості його подальшої модернізації.

Особливе значення для розподілених систем координатометрії має часова складова. Для методу TDOA стабільність опорної частоти, точність синхронізації, режими holdover та характеристики транспортної мережі безпосередньо впливають на якість координатного результату. Тому незалежні джерела синхронізації та можливість збереження часової прив'язки за умов часткової деградації системи доцільно розглядати як складові архітектурної живучості.

Не менш важливою є транспортна мережа. У розподіленому комплексі РТР вона є не лише засобом передачі інформації, а функціональною частиною вимірювальної системи, оскільки забезпечує передачу вимірювань, часову

узгодженість даних та взаємодію між сенсорами. Тому стійкість транспортної мережі безпосередньо впливає як на бойову ефективність, так і на архітектурну живучість комплексу.

Підвищення живучості може забезпечуватися диверсифікацією фізичних принципів отримання інформації. Поєднання спектрального аналізу, фазових вимірювань, інтерферометричних методів, TDOA та IQ TDOA дає можливість використовувати різні інформаційні канали залежно від умов функціонування системи. У такій архітектурі різні методи вимірювання можуть розглядатися не як конкурентні, а як взаємодоповнюючі інструменти забезпечення необхідного результату.

IQ TDOA доцільно розглядати як високоточний спеціалізований канал аналізу пріоритетних джерел, уточнення координат та отримання додаткових параметрів випромінювання. Водночас його доцільно доповнювати каналами первинного виявлення та супроводу, які мають менші вимоги до обчислювальних ресурсів і пропускної здатності каналів передачі даних. Така спеціалізація режимів дозволяє ефективніше розподіляти обчислювальні та інформаційні ресурси комплексу.

Перспективним напрямом подальшої еволюції комплексу є перехід від орієнтації переважно на координатометрію до ширшого використання спектральної та IQ-інформації. Сучасні цифрові дані містять значно більший обсяг інформації, ніж необхідно лише для визначення координат. Їх використання створює можливості для розвитку методів класифікації, асоціації та ідентифікації джерел, аналізу параметрів сигналів і формування додаткових критеріїв прийняття рішень.

Таким чином, розвиток аеростатного комплексу РТР доцільно здійснювати на основі двох взаємопов'язаних системних критеріїв — бойової ефективності та архітектурної живучості. Бойова ефективність характеризує здатність комплексу своєчасно забезпечувати необхідний інформаційний результат у заданих умовах застосування, тоді як архітектурна живучість визначає здатність зберігати цей результат за умов деградації окремих компонентів системи.

Наукова новизна запропонованого підходу полягає у переході від оцінювання ефективності комплексу РТР переважно за точністю координатометрії до інтегрального врахування імовірності отримання результату, його якості та стійкості системи до деградації. Запропонований

підхід створює основу для кількісного порівняння різних архітектур комплексів РТР, визначення критичних компонентів та обґрунтування напрямів їх подальшої еволюції.

Сапронова С. М., курсантка
Запорожченко Ю. І.
Житомирський військовий інститут імені С. П. Корольова

СПЕКТРАЛЬНІ МЕТОДИ ОЦІНЮВАННЯ КУТОВИХ ПАРАМЕТРІВ ДЖЕРЕЛ ВИПРОМІНЮВАННЯ В АДАПТИВНИХ АНТЕННИХ СИСТЕМАХ

Вступ та актуальність теми. Сучасний стан розвитку засобів ведення збройної боротьби характеризується високим ступенем динамічності, мобільністю сил та засобів, а також стрімкою зміною тактичних прийомів застосування сил противника. Зазначені фактори супроводжуються тотальним переходом підрозділів на цифрові засобі зв’язку із високою криптографічною стійкістю. Це призводить до експоненційного зростання щільності та обсягів інформаційних потоків у радіоефірі.

Додатковим ускладнювальним фактором є критичне перенасичення електромагнітного простору як навмисними, так і ненавмисними завадами різного походження (потужні ретрансляційні вузли, комплекси радіоелектронної боротьби, канали управління та телеметрії безпілотних авіаційних комплексів). За таких умов класичні технічні рішення та методи радіоелектронної розвідки (РЕР) і радіоперехоплення втрачають свою потенційну ефективність, оскільки не здатні забезпечити надійне розділення корисних сигналів на тлі інтенсивного завадового фону. Постає гостра науково-технічна задача впровадження високотехнологічних засобів просторової селекції на основі адаптивних антенних решіток (ААР).

Мета роботи. Аналіз ефективності застосування та математичного апарату багатоелементних адаптивних антенних систем із алгоритмами просторового надрозрізнення джерел випромінювання з метою підвищення чутливості та вибірковості постів радіоперехоплення в умовах складної завадової обстановки.

Спектральні методи оцінки кутових параметрів поділяються на дві основні групи: променеутворюючі та підпросторові.

Променеутворюючі методи:

Метод Бартлетта. Найпростіший метод формування пеленгаційного рельєфу. Просторовий спектр визначається виразом:

$$P(\theta) = \frac{A^{\mathrm{H}}(\theta) R A(\theta)}{A^{\mathrm{H}}(\theta) A(\theta)}$$

Де $A(\theta)$ – вектор напрямку (початковій вектор); R – кореляційна матриця

Метод оцінює просторову потужність у всіх напрямках. Напрямки джерел знаходять за положенням максимумів спектра. Метод простий у реалізації та стійкий, однак його роздільна здатність повністю визначається шириною головного променя антенної решітки.

Метод Кейпона (мінімального відхилення). Метод мінімізує потужність на виході при збереженні одиничного підсилення в заданому напрямку. Просторовий спектр має вигляд:

$$P_{CAP(\theta)} = \frac{1}{A^{\mathrm{H}}(\theta) R^{-1} A(\theta)}$$

Завдяки використанню оберненої кореляційної матриці метод забезпечує помітно вищу роздільну здатність порівняно з методом Бартлетта і менше залежить від кількості елементів решітки.

Метод теплового шуму. Розвиток підходу Кейпона. Замість першого степеня оберненої кореляційної матриці використовується її квадрат:

$$P_{TN}(\theta) = \frac{1}{A^{\mathrm{H}}(\theta) R^{-2} A(\theta)}$$

В ідеальних умовах метод забезпечує вищу роздільну здатність, ніж алгоритм Кейпона. Водночас він більш чутливий до помилок оцінки кореляційної матриці та до неідеальностей антенної системи.

Метод Борджотті-Лагунаса. Комбінований метод. Пеленгаційний рельєф формується як відношення спектра методу теплового шуму до спектра методу Кейпона:

$$P_{BL}(\theta) = \frac{P_{TN}(\theta)}{P_{CAP}(\theta)}$$

Де $P_{TN}(\theta)$ – розрахунок пеленгаційного рельєфу за методом теплового шуму, $P_{CAP}(\theta)$ - розрахунок пеленгаційного рельєфу за методом Кейпона.

Такий підхід дозволяє поєднати високу роздільну здатність методу теплового шуму з дещо кращою стійкістю.

Підпросторові методи:

Алгоритм MUSIC. Один із найефективніших методів надрозділення. Використовує властивість ортогональності векторів напрямку сигналів до шумового підпростору. Просторовий спектр визначається як:

$$P_M(\theta) = \frac{A^{\text{н}}(\theta) A(\theta)}{A^{\text{н}}(\theta)\, \Pi^{\perp} A(\theta)}$$

Де $\Pi^{\perp}$ — проектор на шумовий підпростір.

Метод формує надзвичайно гострі максимуми і забезпечує високу роздільну здатність навіть при близькому розташуванні джерел.

Метод аналізу власних векторів (EV). Близький до алгоритму MUSIC. Спектр має вигляд:

$$P_{EV}(\theta) = \frac{A^{\text{н}}(\theta)}{\Pi^{\perp} A(\theta)}$$

Метод також базується на розділенні простору на сигнальний і шумовий підпростори та дає результати, порівнянні з MUSIC.

Алгоритм ESPRIT. Використовує властивість обертальної інваріантності двох однакових підрешіток. На відміну від MUSIC, не потребує побудови просторового спектра. Кутові координати визначаються через власні значення матриці переходу між сигнальними підпросторами підрешіток. Метод є обчислювально ефективнішим.

Таблиця 1. Порівняльний аналіз методів просторової обробки в ААР

Метод обробки інформації	**Математична складність реалізації**	**Розрізнювальна здатність за кутом**	**Залежність втрат від потужності завади**
Метод Бартлетта (формування променя)	Низька (не потребує обернення матриць)	Низька (обмежена критерієм Релея)	Критична (втрати зростають пропорційно потужності)
Метод Кейпона	Середня (потребує обчислення R^{-1})	Висока (суперрозрізнення)	Помірна
Метод теплового шуму	Середня–висока (потребує R^{-2})	Висока (в ідеальних умовах)	Помірна–висока (чутливий до помилок)
Метод Борджотті-Лагунаса	Середня–висока (комбінація двох спектрів)	Висока	Помірна

Метод обробки інформації	**Математична складність реалізації**	**Розрізнювальна здатність за кутом**	**Залежність втрат від потужності завади**
Алгоритм MUSIC	Висока (спектральний аналіз матриці власних чисел)	Екстремально висока (надрозрізнення)	Мінімальна (граничні втрати до 3 дБ)
Метод аналізу власних векторів (EV)	Висока (аналіз власних векторів)	Екстремально висока (надрозрізнення)	Мінімальна (близька до MUSIC)
Алгоритм ESPRIT	Середня (без побудови спектра)	Висока	Низька–помірна

Переваги та обмеження практичної реалізації. Жоден метод не є універсально найкращим. Променеутворюючі методи виграють у простоті та стійкості. Підпросторові методи забезпечують принципово вищу роздільну здатність і точність. Практична цінність спектральних методів полягає в можливості автоматичного визначення кутових координат джерел без попередньої інформації про них. Найбільш раціональним є комбіноване застосування: променеутворюючих методів — на етапі попередньої оцінки, підпросторових — на етапі точного пеленгування.

Проте впровадження таких комплексів у підрозділах радіоелектронної розвідки Збройних Сил України стримується технологічними обмеженнями. Сюди відносяться висока обчислювальна складність алгоритмів (необхідність застосування високопродуктивних сигнальних процесорів FPGA/DSP), жорсткі вимоги до ідентичності та взаємного фазового калібрування приймальних каналів, а також підвищена вартість апаратної частини.

Висновки. Впровадження адаптивних антенних решіток із алгоритмами просторового надрозрізнення (зокрема MUSIC) є перспективним напрямом розвитку технічних засобів радіоперехоплення. Використання спектрального аналізу сигнального та шумового підпросторів дозволяє кардинально підвищити завадозахищеність та інформаційну ємність постів розвідки в умовах складного і насиченого сучасного електромагнітного середовища.

Ставісюк Р. Л., канд. техн. наук, ст. досл.
Сікан Ю. В.
Житомирський військовий інститут імені С. П. Корольова

ПЕРСПЕКТИВИ РОЗРОБЛЕННЯ СПОСОБІВ ДИНАМІЧНОГО ПЛАНУВАННЯ ЗАВДАНЬ СИЛАМ І ЗАСОБАМ РАДІОЕЛЕКТРОННОГО МОНІТОРИНГУ НА ОСНОВІ МУЛЬТИАГЕНТНОГО НАВЧАННЯ З ПІДКРІПЛЕННЯМ

Сучасні умови ведення бойових дій характеризуються швидкою зміною радіоелектронної обстановки та одночасним функціонуванням значної кількості джерел розвідувальних відомостей (ДРВ). Для підрозділів РЕР це вимагає своєчасного виявлення нових ДРВ, оцінювання їх важливості та, за необхідності, зміни пріоритетів роботи постів добування. На даний час для збору, обробки, обміну та відображення розвідувальної інформації підрозділи РЕР застосовують програмні засоби «ЕХО», DELTA та «Стрибо». Їх використання сприяє підвищенню швидкості обміну інформацією, спрощує її обробку та відображення, а також забезпечує командний склад даними, необхідними для оцінювання радіоелектронної обстановки. Разом з тим, функціональні можливості зазначених програмних засобів не охоплюють у повній мірі питання динамічного планування роботи сил і засобів РЕР. У разі появи нового ДРВ офіцеру командного пункту або посту обробки необхідно оцінити отриману інформацію, визначити її важливість для поточного плану РЕР та прийняти рішення щодо коригування завдань постам добування. За умов швидкої зміни радіоелектронної обстановки це може потребувати додаткового часу та збільшувати навантаження на офіцера. Тому виникає необхідність у пошуку способів, які дозволять частково автоматизувати цей процес. Система повинна не замінювати людину, а своєчасно звертати її увагу на зміни обстановки та допомагати визначити можливий варіант коригування поточного плану РЕР та відповідно завдань постам добування.

Одним із перспективних напрямів є застосування мультиагентного навчання з підкріпленням. Доцільність такого підходу пов’язана з тим, що підрозділ РЕР складається з декількох постів, які мають різні можливості та виконують різні завдання. Розгляд їх як окремих взаємодіючих елементів дає можливість оцінювати не лише роботу кожного поста окремо, а й їх спільне

використання для виконання поточних завдань. Наприклад, у разі появи нового ДРВ інтелектуальний модуль може визначити, що отримана інформація потребує перегляду поточних завдань. Після цього система аналізує наявні можливості постів і формує для офіцера пропозицію щодо перерозподілу завдань. При цьому остаточне рішення залишається за офіцером, що забезпечує принцип взаємодії людини та штучного інтелекту. У запропонованому підході програмні засоби «EXO», DELTA та «Стрибо» можуть використовуватися як складові наявного інформаційного середовища, з якого надходять необхідні дані про обстановку. Запропонований інтелектуальний модуль у такому випадку не замінює існуючі програмні рішення, а доповнює їх функцією підтримки динамічного планування та перерозподілу завдань.

Застосування такого підходу може дозволити скоротити час від виявлення нового ДРВ до формування пропозиції щодо зміни завдань, зменшити навантаження на офіцерів командного пункту (посту оброби) та швидше враховувати можливості окремих постів. У подальшому це може підвищити узгодженість роботи різних сил і засобів РЕР та забезпечити більш гнучке використання наявних ресурсів. Перспективність розроблення способів динамічного планування завдань силам і засобам радіоелектронного моніторингу полягає у можливості доповнення вже наявного інформаційного середовища «EXO», DELTA та «Стрибо» інтелектуальним модулем на основі мультиагентного навчання з підкріпленням. Такий підхід спрямований на своєчасне коригування плану РЕР та підтримку офіцера під час перерозподілу завдань відповідно до змін радіоелектронної обстановки.

Луніна К. В., курсант
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

СУЧАСНІ МЕТОДИ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ

Розвиток сучасних систем зв’язку, радіолокації, РЕБ та БПЛА має більші очікування до засобів радіомоніторингу. Потрібно швидко і точно розпізнавати джерела і їх точне місцезнаходженння. Це важливо і в цивільній, і в оборонній

діяльності. Сьогодні радіоелектронний простір характеризується високою щільністю сигналів, застосуванням складних видів модуляції, сигналів із псевдовипадковим перебудуванням робочої частоти та малою ймовірністю перехоплення, що сильно ускладнює використання звичайних методик радіопеленгації.

Сучасні способи знаходження джерел радіовипромінювання за радіосигналом діляться на декілька видів:

1. Амплітудні методи. Ці методи використовують потужності прийнятого сигналу і користуються логарифмічними моделями згасання радіохвиль. Не дивлячись на обчислювальну простоту та легку реалізацію, дані методи здатні забезпечити точність у складних умовах міст та рельєфу через ефект багатопроменевого поширення і затінення.

2. Кутомірні методи. Вони визначають напрямок (азимут і кут) до цілі за допомогою фазових або амплітудних антенних решіток. Щоб підвищити роздільність застосовують надроздільні алгоритми. Вони допомагають розрізняти джерела, що стоять дуже близько один до одного.

3. Часові методи. Дані методи часто використовують у сучасних розподілених мережах радіоспостереження. Його принцип роботи заключається в тому, що здійснюється вимірювання різниці часу, коли сигнал приходить до кількох приймальних пунктів розташованих у просторі і порівнює ці часи за допомогою кореляції. Якщо синхронізувати приймачі дуже точно, наприклад через GPS/GNSS або атомні стандартні частоти, можем точно визначити визначення координат навіть для коротких імпульсних і широкосмугових сигналів.

4. Частотно-часові методи. Вони користуються ефектом Доплера коли рухаються приймачі або джерела сигналу. Поєднання часових та частотних методів дає точну локалізацію рухомих джерел радіовипромінювання, навіть якщо є тільки дві приймальних позиції.

Останнім часом все більше переходять від простих пеленгаторних станцій до розподілених систем із багатьма приймачами які працюють на основі програмно-визначуваного радіо. Гібридні методи допомагають подолати недоліки окремих підходів та підвищити стійкість оцінок в умовах складного електромагнітного оточення.

Крім того машинне навчання та штучний інтелект все активніше використовується у обробці радіосигналів. Глибокі нейронні мережі автоматично шукають сигнали в широкій смузі частот, розрізняють типи

модуляції та фільтрації шуму. Використання штучного інтелекту дозволяє швидко підлаштовувати ваги алгоритмів локалізації за цифровими моделями місцевості і враховувати багатопроменевості.

Отже, сучасні способи пошуку та визначення місцезнаходження джерел радіовипромінювання стають все більш розвмненими. Тепер системи збирають часові та кутові дані і обробляють їх розумними програмами. Це дає точніші результати, оперативність та кращу стійкість радіомоніторингу у складних умовах сучасного радіоелектронного середовища.

Колос Ю. О., канд. техн. наук, доц.
Маслов О. А.
Житомирський військовий інститут імені С. П. Корольова

ОБҐРУНТУВАННЯ НАПРЯМІВ РОЗВИТКУ ЕКСПЕРИМЕНТАЛЬНОЇ БАЗИ ДЛЯ ПРОВЕДЕННЯ НАВЧАННЯ ТА НАУКОВИХ ДОСЛІДЖЕНЬ АНТЕННО-ФІДЕРНИХ ПРИСТРОЇВ В УМОВАХ російсько-УКРАЇНСЬКОЇ ВІЙНИ

Досвід російсько-української війни засвідчує, що швидкий розвиток та застосування радіоелектронних систем забезпечує перевагу в бойових діях. Ефективність функціонування зазначених засобів значною мірою залежить від параметрів і характеристик антен та антено-фідерних пристроїв, які визначають дальність дії роботизованих (безпілотних) засобів, ефективність їх застосування в умовах РЕБ. Це свідчить про зростання актуальності, з одного боку, наукових розробок антено-фідерних пристроїв, в тому числі, досліджень фактичних характеристик антенних пристроїв, які можуть відрізнятися від розрахункових або заявлених виробником унаслідок особливостей конструктивного виконання, монтажу, умов установлення та впливу навколишнього середовища. З другого боку, необхідно покращити підготовку військових фахівців з питань ефективної експлуатації, обслуговування та ремонту антено-фідерних пристроїв. Для цього необхідно розвивати відповідну науково-експериментальну та навчально-лабораторну базу, що забезпечуватиме можливість проведення інструментальних вимірювань, порівняльного оцінювання технічних рішень, перевірки результатів теоретичних досліджень та забезпечення освітнього процесу.

В умовах воєнного стану важливо забезпечити безперервність освітнього процесу та наукових досліджень за необхідності розосередження матеріально-технічної бази й особового складу. Традиційна організація лабораторних досліджень, що передбачає зосередження вимірювального обладнання в одному спеціалізованому приміщенні, не завжди забезпечує необхідну доступність та оновлення експериментальної бази.

Метою роботи є обґрунтування напрямів розвитку лабораторно-експериментальної бази дослідження антено-фідерних, НВЧ пристроїв, закономірностей поширення радіохвиль на основі поєднання стаціонарної та мобільної складових, визначення їхніх функціональних можливостей, необхідного вимірювального обладнання і методичного забезпечення.

З огляду на потреби військ необхідно враховувати такі фактори: використовуються десятки типів антено-фідерних пристроїв різних діапазонів частот, які застосовуються на різних засобах і в різних умовах, швидко впроваджуються або удосконалюються нові типи, особовому складу необхідні навички ремонту, налаштування. Сучасні тенденції розвитку теорії і техніки антено-фідерних пристроїв полягають в широкому застосуванні моделювання, автоматизованого проектування, штучного інтелекту. Тому при створенні навчально-лабораторної та науково-дослідної бази необхідно реалізувати комплексний підхід, що полягає в поєднані засобів моделювання, засобів для прищеплення навичок виготовлення або удосконалення елементів антено-фідерних пристроїв, засобів для експериментального дослідження їх параметрів та характеристик. В умовах розосередження особового складу, оптимізації за критерієм максимум ефективності при заданих затратах пропонується створювати як стаціонарну, так і мобільну, як навчальну, так і науково-дослідницьку складові із забезпеченням методичної узгодженості застосування.

Стаціонарна складова повинна забезпечувати проведення комплексних експериментальних досліджень у контрольованих умовах із використанням спеціалізованих вимірювальних установок, а також проведення лабораторних і практичних занять. Її функціональні можливості доцільно спрямувати на дослідження частотних характеристик і узгодження антен, визначення параметрів антено-фідерних трактів, дослідження діаграм спрямованості та поляризаційних характеристик, а також експериментальну перевірку результатів комп'ютерного моделювання.

Основу вимірювального обладнання такої лабораторії можуть становити векторні аналізатори кіл, аналізатори спектра, генератори високочастотних сигналів, вимірювачі потужності, калібровані антени, вимірювальні кабелі, перехідники, атенюатори та узгоджені навантаження. Для дослідження просторових характеристик необхідно передбачити відповідну вимірювальну зону, опорно-поворотні пристрої та засоби реєстрації рівня прийнятого сигналу. Залежно від вимог до точності вимірювань може виникати потреба у використанні радіопоглинальних матеріалів і засобів зменшення впливу відбитих електромагнітних хвиль.

Вибір обладнання повинен визначатися не лише його технічними характеристиками, але й можливістю використання в межах єдиних методик дослідження. Зокрема, застосування векторних аналізаторів кіл дозволяє досліджувати параметри узгодження антен і фідерних трактів, тоді як визначення просторових характеристик потребує окремої вимірювальної установки з відповідними умовами розташування та позиціювання антен.

Мобільну складову пропонується створювати у вигляді переносних вимірювальних комплектів модульної побудови, призначених для виконання окремих досліджень поза межами стаціонарної лабораторії та забезпечення освітнього процесу в умовах розосередження курсантських підрозділів. До їхнього складу доцільно включати портативні аналізатори антен або векторні аналізатори кіл, комплект калібрування, вимірювальні кабелі, перехідники, узгоджені навантаження, засоби документування результатів та автономного електроживлення. За необхідності функціональні можливості мобільного комплекту можуть розширюватися портативними аналізаторами спектра, вимірювачами потужності та допоміжними пристроями.

Основними завданнями мобільної складової доцільно визначити перевірку параметрів узгодження антен, оцінювання характеристик фідерних ліній і з'єднань, дослідження впливу монтажу й умов установлення на доступні для вимірювання параметри, а також проведення окремих лабораторних і практичних занять у польових умовах.

Використання мобільних вимірювальних комплектів набуває особливого значення в умовах розосередження матеріально-технічної бази та особового складу. Модульний принцип побудови дозволяє розподіляти обладнання відповідно до дослідницьких і навчальних завдань, зменшувати залежність

проведення окремих вимірювань від доступності стаціонарних приміщень та забезпечувати гнучкішу організацію експериментальної діяльності.

Водночас мобільна складова не може повністю замінити стаціонарну лабораторію. Проведення вимірювань у польових умовах супроводжується впливом зовнішніх електромагнітних випромінювань, відбиттів від навколишніх об'єктів, погодних чинників та обмежень щодо організації вимірювальної зони. Тому перелік доступних досліджень необхідно визначати з урахуванням технічних можливостей обладнання та вимог до достовірності отриманих результатів.

Важливою умовою функціонування обох складових лабораторно-експериментальної бази є застосування узгодженого методичного забезпечення. Для кожного виду досліджень необхідно визначити послідовність виконання вимірювань, порядок калібрування обладнання, умови проведення експерименту, способи оброблення результатів та основні джерела невизначеності.

Окремої уваги потребує забезпечення порівнюваності результатів, отриманих у лабораторних і польових умовах. Для цього доцільно використовувати однакові або співставні вимірювальні параметри, контрольні зразки, уніфіковані протоколи досліджень і процедури перевірки стабільності вимірювальних трактів. При цьому відмінності умов проведення вимірювань повинні враховуватися під час аналізу отриманих даних.

Розвиток лабораторно-експериментальної бази пропонується здійснювати поетапно. На початковому етапі необхідно проаналізувати наявне вимірювальне обладнання, його технічний стан, метрологічне забезпечення та можливості використання для виконання визначених дослідницьких завдань. Наступним етапом має стати формування стаціонарних вимірювальних установок і переносних комплектів із використанням наявних засобів та їх доукомплектуванням. Подальший розвиток доцільно спрямувати на розширення можливостей вимірювальної зони, автоматизацію процесів вимірювання й оброблення даних та вдосконалення методик експериментальних досліджень.

Важливим напрямом використання зазначеної бази є забезпечення освітнього процесу та наукової роботи курсантів. Поєднання стаціонарних і мобільних вимірювальних комплектів створює додаткові можливості для

виконання лабораторних робіт, проведення практичних занять, дослідження зразків антен та антено-фідерних пристроїв, виконання кваліфікаційних робіт і формування навичок застосування сучасного вимірювального обладнання.

Використання узагальненого досвіду російсько-української війни під час визначення тематики досліджень дозволить орієнтувати наукову та освітню діяльність на актуальні питання функціонування радіоелектронних засобів. При цьому дослідницькі завдання повинні формуватися з урахуванням доступності технічної інформації, вимог безпеки та можливості проведення експериментів без розкриття відомостей з обмеженим доступом.

Очікуваними результатами реалізації запропонованого підходу є розширення можливостей проведення прикладних досліджень антен та антено-фідерних пристроїв, підвищення доступності вимірювального обладнання в умовах розосередження, удосконалення методичного забезпечення експериментальних робіт і створення додаткових умов для практичної підготовки військових фахівців.

Таким чином, розвиток лабораторно-експериментальної бази дослідження антен та антено-фідерних пристроїв доцільно здійснювати на основі поєднання стаціонарної та мобільної складових, функціональні можливості яких визначаються характером дослідницьких завдань і вимогами до умов проведення вимірювань. Такий підхід створює передумови для раціонального використання наявних матеріально-технічних ресурсів, забезпечення безперервності наукової та освітньої діяльності в умовах воєнного стану й розвитку прикладних досліджень в інтересах Сил оборони України.

Рибалка А. О., канд. техн. наук
Товариство з обмеженою відпвідалністю
"Науково-виробничий центр "Інфозахист""

КОНСТРУКТИВНІ ТА ТЕПЛОВІ ОСОБЛИВОСТІ ПОЛЬОВОЇ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ: АНАЛІЗ ЗРАЗКІВ ADEX 2026

Вступ

Польова радіоелектронна апаратура, зокрема радіолокаційні станції (РЛС), засоби радіоелектронної боротьби (РЕБ) і протидії безпілотним літальним апаратам (БпЛА), оптико-електронні сенсори та засоби зв’язку,

експлуатується в умовах безпосереднього впливу навколишнього середовища. Зростання енергоспоживання таких систем підвищує вимоги до ефективності тепловідведення, захисту від пилу й вологи, стійкості до сонячного нагрівання та механічних навантажень.

Водночас конструктивні рішення, характерні для бортової та вбудованої апаратури, не завжди безпосередньо відповідають умовам експлуатації польових виробів. Тому актуальним є порівняння поширених інженерних підходів із конструктивними рішеннями, представленими сучасними виробниками.

Метою роботи є систематизація конструктивних і теплових особливостей польової радіоелектронної апаратури за результатами огляду зразків, представлених на Азербайджанській міжнародній оборонній виставці ADEX 2026, а також визначення потенційних експлуатаційних ризиків і напрямів удосконалення підходів до проєктування.

Матеріали та методи

Дослідження ґрунтується на аналізі приблизно 25 зразків апаратури, представлених на виставці ADEX 2026 у Баку 30 вересня – 2 жовтня 2026 року, та доступної відкритої документації виробників. Зразки систематизовано за функціональним призначенням, характерними ознаками конструкції корпусу, способом охолодження, наявністю зовнішніх конструктивних елементів і доступними даними про умови експлуатації.

Для порівняння використано загальноприйняті підходи до тепловідведення електронних модулів, зокрема рішення сімейства VITA 48, а також положення MIL-STD-810H щодо адаптації випробувань до умов життєвого циклу виробу. Окрему увагу приділено впливу температури, сонячного випромінювання, пилу, вібрації та ударних навантажень.

Оскільки внутрішню будову більшості виробів неможливо достовірно встановити лише за зовнішнім оглядом, результати розглядаються як порівняльні спостереження. Відомості виробників відокремлено від припущень, зроблених за зовнішніми ознаками.

Результати аналізу

За функціональним призначенням досліджувані зразки умовно розподілено на п’ять класів (табл.1): РЛС із нерухомими полотнами, оптико-електронні сенсори, засоби РЕБ і протидії БпЛА, засоби зв’язку та бортову апаратуру. Кожен із цих класів характеризується специфічними конструктивними рішеннями щодо відведення тепла, захисту корпусу від зовнішніх впливів і організації розміщення обладнання в польових умовах.

Таблиця 1 – Типізація зразків польової радіоелектронної апаратури, представлених на ADEX 2026

Клас	Тепловиділення	Охолодження	Застосування
РЛС з нерухомими полотнами	340–800 Вт (споживання)	Переважно пасивне, оребрений литий корпус	Тринога, щогла, транспортний засіб
Оптико-електронні сенсори	Не публікується	Пасивне, ребра по оболонці	Тринога, бронетехніка
Засоби РЕБ і протидії БпЛА	500–800 Вт (оцінка)	Примусове, ребра з вентиляторами	Щогла, транспортний засіб, портативне
Засоби зв'язку	Не публікується	Пасивне в малих виробах, примусове у вузлах мереж	Портативне, транспортний засіб
Бортова апаратура	Не публікується	Повітряне, крізь жалюзі й пакети ребер	Літальні апарати

У зразках РЛС спостерігалися корпуси з розвиненим оребренням, що створює умови для пасивного відведення тепла. Для окремих засобів РЕБ за зовнішніми ознаками виявлено застосування примусового повітряного охолодження з використанням вентиляторів і ребристих поверхонь. Водночас доступні матеріали не дають змоги однозначно визначити тепловіхарактеристики всіх розглянутих виробів або встановити універсальну межу застосування пасивного й примусового охолодження.

Порівняльний аналіз конструктивних рішень (табл. 2) показав, що орієнтація ребер, форма корпусу, а також використання захисних рамок і козирків визначаються особливостями компонування виробу та передбачуваними умовами його експлуатації. У низці зразків виявлено конструктивні ознаки ущільнення кришок і застосування роз’ємів військового виконання. Водночас візуальний огляд не дає змоги достовірно оцінити фактичний ступінь захисту корпусу від зовнішніх впливів або підтвердити відповідність виробу заявленим технічним вимогам.

Таблиця 2 – Аналіз конструктивних рішень

Аспект	Загальна практика	ADEX 2026
Тепловий шлях без контакту повітря з електронікою	Кондуктивна схема передачі тепла	Пасивні РЛС, засоби РЕБ

Аспект	Загальна практика	ADEX 2026
Ущільнення та роз'єми	Ущільнена оболонка з підтвердженим IP-кодом, круглі роз'єми	Частий крок гвинтів по периметру кришок; IP67
Стійкість до пилу	Герметичний тракт або фільтрація вхідного повітря	Не спостегігалось
Сонячне навантаження	Покриття з урахуванням радіаційних властивостей, козирки	Світлі корпуси й козирки. Окремі вироби були пофарбовані в чорний
Робочий діапазон температур	Діапазон, визначений за профілем експлуатації виробу	−32…+55 °C у РЛС
Теплові дані виробу	Тепловий режим, підтверджений адаптованими випробуваннями	Не вказано, виробники наводять лише споживану потужність і робочі діапазони
Орієнтація й захист ребер, механіка розгортання	Не регламентовано	Вертикальні, радіальні, похилі ребра; рамки, решітки, козирки; щогли, гідроопори

Окремим аспектом є організація повітряного охолодження. Для виробів із відкритими вентиляційними трактами потенційним ризиком є накопичення пилу, яке може зменшувати ефективність теплообміну та спричиняти додаткове теплове навантаження. Водночас відсутність видимих фільтрів під час огляду не є достатньою підставою стверджувати, що відповідний виріб не має внутрішніх засобів пилозахисту. Для підтвердження стійкості необхідні технічна документація або результати відповідних випробувань.

Іншим чинником є нагрівання корпусів від сонця. Кількість поглинутого випромінювання залежить, зокрема, від оптичних властивостей поверхні, геометрії виробу та умов його розміщення. Світлі покриття й козирки можуть зменшувати сонячне навантаження, однак фактичний ефект має оцінюватися з урахуванням матеріалу, кольору, орієнтації поверхонь і теплового режиму обладнання.

Аналіз доступної документації також виявив обмеженість оприлюднених даних про теплові характеристики окремих виробів. Зокрема, не завжди доступні відомості про тепловиділення, тепловий опір корпусу та допустиму тривалу потужність за граничної температури. Через це за відкритими

матеріалами не завжди можливо оцінити тепловий запас виробу в усьому заявленому діапазоні умов експлуатації.

Висновки

За результатами огляду зразків польової радіоелектронної апаратури, представлених на ADEX 2026, систематизовано характерні конструктивні рішення для п’яти функціональних класів обладнання та визначено основні аспекти, що потребують уваги під час оцінювання його експлуатаційної придатності.

Серед ключових чинників, які доцільно враховувати під час проєктування й вибору польової апаратури, — ефективність тепловідведення, захист вентиляційних трактів від пилу, вплив сонячного нагрівання, механічна стійкість конструкції та відповідність заявленим умовам експлуатації.

Зовнішній огляд і відкриті матеріали виробників дають змогу виявити характерні інженерні підходи та сформувати перелік потенційних ризиків, однак не замінюють теплових і кліматичних випробувань. Для обґрунтованого оцінювання виробів доцільно вимагати від постачальників дані про теплові характеристики та умови їх визначення, а під час розроблення власної апаратури передбачати перевірку теплового режиму з урахуванням температури навколишнього середовища, сонячного навантаження й можливого забруднення повітряних трактів.

Отримані спостереження можуть бути використані як основа для подальшого порівняльного аналізу конструктивних рішень і формування рекомендацій щодо проєктування та випробування польової радіоелектронної апаратури.

СЕКЦІЯ 6

Радіоелектронна боротьба

Шельвестер В. Я.
Шейгас В. В.
Житомирський військовий інститут імені С. П. Корольова

КОНТРОЛЬ ХАРАКТЕРИСТИК АНТЕН ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ ЇХ ЕФЕКТИВНОСТІ В УМОВАХ СУЧАСНОЇ ВІЙНИ

Сучасна російсько-українська війна характеризується безпрецедентно високою насиченістю поля бою радіоелектронними засобами, безпілотними літальними апаратами, системами зв'язку та розвідки. У цих умовах засоби радіоелектронної боротьби (далі РЕБ) стали одним із ключових елементів забезпечення живучості військ, протидії безпілотним системам противника та захисту власних інформаційно-комунікаційних мереж. Ефективність роботи будь-якого комплексу РЕБ безпосередньо залежить від технічного стану його антенно-фідерних систем, які забезпечують випромінювання та прийом електромагнітної енергії.

Однією з актуальних проблем є те, що в умовах інтенсивних бойових дій антени засобів РЕБ постійно піддаються впливу несприятливих факторів: механічних пошкоджень від уламків боєприпасів, вібрацій під час транспортування, несприятливих погодних умов, перепадів температур, підвищеної вологості, пилу та забруднень. Крім того, тривала робота на високих рівнях потужності може призводити до деградації окремих елементів антенно-фідерного тракту. Такі впливи викликають зміну електричних параметрів антен, що часто залишається непоміченим без проведення спеціального контролю.

Особливу небезпеку становить поступове погіршення амплітудно-частотних характеристик антен. Навіть незначне відхилення від нормативних параметрів може призвести до зменшення дальності радіоелектронного придушення, утворення «сліпих зон» у робочому діапазоні частот, зниження ефективності боротьби з безпілотними літальними апаратами та засобами зв'язку противника. У результаті противник отримує можливість використовувати окремі канали зв'язку або навігації, які повинні були бути заблоковані засобами РЕБ.

Додатковою проблемою є те, що несправності антен часто маскуються під відмови інших елементів комплексу. Особовий склад може спостерігати зниження ефективності роботи станції РЕБ, не маючи можливості оперативно визначити, чи пов'язано це з передавальною апаратурою, програмним забезпеченням або саме з антенною системою. Відсутність регулярного контролю характеристик антен ускладнює технічну діагностику та збільшує час відновлення боєздатності засобів РЕБ.

Важливою проблемою залишається також забезпечення електромагнітної сумісності на полі бою. Неконтрольовані зміни параметрів антен можуть призводити до появи паразитних випромінювань та створення завад власним системам зв'язку, управління, розвідки та навігації. В умовах сучасних бойових дій, де швидкість обміну інформацією має вирішальне значення, такі явища можуть негативно впливати на управління військами та координацію бойових дій.

Таким чином, проблема необхідності перевірки антен засобів РЕБ в умовах війни в Україні полягає у забезпеченні гарантованої ефективності радіоелектронного придушення, своєчасному виявленні пошкоджень і деградації антенно-фідерних систем, підтриманні електромагнітної сумісності та збереженні бойової готовності комплексів РЕБ. Регулярний контроль амплітудно-частотних характеристик, коефіцієнта стоячої хвилі та інших параметрів антен є необхідною умовою надійного функціонування систем радіоелектронної боротьби та підвищення ефективності їх застосування в сучасній війні.

Контроль АЧХ антен засобів РЕБ складається з декількох етапів:

Етап 1. Підготовка до вимірювань. Перед проведенням контролю необхідно: провести зовнішній огляд антени; перевірити стан кабелів та роз'ємів; переконатися у відсутності механічних пошкоджень; відключити сторонні джерела випромінювання.

Етап 2. Вимірювання коефіцієнта стоячої хвилі (далі КСХ). КСХ є одним із головних показників якості узгодження антени. Для більшості засобів РЕБ прийнятними є значення: КСХ $\leq$ 1,5 – відмінне узгодження; КСХ 1,5–2,0 – допустиме; КСХ > 2,0 – потребує перевірки.

Вимірювання проводять: КСХ-метром; векторним аналізатором мереж (VNA); аналізатором антен.

Етап 3. Вимірювання амплітудно-частотної характеристики. Для цього використовують: векторний аналізатор мереж; аналізатор спектра з генератором стеження; спеціалізовані антенно-вимірювальні комплекси.

Під час вимірювання визначають: робочий частотний діапазон; резонансні частоти; ширину смуги пропускання; нерівномірність АЧХ; рівні побічних максимумів.

Отримані результати порівнюють з еталонними характеристиками.

Етап 4. Контроль діаграми спрямованості. Для антен РЕБ важливо не лише випромінювати потрібну потужність, але й робити це в потрібному напрямку. Для цього перевіряють: положення головного пелюстка; ширину діаграми спрямованості; рівень бічних пелюсток; коефіцієнт підсилення.

Вимірювання виконуються на полігоні або в безвідбивній камері.

Етап 5. Контроль випромінюваної потужності, під час якого визначають: рівень потужності на різних частотах; стабільність випромінювання; рівномірність розподілу енергії в смузі частот.

Етап 6. Порівняння з еталонними параметрами. Після вимірювань результати порівнюються з: заводськими паспортними даними; попередніми контрольними вимірюваннями; нормативами експлуатаційної документації. Якщо виявлено суттєві відхилення, проводиться: локалізація несправності; ремонт антени або фідера; повторний контроль після усунення дефектів.

Основні ознаки погіршення АЧХ антени: зміщення резонансної частоти; зростання КСХ; звуження робочої смуги частот; поява додаткових провалів на АЧХ; зменшення коефіцієнта підсилення; підвищення рівня побічних пелюсток. У бойових умовах це може призвести до зменшення дальності та ефективності радіоелектронного придушення.

Контроль амплітудно-частотних характеристик випромінюючих антен засобів РЕБ необхідний для забезпечення ефективного радіоелектронного подавлення, узгодження антени з передавальним обладнанням, електромагнітної сумісності та своєчасного виявлення технічних несправностей. Правильний контроль передбачає комплекс вимірювань КСХ, АЧХ, діаграми спрямованості та випромінюваної потужності з використанням аналізаторів мереж, аналізаторів спектру та спеціалізованих антенно-вимірювальних комплексів. Регулярний моніторинг цих параметрів є обов'язковою умовою підтримання бойової готовності засобів РЕБ.

Іщенко Д. А., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

ВАРІАНТ КЛАСИФІКАЦІЇ ЗАСОБІВ У СИСТЕМІ ЗАГАЛЬНИХ ТЕХНІЧНИХ ВИМОГ ДО ТЕХНІКИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Розглядається проблема класифікування засобів радіоелектронної боротьби (РЕБ). Розв’язання цієї проблеми є обов’язковою складовою досліджень щодо розроблення системи загальних технічних вимог до військової техніки (СЗТВ ВТ) РЕБ. СЗТВ ВТ РЕБ є складової Комплексної СЗТВ до озброєння та військової техніки (КСЗТВ ОВТ), що розроблюється в Міністерстві оборони та Збройних Сил під загальним організаційним керівництвом уповноваженого органу військового управління. Актуальність розроблення науково обґрунтованого варіанту класифікації пояснюється потребою формування орієнтовних кількісних та якісних характеристик виробів, що належать до класифікаційних угруповань, оскільки відрізняються класифікаційними ознаками. Висока динаміка розвитку та інноваційність ВТ РЕБ зумовлює своєчасність вирішення цієї проблеми. Варіант класифікації повинний бути придатним для нормативного прийняття у складі військового стандарту, орієнтовано - ВСТ 20.39.5865.001 : 20XX (01) “Комплексна система СЗТВ. Техніка РЕБ. Терміни та визначення понять, класифікація”, розроблення якого фахівцями Житомирського військового інституту планується в відповідно до Програми робіт із військової стандартизації (проєкту) на 2027–2029 роки.

Єдиний класифікатор предметів постачання (ДК 020:2016), гармонізований із багатомовним класифікатором НАТО (ACodP-2), не можуть бути використані як базове нормативне підґрунтя класифікації засобів РЕБ. Оскільки у цьому документі у групі 58 “Апаратура зв’язку, виявлення і когерентного випромінювання” об’єднані різні засоби РЕБ в один клас — 5865 “Техніка радіоелектронної боротьби та швидкодіюча апаратура”. Фрагментарне подання окремих характеристик технічних засобів у керівних і розпорядчих документах, наприклад щодо відстаней виявлення та впливу засобами РЕБ тактичного рівня та ближньої дії, також не забезпечує комплексного вирішення науково обґрунтованого варіанту класифікації. Відсутність СЗТВ через нестачу нормативно визначеної класифікації засобів різної складності (зразків,

комплексів, систем), що відрізняються функціональним призначенням (виявлення та подавлення систем управління противника, радіоелектронний захист власних систем, електронна підтримка РЕБ), мобільністю та рівнем застосування, ускладнює уніфікацію, масштабування виробництва, постачання та експлуатацію у бойових умовах.

Отже, обґрунтування класифікації є актуальним науково-практичним завданням, метою якого формування варіанта засобів РЕБ, який поєднує базову конструкторсько-технологічну ієрархію (система — комплекс — зразок — складник) із адаптивним фасетним описом їхніх тактико-технічних функцій для нормативного прийняття в СЗТВ ВТ РЕБ.

Для досягнення поставленої мети використано комплекс наукових методів: системно-об'єктний аналіз — для декомпозиції засобів РЕБ як складних динамічних систем та виділення їхніх інваріантних і варіативних характеристик; методи фасетної класифікації — для формування багатоаспектної структури опису ВТ РЕБ, що дозволяє паралельно класифікувати засоби за незалежними технічними та тактичними ознаками; нормативно-компаративний аналіз — для порівняння архітектури чинної КСЗТВ ОВТ із вимогами перспективних СЗТВ ВТ ВДР.

Варіант класифікації засобів техніки РЕБ, який поєднує традиційну конструкторсько-технологічну ієрархію з фасетним описом тактико-технічних функцій засобів РЕБ представлено у таблиці 1.

Таблиця 1

Варіант класифікації засобів техніки радіоелектронної боротьби

Рівень класифікації
1. Ієрархічна класифікація виробів техніки РЕБ
1.1 система техніки РЕБ
1.2 комплекс техніки РЕБ
1.3 зразок техніки РЕБ
1.4 складник (комплектувальний виріб)
1.5 складанна одиниця
1.6 деталь
2. Фасетна класифікація виробів техніки РЕБ за призначенням
2.1 основні засоби (системи, комплекси, зразки) РЕБ (основних, бойових підрозділів)

2.2 технічні засоби забезпечення застосування основних засобів РЕБ
2.3 технічні засоби навчання особового складу до застосування засобів РЕБ
2.4 технічні засоби підтримання заданого ступеня готовності до застосування виробів техніки РЕБ різного призначення
3. Ієрархічна класифікація основних (2.1) засобів РЕБ
3.1 (2.1.1) зразок (основних засобів) РЕБ (станція)
3.2 (2.1.2) комплекс (основних засобів РЕБ
3.3 (2.1.3) система (основних засобів) РЕБ
4. Фасетна класифікація засобів РЕБ (далі - засоби) за призначенням
4.1 Засоби виявлення та подавлення радіоперешкодами (РП) систем і засобів управління військами і зброєю противника
4.1.01. Засоби виявлення та подавлення РП короткохвильових (КХ) ліній радіозв'язку в оперативно-стратегічній ланці управління противника
4.1.02. Засоби виявлення та подавлення РП КХ ліній радіозв'язку в оперативно-тактичній та тактичній ланках управління противника
4.1.03. Засоби виявлення та подавлення РП ліній супутникового радіозв'язку противника
4.1.04. Засоби виявлення та подавлення РП УКХ ліній радіозв'язку в оперативно-тактичній та тактичній ланках управління противника
4.1.05. Засоби виявлення та подавлення РП командних УКХ радіоліній управління авіацією противника у повітрі
4.1.06. Засоби виявлення та подавлення РП каналів радіоуправління, телеметрії, передачі інформації та бортових приймачі супутникових радіонавігаційних систем безпілотних літальних апаратів противника
4.1.07. Засоби виявлення та подавлення РП каналів стільникового радіозв'язку стандартів 2-5G
4.1.08. Засоби прикриття об'єктів (військ) від ураження боєприпасами із радіопідривниками
4.1.09. Засоби прикриття об'єктів (військ) від ураження радіокерованими фугасами
4.1.10. Засоби прикриття від повітряної радіолокаційної розвідки і прицільних ударів з повітря визначених об'єктів
4.1.11. Засоби подавлення РП бортових радіонавігаційних засобів літаків (вертольотів) противника, головок самонаведення високоточної зброї
4.1.12. Засоби блокування сигналів аналогового та цифрового телебачення
4.2. Засоби радіоелектронного захисту (РЕЗт) своїх систем і засобів управління

4.2.01. Засоби контролю за виконанням заходів РЕЗт радіоелектронних засобів (РЕЗ) в районах розгортання пунктів управління стратегічного рівня та угрупованнях військ (сил)
4.2.02. Засоби контролю за виконанням штабами, військами заходів РЕЗт РЕЗ
4.2.03. Засоби контролю за дотриманням заходів забезпечення електромагнітної сумісності РЕЗ в угрупованнях своїх військ та ефективності РЕП
4.2.04. Засоби виявлення роботи та пошуку незаконнодіючих РЕЗ.
4.2.05. Засоби пошуку, виявлення та усунення дії джерел радіозавад
4.2.06. Засоби організації та контролю за встановленими заборонами (обмеженнями) на використання РЕЗ в районах розгортання пунктів управління стратегічного рівня та угрупованнях військ (сил)
4.3.01. Засоби виявлення роботи, визначення місцеположення та належності РЕЗ
4.3.02. Засоби перехоплення сигналів і радіовипромінювань РЕЗ
4.3.03. Засоби аналізу перехоплених сигналів і радіовипромінювань РЕЗ, режимів їх роботи і характеристик РЕЗ
4.3.04. Засоби контролю ефективності РЕП системи і засобів управління військами (силами) і зброєю противника
4.3.05. Засоби контролю за роботою РЕЗ систем управління військами (силами) і зброєю своїх військ (сил).
4.3.06. Засоби наведення засобів РЕП на виявлені РЕЗ противника
4.3.07. Засоби наведення засобів вогневого ураження на РЕЗ противника для їх знищення (виведення з ладу)
5. Фасетна класифікація засобів РЕБ за мобільністю розгортання, згортання, до швидкого переміщення (пересування), дії
5.1 Стаціонарні (квазістаціонарні), здатні виконувати завдання РЕБ без швидкого переміщення
5.2 Рухомі здатні виконувати завдання РЕБ в русі: польові (автомобільні, гусеничні); повітряні (літакові, вертольотні, кулі); залізничні (вагонні, платформні); корабельні
5.3 Мобільні, здатні до швидкого згортання, переміщення, після розгортання виконувати завдання РЕБ: 5.3.1 Пересувні (на рухомої платформі; причіпні); 5.3.2 Переносні (рюкзакові; портативні)
6. Фасетна класифікація засобів РЕБ за кількістю персоналу, потрібної для приведення в дію та бойового застосування

6.1 індивідуальній засіб РЕБ
6.2 колективний (груповий) засіб РЕБ
7. Фасетна класифікація засобів РЕБ за місцем розміщення (базування) та відповідним класом апаратури застосованої у виробі
7.1 засоби техніки РЕБ наземної (1 клас – апаратура наземного ОВТ)
7.2 засоби техніки РЕБ морського базування (2 клас – апаратура ОВТ морського базування)
7.3 засоби техніки РЕБ бортової авіаційної техніки і озброєння (3 клас – бортова апаратура авіаційної техніки і озброєння)
7.4 засоби техніки РЕБ бортового ракетного озброєння та техніки (4 клас – бортова апаратура ракетного озброєння та техніки)
7.5 засоби техніки РЕБ бортової космічної техніки (5 клас – бортова апаратура космічної техніки)
7.6 засоби техніки РЕБ боєприпасів артилерії (6 клас – апаратура боєприпасів артилерії)
8. Фасетна класифікація засобів РЕБ за рівнем завдань забезпечення дій військових формувань (підрозділів, частин, з’єднань, угруповань) і радіоелектронного прикриття об’єктів
8.1 Засоби тактичного рівня
8.2 Засоби оперативно-тактичного рівня
8.3 Засоби стратегічного рівня

Журавський С. В.
Чолпанов В. О.
Назарчук Я. Ю.
Житомирський військовий інститут імені С. П. Корольова

УДОСКОНАЛЕНИЙ АЛГОРИТМ ВИЯВЛЕННЯ ТА ПОДАВЛЕННЯ ВІДЕОКАНАЛІВ БЕЗПІЛОТНИХ АВІАЦІЙНИХ АПАРАТІВ ІЗ СИСТЕМОЮ FPV

Упродовж останнього століття основою вогневої потужності більшості армій були великі, надзвичайно складні та дуже дорогі платформи: танки, літаки, артилерійські системи чи військові кораблі. Однак поява й масове

впровадження FPV-БпЛА кардинально змінили цей пріоритет. Поєднання відносно невисокої вартості, високої маневреності, оперативності застосування та можливості використання різних типів корисного навантаження сприяло їх масовому поширенню на тактичному рівні.

На відміну від традиційних високоточних засобів ураження, FPV-БпЛА можуть масово та швидко виготовлятися з використанням комерційних компонентів, швидко адаптуватися до нових умов бойового застосування та оперативно модернізуватися відповідно до змін засобів протидії. Така особливість суттєво скорочує цикл технологічної адаптації між засобами нападу та оборони. Якщо раніше оновлення озброєння вимагало років, то нині зміна частотних діапазонів, протоколів передачі інформації, конструкцій антен або алгоритмів керування може здійснюватися протягом декількох тижнів.

Одночасно зі збільшенням масштабів застосування FPV-БпЛА істотно зросли вимоги до засобів радіоелектронної боротьби. Сучасні комплекси РЕБ для боротьби з FPV-БпЛА, створені, в основному, для подавлення цифрових каналів управління, виявилися недостатньо ефективними в умовах масового використання малогабаритних безпілотних систем, які функціонують у різних частотних діапазонах та використовують широкий спектр аналогових передавачів відеоінформації.

Використання широкого спектру передавачів відео з різними частотами передачі відео потребує переходу до нових алгоритмів роботи засобів радіоелектронної боротьби, яка передбачає виявлення факту роботи (функціонування) каналу передачі відео, автоматичне визначення робочої частоти цього каналу, постановку радіоперешкоди, контроль роботи каналу передачі відео, створення нової перешкоди на іншій частоті.

Разом із тим, в умовах застосування противником великої кількості БпЛА з системою FPV зростає і кількість каналів передачі відео, апріорна інформація про які може бути неповною або швидко втрачати актуальність. Унаслідок цього постановка перешкоди в наперед визначеному або в усьому діапазоні роботи передавачів відео не завжди забезпечує необхідний рівень подавлення. Розширення смуги перешкоди або збільшення її потужності призводить до зростання енергетичних витрат і підвищує ризик негативного впливу на власні радіоелектронні засоби. Таким чином, існує суперечність між необхідністю оперативного й вибіркового радіоелектронного впливу на канали передачі саме

ворожих FPV-БпЛА в умовах їхньої динамічної зміни та обмеженими можливостями наявних засобів щодо автоматичного визначення параметрів сигналів і формування відповідної перешкоди в реальному масштабі часу.

Переважна більшість існуючих комплексів та засобів радіоелектронної боротьби функціонує за принципом постановки широкосмугових або вузькосмугових шумових перешкод у наперед визначених діапазонах частот, без можливості зміни параметрів перешкоди. Такий підхід був ефективним для подавлення каналів передачі відео FPV-БпЛА на фіксованих частотах. Однак сьогодні існує можливість змінювати частоту передачі відео з пульта управління в польоті, що істотно зменшує ефективність застосування класичних засобів постановки перешкод та знижує рівень захисту особового складу та техніки.

Зважаючи на те, що передавачі відео працюють в досить широкому діапазоні частот: приблизно від 900 до 8800 МГц залежно від типу обладнання, це істотно ускладнює застосування традиційних засобів радіоелектронного подавлення, оскільки для ефективного впливу необхідно одночасно здійснювати радіоелектронне подавлення декількох незалежних каналів передачі відео, частоти яких можуть змінюватися під час виконання польотного завдання.

Важливою проблемою залишається алгоритм роботи подавлення каналу передачі відео. Найчастіше він функціонує за схемою: виявлення сигналу – визначення частоти – визначення приналежності БпЛА – постановка перешкод.

При чому, класичний алгоритм має такі недоліки:

оператор отримує інформацію про факт наявності FPV-БпЛА від різноманітних засобів виявлення, які не зв’язані між собою в єдину систему виявлення та подавлення, так само, як і засоби РЕБ різних типів;

контроль ефективності подавлення здійснюється після подавлення. Оператор не має інформацію про місцезнаходження безпілотного апарата і ефективність подавлення;

швидкодія такої системи напряму залежить від оператора.

Для того, щоб позбутись цих недоліків пропонується удосконалений алгоритм подавлення каналу передачі відео FPV-БпЛА (рис. 1).

Удосконалення існуючого алгоритму полягає у:

застосуванні SDR-технологій для виявлення сигналу передавача відео з FPV-БпЛА;

використанні передавача, здатного квазіодночасно здійснювати подавлення декількох частот;

ідентифікації FPV-БпЛА за OSD (On-Screen Display) інформацією (назва підрозділу, напругою АКБ, таймером, напрямком до точки зльоту тощо);

паузах для контролю роботи каналу передачі відео з метою оцінювання ефективності радіоподавлення.

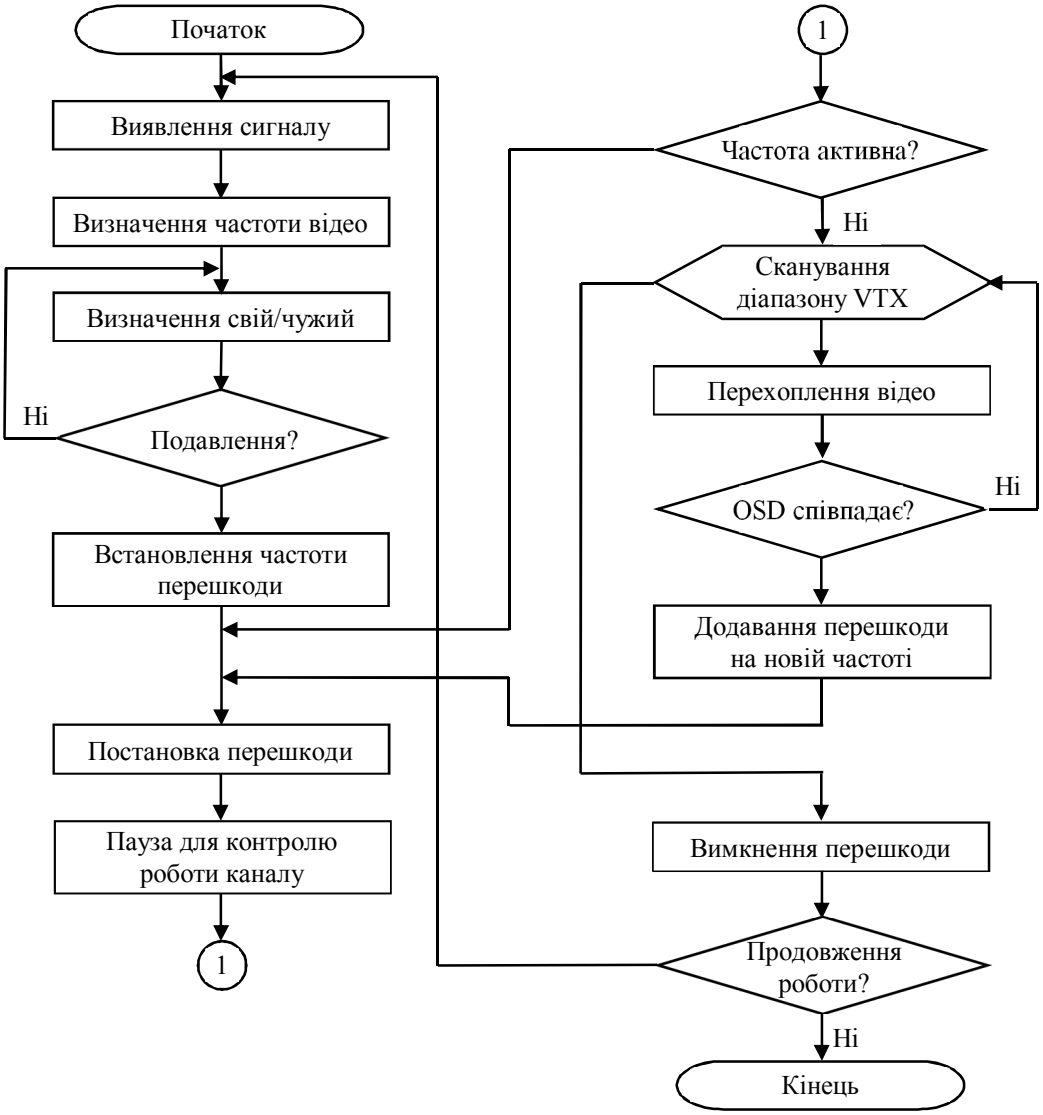


Рис. 1. Удосконалений алгоритм подавлення каналу передачі відео FPV-БпЛА

Опис роботи алгоритму

Виявлення сигналу (радіомоніторинг). На першому етапі засобами виявлення відеоканалу FPV-БпЛА здійснюється безперервний контроль електромагнітної обстановки у визначеному діапазоні частот та виявлення нових джерел випромінювання.

Визначення частоти відео. Під час цього етапу відбувається перехоплення та визначення частотних параметрів сигналу відео.

Визначення свій/чужий. Оператор на основі On-Screen Display інформації здійснює аналіз приналежності БпЛА за принципом “свій/чужий” та приймає рішення щодо створення перешкоди на виявленій частоті відео.

Пауза для контролю роботи каналу. Для визначення ефективності роботи засобу РЕБ подавлення припиняється і відбувається процес контролю частоти, яка подавлювалась. Якщо частота залишається активною, то й перешкода продовжує створюватись на тій самій частоті. Якщо система фіксує відсутність сигналу передачі відео, відбувається сканування саме того діапазону, в якому може працювати передавач відео. За умови знаходження сигналу на новій частоті в межах робочих частот передавача, OSD інформація порівнюється з інформацією попереднього сигналу і, за умови співпадіння, створюється друга перешкода на новій частоті, а разом із тим продовжується подавлення на першій визначеній частоті.

Відмінність запропонованого алгоритму від класичного полягає в:

ідентифікації безпілотного апарата за інформаційними параметрами телеметричної інформації, яка передається в On-Screen Display інформації;

значному зменшенні часу автоматичної дорозвідки каналу передачі відео в порівнянні з часом виконання цієї дії опратором (мілісекунди в порівнянні з секундами);

можливості формуванні квазіодночасно декількох прицільних перешкод на різних частотах на відміну від однієї широкосмугової.

За такого алгоритму роботи засобу РЕБ ефективність визначається не лише його технічними характеристиками, а автоматизацією усіх процесів та узгодженістю функціонування алгоритму та мало залежить від оператора, який при припиненні подавлення та новому скануванні визначеного частотного діапазону не має інформації про подавлення або неподавлення виявленого каналу передачі відео.

Брановицький В. В.
Фриз В. П., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ СПРЯМОВАНОЇ АНТЕНИ ДЛЯ ПІДВИЩЕННЯ ДАЛЬНОСТІ ТА РАДІОЕЛЕКТРОННОЇ СТІЙКОСТІ FM-РАДІОМОВЛЕННЯ В ІНТЕРЕСАХ ПСИХОЛОГІЧНОГО ВПЛИВУ

В умовах сучасної російсько-української війни психологічний вплив на особовий склад противника є одним із напрямів комплексного застосування сил і засобів. Особливого значення набувають технічні засоби, які забезпечують оперативне доведення інформації до визначеної цільової аудиторії на значній відстані, не потребують безпосереднього фізичного контакту та функціонують незалежно від доступності до мережі Інтернет.

Одним із перспективних технічних засобів такого впливу є FM-радіомовлення, яке дає змогу передавати інформаційні повідомлення на значну територію та забезпечувати їх приймання за допомогою автомобільних та індивідуальних радіоприймальних пристроїв. Для організації FM-радіомовлення підрозділами психологічних операцій застосовуються тактичні FM-передавачі типу RIAB потужністю 750 та 1000 Вт, а також передавач RT-FMS-3001 потужністю 3 кВт. Зазначені засоби, як правило, комплектуються антенними системами з ненаправленою (круговою) діаграмою спрямованості, що не забезпечує концентрації електромагнітної енергії в заданому напрямку.

В сучасних умовах ведення бойових дій особливої актуальності набуває питання забезпечення радіоелектронної стійкості FM-радіомовлення в умовах протидії засобам радіоелектронної боротьби (РЕБ) противника. Навмисне створення радіоперешкод противником призводить до погіршення співвідношення сигнал/шум, зменшення дальності впевненого приймання та, як наслідок, зниження ефективності передавання інформації до цільової аудиторії.

Одним із технічних підходів до підвищення просторової вибірковості радіосистеми є застосування спрямованої передавальної антени. На відміну від неспрямованої антени, вона формує концентрує основну частину випромінювання у визначеному напрямку. Це дозволяє підвищити рівень корисного сигналу в зоні розташування цільової аудиторії. Важливою додатковою властивістю спрямованої антени є просторове ослаблення

випромінювання за межами основної пелюстки діаграми спрямованості. Унаслідок цього зменшується рівень енергії, що випромінюється в інших напрямках. Така просторова селективність може мати значення для забезпечення радіоелектронної стійкості системи, оскільки зменшує вплив сигналів та перешкод, що надходять із напрямків, у яких антена має значне ослаблення.

Метою дослідження є експериментальне оцінювання впливу спрямованих властивостей передавальної антени на дальність впевненого приймання FM-радіосигналу та визначення практичної значущості просторової вибірковості антенної системи для підвищення стійкості радіомовлення до зовнішніх радіоперешкод.

Експериментальні дослідження проведено із використанням FM-передавача потужністю 3 кВт, що працював на частоті 99,9 МГц, та чотириелементної спрямованої антени типу «хвильовий канал». Передавальну антену встановлено на висоті 25 м. Коефіцієнт стоячої хвилі антено-фідерного тракту становив 1,1, що свідчить про належне узгодження антени з фідером та невисокий рівень відбитої потужності. Коефіцієнт підсилення антени становив 5,4 дБ.

Оцінювання дальності здійснювалося за фактом стабільного та розбірливого приймання FM-сигналу автомобільним приймальним пристроєм. Випробування проводилися у різних просторових напрямках відносно осі основної пелюстки діаграми спрямованості передавальної антени.

За результатами експериментальних досліджень встановлено, що в напрямку основної пелюстки діаграми спрямованості впевнений прийом FM-сигналу забезпечувався на відстані до 60 км. У напрямку задньої пелюстки дальність стабільного приймання становила до 40 км, тоді як у напрямках бічних пелюсток до 20 км.

Отримані результати демонструють виражену просторову нерівномірність зони радіопокриття. Різниця між дальністю приймання в напрямку основної та бічних пелюсток свідчить про ефективне просторове формування випромінювання передавальної антени. Відповідно, основна енергія передавача використовується для формування необхідного рівня сигналу у визначеному напрямку, тоді як випромінювання в інших напрямках є суттєво меншим.

З точки зору радіоелектронної стійкості така властивість є важливою перевагою спрямованої антени. Для забезпечення необхідного рівня корисного сигналу в заданій зоні не обов'язково збільшувати потужність передавача, оскільки

частина енергетичного ресурсу забезпечується просторовим підсиленням антени. Одночасно ослаблення випромінювання поза основною пелюсткою зменшує просторову «видимість» сигналу в інших напрямках порівняно з використанням антени з близькою до кругової діаграмою спрямованості.

Таким чином, спрямована антена має подвійну функціональну перевагу: з одного боку, забезпечує збільшення рівня корисного сигналу та дальності його впевненого приймання в заданому напрямку, а з іншого – формує просторово селективне випромінювання, що може сприяти підвищенню стійкості системи до зовнішніх радіоперешкод.

Для додаткового оцінювання отриманих результатів визначено розрахункову дальність радіовидимості. За висоти передавальної антени 25 м та висоти приймальної антени близько 2 м її значення становило приблизно 26 км. Експериментальна дальність впевненого приймання в напрямку основної пелюстки становила до 60 км, що приблизно у 2,3 рази перевищує розрахункове геометричне значення.

Отримані експериментальні результати підтверджують, що збільшення потужності передавача та коефіцієнта підсилення антени в заданому напрямку підвищує рівень сигналу в точці приймання, тоді як характеристики приймального пристрою, зокрема його чутливість, визначають мінімальний рівень сигналу, за якого можливе впевнене приймання.

Водночас застосування спрямованої антени дозволяє сформувати просторово селективну зону радіопокриття. Це є принциповою відмінністю від використання антени круговою діаграмою спрямованості, оскільки енергетичний ресурс передавача концентрується в необхідному напрямку, а випромінювання в інших напрямках послаблюється.

З практичної точки зору це може підвищувати радіоелектронну стійкість FM-радіомовлення в умовах зовнішніх радіоперешкод. Водночас ступінь такого підвищення потребує окремого експериментального дослідження з контрольованим рівнем і напрямком перешкоди та кількісним визначенням зміни співвідношення сигнал/шум і дальності впевненого приймання.

Таким чином, проведене дослідження підтвердило доцільність застосування спрямованої передавальної антени для підвищення дальності FM-радіомовлення та формування просторово селективної зони радіопокриття.

Філіппов М. О., канд. психол. наук, доц.
Пак Д. Є.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ НАВІГАЦІЇ БЕЗПІЛОТНИХ СИСТЕМ В УМОВАХ ПОРУШЕННЯ ТА НЕДОСТУПНОСТІ СУПУТНИКОВИХ НАВІГАЦІЙНИХ СИГНАЛІВ

Зростання ролі безпілотних систем у сучасних операціях підвищує вимоги до безперервності та достовірності навігаційного забезпечення. Значна частина безпілотних платформ використовує глобальні навігаційні супутникові системи (GNSS) як основне джерело координатно-часової інформації. Водночас залежність від одного зовнішнього джерела створює системний ризик: погіршення приймання сигналів, їх тимчасова недоступність, спотворення навігаційного поля або складні умови поширення можуть призводити до накопичення помилок, некоректного визначення положення та переходу платформи у небажаний режим. Тому стійкість навігації доцільно розглядати як властивість усієї безпілотної системи зберігати прийнятний рівень просторової орієнтації при деградації або втраті супутникової навігації.

Обґрунтовано принципи побудови багатоканальної навігаційної архітектури БпС, здатної своєчасно виявляти зниження достовірності даних GNSS, переходити на альтернативні джерела навігаційної інформації та забезпечувати безпечне функціонування системи до відновлення основного каналу. На відміну від підходу, за якого резервний засіб розглядається лише як дублер, пропонується концепція постійного взаємного контролю декількох навігаційних джерел. У такій системі важливо оцінювати не лише поточне значення координат, а й ступінь довіри до кожного джерела, узгодженість між ними та швидкість зміни похибки.

Базовою складовою резервування є інерціальна навігаційна система (ІНС), яка забезпечує автономне оцінювання руху без зовнішнього радіосигналу. Її перевагою є незалежність від умов приймання, а обмеженням – накопичення похибки з часом. Отже, практична стійкість визначається не самою наявністю ІНС, а здатністю системи регулярно коригувати інерціальну оцінку за іншими незалежними ознаками. Для різних типів БпС такими

ознаками можуть бути візуальні та теплові особливості місцевості, геометрія навколишніх об'єктів, барометрична висота, параметри власного руху, цифрова модель рельєфу або інші доступні сенсорні вимірювання. Комбінація різнорідних джерел зменшує ймовірність одночасної відмови всієї навігаційної підсистеми.

Перспективним напрямом є візуально-інерціальна навігація, у якій оцінка переміщення формується за послідовністю зображень із корекцією на дані інерціальних датчиків. Такий підхід може бути ефективним там, де є достатня кількість стійких візуальних ознак, однак його працездатність залежить від освітлення, погодних умов, висоти руху, якості оптики та обчислювальних ресурсів. Тому візуальний канал не повинен розглядатися як універсальна заміна GNSS. Доцільною є адаптивна система, яка визначає інформативність поточного зображення і, за її зниження, підвищує вагу інших джерел або переходить до режиму обмеженої функціональності.

Для наземних і низьковисотних платформ додатковим джерелом можуть бути методи зіставлення поточних спостережень із попередньо підготовленими картографічними даними. Їх застосування доцільно оцінювати за принципом достатності, а не абсолютної точності: у багатьох задачах важливішим є гарантоване утримання платформи в допустимій зоні та своєчасне розпізнавання накопичення помилки, ніж отримання координат максимальної точності в кожний момент часу. Такий підхід дозволяє формувати навігаційну систему з декількома рівнями якості – штатним, деградованим і безпечним – із чітко визначеними правилами переходу між ними.

Ключовим елементом стійкої навігації є контроль цілісності. Система повинна мати засоби виявлення ситуації, коли навігаційні дані формально доступні, але їхня достовірність знизилася. Для цього можуть використовуватися взаємні перевірки між GNSS, ІНС і сенсорними каналами, аналіз фізичної правдоподібності зміни швидкості та положення, а також контроль узгодженості часових міток. Важливо, щоб виявлення аномалії не обмежувалося сигналом для оператора, а автоматично запускало наперед визначений безпечний сценарій: обмеження швидкості, стабілізацію руху, перехід на резервний канал, утримання району або завершення завдання у безпечній конфігурації залежно від типу платформи.

Застосування методів машинного навчання в навігаційній підсистемі є доцільним насамперед для розпізнавання складних просторових ознак,

оцінювання якості сенсорних даних і прогнозування достовірності навігаційного рішення. При цьому критичні функції контролю безпеки мають залишатися перевіртними і відокремленими від моделей, поведінку яких складно формально описати. Раціонально використовувати гібридну архітектуру: математично визначені алгоритми забезпечують базову оцінку та контроль обмежень, а інтелектуальні модулі підвищують якість сприйняття середовища і вибирають найбільш інформативні джерела. Це зменшує ризик того, що помилка окремої моделі призведе до неконтрольованої зміни навігаційного режиму.

Окремою вимогою є обчислювальна та енергетична ефективність. Резервна навігація повинна зберігати працездатність на бортовому обчислювачі без обов’язкової постійної взаємодії з зовнішнім сервером. Це особливо важливо для малих платформ, де маса, енергоспоживання та тепловиділення мають жорсткі обмеження. Відповідно, доцільно застосовувати модульний підхід, за якого складні алгоритми активуються лише при погіршенні основного каналу або за наявності достатнього енергетичного резерву, тоді як базові засоби стабілізації, інерціальної оцінки та контролю цілісності функціонують постійно.

Важливим завданням є уніфікація інтерфейсів між навігаційними модулями. Для різних класів БпС склад сенсорів може суттєво відрізнятися, однак принципи оцінювання якості даних, передавання показника довіри та переходу між режимами можуть бути стандартизовані. Це дозволить швидше інтегрувати нові датчики, порівнювати різні рішення за єдиними критеріями та зменшувати залежність програмного забезпечення від конкретного апаратного компонента. У перспективі така уніфікація є важливою передумовою масштабування виробництва й модернізації наявних систем без повної перебудови бортової архітектури.

Перевірка стійкості навігації має проводитися за сценарним принципом. До набору випробувань доцільно включати поступове погіршення якості супутникової навігації, раптову її втрату, суперечливі показання окремих сенсорів, недостатню кількість візуальних орієнтирів, складні метеорологічні умови та часткові відмови бортового обладнання. Оцінювати слід не лише кінцеву похибку координат, а й час виявлення деградації, стабільність переходу між режимами, швидкість накопичення помилки, здатність утримувати допустиму зону та коректність відновлення штатного режиму. Така методика дозволяє перевіряти поведінку системи як цілісного комплексу, а не окремого алгоритму.

Для підготовки операторів принципово важливим є відображення рівня достовірності навігації у зрозумілій формі. Оператор повинен бачити не лише поточне положення платформи, а й ознаку якості рішення, активне джерело навігаційних даних та факт переходу в деградований режим. Це зменшує ризик помилкового трактування координат як достовірних та дозволяє своєчасно прийняти рішення про зміну завдання. Тренування мають включати роботу в умовах часткової та повної недоступності супутникової навігації, щоб дії персоналу відповідали логіці автоматичних режимів і не створювали конфлікту між ручним та автономним керуванням.

Таким чином, стійкість навігації БпС в умовах порушення або недоступності супутникових сигналів повинна забезпечуватися не одним резервним датчиком, а багаторівневою системою, що поєднує інерціальну оцінку, сенсорне сприйняття середовища, контроль цілісності, адаптивне зважування джерел і безпечні режими деградації. Основними критеріями ефективності такої системи є своєчасність виявлення недостовірних даних, прогнозованість поведінки, обмеження швидкості накопичення похибки, працездатність без постійного зовнішнього зв’язку та можливість підтвердження характеристик у сценарних випробуваннях. Реалізація зазначених принципів підвищує автономність БпС і зменшує критичну залежність їх функціонування від безперервної доступності сигналів глобальних навігаційних супутникових систем.

Рихальський О. Р. канд. техн. наук, доц.
Борисов П. С., канд. техн. наук
Дем’яненко Є. О.
Житомирський військовий інститут імені С .П. Корольова

ДОСЛІДЖЕННЯ ВПЛИВУ УЗГОДЖЕННЯ ШИРОКОСМУГОВОЇ АНТЕНИ ДЛЯ ТЕХНІКИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ НА РОБОЧУ СМУГУ ЧАСТОТ

Для досягнення кінцевої мети сучасних бойових і спеціальних дій впливає ефективне використання безпілотних авіаційних комплексів (БпАК), які використовуються для розвідки, спостереження поля бою, корегування дій

щодо вогневого ураження тощо. Про це свідчить бойовий досвід підрозділів Збройних Сил України в росі́йсько-Украї́нській війні. З аналізу застосування БпАК, до складу якого входять безпілотні літальні апарати (БпЛА) та пункти управління (ПУ), встановлено закономірність щодо залежності результативності застосування БпЛА за цільовим призначенням від радіоелектронного впливу комплексів радіоелектронної боротьби (РЕБ) на радіоелектронні системи (РЕС) БпАК та радіоелектронного подавлення (РЕП) радіоелектронних засобів (РЕЗ) БпЛА.

У зв’язку із зростаючою кількістю різних типів БпЛА та їх можливостями, радіоелектронна протидія стала однією з найбільш важливих задач засобів РЕБ сил оборони України. Різноманіття тактико-технічних характеристик БпЛА, які мають широкий діапазон робочих частот радіоліній управління з псевдовипадковою перебудовою робочої частоти та з різною смугою радіоканалів, їх кількість та послідовність вибирається оператором ПУ. Крім того, БпЛА приймають сигнали в широкому частотному діапазоні навігаційних систем GPS, GLONASS, Galileo, Beidou та космічної системи фіксованого супутникового зв’язку на низький орбіті Starlink, що потребує організації ефективного РЕП РЕЗ ударних БпЛА противника з метою блокування дистаційного управління, каналів передавання даних та сигналів супутникової навігації. Відповідно, в сучасних та перспективних засобах РЕБ доцільно використовувати широкосмугові підсилювачі з програмно керованими синтезаторами перешкод.

Отже, актуальність зазначеної проблеми обумовлює потребу пошуку нових способів та засобів протидії, у тому числі й радіотехнічних широкосмугових, таким засобам противника щодо недопущення ураження ними важливих об`єктів.

В доповіді подано огляд сучасних ультраширокосмугових антен. Головну увагу зосереджено на антенах самодоповніючої структури, зокрема конічної спіральної антени, її узгодження з фідерним трактом, з метою застосування даних антено-фідерних пристроїв для техніки радіоелектронної боротьби.

За допомогою програм Antena Magus та CST Studio здійснено моделювання конічної спіральної антени різної конфігурації та з різними узгоджуючими пристроями, які є плавним переходом від коаксіального поперечного перерізу до біаксіального. Крім того, досліджено за допомогою портативного векторного мережевого аналізатора LiteVNA конічну спіральну

антену, яка була розроблена в Україні та застосовувалася для бортових телеметричних систем різних модифікацій українських КА серії «АУОС-3», КА «Січ-1», Січ-1М» і інших у тому числі, для КА типу «AUREOL-3» за замовленням Франції. Що підтвердило результати моделювання з дослідженнями реальної конічної спіральної антени.

Таким чином, для ШСА характерним є той факт, що антена та узгоджувальний пристрій представляють собою єдину конструкцію і розробка та оптимізація узгоджувального пристрою є чи не більш складною процедурою ніж розробка форми антени. Крім того, при розробці антен, які здатні працювати у широкій смузі частот і на різних поляризаціях, важливе місце займають питання по зменшенню масо габаритних параметрів, її собівартості та скорочення термінів введення в експлуатацію.

Лазуріна Н. П., канд. філос. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

СТРАТЕГІЧНІ ПРІОРИТЕТИ ІНТЕГРАЦІЇ ВИЩОЇ ОСВІТИ УКРАЇНИ ДО ЄВРОПЕЙСЬКОГО ОСВІТНЬОГО ПРОСТОРУ

В умовах масштабних безпекових викликів процес інтеграції вищої освіти України набуває прискореного характеру, що виступає викликом всій системі Європейського освітнього простору. До академічної мобільності та укладання міжнародних угод в сфері освіти, все активніше додаються: уніфікація змісту освітніх програм, спільна організація наукових досліджень та механізмів забезпечення якості освіти. В першу чергу, це позитивно впливає на розвиток цифрових форматів академічної взаємодії та удосконалення діяльності міжнародних освітніх організацій. Але процес інтернаціоналізації вишів України до Європейського освітнього простору нагально потребує створення цілісної системи стратегічного управління для забезпечення узгодження організаційних та ресурсних механізмів та одночасного урахування безпекових викликів цифрових трансформацій у міжнародній діяльності закладів вищої освіти. Тому, інтеграція міжнародної діяльності в управління закладами вищої освіти України зумовлює актуальність визначення стратегічних пріоритетів процесу інтернаціоналізації до Європейського освітнього простору.

Основними стратегічними пріоритетами діяльності закладів вищої освіти України, направленими на процес інтернаціоналізації, за результатами досліджень, повинні стати:

1. інституційне партнерство (стратегічні угоди, міжнародні мережі університетських альянсів);
2. освітня інтеграція (спільні освітні програми, механізми забезпечення якості освіти, подвійні дипломи);
3. наукова співпраця (спільні дослідження, міжнародні гранти);
4. академічна мобільність (навчання, стажування, викладання в закладах вищої освіти Європейського простору);
5. цифрова інтернаціоналізація (спільні онлайн-курси, віртуальна мобільність).

Практичним результатом реалізації стратегічних пріоритетів інтеграції можна очікувати:

1. розширення міжнародної взаємодії;
2. розвиток довгострокової співпраці та партнерства;
3. доступ до сучасної дослідницької інфраструктури та зростання наукової продуктивності;
4. розвиток професійних та мовних компетентностей;
5. підвищення якості підготовки та міжнародної конкурентоспроможності;
6. інтеграція до європейського академічного простору.

У концепції Європейської асоціації університетів саме відкритість, транснаціональна взаємодія, інституційна автономія та відповідальність розглядаються як основа розвитку університетів до 2030 року. Отже, для підвищення результативності інтернаціоналізації українських вишів до європейського освітнього простору необхідно інтеграція міжнародної діяльності до стратегічного управління університетами, розширення участі в європейських альянсах і консорціумах, підтримка молодих дослідників, удосконалення роботи міжнародних офісів та спрощення державних механізмів реалізації міжнародних проєктів.

Ільченко М. О.
Бібік А. В.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ І ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ: УДОСКОНАЛЕННЯ ФОРМ І СПОСОБІВ ВЕДЕННЯ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ СИЛАМИ ОБОРОНИ УКРАЇНИ

Сучасні збройні конфлікти характеризуються інтенсивним застосуванням високотехнологічних систем озброєння, безпілотних літальних апаратів, засобів супутникової навігації, цифрових систем зв'язку та автоматизованих комплексів управління військами. За таких умов радіоелектронна боротьба (РЕБ) набуває особливого значення як складова забезпечення стійкості функціонування систем військового управління, захисту особового складу, озброєння та військової техніки від сучасних загроз. Досвід російсько-української війни засвідчив, що ефективність бойових дій дедалі більше залежить від здатності сторін використовувати електромагнітний спектр, забезпечувати захист власних радіоелектронних засобів і протидіяти аналогічним можливостям противника. Відповідно до підходів НАТО, електромагнітна боротьба охоплює заходи, спрямовані на використання електромагнітної енергії для отримання інформаційної переваги, забезпечення захисту власних систем та обмеження можливостей противника щодо використання електромагнітного спектра.

Метою дослідження є аналіз сучасного стану систем і засобів радіоелектронної боротьби, визначення основних тенденцій їх технологічного розвитку та обґрунтування перспективних напрямів удосконалення організаційних підходів до ведення РЕБ Силами оборони України.

Сучасний стан розвитку засобів РЕБ характеризується переходом від використання переважно спеціалізованих комплексів до більш широкого впровадження мобільних, малогабаритних і програмно-керованих систем. Особливого значення набувають технології програмно-визначуваного радіо (Software Defined Radio, SDR), цифрового оброблення сигналів, автоматизованого аналізу радіочастотної обстановки та інтелектуальної

підтримки прийняття рішень. Розвиток електронної компонентної бази, мініатюризація обладнання та підвищення обчислювальних можливостей цифрових пристроїв сприяють розширенню функціональних можливостей сучасних засобів РЕБ. Водночас збільшення кількості радіоелектронного обладнання у військових формуваннях ускладнює забезпечення електромагнітної сумісності та підвищує вимоги до ефективного управління радіочастотним ресурсом.

Важливою тенденцією є розвиток вітчизняного виробництва засобів РЕБ і радіоелектронної розвідки (РЕР). За інформацією Міністерства оборони України, протягом перших семи місяців 2025 року до експлуатації було допущено майже 80 нових зразків засобів РЕБ та РЕР, переважна більшість яких розроблена українськими виробниками. Це свідчить про зростання технологічного потенціалу національного оборонно-промислового комплексу, розширення можливостей щодо створення спеціалізованого обладнання та необхідність подальшого розвитку механізмів оцінювання його технічної й експлуатаційної ефективності. Разом із тим швидкі темпи технологічних змін зумовлюють потребу в постійному оновленні технічних рішень, удосконаленні нормативно-технічної документації та забезпеченні належного рівня підготовки фахівців, які здійснюють експлуатацію відповідних систем.

Одним із ключових чинників трансформації радіоелектронної боротьби стало масове використання безпілотних систем різного функціонального призначення. Їх поширення зумовило зростання потреб у засобах радіоелектронного моніторингу, захисту каналів управління, забезпечення стійкості систем навігації та протидії радіоелектронним загрозам. Водночас розвиток автономних систем навігації, інерціальних засобів орієнтування та технологій оброблення інформації безпосередньо на борту безпілотних платформ поступово змінює характер електромагнітного середовища. За таких умов ефективність традиційних підходів до радіоелектронного впливу може знижуватися, що актуалізує необхідність комплексного розвитку технічних засобів, систем спостереження та організаційних механізмів протидії новим загрозам.

Перспективним напрямом розвитку систем РЕБ є інтелектуалізація процесів радіоелектронного моніторингу. Застосування методів машинного навчання та штучного інтелекту створює передумови для автоматизованої класифікації сигналів, виявлення аномалій у радіочастотному середовищі,

аналізу змін електромагнітної обстановки та зменшення інформаційного навантаження на операторів. Використання інтелектуальних алгоритмів дозволяє підвищувати ефективність оброблення значних обсягів інформації, скорочувати тривалість виконання аналітичних процедур і забезпечувати інформаційну підтримку управлінських рішень. Водночас упровадження таких технологій потребує забезпечення достовірності отриманих результатів, захисту інформації, перевірки стійкості алгоритмів до помилкових даних та збереження належного рівня контролю з боку людини.

Не менш важливим напрямом є розвиток адаптивних і програмно-керованих радіоелектронних систем. Використання модульної архітектури, SDR-технологій і програмного оновлення функціональних можливостей обладнання сприяє підвищенню його гнучкості, ремонтопридатності та технологічної актуальності. На відміну від традиційних систем із жорстко визначеною апаратною конфігурацією, програмно-керовані комплекси мають ширші можливості модернізації без необхідності повної заміни основних складових. Це особливо важливо за умов швидкого розвитку цифрових технологій і постійного вдосконалення радіоелектронного обладнання. При цьому перспективність таких рішень визначається не лише їх функціональними можливостями, а й надійністю програмного забезпечення, захищеністю каналів оновлення, сумісністю з наявною технікою та економічною доцільністю впровадження.

Особливе значення має інтеграція засобів РЕБ у єдиний інформаційний простір військового управління. Розвиток інформаційної взаємодії між системами радіоелектронного моніторингу, зв’язку, розвідки та автоматизованого управління сприятиме формуванню узгодженого уявлення про електромагнітну обстановку, підвищенню якості інформаційного забезпечення командування та зменшенню ризиків взаємного впливу власних радіоелектронних засобів. Важливими передумовами такої інтеграції є стандартизація форматів обміну інформацією, забезпечення сумісності програмно-апаратних комплексів, упровадження захищених механізмів передавання даних та розвиток автоматизованих засобів оброблення інформації. Відповідні підходи узгоджуються із сучасними тенденціями розвитку електромагнітних операцій і необхідністю комплексного врахування електромагнітних та кібернетичних чинників у системах військового управління.

Важливим напрямом технологічного вдосконалення засобів РЕБ є підвищення їх енергоефективності, мобільності та експлуатаційної надійності.

Використання сучасної елементної бази, енергоощадних технологій і модульних систем електроживлення створює передумови для зменшення масогабаритних характеристик обладнання та збільшення тривалості його автономного функціонування. Удосконалення систем живлення, контролю технічного стану й діагностування несправностей сприятиме скороченню експлуатаційних витрат, підвищенню готовності обладнання до використання та зменшенню залежності від складної інфраструктури технічного обслуговування. Окремого значення набуває впровадження методів прогнозування технічного стану радіоелектронних пристроїв, що дозволить своєчасно виявляти ознаки можливих відмов і підвищувати загальну надійність відповідних систем.

Удосконалення форм і способів ведення радіоелектронної боротьби Силами оборони України необхідно розглядати як комплексний процес, що охоплює організаційні, технологічні, інформаційні та освітні складові. На організаційному рівні важливого значення набувають розвиток міжвідомчої взаємодії, удосконалення нормативно-методичного забезпечення, стандартизація процедур інформаційного обміну та формування узгоджених підходів до оцінювання результативності застосування радіоелектронних засобів. При цьому особлива увага повинна приділятися забезпеченню електромагнітної сумісності, захисту власних систем електронних комунікацій та узгодженню використання радіочастотного ресурсу різними складовими Сил оборони України.

Важливою передумовою вдосконалення організаційних форм РЕБ є впровадження системного підходу до управління електромагнітним спектром. Такий підхід передбачає комплексне врахування потреб у використанні радіочастотного ресурсу, технічних характеристик обладнання, вимог електромагнітної сумісності та необхідності підтримання стійкості власних систем зв’язку й управління. Досвід НАТО підтверджує актуальність розвитку спільних стандартів, підготовки фахівців, удосконалення механізмів координації та забезпечення взаємосумісності радіоелектронних систем різного призначення. Використання таких підходів у процесі розвитку вітчизняних систем РЕБ сприятиме підвищенню узгодженості організаційних рішень та формуванню єдиних принципів використання електромагнітного спектра.

Окремої уваги потребує вдосконалення системи підготовки фахівців із радіоелектронної боротьби. Сучасні освітні програми мають враховувати

розвиток цифрового оброблення сигналів, програмно-визначуваних радіосистем, технологій штучного інтелекту, автоматизованого аналізу радіочастотної обстановки та методів оцінювання електромагнітної сумісності. Перспективним є використання комп'ютерного моделювання, віртуальних лабораторій, програмно-апаратних тренажерів і ситуаційно-орієнтованих методів навчання. Застосування зазначених технологій дозволить підвищити рівень практичної спрямованості освітнього процесу, забезпечити формування навичок аналізу радіоелектронної обстановки та вдосконалити здатність майбутніх фахівців приймати обґрунтовані рішення в умовах обмеженості інформації.

Перспективним також є запровадження систематизованого аналізу досвіду експлуатації та технічного обслуговування засобів РЕБ. Накопичення й узагальнення інформації щодо надійності обладнання, умов його використання, характерних несправностей, особливостей технічного обслуговування та результатів підготовки персоналу дозволить сформувати обґрунтовані вимоги до перспективних радіоелектронних систем. На основі отриманих даних можуть удосконалюватися методики оцінювання технічної ефективності, підходи до планування модернізації обладнання та програми професійної підготовки відповідних спеціалістів.

Таким чином, сучасний розвиток систем і засобів радіоелектронної боротьби характеризується інтелектуалізацією, цифровізацією, мініатюризацією та поступовим переходом до програмно-керованих, адаптивних і функціонально інтегрованих технічних рішень. Досвід російсько-української війни підтверджує, що радіоелектронна боротьба є невід'ємною складовою сучасних бойових дій, ефективність якої визначається не лише технічними характеристиками обладнання, а й рівнем організаційної взаємодії, підготовки персоналу, інформаційного забезпечення управління та здатністю до своєчасного технологічного оновлення. Подальше вдосконалення форм і способів ведення РЕБ Силами оборони України доцільно пов'язувати з розвитком автоматизованих систем аналізу електромагнітної обстановки, упровадженням адаптивних технологій, підвищенням електромагнітної сумісності, забезпеченням стійкості систем військового зв'язку та вдосконаленням підготовки фахівців. Комплексна реалізація зазначених напрямів створюватиме передумови для підвищення технологічної спроможності Сил оборони України, ефективності використання радіоелектронних засобів і стійкості систем військового управління в умовах сучасних викликів та загроз.

Делех В. А.
Висоцький О. В.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПРОТИДІЇ РАДІОТЕХНІЧНИХ ПІДРОЗДІЛІВ ЗАСОБАМ ТЕХНІЧНОЇ РОЗВІДКИ ТА РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ПРОТИВНИКА

Сучасні збройні конфлікти, зокрема російсько-українська війна, засвідчили, що радіоелектронний простір став самостійною сферою ведення бойових дій. Радіотехнічні підрозділи, які здійснюють розвідку повітряного простору та забезпечують інформацією сили і засоби протиповітряної оборони, належать до пріоритетних об’єктів впливу противника. Для їх виявлення та ураження застосовуються засоби радіотехнічної і радіолокаційної розвідки, станції радіоелектронного подавлення, розвідувально-ударні безпілотні комплекси та боєприпаси, наведені на джерела радіовипромінювання. Зростання щільності й різноманітності цих засобів знижує живучість радіотехнічних підрозділів і стійкість радіолокаційної інформації, що зумовлює потребу в розробленні системних пропозицій щодо протидії.

Метою дослідження є розроблення пропозицій щодо підвищення живучості радіотехнічних підрозділів та збереження їхньої здатності вести розвідку повітряного простору в умовах впливу засобів технічної розвідки і радіоелектронної боротьби противника.

У роботі проаналізовано склад і можливості засобів розвідки та радіоелектронної боротьби противника. Встановлено, що радіотехнічні підрозділи виявляються за комплексом демаскувальних ознак: параметрами випромінювання (несуча частота, тривалість та період повторення імпульсів, режим огляду простору), тривалою роботою на одній позиції, характерним транспортним рухом, тепловим та акустичним випромінюванням, а також ознаками систем енергозабезпечення і зв’язку. Визначено, що радіоелектронний вплив реалізується у формі маскувальних та імітувальних завад, активних і пасивних, спрямованих як на приймальний тракт радіолокаційних станцій, так і на канали передавання радіолокаційної інформації.

Аналіз показав, що наявні способи захисту мають переважно одиничний характер і не узгоджені між собою за часом, простором та частотним діапазоном. Тому запропоновано розглядати протидію як єдину систему заходів, спрямованих на зниження ймовірності виявлення, розпізнавання та ураження радіотехнічних засобів, а також на збереження їхньої розвідувальної здатності в умовах радіоелектронного впливу. До складу системи віднесено організаційні, тактичні, маскувальні, технічні та захисні заходи.

Організаційні заходи передбачають планування та контроль режимів випромінювання, постійний аналіз радіоелектронної обстановки, розмежування завдань між засобами різних діапазонів і підготовку особового складу до дій в умовах активної радіоелектронної боротьби. Тактичні заходи охоплюють маневр засобами та часту зміну позицій, розосередження й ешелонування бойового порядку, використання резервних і хибних позицій, чергування засобів у режимі випромінювання, обмеження часу роботи на одній позиції залежно від оцінки рівня загрози та використання рельєфу місцевості.

Маскувальні заходи включають інженерне та оптичне маскування, застосування макетів та імітаторів радіовипромінювання, радіомаскування і зниження демаскувальних ознак транспортного руху та енергозабезпечення. Технічні заходи спрямовано на адаптивний вибір робочих частот і параметрів зондувальних сигналів, застосування методів захисту від активних та пасивних завад, використання пасивних і багатопозиційних способів розвідки, а також комплексування даних різнорідних джерел, що дає змогу компенсувати втрату інформації від окремих засобів. Захисні заходи передбачають прикриття позицій засобами протиповітряної оборони, інженерне облаштування та укриття, забезпечення швидкого відновлення працездатності.

Для обґрунтування запропонованих заходів доцільно використовувати показники живучості підрозділу, ймовірності збереження розвідувальної здатності та тривалості перебування на позиції. Порівняння варіантів пропонується виконувати експертними методами та імітаційним моделюванням з урахуванням ресурсних і ситуаційних обмежень. Окрему увагу приділено узгодженню заходів за часом, простором і частотою, оскільки саме це забезпечує їх сукупний ефект.

За результатами дослідження доведено, що ефективна протидія засобам технічної розвідки та радіоелектронної боротьби противника досягається лише

за умови комплексного застосування організаційних, тактичних, маскувальних, технічних і захисних заходів. Розроблені пропозиції дозволяють підвищити живучість радіотехнічних підрозділів та стійкість розвідувальної інформації. Перспективою подальших досліджень є створення моделі оцінювання ефективності заходів протидії та автоматизація підтримки рішень командира щодо вибору режимів роботи й позицій.

Ничипорчук В. М.
Чернишов Л. В.
Житомирський військовий інститут імені С. П. Корольова

ТЕХНІЧНІ АСПЕКТИ РАДІОЕЛЕКТРОННОГО ВПЛИВУ НА НИЗЬКООРБІТАЛЬНУ СИСТЕМУ ШИРОКОСМУГОВОГО ЗВ’ЯЗКУ «РАССВЕТ»

Низькоорбітальні системи широкосмугового зв’язку набувають дедалі більшого значення для забезпечення військових інформаційних потреб. Такі системи можуть використовуватись для передачі даних управління, розвідувальної інформації та потокового відео від безпілотних літальних апаратів.

російська федерація розгортає власну систему широкосмугового зв’язку під назвою «Рассвет», яка розроблена компанією «Бюро 1440». Перший пакет із 16 серійних космічних апаратів було запущено 23 березня 2026 року, другий — 19 липня 2026 року. До 2027 року розробники планують збільшити орбітальне угруповання до більш ніж 250 апаратів. Заявлена архітектура системи відповідає концепції 5G NTN (Non-Terrestrial Networks), передбачає використання лазерних терміналів для міжсупутникового зв’язку та плазмових двигунів.

Процес розгортання системи супроводжується технічними проблемами. 6 червня 2026 року один із 16 апаратів першої серійної партії зійшов з орбіти та припинив існування внаслідок входження в атмосферу. За даними відкритого орбітального моніторингу, наведеними Business Insider із посиланням на дані Космічних сил США, апарати другого запуску залишилися на висоті близько 300–400 км замість запланованих 800 км. Водночас розробник офіційно цю інформацію не підтвердив.

Точні робочі діапазони частот та параметри сигналів системи у відкритих джерелах відсутні. Тому наведені далі оцінки мають ілюстративний характер і не можуть розглядатися як точні характеристики конкретної супутникової системи.

Для оцінювання фізичних і технічних обмежень радіоелектронного впливу на низькоорбітальні системи широкосмугового зв'язку доцільно використати бюджет лінії зв'язку. Потужність сигналу на вході приймача визначається ефективною потужністю передавача, коефіцієнтом підсилення антени в напрямку джерела сигналу та втратами під час поширення радіохвиль.

За висоти орбіти 800 км відстань до апарата змінюється від приблизно 800 км у зеніті до близько 2400 км за кута місця 10°. Для дальності близько 800 км втрати у вільному просторі в Ku-діапазоні становлять орієнтовно 172–176 дБ залежно від робочої частоти. Зі збільшенням похилої дальності до приблизно 2,4 тис. км вони зростають приблизно на 9,4 дБ. Зі зміною кута місця вони можуть додатково змінюватися приблизно на 9–10 дБ.

Одним із визначальних факторів є різниця коефіцієнтів підсилення антени в напрямках на джерело корисного сигналу і на джерело перешкоди. За відкритими джерелами, користувацькі термінали системи використовують активні фазовані антенні решітки з електронним керуванням променем діаграми спрямованості, що забезпечує його орієнтацію на космічний апарат. Наземне джерело перешкоди, як правило, розташоване поза основною діаграмою спрямованості антени та потрапляє до зони бічних пелюсток.

Дискримінація антени безпосередньо впливає на необхідну потужність перешкоди. Для фазованих антенних систем значна просторова дискримінація між основною пелюсткою діаграми спрямованості та напрямками бічних пелюсток може істотно збільшувати необхідний рівень перешкоди. Зокрема, зростання дискримінації на 10 дБ потребує десятикратного збільшення потужності перешкоди для досягнення аналогічного ефекту. Якщо антенна система підтримує адаптивне формування «нуля» діаграми спрямованості в напрямку джерела перешкоди, необхідний рівень завади додатково зростатиме.

Вплив на лінію «апарат — термінал» здійснюється безпосередньо на приймач користувацького терміналу на землі, тому вплив на космічний сегмент системи для досягнення локального ефекту не є обов'язковим. Результативність такого впливу визначається не лише геометрією взаємного розташування об'єктів, а й характеристиками сигналу.

У системах 5G NR NTN, побудованих на OFDM-подібних сигнальних структурах, ефективність подавлення залежить від кількості піднесучих, на які поширюється вплив. За наявності достатнього запасу перешкодостійкості часткове подавлення окремих піднесучих може і не призвести до істотного погіршення якості зв’язку.

Вплив на лінію «термінал — апарат», навпаки, передбачає створення перешкод космічному приймачу з широким охопленням. Для його реалізації необхідні точне наведення діаграми спрямованості на швидкорухомий об’єкт і значна потужність випромінювання. Додатковим обмеженням є необхідність роботи в умовах забезпечення електромагнітної сумісності, що істотно ускладнює практичне застосування такого підходу в тактичних умовах.

Для Ku-діапазону та швидкості близько 7,5 км/с максимальний доплерівський зсув може мати порядок сотень кілогерц залежно від геометрії руху та робочої частоти і повинен постійно компенсуватися терміналом.

Тривалість видимого проходження космічного апарата над конкретним терміналом обмежена та залежить від висоти орбіти, геометрії проходження і встановленого мінімального кута місця та може лежати в межах 5-15 хвилин, після чого обслуговування переходить до іншого апарата. У зв’язку з цим у процесі розгортання угруповання додається необхідність оперативного перемикання променів діаграми спрямованості антенних систем.

Для засобів РЕБ це означає швидку зміну параметрів цілі та, відповідно, обмежену ефективність завчасно налаштованого впливу. Вузькі промені діаграми спрямованості антен і значна кількість космічних апаратів також зменшують імовірність тривалого подавлення окремого каналу.

За умови одночасного обслуговування кількох терміналів у межах одного променя подавлення одного користувацького каналу не обов’язково призведе до припинення обслуговування інших терміналів

Оскільки створення ефективних перешкод для таких систем є надскладним завданням, пріоритет має переміщуватися з безпосереднього подавлення каналів зв'язку на розвиток спроможностей радіоелектронної розвідки.

У пунктах, розташованих поза основною діаграмою спрямованості терміналу, сигнал може прийматися переважно через бічні та задні пелюстки діаграми спрямованості.

Для виявлення та пеленгування таких сигналів необхідні високочутливі приймальні засоби, рознесені у просторі, які забезпечують вимірювання різниці

часу та частоти приходу сигналів (TDOA — Time Difference of Arrival; FDOA — Frequency Difference of Arrival).

Додаткові можливості можуть забезпечувати носії, здатні наближатися до району розташування цілі або здійснювати підйом над місцевістю. Отримані координати можуть використовуватися для подальшої передачі інформації до відповідних засобів ураження.

Міжсупутникові лазерні лінії зв'язку не є безпосереднім об'єктом радіоелектронного подавлення, оскільки функціонують в оптичному діапазоні. Водночас шлюзові станції, центри управління та елементи мережевої інфраструктури можуть розглядатися як об'єкти впливу іншими засобами, в тому числі вогневими.

Перспективними напрямами подальших досліджень є створення мобільних засобів радіорозвідки, здатних працювати зі слабкими бічними випромінюваннями терміналів та автоматично визначати тип сигналу. Окремого опрацювання потребують методи багатопозиційної локалізації з оперативним обміном результатами вимірювань.

Доцільним також є проведення модельних досліджень впливу на приймальні тракти та оцінювання стійкості різних типів сигналів до перешкод. Важливим залишається узгодження роботи засобів РЕБ із власними користувачами радіочастотного спектра для запобігання взаємним перешкодам.

Додатковим джерелом інформації про розвиток системи «Рассвет» може бути моніторинг її угруповання за відкритими даними.

Нагорнюк О. А., канд. техн. наук
Журавський С. В.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА ДОСЛІДЖЕННЯ ЗАСОБІВ ВИЯВЛЕННЯ РАДІОСИГНАЛІВ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ЛАБОРАТОРНИХ УМОВАХ

Стрімкий розвиток безпілотних літальних апаратів (БпЛА) та інтенсифікація їх застосування в сучасних збройних конфліктах потребують удосконалення існуючих та розроблення нових засобів та способів виявлення

фактів їх застосування противником. Одним із найбільш ефективних способів виявлення радіокерованих БпЛА є радіоперехоплення сигналів їх бортових радіопередавачів. Для цього широко використовуються різнотипні засоби виявлення (детектори радіосигналів БпЛА), які можуть бути як стаціонарними, так і мобільними (переносними). Процеси розроблення та тестування засобів виявлення радіосигналів БпЛА передбачають проведення практичних досліджень їх тактико-технічних характеристик та перевірки їх відповідності вимогам, що висуваються до даної групи засобів.

Дослідження засобів виявлення радіосигналів БпЛА доцільно попередньо проводити в лабораторних умовах, що мають ряд переваг перед польовими. Зокрема, з’єднання приймально-передавальних пристроїв коаксіальними кабелями в вимірювальному стенді дозволяє створити контрольоване середовище, в якому всі сторонні випромінення усунені та не впливають на результати вимірювання. Крім того, проведення досліджень у лабораторних умовах дозволяє використовувати більшу кількість контрольно-вимірювальної апаратури та, у разі необхідності, проводити доопрацювання (налаштування) засобу виявлення відповідно до отриманих поточних результатів.

У доповіді пропонується вимірювальний стенд та методика досліджень засобів виявлення радіосигналів БпЛА в лабораторних умовах.

До складу вимірювального стенду входять:

джерело радіосигналу БпЛА (реальний передавач або програмно-визначений трансивер);

сталі та регульовані атенюатори для зміни потужності радіосигналу;

формувач радіоелектронної обстановки на основі програмновизначеного трансивера (шум, радіоперешкоди, сторонні випромінювання тощо);

підсилювач потужності;

суматор та дільник радіосигналів для формування сигнально-перешкодової суміші, одночасного її подання на детектор радіосигналів БпЛА та засоби вимірювання;

контрольно-вимірювальна апаратура на основі програмновизначеного трансивера та персональної обчислювальної машини із спеціальним програмним забезпеченням для відображення частотно-часової структури радіосигналу і перешкод та вимірювання їх потужності;

засоби живлення;

коаксіальні кабелі з перехідниками для з'єднання високочастотних входів та виходів елементів стенду.

Запропонована методика досліджень дозволяє визначити порогову чутливість детектора радіосигналів, швидкодію (час виявлення радіосигналу в заданій смузі частот), ймовірності правильного виявлення та хибної тривоги, критичне відношення сигнал/перешкода, а також встановити можливість виявлення радіосигналів, що випромінюються на нестандартних частотах (актуально під час дослідження детекторів радіосигналів передавачів аналогового відео). Розроблено математичний апарат для обчислення теоретичної дальності дії засобу виявлення на основі отриманих результатів вимірювання. Оскільки приймально-передавальні пристрої стенду з'єднані коаксіальними кабелями, то визначення вказаних показників засобів виявлення радіосигналів БпЛА здійснюються в ідентичних умовах, що дозволяє порівнювати ефективність різних детекторів, а також отримати найбільш раціональні налаштування їх робочих параметрів.

Нагорнюк О. А., канд. техн. наук
Борисов П. С., канд. техн. наук
Зелінський А. В.
Житомирський військовий інститут імені С. П. Корольова

ВИМІРЮВАЛЬНИЙ СТЕНД ДЛЯ ДОСЛІДЖЕННЯ ПЕРЕШКОДОСТІЙКОСТІ АДАПТИВНИХ АНТЕННИХ РЕШІТОК ІЗ КЕРОВАНОЮ ДІАГРАМОЮ СПРЯМОВАНОСТІ

У системах навігації та наведення переважної більшості засобів повітряного нападу (ЗПН) використовується інформація з апаратури споживачів (АС) супутникових радіонавігаційних систем (СРНС), яка є основним джерелом навігаційної інформації або складовою більш складної навігаційної системи, що може включати інші підсистеми забезпечення польоту ЗПН та наведення його на ціль.

Подавлення приймачів радіосигналів СРНС ЗПН призводить до відхилення ЗПН від запрограмованого маршруту польоту, унеможливлення виходу в заданий район для пошуку й захоплення цілі та підвищення

ймовірності ураження ЗПН засобами протиповітряної оборони. Для зменшення впливу радіоперешкод в АС СРНС використовують перешкодостійкі адаптивні антенні решітки (ААР) з керованою діаграмою спрямованості, побудовані за технологією CRPA (Controlled Reception Pattern Antenna). Такі ААР здійснюють просторову фільтрацію радіоперешкод шляхом формування “нулів” (провалів) у діаграмі спрямованості у напрямку на передавачі перешкод.

Наразі ефективним способом протидії АС СРНС із ААР є одночасне використання сукупності просторово рознесених джерел радіоперешкод, кількість яких визначається числом антенних елементів ААР. Результативність такого способу опосередковано підтверджується постійним збільшенням кількості елементів ААР.

Оцінювання ефективності різних видів радіоперешкод для подавлення АС СРНС із ААР, пошук потенційних вразливостей ААР та результативних способів боротьби з ними потребує розроблення відповідної матеріальної бази та методичного апарату для проведення досліджень.

У доповіді пропонуються вимірювальний стенд та методика для дослідження перешкодостійкості ААР з керованою діаграмою спрямованості.

Вимірювальний стенд дозволяє в лабораторних умовах досліджувати вплив структури та параметрів радіоперешкод, кількості передавачів перешкод та їх просторового розміщення на ефективність радіоподавлення АС СРНС із ААР. До складу вимірювального стенду входять такі основні елементи:

ААР з керованою діаграмною спрямованості, що досліджується;

засоби приймання радіосигналів СРНС, отримання навігаційного рішення, відображення інформації та запису поточних даних до файлу;

формувач радіоперешкод на основі програмновизначеного трансивера, що керується персональною обчислювальною машиною;

підсилювач для збільшення потужності радіоперешкод;

набір дільників радіосигналів;

набір однотипних антен, робочі частоти яких відповідають діапазонам частот СРНС;

набір еквівалентних навантажень для поглинання енергії радіоперешкод на незадіяних виходах дільників;

набір коаксіальних кабелів для з’єднання формувача радіоперешкод, підсилювача потужності та дільників;

контрольно-вимірювальна апаратура для визначення потужності радіоперешкод на вході ААР;

СПЗ для генерування різних типів радіоперешкод, обчислення їх потужності та автоматизованого аналізу результатів дослідження.

Дослідження перешкодостійкості ААР з керованою діаграмою спрямованості базується на комплексному оцінюванні її здатності здійснювати захоплення та супроводження навігаційних радіосигналів в умовах дії просторово-рознесених джерел радіоперешкод. Методика дослідження включає ряд етапів, виконання яких дозволяє визначити такі показники:

критичний рівень радіоперешкоди – мінімальне значення потужності радіоперешкоди на вході елементів АРР, при якому приймач СРНС втрачає захоплення або супроводження;

кількість джерел радіоперешкод, що подавляються – максимальна кількість незалежних просторово-рознесених передавачів перешкод, випромінювання яких просторово фільтруються ААР;

час адаптації – інтервал часу від моменту постановки радіоперешкоди до формування стійкого провалу в діаграмі спрямованості; даний час необхідний для перерахунку вагових коефіцієнтів після ввімкнення радіоперешкоди;

похибка визначення координат – зсув та середньоквадратичне відхилення точкового оцінювання координат під дією радіоперешкод;

поляризаційна розв'язка – вплив виду поляризації радіоперешкоди на критичний рівень радіоперешкоди;

Методика дослідження перешкодостійкості ААР складається із таких основних етапів:

калібрування та зняття базових характеристик;

визначення перешкодостійкості до одиночної радіоперешкоди;

визначення перешкодостійкості до кількох просторово-рознесених джерел радіоперешкод;

визначення динамічних характеристик та часу адаптації;

оцінювання похибки обчислення координат.

Галяс А. В.
Біховський О. В.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ ОПТИКО-ЕЛЕКТРОННИХ ЗАСОБІВ ПОДАВЛЕННЯ ДЛЯ ПРИКРИТТЯ КРИТИЧНИХ ОБ’ЄКТІВ ШЛЯХОМ ВПЛИВУ НА СИСТЕМИ КОМП’ЮТЕРНОГО ЗОРУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Постійний розвиток та модернізація безпілотних літальних апаратів (далі – БпЛА), удосконалення систем управління, навігації та передавання даних створюють нові виклики для засобів протидії безпілотним системам. Застосування різних частотних діапазонів, зміна архітектури каналів управління та передавання даних, а також поширення БпЛА з використанням оптоволоконних ліній зв’язку можуть обмежувати ефективність традиційного радіоелектронного впливу. У таких умовах актуальним є пошук додаткових способів протидії, спрямованих на інші функціональні компоненти безпілотної системи. Одним із перспективних напрямів є вплив на оптико-електронний інформаційний канал БпЛА, який забезпечує отримання даних про навколишню обстановку та їх подальшу обробку системами комп’ютерного зору. Зміна характеристик вхідної оптичної інформації може знижувати ефективність автоматизованого виявлення, розпізнавання, класифікації та супроводження об’єктів. Це обумовлює доцільність дослідження можливостей застосування засобів оптико-електронного подавлення (далі – ОЕП) як одного з елементів комплексного прикриття критичних об’єктів.

Метою дослідження є обґрунтування можливості застосування оптико-електронних засобів подавлення для прикриття критичних об’єктів та визначення характеру їхнього впливу на оптичний інформаційний канал і системи комп’ютерного зору БпЛА.

У роботі використано методи аналізу, систематизації та узагальнення науково-технічної інформації щодо принципів функціонування оптико-електронних систем БпЛА, систем комп’ютерного зору та засобів оптико-електронного впливу. Застосовано системний і структурно-функціональний підходи для визначення взаємозв’язку між характеристиками вхідної оптичної інформації та результативністю її автоматизованої обробки. Використано

порівняльний аналіз функціональних можливостей радіоелектронного та оптико-електронного впливу.

Оптико-електронна система БпЛА забезпечує отримання інформації про навколишнє середовище за допомогою бортових оптичних сенсорів. Сформоване зображення надалі може використовуватися оператором або надходити до системи комп'ютерного зору для автоматизованого аналізу. Типовий цикл обробки включає отримання інформації оптичним сенсором, її попередню обробку, виділення інформативних ознак, а також подальше виявлення, розпізнавання, класифікацію та супроводження об'єктів.

Таким чином, ефективність роботи системи комп'ютерного зору безпосередньо пов'язана з якістю та інформативністю вхідних оптичних даних. Вплив на цей інформаційний етап може розглядатися як окремий напрям протидії БпЛА, особливо у випадках, коли вплив на радіоканали управління або передавання даних є обмеженим.

Оптико-електронне подавлення полягає у створенні умов, за яких оптична інформація, що надходить до сенсорної системи БпЛА, частково втрачає інформативність або стає складнішою для автоматизованої обробки. На функціональному рівні це може проявлятися у зниженні контрастності, втраті окремих візуальних ознак, виникненні оптичних перешкод, зміні структури зображення або зниженні його придатності для подальшого аналізу. У результаті алгоритму стає складніше встановити відповідність між отриманими даними та реальним об'єктом спостереження.

Особливе значення це має для систем, у яких комп'ютерний зір використовується не лише для формування зображення оператору, а й для автоматичного аналізу отриманої інформації. Порушення якості оптичної інформації може призводити до зниження достовірності виявлення та розпізнавання об'єктів, помилкової класифікації або втрати стійкості їх супроводження. Водночас ефективність такого впливу не є однаковою для всіх БпЛА, оскільки залежить від типу оптичного сенсора, алгоритмів комп'ютерного зору та здатності системи адаптуватися до змін вхідних даних.

Для прикриття критичних об'єктів засоби ОЕП можуть формувати додатковий рівень протидії, спрямований на обмеження можливостей БпЛА щодо отримання та автоматизованого використання візуальної інформації.

У такому випадку об'єктом впливу є не сам БпЛА як фізична платформа, а його функціональна підсистема – оптико-електронний канал спостереження та

пов’язані з ним засоби обробки інформації. Такий підхід є актуальним для захисту об’єктів критичної інфраструктури, пунктів управління та інших важливих об’єктів, які можуть бути цілями повітряної розвідки.

Застосування ОЕП у цьому випадку доцільно розглядати як складову комплексної системи протидії БпЛА, яка доповнює радіоелектронні та інші засоби впливу. На відміну від засобів, спрямованих на канали управління, навігації чи передавання даних, оптико-електронне подавлення впливає на інший функціональний компонент безпілотної системи – її оптичний інформаційний канал. Це дозволяє враховувати особливості конкретного БпЛА та зменшувати залежність ефективності протидії від способу організації його каналів управління і передавання даних.

Результатом застосування такого підходу може бути зниження достовірності інформації, яку БпЛА отримує за допомогою оптичної системи, та зменшення ефективності автоматизованого виявлення, розпізнавання і супроводження об’єктів. Водночас результативність ОЕП визначається сукупністю характеристик оптичного сенсора, системи обробки зображень та алгоритмів комп’ютерного зору, тому потребує окремого дослідження для різних типів безпілотних систем.

Отже, оптико-електронне подавлення є перспективним напрямом комплексної протидії БпЛА, оскільки дає змогу впливати на оптичний інформаційний канал незалежно від архітектури його радіоканалів управління та передавання даних. Встановлено, що зміна інформативності вхідних оптичних даних потенційно може призводити до зниження ефективності виявлення, розпізнавання, класифікації та супроводження об’єктів системами комп’ютерного зору.

Застосування ОЕП доцільно розглядати як додатковий функціональний рівень захисту критичних об’єктів у складі комплексної системи протидії БпЛА. При цьому результативність такого впливу визначається характеристиками сенсорної системи та алгоритмів обробки зображень, що обумовлює необхідність подальшого дослідження критеріїв оцінювання ефективності ОЕП для різних типів оптико-електронних систем БпЛА.

Трохименко О. В.
Житомирський військовий інститут імені С. П. Корольова

ЕЛЕКТРОМАГНІТНИЙ ТА КІБЕРПРОСТІР. ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ ПОДАЛЬШОЇ ІНТЕГРАЦІЇ

Питання інтеграції електромагнітного спектра та кіберпростору не нове, проте його актуальність не знижується. Сучасні збройні конфлікти дедалі більшою мірою залежать від здатності протиборчих сторін контролювати інформаційне середовище. Зв'язок, навігація, розвідка, системи ситуаційної обізнаності та управління військами, озброєнням, безпілотними системами, а з ними і радіоелектронна боротьба з її складовими, поступово перемістились у цифрове середовище, що залежне від комп'ютерних систем та мереж. Разом з цим, їх успішне застосування значною мірою залежить від контрольованості та сприятливих умов електромагнітного середовища - електромагнітного спектру (ЕМС). Ключем проблеми є високий ступінь взаємозалежності кіберпростору і ЕМС: радіоканали є вектором проникнення в мережі, а через мережі здійснюється управління засобами випромінювання у спектрі (програмне управління).

Першими можливості і переваги кіберпростору оцінили та визнали його окремим середовищем ведення операцій у ЗС США. Результатом отриманих висновків стало створення Кіберкомандування (USCYBERCOM, 2010). Водночас, досвід воєнних дій в Іраку та Афганістані, зокрема перші інформаційні і кібернетичні операції та боротьба з радіокерованими саморобними вибуховими пристроями, показали необхідність координації при використанні ЕМС. У Сухопутних військах США було сформовано концепт єдиного планування кібернетичних та електромагнітних дій, оскільки їх роздільне планування застосування потребує витрати значних додаткових зусиль на узгодження. При цьому, втрата контролю (переваги) у будь-якому з них може мати вирішальний вплив на загальний результат застосування військ (сил).

Першим практичним механізмом вирішення питання інтеграції цих двох середовищ стала поява у США військової концепції **СЕМА** (*Cyber Electromagnetic Activities*) - **кібер-електромагнітної діяльності.** Термін було доктринально закріплено польовим статутом **FM 3-38** *"Cyber Electromagnetic Activities"* (2014 р.). Концепція ґрунтується на фундаментальній основі, згідно якої фізичний рівень кіберпростору безпосередньо включає в себе методи передачі даних з використанням ЕМС (радіохвилі, радіоканали тощо).

Результатом реалізації цієї концепції стала поява у штабах бригад СВ США і вище додаткових підрозділів, відповідальних за СЕМА.

Черговим етапом розвитку концепції стало видання доктрини СВ США **FM 3-12** *"Cyberspace Operations and Electronic Warfare"* (2017, оновлена 2021р) – оновленої формули СЕМА. Вона об'єднала операції в кіберпросторі та РЕБ, закріплюючи фундаментальний підхід, що безпровідні мережі та інфраструктура кіберпростору функціонують через електромагнітний спектр, який надає можливості маневру для проведення кібероперацій. На основі даної доктринальної платформи було сформовано та видано доктрину МО США **JP 3-85** *"Joint Electromagnetic Spectrum Operations"* (2020), що прямо пов'язує цей зв'язок.

Паралельно з розвитком цієї концепції у США провідними країнами світу формувались схожі нормативно-правові підходи з використанням власної термінології.

Великобританія. Міністерством оборони офіційно використовується інтегрований підхід до кібернетичного та електромагнітного доменів, про що доктринально зазначено у **JDP 0-50** ***(****Joint Doctrine Publication 0-50: Cyber and Electromagnetic Activities — UK Gov)*. У ній зазначено, що "кібероперації та електромагнітні операції проводяться у єдиному просторі, а фізичний рівень кіберпростору є невід'ємною частиною електромагнітного спектра".

НАТО інтегрувало американську та британську моделі СЕМА у свою доктрину **AJP-3.20** *(Allied Joint Doctrine for Cyberspace Operations).* Доктринально фіксується, що кібероперації використовують фізичну інфраструктуру та радіоканали, що потребує обов'язкової координації з операціями в електромагнітному спектрі.

Китай. У військовій доктрині Народно-визвольної армії Китаю (НВАК) використовується офіційний термін "Мережеелектромагнітний простір" *(网络电磁空间 – кит, Network-Electromagnetic Space- англ.*), що об'єднує кібер- та електромагнітний простір у єдину сферу військової діяльності. У "Китайській воєнній стратегії" (China's Military Strategy, *т.н. "Біла книга з оборони КНР",2015*) "Мережеелектромагнітний простір" проголошено "стратегічною висотою сучасної військової боротьби" та започатковано створення окремого виду збройних сил– Сил стратегічної підтримки НВАК, який об'єднав кіберсили (підрозділи) та сили РЕБ.

Російська федерація. У доктринальних документах зс рф замість терміну "кіберпростір" переважає використання терміну "інформаційний простір". У свою, чергу інформаційний простір офіційно ділиться на "інформаційно -

технічне" середовище (включаючи критичну інформаційну інфраструктуру, електромагнітне середовище та РЕБ) та "інформаційно-психологічне" середовище (інфраструктура та контент для когнітивного впливу). У документі зс рф "Концептуальные взгляды на деятельность Вооруженных Сил РФ в информационном пространстве" (МО рф, 2011), який за своїм статусом можна вважати доктринальним, інформаційний простір визначається як "сфера діяльності, пов'язана з формуванням, змінами (перетворенням-*авт*.) та знищенням інформації ", у якому технічна складова включає до свого складу електромагнітну та мережеву компоненти.

Зазначена діяльність проводилась і військовій сфері інших країн, проте принцип СЕМА залишався центральним.

Від започаткування і дотепер, концепція СЕМА стрімко розвивалась, і масштабувалась, методи і способи її реалізації удосконалювались на практиці застосування військ (сил) на театрах воєнних дій в Іраку, Афганістані, Сирії та Україні.

Динамічний технологічний прорив останнього десятиліття, зокрема в області кібертехнологій та досвід активної війни України проти рф, надав потужний поштовх у розвитку концепції.

Повномасштабна війна в Україні різко прискорила розвиток як безпілотних систем так і контрзаходів щодо їх застосування, РЕБ, ППО та ін, розширивши боротьбу за спектр до тактичного рівня.

Насьогодні, враховуючи поточний загальний рівень розвитку технологій **основними тенденціями розвитку** СЕМА можна визначити:

1. **Конвергенція кібервпливу та засобів радіоелектронної боротьби.**

Розвиток технологій зразка *RF-enabled cyber attacks* - цільового кібервпливу (інформаційного впливу), спрямованого на складно доступні або автономні мережі, шляхом інфільтрації в них через інфраструктуру РЕБ.

Радіоканали, утворені засобами РЕБ стають "мостом" до мереж, вхідних вузлів приймальних засобів, комунікаційних точок (шлюзів, порталів) інформаційної інфраструктури об'єктів з подальшою інфільтрацією до них. Водночас, системи (засоби, станції) РЕБ керуються з автоматизованих робочих місць (комп'ютерів, ноутбуків, планшетів), шо використовують програмне забезпечення та програмно керовані засоби (контролери, мережеві інтерфейси та ін.), що автоматично робить їх об'єктами кібервпливу.

2. **Програмно-визначувані системи та засоби *SDR (Software Defined Radio*).**

Використання спецрадіосистем (засобів), у яких реалізація базових функцій (діапазон частот, тип модуляції, вихідна потужність тощо) відбувається за рахунок програмного забезпечення. Швидка і гнучка програмна зміна архітектури засобів дає змогу у мінімально можливі терміни адаптувати засоби РЕБ, без потреби фізичних змін та перетворень (виготовлення нових мікросхем, засобів, моделей тощо).

3. **Штучний інтелект і когнітивне РЕБ.**

Інноваційні технології РЕБ, що інтегрують штучний інтелект та машинне навчання для автономного реагування на загрози в електромагнітному спектрі в режимі реального часу - автоматична детекція, розпізнавання та ідентифікація сигналів і засобів випромінювання, їх адаптивне подавлення, підбір частот без участі оператора.

4. **Безпілотні системи як головний стимул розвитку.**

Розвиток БПС стимулює розвиток протидії ним і навпаки, ефективна СЕМА мотивує подальше удосконалення БПС та пошук нових технологічних рішень. Масовість застосування БпЛА обумовила розвиток портативних засобів РЕБ, створення та застосування внутрішніх систем (вузлів, блоків), стійких до подавлення каналів управління, управління через оптоволокно, автономних систем навігації та донаведення.

5. **Боротьба за навігацію та канали зв’язку.**

GPS, GLONASS, GALILEO та інші глобальні навігаційні системи є критичною інфраструктурою при застосуванні усього переліку систем та засобів озброєння: практично усіх типів безпілотних систем, артилерії, авіації, флоту і т.д. Окрім звичайної протидії супутниковому зв’язку (подавлення каналів навігації) широко застосовуються технології заміни/підміни навігаційних даних. Паралельно йде боротьба за супутниковий зв’язок – блокування приймачів, перехоплення управління тощо.

6. **Керування сигнатурою.**

Використання технологій, що мінімізують випромінювання (помітність) в ЕМС, застосування сигналів із низькою ймовірністю перехоплення (LPI/LPD-сигнали), використання ППРЧ та ін.

7. **Зміщення СЕМА на тактичний рівень.**

Підрозділи/групи СЕМА поступово впроваджуються на тактичний рівень (бригада і нижче). Зазначені підрозділи також широко залучаються для організації прикриття ОКІ.

8. **Інтеграція з розвідкою.**

Формування єдиної спектральної картини в реальному часі як основи для прийняття рішень командиром: розвідка, управління спектром та проведенням кібервпливу поєднуються в єдину систему.

9. **Використання комерційних і подвійних технологій.**

Класичний цикл впровадження розробок у застосування військ (сил) є доволі інерційним. В умовах гострої потреби актуальних технологічних та технічних рішень для підвищення ефективності застосування власних систем (засобів) озброєння або ж протидії системам (засобам) озброєння противника застосовуються спрощені механізми впровадження. Такий підхід пов'язаний зі пришвидшеною і гнучкою комерційною реакцією пропозиції на потребу. Адаптація комерційних невійськових рішень під виконання військових завдань надає можливість суттєвого скорочення циклу "загроза – протидія".

10. **Доктринальна інтеграція.**

Концепції багатодоменних операцій МО США (MDO - *Multi-domain operations*, JADO - *Joint all-domain operations*) та концепція операцій в електромагнітному просторі НАТО (EMSO - *Electromagnetic Spectrum Operations*) мають принципово різні підходи: перші розглядають рівність кіберпростору та ЕМС з іншими військовими доменами, друга передбачає пріоритет ЕМС над ними (*т.н. спектральна перевага*). Такі підходи, а також тенденції, що наведені вище, при спільному застосуванні, потребують обов'язкового доктринального узгодження, як мінімум на рівні союзних сторін та/або країн-членів Альянсу.

Висновок.

Концепція СЕМА була сформована як відповідь на зростання взаємозалежності кіберпростору й електромагнітного спектра. Від окремих напрямів РЕБ і зв'язку через кібероперації військова думка дійшла до висновку, що ці сфери потребують спільнокоординованого планування та застосування. Досвід війни в Україні підтвердив, що контроль над спектром і мережами безпосередньо впливає на результат бойових дій, а темпи адаптації засобів і тактики їх застосування стали критичним фактором.

Подальший розвиток СЕМА пов'язаний зі штучним інтелектом, програмно-визначуваними системами, автоматизацією процесів аналізу спектра та інтеграцією цих можливостей на всіх рівнях управління військами (силами).

Столяренко М. П.
Науково-дослідний центр ракетних військ і артилерії

РАДІОЕЛЕКТРОННИЙ ЗАХИСТ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ АРТИЛЕРІЙСЬКОЇ РОЗВІДКИ

Функціонування радіолокаційних станцій (далі – РЛС) артилерійської розвідки відбувається в умовах складної та динамічної електромагнітної обстановки. На якість радіолокаційної інформації можуть впливати природні й штучні джерела електромагнітних випромінювань, взаємні радіоелектронні завади, навмисне створення перешкод, а також особливості функціонування власних радіоелектронних засобів. У зв’язку з цим одним із важливих завдань артилерійських підрозділів є радіоелектронний захист РЛС артилерійської розвідки.

Радіоелектронний захист радіолокаційних станцій – це сукупність організаційних, технічних, програмних та інформаційних заходів, спрямованих на забезпечення стійкої роботи РЛС в умовах впливу засобів радіоелектронної боротьби (далі – РЕБ) противника.

Загальну систему заходів радіоелектронного захисту можна представити у вигляді трьох взаємопов’язаних рівнів.

Перший рівень – організаційний. Він передбачає планування роботи радіоелектронних засобів, контроль електромагнітної обстановки, організацію взаємодії між підрозділами та підготовку персоналу.

Другий рівень – технічний. Передбачає використання конструктивних і програмних можливостей РЛС для підвищення її завадостійкості, фільтрації небажаних сигналів, контролю працездатності обладнання та забезпечення електромагнітної сумісності.

Третій рівень – інформаційний. Призначений для збереження достовірності результатів радіолокаційного спостереження шляхом комплексного аналізу отриманих даних, виявлення аномалій та оцінювання рівня їхньої достовірності.

Як показує досвід ведення бойових дій артилерійськими підрозділами, для захисту РЛС та протидії радіоелектронним засобам розвідки противника доцільно проводити наступні заходи:

1. Використання фазованих антенних решіток в антенних модулях РЛС, які здатні змінювати діаграму спрямованості для пригнічення перешкод та зменшення рівня бічних пелюсток при випромінюванні.

2. Встановлення тимчасових, просторових, частотних та енергетичних обмежень при бойовому використанні РЛС.

3. Застосовування для настройки і перевірки функціонування радіолокаційних станцій еквівалентів антен і вбудованої апаратури контролю.

4. Виявлення частот, на які впливають завади противника, зміна бісектриси сектору або величини сектору розвідки.

5. Використання маскувальних властивостей місцевості з урахуванням особливостей розповсюдження електромагнітних хвиль, а також табельних маскувальних засобів.

6. Здійснення оптимального вибору позиції РЛС. РЛС доцільно розміщувати на рівній місцевості, яка має пологий нахил вниз протягом перших 200-300 метрів перед радаром, а потім різкий підйом до екрануючого гребня.

7. Використання адаптивних алгоритмів обробки радіолокаційної інформації. Здійснення передачі інформації відповідно до вимог безпеки зв'язку.

8. Зменшення часу роботи на випромінювання РЛС з періодичною зміною несучої частоти та періодичною зміною позицій.

Час випромінювання має бути скорочено залежно від можливостей виявлення противником. Як правило, час безперервного випромінювання не повинен перевищувати двох хвилин, коли противник має можливість здійснювати радіоелектронну протидію. Загальний час випромінювання має бути скоригований залежно від тактичної обстановки.

9. Проведення переналаштування несучої частоти без випромінювання електромагнітної енергії в простір. З цією метою станцію необхідно перемкнути на еквівалент антени.

Таким чином, радіоелектронний захист радіолокаційних станцій артилерійської розвідки є комплексною системою заходів, спрямованих на забезпечення стійкості, надійності та достовірності функціонування радіолокаційних засобів в умовах складної електромагнітної обстановки.

Сухотеплий М. В.
Гота О. С.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ДЕЦЕНТРАЛІЗОВАНИХ MESH-МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ЗВ’ЯЗКУ СИЛ ОБОРОНИ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ ВІЙНИ

Досвід повномасштабної війни показав, що управління військами на тактичному рівні найчастіше втрачається не через нестачу радіозасобів, а через те, що їх легко виявити й заглушити. Противник розгорнув велику кількість засобів радіоелектронної боротьби (РЕБ), тож радіозв’язок на одній частоті з кількома вузловими станціями нестійкий.

Одним із напрямів вирішення стали децентралізовані MESH-мережі, де кожна радіостанція є і абонентом, і ретранслятором, а головного вузла немає. Коли станція вибуває через ураження чи завади, решта сама перебудовує маршрути. Серед зразків Сил оборони найбільш відомі радіостанції Silvus серії StreamCaster: вони контролюють ефір, обходять заглушені частоти (залежно від ліцензій) і працюють без прямої видимості.

Проте MESH-мережа не знімає проблему РЕБ. Станція випромінює майже постійно, тож її можна запеленгувати, а вузол поруч із пунктом управління вказує на нього противнику. Ретранслятори краще виносити на окремі позиції й обмежувати потужність. Потужне глушіння знижує пропускну здатність, тож передавати можливо мінімум даних.

Друга особливість є швидкість розгортання. Після завантаження єдиних налаштувань і ключів станцію достатньо ввімкнути, антени наводити не потрібно. Ретранслятором може слугувати автомобіль, щогла або безпілотний літальний апарат (БпЛА), а через Ethernet мережа обслуговує і голос, і дані, зокрема відеоканали БпЛА.

Пропонується використовувати MESH-мережу на рівні рота чи батальйон як основний шар зв’язку, а вихід на вищу ланку дублювати окремим каналом. Потрібні типові схеми розгортання з ретрансляторами, зокрема на БпЛА, шаблони налаштувань і підготовлені зв’язківці.

Отже, MESH-мережа не робить зв’язок невразливим до РЕБ, але ускладнює противнику завдання й скорочує час відновлення після втрат. Найбільший ефект вона дає разом з дисципліною випромінювання.

Цимбалюк В. М
Поліщук Д. О
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Сучасний розвиток засобів радіоелектронної боротьби (РЕБ) відбувається в умовах постійного ускладнення радіоелектронної обстановки, збільшення кількості джерел випромінювання та швидкої зміни характеристик сигналів. За таких умов важливого значення набувають технології, здатні оперативно обробляти значні обсяги даних, виявляти закономірності й підтримувати прийняття рішень. Одним із перспективних напрямів є застосування штучного інтелекту (ШІ), зокрема методів машинного навчання та інтелектуального аналізу сигналів.

Метою роботи є узагальнення основних напрямів застосування штучного інтелекту для підвищення ефективності систем РЕБ, а також визначення переваг, обмежень і перспектив упровадження таких технологій.

Одним із ключових напрямів є автоматизоване виявлення та класифікація радіосигналів. Алгоритми машинного навчання можуть аналізувати часові, частотні та спектральні характеристики сигналів і допомагати розрізняти типові класи випромінювань. На відміну від суто ручного аналізу, такі підходи дають змогу обробляти великі масиви даних і швидше виявляти ознаки змін у радіоелектронній обстановці. Водночас достовірність результатів залежить від якості навчальних даних, репрезентативності вибірки та здатності алгоритмів працювати за наявності шумів і перешкод.

Іншим важливим напрямом є підтримка ситуаційної обізнаності. Системи на основі ШІ можуть об’єднувати дані з різних сенсорів, зіставляти спостереження в часі та формувати узагальнену картину радіоелектронної обстановки. Це може полегшувати виявлення нетипових подій, визначення

пріоритетності повідомлень і скорочувати навантаження на оператора. При цьому остаточна оцінка обстановки має враховувати контекст, похибки вимірювань і можливість хибних спрацювань.

ШІ також може використовуватися для прогнозування змін у роботі радіоелектронних систем і технічного стану обладнання. Аналіз історичних даних дає змогу виявляти ознаки деградації компонентів, планувати технічне обслуговування та зменшувати ризик неочікуваних відмов. У навчальних і дослідницьких середовищах моделі можуть застосовуватися для моделювання різних сценаріїв радіоелектронної обстановки, оцінювання стійкості алгоритмів та перевірки їхньої роботи в контрольованих умовах.

До основних переваг застосування ШІ належать швидкість обробки даних, можливість виявлення складних закономірностей, адаптація моделей до нових прикладів і підтримка оператора під час ухвалення рішень. Водночас існують суттєві обмеження. Результати роботи моделей можуть погіршуватися за зміни умов, появи невідомих типів сигналів або навмисного спотворення вхідних даних. Додатковими чинниками є потреба в обчислювальних ресурсах, якісних наборах даних, кіберзахисті та пояснюваності результатів.

Тому впровадження інтелектуальних технологій має здійснюватися поетапно: від лабораторного тестування й моделювання до перевірки в контрольованих умовах і подальшого оцінювання надійності. Важливо передбачати контроль з боку фахівця, можливість перевірки рекомендацій системи, журналювання результатів і резервні процедури на випадок помилок. ШІ доцільно розглядати як засіб підтримки професійних рішень, а не як безумовну заміну людського контролю.

Отже, штучний інтелект має значний потенціал для підвищення ефективності систем РЕБ завдяки автоматизованому аналізу сигналів, узагальненню даних і прогнозуванню технічних станів. Практичний результат залежить від якості даних, стійкості алгоритмів, належного тестування та збереження контролю фахівця. Подальші дослідження доцільно спрямувати на підвищення надійності моделей, їхню адаптивність і безпечну інтеграцію в наявні інформаційно-аналітичні комплекси.

Дубина О. Ф., канд. техн. наук, доц.
Авсієвич Р. О., Ph. D.
Дацько Д. В., курсант
Житомирський військовий інститут імені С. П. Корольова

АВТОМАТИЗАЦІЯ СИСТЕМ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Сучасні військові системи дедалі активніше використовують електромагнітний спектр для зв'язку, навігації, розвідки та управління. Це збільшує обсяг інформації, яку необхідно своєчасно виявляти, обробляти та оцінювати в системах радіоелектронної боротьби. За таких умов ефективність радіоелектронної боротьби значною мірою залежить не лише від технічних характеристик окремих засобів, а й від швидкості виявлення, аналізу та обробки інформації. Автоматизація дає змогу перенести частину рутинних операцій із людини на програмно-апаратні комплекси, скоротити час обробки даних та підвищити оперативність прийняття рішень. Окремого значення набувають цифрова обробка сигналів, машинне навчання, штучний інтелект та інтеграція засобів радіоелектронної боротьби з єдиними інформаційними системами. У роботі розглянуто сучасні напрями автоматизації РЕБ, основні проблеми їх реалізації та перспективи подальшого розвитку.

Електромагнітний спектр є одним із важливих середовищ сучасних військових операцій. НАТО розглядає електромагнітну боротьбу як комплекс дій, спрямованих на використання електромагнітної енергії для отримання ситуаційної обізнаності та створення необхідних ефектів. Розвиток технологій змінює вимоги до таких спроможностей, що підвищує значення автоматизованої обробки інформації.

Зі зростанням кількості радіотехнічних засобів збільшується обсяг інформації, яку необхідно обробляти системам РЕБ. Ручна обробка значної кількості сигналів обмежує швидкість реагування, тому автоматизація стає важливим напрямом розвитку сучасних систем РЕБ. НАТО пов'язує цифрову трансформацію із застосуванням автоматизації, обробки даних та штучного інтелекту для скорочення часу між отриманням інформації та прийняттям рішення.

Саме тому автоматизація систем РЕБ є не окремою функцією, а одним із ключових напрямів їхнього технологічного розвитку.

Сучасний стан автоматизації систем РЕБ

Одним із фундаментальних напрямів автоматизації є цифрова обробка радіосигналів. Сучасні дослідження використовують методи глибокого навчання для автоматичного виявлення сигналів та визначення їхніх параметрів. Наприклад, у дослідженні 2024 року, опублікованому IEEE, запропоновано метод, який забезпечує одночасне виявлення радіолокаційного сигналу, визначення його положення в часі та оцінювання робочої смуги частот. Такий підхід дає змогу зменшити обсяг ручної обробки під час подальшого аналізу.

Штучний інтелект і машинне навчання в автоматизації РЕБ

Для систем РЕБ це має практичне значення насамперед під час роботи з великими масивами радіочастотної інформації. Машинне навчання може застосовуватися для автоматичного вилучення ознак радіосигналів, їх класифікації та оцінювання електромагнітної обстановки. DARPA розглядала такі підходи, зокрема, для радіотехнічної розвідки, електронної боротьби та формування ситуаційної обізнаності щодо використання радіочастотного спектра. Окремі сучасні наукові роботи вже поєднують штучний інтелект із системами радіомоніторингу та визначенням напрямку на джерела випромінювання; у таких дослідженнях використовуються, зокрема, моделі глибокого навчання для автоматизованої класифікації сигналів.

Водночас застосування штучного інтелекту висуває підвищені вимоги до надійності та стійкості автоматизованих систем. NIST відносить до ключових характеристик довіреного AI валідність і надійність, безпечність, захищеність, стійкість, прозорість та пояснюваність. Окрему увагу приділено перевірці здатності моделей коректно працювати за умов, що відрізняються від умов їх розроблення.

Для РЕБ ця проблема є особливо важливою, оскільки радіоелектронна обстановка є змінною, а характеристики сигналів можуть відрізнятися від тих, на яких проводилося навчання алгоритмів. Тому перспективною є не просто максимізація точності моделі, а створення систем, здатних визначати межі своєї достовірності, виявляти невизначеність і передавати оператору інформацію для остаточної оцінки.

Інтеграція та мережева автоматизація

Наступним етапом розвитку є перехід від автоматизації окремого комплексу РЕБ до інтегрованих інформаційних систем. У такому випадку окремі засоби перестають працювати як ізольовані елементи, а інформація між ними передається в цифровому вигляді та використовується для формування спільної картини обстановки.

Прикладом практичної цифровізації Сил оборони України є бойова система DELTA. Міністерство оборони України повідомляло про її впровадження на всіх рівнях Сил оборони. Система забезпечує формування єдиної ситуаційної картини, обмін інформацією та роботу з даними в цифровому середовищі. Подальший розвиток таких систем створює основу для інтеграції інформації від різних засобів розвідки та інших компонентів оборони.

Основні проблеми автоматизації

Попри значні перспективи, автоматизація систем РЕБ має низку обмежень. Першою проблемою є якість і репрезентативність даних. Алгоритм машинного навчання залежить від даних, на яких він створюється та перевіряється. NIST наголошує, що межі узагальнення моделі за умовами, які відрізняються від середовища її розроблення, повинні бути документовані та перевірені.

Окремим завданням залишається забезпечення сумісності різних інформаційних і технічних систем. Для ефективної автоматизації необхідні узгоджені механізми обміну даними та можливість інтеграції різних національних спроможностей. Такий підхід відповідає сучасному курсу НАТО на підвищення взаємосумісності та інтеграцію інформаційних систем.

Перспективи розвитку

Перспективним напрямом є розширення застосування AI для автоматичного аналізу великих потоків даних та скорочення часу від отримання інформації до прийняття рішення. У межах проєкту Next Generation Targeting НАТО розвиває інтеграцію національних систем за допомогою модульного штучного інтелекту та федеративних потоків даних.

Другим напрямом є розвиток розподілених і мережевих систем. Перспективними стають архітектури, в яких інформація від різних засобів об’єднується, корелюється та передається між елементами системи без необхідності повторної ручної обробки. Саме такий підхід лежить в основі сучасних ініціатив НАТО щодо федеративних потоків даних та модульних AI-компонентів.

Для України перспективним напрямом також є подальша інтеграція РЕБ із цифровими системами управління, розвідки та логістики. Українське Міністерство оборони вже розвиває цифрові інструменти для управління, обліку та інтеграції засобів РЕБ, що створює основу для подальшого переходу до більш автоматизованого управління інформаційними потоками.

Водночас перспективний розвиток не повинен зводитися до повної автономізації. За сучасними підходами НАТО та NIST, ефективна система

повинна поєднувати автоматизовану обробку інформації з контролем людини, перевіркою результатів та вимогами до надійності, безпеки й пояснюваності.

Висновки

Основна мета полягає у скороченні часу обробки інформації, зменшенні навантаження на оператора та підвищенні оперативності реагування на зміни електромагнітної обстановки. Сучасний етап характеризується широким використанням цифрової обробки сигналів, машинного навчання, штучного інтелекту та інтегрованих цифрових інформаційних систем.

Досвід НАТО та України демонструє перехід від автоматизації окремих операцій до інтегрованого опрацювання інформації, обміну даними та підтримки прийняття рішень. Подальший розвиток систем РЕБ пов’язаний із використанням машинного навчання та штучного інтелекту, підвищенням адаптивності алгоритмів, розвитком розподілених систем і забезпеченням їхньої взаємосумісності.

Сергієнко А. Я., слухач
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ТА РАДІОЗВ’ЯЗКУ В СУЧАСНИХ УМОВАХ

Сучасні військові системи управління поєднують значну кількість радіоелектронних засобів різного призначення. Системи радіозв’язку забезпечують передавання інформації, тоді як засоби радіоелектронної боротьби (РЕБ) змінюють електромагнітну обстановку. Це створює ризик взаємних перешкод. Актуальність дослідження визначається потребою збереження працездатності радіозв’язку за одночасної роботи різних типів апаратури.

Метою дослідження є систематизація чинників електромагнітної сумісності (ЕМС) засобів РЕБ та радіозв’язку й обґрунтування підходу до попереднього оцінювання ризиків їх взаємного впливу. Застосований системний аналіз, функціональне порівняння та якісне оцінювання ризиків. Практичні випробування та вимірювання конкретних комплексів не проводилися.

Електромагнітна сумісність означає здатність обладнання належно функціонувати в певному електромагнітному середовищі, не створюючи радіоперешкод іншому обладнанню. Для радіозв'язку важлива якість обміну даними, а для РЕБ — вплив випромінювання на інші компоненти системи. Тому ЕМС залежить не лише від характеристик окремих пристроїв, а й від умов їх взаємодії. Технічна справність кожного засобу не є достатнім доказом сумісності всіх цих сукупних засобів.

До основних чинників ЕМС належать спектральні властивості випромінювань, чутливість і вибірковість приймачів, параметри антенних систем, просторові та часові умови роботи обладнання. Важливо враховувати позасмугові та побічні випромінювання, а також блокування чи перевантаження приймальних трактів сильними сигналами. Відсутність збігу робочих частот не гарантує відсутності взаємного впливу.

Особливість взаємодії засобів РЕБ та радіозв'язку полягає у відмінності функціональних вимог. Радіозв'язок потребує доступності каналів і надійного передавання даних. Функціонування засобів РЕБ може збільшувати загальне електромагнітне навантаження. Відтак виконання одного завдання здатне обмежувати якість іншого. Системний аналіз має охоплювати не лише технічні ознаки перешкоди, а й можливе погіршення функції, яку забезпечує відповідний канал зв'язку.

Запропоновано трирівневий підхід до забезпечення ЕМС, який охоплює технічний, системний та організаційний аспекти. Мета цього пов'язати характеристики обладнання з вимогами до функціонування спільної системи та правилами перевірки, та поєднати висновків. Цей підхід задає логіку виявлення потенційних несумісностей, але не встановлює універсальних режимів роботи апаратури й не замінює нормативних процедур контролю.

На технічному рівні розглядають підтверджені характеристики передавальних і приймальних пристроїв, їхні обмеження та стійкість до небажаних сигналів. Необхідно відокремлювати паспортні дані й результати випробувань від припущень. Якщо наявних відомостей недостатньо, невизначеність фіксують як окремий результат аналізу, а не як доказ сумісності. Перевіряють також межі застосовності наявних даних.

На системному рівні встановлюють функції, що залежать від відповідних каналів радіозв'язку, та можливі наслідки погіршення їх роботи. Тотожний за

фізичною природою вплив може мати різне значення залежно від ролі каналу. Враховують критичність функції, можливість виявлення погіршення якості та збереження працездатності системи. Це дозволяє відрізняти локальну проблему від ризику для всієї системи.

На організаційному рівні необхідні узгоджені вимоги, документування виявлених проблем, обмін перевіреною технічною інформацією та своєчасний перегляд оцінок. Для відтворюваності аналізу слід розмежовувати підтверджені факти, прогнозні оцінки й припущення. Це підвищує прозорість висновків і запобігає необґрунтованим узагальненням.

Для попереднього оцінювання запропоновано матрицю з ризику взаємного електромагнітного впливу. Для кожної потенційної несумісності аналізують три ознаки: імовірність прояву за визначених умов, значущість можливих наслідків та достовірність вихідних даних. Імовірність і наслідки розглядають за якісними показниками «низька», «помірна», «висока». Достовірність даних фіксують окремо, щоб припущення не сприймалося як перевірений факт. За сукупністю ознак визначають пріоритет додаткової перевірки. Отримана категорія не є виміряним рівнем перешкод або показником ефективності апаратури.

Умовний приклад ілюструє роботу підходу: під час одночасного функціонування двох радіоелектронних пристроїв зауважено погіршення якості радіозв’язку, але результати вимірювань відсутні. Можливі наслідки для інформаційного обміну є значущими, тоді як причина порушення не встановлена. Тому випадок потребує пріоритетної перевірки, але не дає підстав стверджувати, що електромагнітну несумісність уже доведено. У цьому полягає відмінність між попередньою якісною оцінкою ризику та встановленим технічним результатом.

Якість запропонованого аналізу доцільно оцінювати за повнотою охоплення взаємодіючих засобів, простежуваністю вихідних відомостей, явним зазначенням припущень і відповідністю висновків конкретним умовам. Окремим критерієм є можливість обґрунтувати черговість подальших перевірок. Водночас фактичну працездатність радіоканалів потрібно підтверджувати належним моделюванням, вимірюваннями або випробуваннями. Отже, якість процедури аналізу й технічні характеристики системи не можна ототожнювати.

Основне обмеження запропонованого рішення — її якісний характер: вона не описує в повному обсязі поширення радіохвиль, нелінійні ефекти в приймальних трактах та інші властивості реального середовища. Тому підхід призначений насамперед для визначення пріоритетів аналізу та має доповнювати, а не замінювати нормативний контроль і кількісні розрахунки. Кількісна перевірка потребує достовірних даних.

Отже, систематизовано чинники електромагнітної сумісності засобів РЕБ і радіозв'язку та запропоновано трирівневий підхід до її попереднього аналізу з використанням якісної матриці ризику. Практична цінність підходу полягає в розмежуванні підтверджених даних і припущень, а також в обґрунтуванні черговості перевірки потенційних несумісностей. Подальші дослідження доцільно спрямувати на перевірку придатності запропонованих критеріїв за результатами моделювання та відкритих експериментальних даних.

Глущенко О. О., слухач
Біховський О. В.
Житомирський військовий інститут імені С. П. Корольова

ПРИКРИТТЯ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ ЗАСОБАМИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

В умовах сучасних збройних конфліктів об'єкти критичної інфраструктури залишаються важливими елементами забезпечення життєдіяльності держави, зокрема енергетики, зв'язку, транспорту та водопостачання. Застосування безпілотних літальних апаратів, систем радіолокації та засобів керування на основі радіоканалів створює додаткові загрози для таких об'єктів. У зв'язку із цим актуальним є дослідження можливостей використання засобів радіоелектронної боротьби (далі – РЕБ) як складової комплексної системи захисту інфраструктури.

Мета дослідження полягає в аналізі ролі засобів радіоелектронної боротьби у прикритті об'єктів інфраструктури, визначенні основних напрямів їх застосування, переваг та обмежень, а також обґрунтуванні необхідності інтеграції РЕБ з іншими заходами безпеки.

У роботі використано методи аналізу й узагальнення інформації, системний підхід до розгляду захисту інфраструктурних об’єктів та порівняльний аналіз функціональних можливостей засобів РЕБ у контексті протидії радіоелектронним загрозам.

Радіоелектронна боротьба є сукупністю заходів і засобів, спрямованих на виявлення, аналіз, використання та протидію випромінюванням електромагнітного спектра. У системі захисту інфраструктури її роль полягає передусім у зменшенні ефективності тих загроз, які залежать від використання радіоканалів, супутникової навігації та інших електронних систем. Водночас РЕБ не є універсальним засобом захисту, оскільки її ефективність залежить від характеристик загрози, умов застосування та сумісності з іншими системами безпеки.

Одним із важливих напрямів використання РЕБ є радіоелектронний моніторинг. Він передбачає спостереження за електромагнітною обстановкою, виявлення нетипової активності та аналіз радіосигналів у межах наявних технічних можливостей. Отримана інформація може використовуватися для оцінювання потенційних загроз і своєчасного інформування відповідальних підрозділів. При цьому результати радіоелектронного моніторингу доцільно розглядати разом з іншими даними спостереження, оскільки окремий сигнал не завжди свідчить про наявність небезпеки.

Іншим напрямом є радіоелектронна протидія, яка за відповідних умов може знижувати ефективність окремих систем керування та навігації, що використовуються безпілотними апаратами. Проте результативність таких заходів не є гарантованою для всіх типів загроз. Вона залежить від технічних характеристик обладнання, особливостей сигналів, наявності альтернативних каналів керування та здатності потенційного противника адаптуватися до перешкод. Крім того, створення радіоперешкод може впливати на легітимні системи зв’язку, навігації та автоматизованого керування самого інфраструктурного об’єкта. Тому застосування відповідних засобів потребує оцінювання ризиків і дотримання встановлених вимог.

Важливою умовою ефективного прикриття є інтеграція засобів РЕБ із загальною системою безпеки об’єкта. Така система може охоплювати технічне спостереження, засоби виявлення повітряних загроз, фізичну охорону, оповіщення персоналу, резервування критичних систем та плани реагування на надзвичайні ситуації. Узгоджене функціонування цих елементів дає змогу

зменшити залежність від одного засобу захисту та підвищити стійкість об’єкта до різних типів загроз.

Під час організації захисту необхідно враховувати специфіку конкретного об’єкта. Для енергетичних підприємств особливе значення має безперервність технологічних процесів; для транспортної інфраструктури – безпека руху та стабільність систем керування; для об’єктів зв’язку – доступність каналів передавання інформації. Відповідно, рішення щодо використання РЕБ повинні враховувати критичність функцій об’єкта, можливі наслідки радіоперешкод для власного обладнання та вимоги до безперервності роботи.

За результатами аналізу визначено, що засоби РЕБ доцільно розглядати як один із компонентів багаторівневої системи захисту інфраструктури. Їх використання має ґрунтуватися на попередньому оцінюванні загроз, перевірці сумісності обладнання, підготовці персоналу та періодичному оцінюванні готовності системи до реагування. Важливе значення також мають резервні канали зв’язку, захист технологічних мереж, розроблення планів відновлення та проведення навчань. Такий підхід дає змогу не лише протидіяти окремим радіоелектронним загрозам, а й зменшувати можливі наслідки порушення роботи критичних систем.

Висновки.

Засоби радіоелектронної боротьби можуть відігравати важливу роль у прикритті об’єктів інфраструктури завдяки можливостям радіоелектронного моніторингу та протидії окремим загрозам, що використовують радіоканали. Водночас їх застосування потребує врахування технічних обмежень і можливого впливу на власні системи зв’язку та керування. Найбільш обґрунтованим підходом є інтеграція РЕБ із засобами виявлення, оповіщення, фізичного захисту та забезпечення безперервності функціонування інфраструктури.

Ковтонюк Д. В., слухач
Житомирський військовий інститут імені С. П. Корольова

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ ІЗ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Стрімкий розвиток сучасних інформаційних технологій та засобів радіоелектронної боротьби зумовлює необхідність постійного вдосконалення системи підготовки фахівців. У сучасних умовах радіоелектронна обстановка характеризується значною складністю, швидкою зміною умов функціонування засобів зв’язку та навігації, а також широким використанням безпілотних авіаційних комплексів. Це вимагає від фахівців з РЕБ ґрунтовних теоретичних знань, практичних навичок, здатності аналізувати технічну інформацію та оперативно приймати обґрунтовані рішення. Одним із перспективних напрямів удосконалення військової освіти є використання технологій штучного інтелекту, які відкривають нові можливості для персоналізації навчання, моделювання професійного набуття та послідовне оцінювання рівня підготовленості військовослужбовців.

Метою дослідження є визначення основних напрямків використання штучного інтелекту в процесі з підготовки фахівців з радіоелектронної боротьби, а також аналіз можливостей його застосування для підвищення якості навчання та формування професійних навичок.

Одним із перспективних напрямків застосування штучного інтелекту є використання інтерактивних тренажерів і віртуальних навчальних середовищ. Вони дають змогу відпрацьовувати та провести аналіз радіосигналів, вивчати принципи функціонування засобів радіозв’язку та радіоелектронного обладнання, а також оцінювати вплив різних чинників на якість передачі сигналу. Наприклад, штучний інтелект зможе, в системі управління засобами РЕБ на мапі виставляти цілі і управляти ними, змінювати частоти управління, показувати різні властивості, по відношенню до інших засібів, як будуть вести себе вони під перешкодами, як впливає рельєф, погодні умови, що впливають на якість перешкоди і т.д. Завдяки моделюванню навчальних ситуацій здобувачі освіти можуть набувати практичного досвіду без необхідності постійного залучення реального обладнання. Крім того, штучний інтелект може забезпечувати автоматизований аналіз дій курсантів, визначати типові помилки та надавати рекомендації щодо вдосконалення їхніх професійних навичок.

Важливе значення має використання інтелектуальних систем для адаптації навчального процесу до індивідуального рівня підготовки. На основі результатів тестування та виконання практичних завдань такі системи можуть визначати теми, які потребують додаткового опрацювання, пропонувати відповідні навчальні матеріали та поступово підвищувати складність завдань. Це сприяє ефективнішому засвоєнню складних технічних дисциплін.

Разом із перевагами впровадження штучного інтелекту супроводжується певними обмеженнями. Ефективність таких технологій залежить від достовірності навчальних даних, якості програмного забезпечення та відповідності навчальних сценаріїв реальним професійним завданням. Крім того, результати, сформовані інтелектуальними системами, потребують перевірки викладачем, оскільки можливі помилки, неточності або неповне врахування специфіки військової діяльності. Особливу увагу необхідно приділяти захисту інформації, дотриманню вимог інформаційної безпеки та недопущенню використання конфіденційних даних у відкритих системах штучного інтелекту. Важливо також пам’ятати, що цифрові інструменти мають доповнювати, а не замінювати практичну підготовку, роботу з реальним обладнанням і професійне оцінювання з боку викладачів.

Таким чином, використання штучного інтелекту є перспективним напрямом удосконалення системи підготовки фахівців з радіоелектронної боротьби. Його впровадження дає змогу підвищити індивідуалізацію навчання, розширити можливості практичного моделювання, автоматизувати оцінювання знань і сприяти формуванню необхідних професійних компетентностей. Подальший розвиток цього напряму пов’язаний із розробленням спеціалізованих навчальних платформ, удосконаленням віртуальних тренажерів та інтеграцією інтелектуальних технологій в освітній процес військових навчальних закладів. Комплексне поєднання штучного інтелекту, традиційних методів навчання та практичної підготовки сприятиме підвищенню якості військової освіти й готовності фахівців РЕБ до виконання професійних завдань у сучасних умовах.

Трачук Є. С., слухач
Житомирський військовий інститут імені С. П. Корольова

АЛГОРИТМ РОЗРАХУНКУ ЕФЕКТИВНОСТІ ЗАСОБУ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Сучасний оперативно-бойовий простір характеризується високою насиченістю радіоелектронними засобами, широким застосуванням безпілотних систем та активним використанням засобів зв’язку і управління. У таких умовах особливого значення набувають засоби радіоелектронної боротьби, ефективність яких безпосередньо впливає на успішність виконання бойових завдань.

Існуючі підходи до оцінки ефективності засобів радіоелектронної боротьби здебільшого базуються на спрощених аналітичних моделях, що не враховують динамічний характер радіоелектронної обстановки, зміну параметрів сигналів та адаптивні можливості засобів противника. Це зумовлює необхідність розробки більш досконалих алгоритмів, здатних забезпечити адекватну оцінку ефективності в реальному масштабі часу.

У зв’язку з цим метою роботи є розробка алгоритму оцінки ефективності засобу радіоелектронної боротьби, який враховує комплекс енергетичних, часових та ймовірнісних характеристик функціонування системи.

Запропонований алгоритм передбачає багаторівневу оцінку ефективності, що включає визначення рівня впливу завад на роботу радіоелектронних засобів противника, оцінювання ймовірності впливу на їх функціонування, аналіз часових характеристик по впливу, а також врахування просторових параметрів, таких як дальність дії засобів, напрямок та зона впливу засобами РЕБ на певні ділянки.

Особливістю алгоритму є його адаптивність, що реалізується шляхом динамічного коригування параметрів залежно від змін радіоелектронної обстановки. Це дозволяє підвищити точність оцінювання ефективності та забезпечити стійкість роботи системи в умовах невизначеності та інтенсивних радіоперешкод.

Практична реалізація алгоритму може бути реалізована на базі програмно-визначених радіосистем, що забезпечують гнучкість обробки сигналів та можливість оперативної зміни режимів роботи. Використання

сучасних методів цифрової обробки сигналів та елементів інтелектуального аналізу даних дозволяє підвищити швидкодію алгоритму та автоматизувати процес прийняття рішень.

Результати дослідження можуть бути використані при проєктуванні та модернізації засобів радіоелектронної боротьби, а також у системах електронної підтримки радіоелектронної боротьби в частині прийняття рішень для оцінки ефективності їх застосування в реальних умовах.

Отже, розробка адаптивного алгоритму оцінки ефективності засобів радіоелектронної боротьби є актуальним науково-практичним завданням, вирішення якого дозволяє підвищити результативність їх застосування в сучасних умовах ведення бойових дій.

Загорулько К. М., слухач
Коваленко К. А., слухач
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ НЕДОЛІКІВ ВИКОРИСТАННЯ MESH-МЕРЕЖІ ТА МОДЕМІВ У ПЕРЕДАЧІ ДАНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Сучасні безпілотні літальні апарати (БПЛА) відіграють ключову роль у виконанні завдань різного призначення, де критично важливим є забезпечення стабільного, швидкого та захищеного каналу передачі даних. Для розширення відстані дії та підвищення стійкості зв'язку все частіше застосовуються децентралізовані мережеві топології, зокрема mesh-мережі. Проте попри високу гнучкість таких архітектур, їх практичне впровадження у складних умовах експлуатації стикається з низкою суттєвих технічних обмежень і недоліків.

Архітектура mesh-мереж передбачає динамічну ретрансляцію пакетів даних через проміжні вузли (ретранслятори або інші БПЛА), що дозволяє обходити перешкоди та збільшувати загальну зону покриття. Однак такий підхід породжує велику кількість критичних недоліків:

Зростання затримки передачі даних. Кожен додатковий стрибок (hop) у mesh-мережі додає час на обробку та пересилання пакетів. У завданнях реального часу, таких як дистанційне пілотування або передача відеопотоку

високої роздільної здатності, накопичення затримок може призвести до втрати керування БпЛА.

Обмеження пропускної здатності каналу. Оскільки вузли мережі одночасно приймають і передають трафік на суміжних або тих самих частотах, ефективна пропускна здатність мережі суттєво знижується пропорційно кількості ретрансляцій.

Демаскуючі фактори та вразливість до радіоелектронної боротьби (РЕБ). Постійний активний радіообмін між вузлами mesh-мережі створює значне електромагнітне поле, яке легко виявляється засобами радіотехнічної розвідки (РТР). Крім того, наявність безлічі активних приймально-передавальних пристроїв збільшує поверхню атаки для засобів подавлення супротивника.

Особливу проблематику створюють характеристики використовуваних бортових і наземних модемів. Сучасні цифрові модеми передачі даних часто критично залежні від стабільності співвідношення сигнал/шум. До основних недоліків модемів належать:

висока чутливість до вузькосмугових та загороджувальних перешкод у разі використання стандартних модуляторів;

обмежені можливості адаптації до різких змін умов поширення радіохвиль (наприклад, при переході з прямої видимості в зону закриту рельєфом);

Аналіз показує, що використання mesh-мереж та стандартних модемів у каналах зв'язку БПЛА забезпечує гнучкість покриття, але супроводжується значними втратами у швидкодії, критичною уразливістю до затримок та високим ризиком виявлення для електронної підтримки та подавлення засобами радіоелектронної боротьби. Подальші дослідження мають бути спрямовані на розробку гібридних протоколів маршрутизації, оптимізацію алгоритмів динамічного перемикання каналів.

Гулюк Д. С., слухач
Біховський О. В.
Житомирський військовий інститут імені С. П. Корольова

ЗМІНА ТАКТИКИ ЗАСТОСУВАННЯ російськими УДАРНИМИ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ ВИКОРИСТАННЯ MESH-МЕРЕЖ

Сучасна війна характеризується постійним удосконаленням безпілотних авіаційних систем, які застосовуються для ураження об’єктів, ведення розвідки та спостереження за змінами обстановки. Одним із напрямів розвитку таких систем є використання мережевих технологій передавання інформації, що забезпечують взаємодію між безпілотними літальними апаратами та зовнішніми пунктами управління. Особливого значення в цьому контексті набувають MESH-мережі, які за відповідної архітектури дають змогу окремим вузлам передавати інформацію через інші вузли мережі.

Актуальність проблеми підтверджується повідомленнями українських офіційних осіб щодо використання російською федерацією мережевих систем зв’язку для забезпечення функціонування ударних БпЛА. Зокрема, 26 грудня 2025 року Президент України повідомив про розміщення на території Білорусі обладнання, яке, за даними української розвідки, використовувалося для сприяння наведенню російських безпілотників на об’єкти в західних областях України. 27 лютого 2026 року Міністр оборони України повідомив про ліквідацію MESH-мережі, яку використовували «Шахеди» на півночі України. За поясненням радника Міністерства оборони України Сергія Бескрестнова, така мережа забезпечувала ретрансляцію сигналів між її учасниками, а зв’язок із пунктами управління підтримувався через відповідні вузлові точки.

Застосування подібних технологій створює додаткові труднощі для підрозділів радіоелектронної боротьби. Вплив на один безпілотний літальний апарат не обов’язково призводить до втрати зв’язку іншими учасниками мережі. За наявності альтернативних маршрутів передавання даних або можливості повторного встановлення з’єднання система може зберігати працездатність навіть після втрати окремого вузла. Тому оцінювання ефективності протидії має враховувати не лише результат впливу на окрему ціль, а й зміни у функціонуванні мережі загалом.

Одним із ключових напрямів дослідження є комплексне порушення мережевої взаємодії. Його сутність полягає в тому, що результативність протидії визначається ступенем порушення обміну інформацією між вузлами мережі, а не лише фактом припинення зв’язку з одним безпілотним апаратом. За такого підходу предметом оцінювання стають зв’язність мережі, доступність каналів передавання даних, здатність її учасників взаємодіяти між собою та можливість продовження виконання поставленого завдання. Водночас необхідно враховувати, що порушення мережевого зв’язку не завжди призводить до припинення польоту, оскільки окремі БпЛА можуть використовувати автономні алгоритми навігації.

Іншим важливим напрямом є дослідження ролі ретрансляційних вузлів, які забезпечують зв’язок між повітряною мережею безпілотних апаратів над територією України та зовнішньою інфраструктурою передавання інформації, зокрема розташованою на території Білорусі. У такій системі повітряний БпЛА може виконувати функцію проміжного ретранслятора, тоді як наземне обладнання забезпечує зв’язок із віддаленим пунктом управління. Втрата окремої ретрансляційної ланки потенційно може сутево вплинути на обмін інформацією між частинами системи, якщо відсутні альтернативні маршрути зв’язку. Тому важливим завданням є визначення залежності мережі від окремих вузлів та оцінювання наслідків порушення їхньої роботи.

Таким чином, комплексна протидія передбачає розгляд двох взаємопов’язаних аспектів: порушення взаємодії між учасниками MESH-мережі та оцінювання ролі ретрансляційної інфраструктури, яка забезпечує зв’язок із зовнішніми пунктами управління. При цьому необхідно враховувати реальну топологію мережі, наявність резервних каналів і можливість автономного функціонування окремих безпілотних апаратів. Саме ці чинники визначають, чи призводить порушення окремого зв’язку до локального погіршення роботи системи, чи впливає на її функціонування загалом.

Окремого значення набуває взаємодія суміжних підрозділів РЕБ. Можливості одного підрозділу можуть обмежуватися технічними характеристиками наявних засобів, дальністю їхньої дії, особливостями радіоелектронної обстановки та встановленими зонами відповідальності. У таких умовах координація з іншими підрозділами дає змогу узгоджувати оцінювання повітряної обстановки, забезпечувати своєчасний обмін інформацією та формувати єдине уявлення про функціонування мережевої системи.

Ефективна взаємодія передбачає не лише передавання відомостей про виявлені загрози, а й узгоджене оцінювання результатів застосування засобів РЕБ. Важливо встановлювати, чи зберігає мережа можливість передавання інформації, чи відновлюється її зв'язність і чи вплинули вжиті заходи на здатність безпілотної системи виконувати поставлене завдання. При цьому необхідно враховувати сумісність обладнання, безпеку власних каналів зв'язку та ризик ненавмисного впливу на дружні системи.

Перспективним напрямом подальших досліджень є розроблення методики оцінювання стійкості MESH-мереж до радіоелектронного впливу. Така методика може включати аналіз кількості доступних маршрутів передавання інформації, стабільності зв'язку, затримок обміну даними, залежності мережі від ретрансляційних вузлів та здатності відновлювати працездатність після подавлення таких вузлів. Застосування зазначених критеріїв у навчальному моделюванні дасть змогу вдосконалити підготовку фахівців РЕБ та відпрацьовувати взаємодію між підрозділами в контрольованих умовах.

Отже, розвиток мережевих технологій у безпілотних авіаційних системах потребує вдосконалення підходів до організації та оцінювання ефективності радіоелектронної боротьби. Вплив на окремий безпілотний літальний апарат не завжди забезпечує порушення функціонування всієї мережі, оскільки інші вузли можуть зберігати зв'язок і продовжувати передавання інформації.

Основним напрямом дослідження має бути комплексне оцінювання порушення мережевої взаємодії та залежності системи від ретрансляційної інфраструктури. Важливо враховувати як взаємозв'язки між повітряними вузлами, так і роль зовнішніх пунктів зв'язку, зокрема обладнання на території Білорусі, використання якого для підтримання функціонування російських ударних БпЛА висвітлювалося в офіційних повідомленнях України.

Необхідною умовою підвищення ефективності протидії є взаємодія суміжних підрозділів РЕБ, своєчасний обмін інформацією та узгоджене оцінювання результатів. Поєднання мережевого аналізу, об'єктивних критеріїв оцінювання та міжпідрозділової координації створює передумови для вдосконалення системи протидії сучасним безпілотним загрозам.

Колот В. В., слухач
Житомирський військовий інститут імені С. П. Корольова

ВИКОРИСТАННЯ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ НА НАЗЕМНИХ РОБОТИЗОВАНИХ ПЛАТФОРМАХ З ІНЕРЦІАЛЬНОЮ СИСТЕМОЮ

Розвиток безпілотних і роботизованих технологій та досвід російсько-української війни зумовили зростання уваги до наземних роботизованих платформ як засобів виконання завдань у складних умовах.

Одним із перспективних напрямів є поєднання таких платформ із засобами радіоелектронної боротьби (РЕБ) та інерціальними системами навігації, що дає змогу підвищити автономність і стійкість функціонування за умов нестабільного супутникового сигналу.

Особливої актуальності набуває питання узгодження навігації, керування та роботи спеціального обладнання в середовищі, де можливі перешкоди, обмеження зв’язку й вплив зовнішніх чинників.

Наземна роботизована платформа із засобами РЕБ може розглядатися як комплекс, до складу якого входять:

- інерціальна навігаційна система – забезпечує оцінювання положення та орієнтації платформи за даними інерціальних датчиків;

- засоби радіоелектронної боротьби – призначені для виконання визначених завдань радіоелектронного впливу або захисту електронних систем у межах установлених режимів;

- система керування – об’єднує дані навігації, стан платформи та контроль роботи обладнання;

- канали зв’язку й контролю – забезпечують обмін службовою інформацією та передавання команд за наявності доступного каналу.

Використання інерціальної системи є важливим у випадках, коли супутникова навігація недоступна або її точність знижена. Водночас похибка інерціального визначення координат із часом накопичується, тому доцільно передбачати періодичне уточнення навігаційних даних за доступними незалежними джерелами.

Під час інтеграції РЕБ та навігаційного обладнання необхідно враховувати електромагнітну сумісність, енергоспоживання, тепловий режим,

масогабаритні обмеження й вплив вібрацій на датчики. Окрему увагу слід приділяти безпечному розміщенню антен, екрануванню чутливих компонентів і контролю взаємних перешкод.

Ключовими напрямами вдосконалення таких комплексів є:

- модульна архітектура, що спрощує заміну та обслуговування окремих вузлів;
- резервування критичних функцій і контроль справності сенсорів для зменшення ризику втрати керованості;
- поєднання інерціальних даних з іншими доступними засобами навігації та оцінювання руху;
- автоматизований контроль енергетичного балансу, температури й електромагнітної сумісності;
- проведення стендових і полігонних випробувань у різних умовах із фіксацією похибок та відмов.

Таким чином, використання засобів РЕБ на наземних роботизованих платформах з інерціальною системою потребує комплексного підходу, що поєднує навігаційне забезпечення, стійке керування та сумісність електронного обладнання.

Інерціальна система підвищує здатність платформи продовжувати оцінювання власного руху за обмеженої доступності супутникової навігації, однак не усуває накопичення похибок і потребує періодичного уточнення даних.

Ефективність комплексу визначається не лише характеристиками окремих пристроїв, а й якістю їх інтеграції, енергетичним забезпеченням, надійністю програмно-апаратних засобів та результатами випробувань.

Пріоритетними напрямами подальшої роботи є модульність конструкції, електромагнітна сумісність, резервування критичних функцій і перевірка роботи системи в умовах перешкод та змінного навантаження.

Верховцев Ю. Ю., курсант
Шостачук А. М., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

СТАН І ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МЕТОДІВ ТА ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ В УМОВАХ СУЧАСНОЇ ВІЙНИ

Радіоелектронна боротьба – це сукупність методів, пристроїв і комплексів, що реалізують радіоперешкоди, радіоелектронну розвідку, глушіння сигналів супутникового й мобільного зв’язку, навігації, а також управління безпілотними літальними апаратами (БПЛА). В даний час РЕБ – вид оперативного (бойового) забезпечення.

РЕБ організується і ведеться в тісній взаємодії з бойовими діями родів військ і спеціальних військ по знищенню (захопленню, виводу з ладу) пунктів управління й інших важливих радіоелектронних об’єктів із заходами щодо розвідки, оперативного (військового) маскування й іншим видам оперативного (бойового) забезпечення.

У широкому розумінні РЕБ – це протиборство (сукупність заходів і дій військ), у якому воюючі сторони вирішують свої задачі шляхом застосування електромагнітних коливань.

Тобто, основною відмінною рисою РЕБ, що обмежує область її застосування, є застосування в збройній боротьбі електромагнітних коливань.

РЕБ, як вид бойового забезпечення, спрямована на досягнення високої ефективності застосування своїх військ і зброї і зниження ефективності дій військ протиборчої сторони. Іншими словами, РЕБ спрямована на вирішальний внесок у досягнення такої мети, як забезпечення переваги над супротивником в управлінні військами і зброєю при підготовці й у ході ведення операцій (бойових дій).

Вперше радіоелектронна боротьба була застосована силами ВМФ Російської імперії у ході Російсько-японської війни. 15 квітня 1904 року під час артилерійського обстрілу, який японська ескадра вела по внутрішньому рейду Порт-Артура, радіостанції російського броненосця «Побєда» і берегового поста «Золотая гора» шляхом створення навмисних перешкод серйозно ускладнили передавання телеграм ворожих кораблів-коректувальників.

Тим не менш, радіозасоби на ті часи, загалом, використовувалися для забезпечення зв'язку, виявлення каналів зв'язку і перехоплення інформації, яка

передається ними. Перевага надавалась перехопленню радіопередач, а не їх придушення. Однак, у роки Першої світової війни, радіоперешкоди стали час від часу застосовуватися для порушення радіозв'язку між штабами армій, корпусів і дивізій і між військовими кораблями. Разом з тим, у німецькій армії вже тоді з'явилися спеціальні станції радіоперешкод.

У проміжок між світовими війнами активно розвивається радіозв'язок, з'являються засоби радіопеленгування, радіокерування і радіолокації. У підсумку, серйозно змінюється концепція керування і взаємодії сухопутних військ, ВПС і ВМФ. Все це призвело до подальшого розвитку РЕБ та способів і засобів протидії РЕЗ противника.

У сучасному військовому середовищі засоби радіоелектронної боротьби (РЕБ) стали невід'ємною частиною систем безпеки, захисту об'єктів критичної інфраструктури, військової техніки і підрозділів. У цьому матеріалі ми розглянемо класифікацію засобів РЕБ за різними ознаками: за дальністю дії, за мобільністю та розгортанням, за принципом дії, а також за типом загроз, проти яких вони застосовуються.

Пропонуються на ступні класифікації засобів РЕБ:

1. За дальністю дії (радіусом впливу):

- Тактичні системи РЕБ: мають радіус дії до 50 км. Основне завдання — прикриття передових позицій, бойової техніки, опорних пунктів та рухомих тактичних груп.
- Оперативно-тактичні комплекси РЕБ: діють на відстані до 500 км. Призначені для виявлення повітряних і наземних цілей, блокування каналів зв'язку та супутникового управління противника в оперативно-тактичній глибині.
- Стратегічні системи РЕБ: мають зону впливу понад 500 км. Здатні охоплювати значні території, впливати на супутникові лінії зв'язку, радіолокаційні системи, авіаційні та морські комплекси у глибокому тилу противника.

2. За ступенем мобільності:

- Стаціонарні станції РЕБ: розгортаються на базі постійних об'єктів критичної або військової інфраструктури, командних пунктів та захищених позицій для їхнього тривалого та безперервного прикриття.
- Мобільні станції РЕБ: встановлюються на колісну, гусеничну платформу (пікапи, бронеавтомобілі, важка техніка) або виконуються у носимому (портативному/окопному) форматі, що дозволяє швидко змінювати вогневі та оперативні позиції в умовах маневреного бою.

3. За використанням технологій штучного інтелекту (ШІ):

- Станції РЕБ без використання ШІ: функціонують за наперед заданими алгоритмами та потребують постійної прямої участі оператора для аналізу радіоелектронної обстановки, вибору частот та прийняття рішень про постановку завад.
- Станції РЕБ з використанням ШІ: оснащені інтелектуальними системами автоматичного аналізу радіоелектромагнітного спектра, здатні самостійно виявляти, ідентифікувати й класифікувати типи загроз (зокрема нові або частотно-скакуючі сигнали FPV-дронів) та в режимі реального часу без затримки формувати оптимальні завади мінімально необхідної потужності.

Ця класифікація дозволяє чітко розуміти, для яких завдань призначений конкретний комплекс: чи це забезпечення безпеки передової, чи прикриття оперативного простору, чи стратегічна електронна протидія.

Під час російсько-української війни радіоелектронна боротьба зазнала фундаментальних змін, перетворившись із допоміжного виду забезпечення на один із вирішальних факторів виживання сил і збереження техніки на полі бою. Вибуховий розвиток безпілотних технологій (зокрема FPV-дронів та ударних БПЛА) спровокував аналогічний за темпами «технологічний стрибок» у сфері РЕБ.

Основними напрямками еволюції апаратури та методів ведення РЕБ у ході даного конфлікту стали:

1) децентралізація та концепція «окопного РЕБ»: Якщо на початку війни перевага надавалася великим громіздким комплексам оперативно-тактичного рівня, то зараз затребуваними є портативні та компактні модулі (рюкзачного або окопного типу) та купольні системи РЕБ, що встановлюються безпосередньо на бронетехніку, пікапи чи евакуаційні машини для захисту від FPV-дронів у радіусі 50–300 метрів.

2) динамічна зміна робочих частот та смуг придушення: Завдяки швидкій адаптації операторів БПЛА, які постійно зміщують частоти керування (переходячи у нестандартні діапазони 300–500 МГц, 700–1000 МГц та понад 2,4–5,8 ГГц), сучасні станції РЕБ перейшли від статичних завад до мультидіапазонних та програмно-конфігурованих завадоутворювачів (SDR — Software Defined Radio).

3) розвиток технологій спуфінгу замість простого засліплення (джаммінгу): Подавлення GPS-сигналу виявилося недостатньо ефективним

проти високоточних боєприпасів та ракет із інерціальним наведенням. Тому ключовим методом стало використання навігаційного спуфінгу — активної підміни координат, що змушує високоточні снаряди, КАБ або БПЛА хибно визначати своє місцезнаходження та відхилятися від цілі.

4) автоматизація та застосування штучного інтелекту (ШІ): Через значну щільність радіовипромінювань у зоні бойових дій людський чинник стає обмеженням. Сучасні станції РЕБ оснащуються елементами ШІ для автоматичного сканування ефіру, розпізнавання протоколів зв'язку ворожих БПЛА за їх цифровим «підписом» (сигнатурою) та миттєвого ввімкнення прицільних завад лише у момент загрози, що дозволяє економити енергію та зменшує вразливість самої станції РЕБ до радіолокаційного виявлення.

Щодо використання РЕБ у сучасній війні, ми б хотіли би зосередити увагу на ефективному комплексі «Буковель-AD», який активно застосовують на першій та другій лініях оборони в умовах так званої «війни дронів». Абревіатура AD у його назві розшифровується як Anti-Drone (антидроновий), що безпосередньо вказує на його основне призначення. У сучасних бойових діях цей засіб демонструє надзвичайно високу ефективність.

Призначений для зриву виконання завдань безпілотними літальними апаратами шляхом подавлення радіоперешкодами приймачів сигналів супутникових радіонавігаційних систем, радіоліній управління БПЛА, каналів телеметрії та каналів передачі даних цільового навантаження.

Виходячи з вищенаведеного, ми бачимо наступні шляхи розвитку засобів РЕБ:

– розвиток компактності та мобільності станцій: заміна величезних застарілих комплексів на базі «Уралів» чи «КрАЗів», які є першочерговою ціллю для артилерії та дронів, на мобільні станції, що базуються на пікапах, бронеавтомобілях або є портативними.

– розширення діапазону придушення: ворог постійно зміщує робочі частоти FPV-дронів (переходить нижче 400 МГц або вище 1000 МГц). Тому розробка та впровадження мультидіапазонних систем є одним із ключових напрямків розвитку РЕБ.

– спуфінг та протидія високоточному озброєнню: просте подавлення GPS (джаммінг) вже не завжди ефективне, оскільки крилаті ракети та КАБи оснащені інерціальними системами наведення. Ключовий вектор тут – спуфінг (підміна супутникових координат), який дозволяє відхилити ворожу ракету або дрон-камікадзе від цілі й спрямувати їх у поле чи лісосмугу.

– захист власних каналів (Радіоелектронний захист – РЕЗ): цей напрямок полягає в оснащенні наших БПЛА та техніки адаптивними антенними решітками (CRPA), які «вирізають» напрямок, з якого здійснює вплив ворожий РЕБ, і забезпечують стійкий зв’язок.

Висновки

1. Роль РЕБ у сучасній війні: РЕБ стала ключовим фактором захисту військ, що дозволяє зривати управління противника та нейтралізувати його дрони й високоточне озброєння.

2. Ефективність «Буковель-AD»: Комплекс довів свою високу результативність на 1–2 лініях оборони, виявляючи БПЛА на відстані до 25 км та придушуючи їх на відстані до 15 км.

3. Напрямки розвитку: Головний вектор РЕБ – це мобільність (базування на пікапах), розширення частотного діапазону, використання спуфінгу та захист власних каналів зв'язку (РЕЗ).

Smyrynska N. B.
Naval Institute of the National University “Odessa Maritime Academy”

ANALYSIS OF FAILURE MECHANISMS IN UAV ONBOARD ELECTRONIC SYSTEMS UNDER INTENTIONAL HIGH-POWER ELECTROMAGNETIC EXPOSURE

Onboard electronic systems of unmanned aerial vehicles (UAVs) comprise functionally interconnected flight control, navigation, communications, power supply, and information processing subsystems. Their operational integrity depends not only on the immunity of individual electronic components but also on the ability of the integrated system to maintain its required functions under external electromagnetic disturbances. Of particular concern is intentional high-power electromagnetic (HPEM) exposure, which may induce transient functional disruptions, persistent failures, and irreversible damage to electronic hardware.

Recent studies investigating the effects of high-power microwave and ultra-wideband electromagnetic pulses on UAVs have demonstrated a variety of mechanisms responsible for the degradation or loss of onboard system functionality. The consequences of electromagnetic exposure depend not only on the characteristics

of the incident electromagnetic radiation but also on the coupling mechanisms between the external field and internal electrical circuits, equipment design, and functional interdependencies among onboard subsystems. Furthermore, the loss of specific system functions does not necessarily involve physical damage to electronic components.

High-power electromagnetic radiation couples into onboard electronic equipment through antenna–feeder systems, cable interconnections, conductive structural elements, and other electromagnetic coupling paths. This interaction induces transient currents and voltages in internal electrical circuits, whose characteristics depend on the spectral properties of the incident electromagnetic field, the electrical characteristics of the coupling paths, and the system configuration. Antenna–feeder networks and cable structures may modify the spectral content of disturbances reaching electronic devices. Consequently, external electromagnetic field parameters cannot be directly equated with the electrical stresses experienced at electronic component terminals.

At the electronic component level, induced interference causes critical distortion of information signals, false triggering of logic elements (bit flips), clock desynchronization, and data processing algorithm errors. These phenomena give rise to functional upsets (malfunctions) that are reversible in nature and can be mitigated after the interference ceases or via a hardware-software device reset. Concurrently, extreme electrical overloads lead to thermal and electrical breakdown of semiconductor structures, degradation of their physical parameters, and complete destruction of the electronic components. The mechanisms of temporary functional upsets and irreversible damage fundamentally differ in terms of their internal chip-level processes and consequences, thereby requiring separate modeling and vulnerability assessment.

At the system level, the malfunction of an individual electronic component or computing node leads to a loss data integrity (affecting navigation and telemetry), control signal desynchronization, or critical termination of mission functions. However, a local upset or even a hard failure of a specific element is not equivalent to an immediate loss of overall UAV operability. The ultimate consequences are determined by the functional criticality of the affected node, the structural-functional redundancy of the subsystems, and the availability of algorithms for automatic recovery and failure compensation. Accordingly, the threshold levels of

electromagnetic immunity for informational jamming, temporary functional failure, and irreversible catastrophic damage of the system are fundamentally different.

Thus, analyzing the mechanisms of intentional HPEM effects on UAV onboard electronic systems requires a systematic examination of electromagnetic coupling between the incident field and internal circuits, the response of electronic components to induced disturbances, and the resulting functional consequences for interconnected subsystems. Distinguishing these processes prevents local electrical disturbances from being equated with system-level failures and functional loss of operability from being conflated with irreversible hardware damage.

Further research should focus on establishing the interconnection between the characteristics of induced electrical disturbances, functional disruptions in onboard electronic equipment, and their consequences for UAV operability. The obtained results may contribute to the development and substantiation of approaches for assessing the electromagnetic vulnerability of UAV onboard electronic systems.

Червоненко Д. В., курсант
Площик А. С.
Національна академія Державної прикордонної служби України

ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ ШЛЯХИ ВДОСКОНАЛЕННЯ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ З БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

Постійний розвиток безпілотних літальних апаратів впливає на постійне вдосконалення засобів радіоелектронної боротьби. Зміни частотних діапазонів, способів керування та передавання відеосигналу ускладнюють своєчасне виявлення безпілотників і протидіяти їм. Тому обладнання, яке розраховане на певні характеристики, потребує регулярного оновлення до нових загроз. Основна проблема полягає в невідповідності між швидкістю розвитку безпілотних технологій та темпами оновлення засобів протидії. Її розв'язання потребує уваги не лише до технічних характеристик обладнання, а й до програмного забезпечення, організації роботи та підготовки фахівців. Адже радіоелектронна боротьба охоплює взаємопов'язані процеси: отримання інформації про загрозу, її аналіз, вибір засобів протидії та оцінювання її

ефективності. Недоліки на будь-якому з цих етапів можуть знижувати результати захисту, тому адаптація до нових загроз має охоплювати всі складові роботи РЕБ.

Для розв’язання зазначеної проблеми необхідно систематично збирати й узагальнювати інформацію про ворожі БПЛА, зокрема про зміни частот, які вони використовують. Ці дані мають бути основою для регулярного оновлення програмного забезпечення засобів РЕБ із подальшою перевіркою коректності його роботи. Важливо також налагодити зворотний зв’язок між фахівцями, які застосовують ці засоби, та розробниками. Це дозволить враховувати досвід практичного застосування, своєчасно виявляти недоліки й визначати пріоритети подальшої модернізації.

Для перевірки роботи програмного забезпечення після оновлень доцільно розглянути застосування методів машинного навчання, вибір яких залежить від структури та якості наявних даних. Зокрема, ізоляційний ліс може використовуватися для виявлення нетипових поєднань числових показників, отриманих із програмних журналів і даних технічної діагностики. За наявності прикладів із попередньо визначеними типами помилок можна розглянути випадковий ліс для їх класифікації. Для аналізу послідовностей подій у програмних журналах можуть застосовуватися нейронні мережі LSTM, які дозволяють виявляти відхилення від звичного порядку виконання операцій. Застосування цих методів має супроводжуватися порівнянням результатів діагностики до й після оновлення програмного забезпечення. На основі отриманих результатів фахівець має перевірити, чи свідчать виявлені відхилення про помилки, та з’ясувати їхні причини.

Водночас оновлення технічних засобів і впровадження нових програмних інструментів потребують відповідної підготовки персоналу. Для цього необхідно актуалізувати навчальні програми відповідно до змін обладнання та програмного забезпечення. Навчання має поєднувати теоретичну підготовку з практичною роботою й формувати розуміння можливостей та обмежень технічних засобів і моделей машинного навчання.

Також не потрібно забувати, що засоби РЕБ впливають на власні системами зв’язку та безпілотні комплекси. Узгодження їхньої роботи дозволить зменшити ризик взаємних перешкод.

Отже, запропонована система вдосконалення засобів РЕБ поєднує оновлення програмного забезпечення, технічну діагностику, підготовку

фахівців та узгодження роботи обладнання з власними системами. Машинне навчання розглядається як допоміжний інструмент перевірки програмних оновлень, результати якого потребують підтвердження фахівцем. Такий підхід спрямований на забезпечення стабільної роботи засобів РЕБ та їх послідовної адаптації до змін безпілотних технологій.

Солдатенко А. О., здобувач
Хіжнюк О. А
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ОБҐРУНТУВАННЯ НАПРЯМКІВ МОДЕРНІЗАЦІЇ СТАНЦІЇ ОПТИКО-ЕЛЕКТРОННОГО ПОДАВЛЕННЯ ВЕРТОЛЬОТА З УРАХУВАННЯМ СТАНДАРТІВ НАТО

Станції оптико-електронного подавлення (СОЕП) є ключовим елементом бортових комплексів оборони вертольотів, призначеним для протидії ракетам з інфрачервоними головками самонаведення (ІЧ ГСН). Досвід сучасного збройного протистояння засвідчує, що переносні зенітно-ракетні комплекси (ПЗРК) залишаються однією з головних загроз для вертольотів, а традиційні некогерентні СОЕП втрачають ефективність проти сучасних ракет з багатоспектральними ГСН та засобами протидії.

Метою дослідження є обґрунтування напрямків модернізації станції оптико-електронного подавлення вертольоту з урахуванням вимог та стандартів НАТО, зокрема у частині сумісності, ефективності та архітектурних рішень.

Поточний стан та обмеження існуючих СОЕП нескладно відстежити на прикладі станції “Адрос” КТ-01АВ, що розроблена НВФ “Адрон”, та являє собою типовий приклад некогерентної СОЕП. Вона забезпечує кругову зону захисту, не потребує інформації про тип ІЧ ГСН ракети та працює без системи виявлення пусків. Ймовірність зриву атаки ракети з ІЧ ГСН становить 0,8, що перевищує показники більшості аналогів (не більше 0,5). Станція сумісна з бортовим обладнанням вертольотів Мі-8 та Мі-24, а її серійне виробництво здійснювало НВК “Прогрес”.

Разом з тим, система “Адрос” КТ-01АВ має фізичні обмеження, характерні для некогерентних систем, такі як відносно невисоку спектральну

щільність потужності в робочому діапазоні, на рівні від1,8 до 5,5 мкм, та залежність ефективності від типу ГСН. Час, необхідний для відхилення ракети типу "Stinger" з курсу, становить 0,5–0,8 с, а ймовірність подолання — 0,7–0,8. Для сучасних ракет із захищеними ГСН ці показники можуть бути недостатніми.

Згідно стандартів НАТО, релевантних до СОЕП вертольотів, проведено аналіз чинних стандартизаційних документів НАТО, що дозволяє відокремити ключові вимоги, які мають бути враховані при модернізації СОЕП.

Напрклад, STANAG 4349 визначає вимоги до мінімальної розрізнюваної температурної різниці (MRTD) тепловізійних систем, що безпосередньо впливає на здатність СОЕП виявляти та ідентифікувати загрози. Для сучасних систем цей показник має становити ≤ 0,10 К у вузькому полі зору.

В той же час STANAG 4347 регламентує процедури визначення дальності виявлення, розпізнавання та ідентифікації цілей з використанням тепловізійних систем. Для СОЕП це означає необхідність відповідності розрахункових характеристик виявлення атакуючих ракет стандартизованим методикам.

Існує також STANAG 3873, він же "Electromagnetic Warfare in Air Operations", це документ, що знаходиться на стадії оновлення (редакція 7.1, 2024 р.). Цей документ безпосередньо стосується електромагнітного бою у повітряних операціях. Для СОЕП це означає необхідність інтеграції в єдину систему електромагнітного захисту та відповідності протоколам взаємодії з іншими засобами РЕБ.

Згідно з AQAP (Allied Quality Assurance Publications), або стандартів НАТО із забезпечення якості, зокрема AQAP 2310 для складних авіаційних та оборонних проєктів, визначаються вимоги до систем управління якістю постачальників. Відповідність AQAP є обов'язковою умовою для інтеграції українських СОЕП у спільні проєкти з країнами НАТО.

Під час дослідження напрямків розвитку СОЕП у країнах НАТО було проведено аналіз сучасних західних систем, що дозволяє визначити ключові технологічні тренди, які мають бути враховані при модернізації.

Перша тенденція – це спрямовані засоби ІЧ протидії (DIRCM). Система CIRCM виробництва Northrop Grumman є найбільш поширеною DIRCM-системою у світі, тому що понад 700 одиниць встановлено на вертольотах AH-64, CH-47 та UH-60, статистика вказує на понад 70 000 операційних годин нальоту без втрат. CIRCM використовує лазерне випромінювання для

подавлення ГСН ракети, що забезпечує значно вищу ефективність проти сучасних загроз порівняно з некогерентними системами. У 2026 році Німеччина отримала 47 систем CIRCM для своїх нових вертольотів CH-47 Chinook у рамках вимог НАТО до бойової готовності.

Інший підхід до проблеми показує ізраїльська система SPREOS у складі комплексу AMPS (BIRD Aerosystems), що поєднує радіолокаційне та інфрачервоне відстеження для виявлення, верифікації та нейтралізації атакуючих ракет. Система встановлюється на вертольоти Мі-17 та Мі-24, що свідчить про можливість інтеграції сучасних DIRCM-рішень у платформи радянського виробництва, аналогічні українським.

Компенсаційна система AN/AAR-47(V) виробництва Northrop Grumman являє собою пасивну ІЧ систему попередження про ракетну атаку (MAWS), що призначена для тихохідних літальних апаратів, включаючи вертольоти. Система автоматично ініціює викид теплових пасток при виявленні загрози. Інтеграція подібних MAWS з СОЕП є стандартною практикою в країнах НАТО.

На основі проведеного аналізу можна обґрунтувати декілька напрямків модернізації типової станції оптико-електронного подавлення, наприклад, перехід від некогерентних до лазерних СОЕП (DIRCM-класу). Лазерні системи забезпечують значно вищу спектральну щільність потужності в діапазоні чутливості сучасних ІЧ ГСН, що дозволяє ефективно протидіяти ракетам із захищеними ГСН. Досвід експлуатації CIRCM засвідчує практичну відсутність втрат вертольотів, обладнаних цією системою. Для українських вертольотів Мі-8 та Мі-24 доцільним є створення лазерної СОЕП з масою не більше 60–65 кг, сумісної з існуючими системами викиду теплових пасток (КУВ 26-50).

Наступний крок – це інтеграція з системою попередження про ракетну атаку (MAWS). Некогерентні СОЕП працюють у постійному режимі, що створює демаскуючий фактор та підвищує енергоспоживання. Інтеграція з MAWS дозволяє перевести СОЕП у черговий режим з активацією подавлення лише при виявленні пуску. Це відповідає архітектурі західних систем, зокрема AN/AAR-47(V) у поєднанні з DIRCM.

Технічні обмеження модернізації полягають в необхідності забезпечення сумісності з стандартами НАТО. Модернізована СОЕП має відповідати вимогам STANAG 4349, це чутливість $\leq$ 0,10 К, в комплексі із STANAG 4347, що регламентує стандартизовані методики визначення дальності, а також враховувати

положення STANAG 3873 щодо електромагнітного бою. Для забезпечення якості виробництва та інтеграції необхідною є відповідність AQAP 2310.

Вкрай важливою умовою для впровадження таких модернізацій буде забезпечення ITAR-free постачання. Досвід канадської компанії GSCI, яка позиціонує свої оптико-електронні системи як ITAR-free, засвідчує стратегічну важливість незалежності від американських експортних обмежень для країн НАТО та їх партнерів. Для української СОЕП це означає необхідність використання компонентів та технологій, що не підпадають під обмеження ITAR, з метою забезпечення безперешкодної інтеграції та постачання.

Ефективні комплекси та системи відрізняються модульністю та відкритою архітектурою. Сучасні західні системи, зокрема CIRCM, будуються за принципом відкритої архітектури, що забезпечує можливість швидкого оновлення та інтеграції нових технологій без повної заміни системи. Для української СОЕП доцільним є модульний дизайн, який дозволяє окремо модернізувати лазерний модуль, систему наведення та блок управління.

В якості висновків доцільно зазначити, що модернізація станції оптико-електронного подавлення вертольоту має здійснюватися за декількома стратегіями. Це перехід до лазерних DIRCM-технологій, інтеграція з MAWS для переходу в черговий режим, забезпечення відповідності STANAG 4349, 4347 та 3873, використання ITAR-free компонентів та впровадження модульної архітектури з можливістю поетапного оновлення. Реалізація цих напрямків дозволить підвищити ефективність захисту вертольотів ЗС України від сучасних ПЗРК та забезпечити сумісність з бортовими системами країн НАТО.

Сушко О. Ю., Ph. D., доц.
Товариство з обмеженою відповідальністю
"Науково-виробничий центр "Інфозахист""

РОЗРОБКА ТА ЗАСТОСУВАННЯ УЛЬТРАШИРОКОСМУГОВОЇ АНТЕНИ ДЛЯ РОБОТИ НА ВИСОКИХ ПОТУЖНОСТЯХ

Вступ

Сучасні військові конфлікти демонструють критичну роль засобів радіоелектронної боротьби (РЕБ) у досягненні переваги на полі бою. Особливо актуальним це питання стало для України, де значна кількість загроз пов'язана

із застосуванням безпілотних літальних апаратів, засобів зв’язку, навігації та телеметрії, що працюють у широкому діапазоні частот. Ефективна протидія таким системам потребує створення високопотужних широкосмугових засобів постановки перешкод, ключовим елементом яких є антени.

Типові передавачі РЕБ працюють у діапазоні потужностей від десятків до сотень ват на канал. Для мобільних систем характерні рівні 20-100 Вт, тоді як стаціонарні або спеціалізовані комплекси можуть використовувати потужності 200-400 Вт і більше, в залежності від діапазону частот. Збільшення вихідної потужності – це один із шляхів підвищення ефективності засобів РЕБ, разом із збільшенням підсилення антени (але за рахунок зменшення ширини діаграми спрямованості) та використання спеціальних сигналів, що мають вище ефективність проти заданого каналу зв’язку. Відповідно, розробка антенних систем, що підтримують роботу на таких рівнях потужності в широкому діапазоні частот є актуальною задачею.

Проблематика високопотужних широкосмугових антен

Основними факторами, що обмежують роботу широкосмугових антен на високих потужностях, є:

- локальний перегрів у точках живлення;
- складність забезпечення низького коефіцієнта стоячої хвилі у широкому діапазоні частот.
- ризик електричного пробою при високій напруженості електричного поля;

Для систем РЕБ, що повинні одночасно перекривати декілька діапазонів зв’язку та навігації, додатковою складністю є необхідність забезпечення стабільних характеристик антени в діапазоні, ширина якого може перевищувати одну декаду частот.

Типові вимоги до подібних антен включають:

- роботу в широкому частотному діапазоні;
- низький КСХН;
- високий допустимий рівень потужності;
- достатнє підсилення;
- помірні габарити та масу;
- можливість побудови антенних решіток.

Серед найбільш поширених рішень застосовуються рупорні антени, спіральні антени та логоперіодичні антени. Логоперіодична антена (ЛПА) забезпечує оптимальний компроміс між широкосмуговістю, коефіцієнтом підсилення, масогабаритними характеристиками та технологічністю виготовлення.

Розроблена антена

Для вирішення зазначених задач була розроблена, виготовлена та експериментально протестована ультраширокосмугова логоперіодична антена з робочим діапазоном частот від 0,3 до 8 ГГц.

Конструкція антени виконана за класичною схемою логоперіодичного випромінювача з набором дипольних елементів змінної довжини, розташованих на двопровідній лінії живлення. Низькочастотні елементи були модифіковані до Т- та Г-подібної форми для досягнення компактнішого розміру при тій же робочій смузі частот за рахунок певного зменшення коефіцієнту підсилення. Особливу увагу під час проєктування було приділено вузлу живлення, оскільки саме він зазнає найбільших теплових навантажень при роботі на високій потужності та критично впливає на узгодження антени.

Для зниження втрат використано коаксіальний кабель збільшеного перерізу із низькими втратами. Але варто враховувати, що при збільшенні діаметру коаксіальонго кабелю його вплив на узгодження антени також зростає. Полотно антени виконано із латуні для збільшення теплопровідності і ефективнішого відведення тепла від локальних точок нагріву. Конструкція також передбачає наявність антенного укриття/радому із радіопрозорого матеріалу.

Основні характеристики

Результати експериментальних вимірювань показали, що коефіцієнт підсилення антени змінюється від 5 до 9 дБ у всьому робочому діапазоні частот.

Показники КСХН залишаються на рівні менше 1,5 у діапазоні 0,3-8 ГГц, що свідчить про якісне узгодження антени з трактом передачі, що є критичним для антен для високих потужностей.

Антена має лінійну поляризацію, типові виміряні ширини діаграми спрямованості становлять близько 60° в Е-площині та 90° в Н-площині та є частото-незалежними.

Такі характеристики забезпечують достатньо широкий сектор покриття, що є важливою вимогою для систем постановки перешкод, де необхідно впливати на значну просторову область без застосування складних систем наведення.

Теплові випробування

Одним з головних завдань під час розробки стало підтвердження працездатності антени при підведенні підвищених рівнів потужності.

Під час випробувань на частотах робочого діапазону до антени підводилась безперервна потужність 75 Вт. За результатами 10-хвилинного тесту максимальна температура у точці живлення досягла сталого значення в 50 °С при температурі навколишнього середовища рівній 17 °С.

Для попередньої оцінки роботи антени на вищих потужностях виконано екстраполяцію теплових режимів. Враховуючи, що джоулеві втрати пропорційні квадрату струму і лінійно пов’язані з переданою потужністю, а також закон Стефана-Больцмана, отримано наступні оцінки:

- при потужності 300 Вт температура точки живлення досягне 130-140 °С;
- при потужності 500 Вт температура досягне 190-200 °С без застосування додаткових заходів охолодження.

При таких температурах важливо використовувати спеціальні тугоплавкі припої та переконатись, що матеріали в точках перегріву мають робочі температури нижче за максимальні оціночні.

Застосування в антенних решітках

Перспективним варіантом використання розробленої антени є побудова антенних решіток для підвищення ефективності подавлення за рахунок збільшення сумарної еквівалентної випромінюваної потужності. Наприклад, для решітки з двох антен при несинфазному включенні можемо отримати виграш 3 дБ в порівнянні із використанням однієї антени, що в теорії дає 41% приріст ефективної дальності подавлення. При синфазному включенні виграш зростає до 6 дБ та близько 100% відповідно.

Вибір поляризації також є важливим аспектом практичного застосування. Якщо відома поляризація цілі, то найбільш ефективно буде використати узгоджену поляризацію. Якщо не відома, то часто використовують похилу поляризацію орієнтацією антен під ±45°. Це дозволяє забезпечити універсальність роботи проти цілей на різних поляризаціях при втраті 3 дБ ефективності в найгіршому випадку.

Висновки

Розроблено ультраширокосмугову логоперіодичну антену для систем радіоелектронної боротьби з робочим діапазоном частот 0,3-8 ГГц. Антена

забезпечує коефіцієнт підсилення від 5 до 9 дБ, ширину діаграми спрямованості близько 60° та 90° в Е- та Н-площинах відповідно, а також КСХН менше 1,5 у всьому робочому діапазоні.

Проведені теплові випробування підтвердили можливість роботи з потужністю 75 Вт у безперервному режимі без критичного перегріву. Аналіз показав потенційну можливість масштабування використання даного рішення для рівнів потужності 300…400 Вт без впровадження додаткових заходів тепловідведення.

Завдяки поєднанню широкосмуговості, високої допустимої потужності та можливості формування антенних решіток запропонована антена є перспективним рішенням для сучасних систем РЕБ, призначених для протидії безпілотним платформам та іншим радіоелектронним засобам противника.

СЕКЦІЯ 7
Скрите управління військами

Sheihas V. V.
Vasiyk P. S.
Korolov Zhytomyr Military Institute

MODERN DEVICES FOR COVERT INFORMATION ACQUISITION

The rapid development of microelectronics, wireless technologies and artificial intelligence has radically changed the field of information security. Devices for covert information acquisition (covert devices), which were previously available exclusively to special services, have today become miniature, cheap and technologically advanced. The problem of unauthorized data collection is critical for both the commercial sector (industrial espionage), for the private life of citizens, and for the defense sector (confidential information, state secrets). Privacy protection requires a clear understanding of the modern classification of these devices and the principles of their operation.

Modern special technical means of covert information acquisition are classified by the type of information they intercept: acoustic, visual, geolocation and complex (combined).

GSM/LTE radio microphones that operate via mobile networks. A regular SIM card is installed in the device. The attacker calls her number and secretly listens to the conversation within the microphone's range. The data transmission range of such devices is unlimited, provided there is network coverage.

Super-miniature digital voice recorders, smaller than a 50-kopeck coin, do not emit radio waves (they cannot be detected by field detectors). They are equipped with a voice activation system (VAS) and can record hundreds of hours on built-in memory.

Indirect capture sensors (stethoscopes and lasers). Stethoscope microphones capture voice vibrations from walls or pipes. Laser microphones direct a beam onto window glass from a distance of up to 500 meters. The vibration of the glass from the human voice modulates the laser beam, which returns to the receiver and is decoded back into sound.

Thanks to Pinhole technology (a lens with a narrow entrance hole with a diameter of 1–2 mm), video cameras have become almost invisible to the naked eye.

Autonomous GPS/GLONASS trackers have powerful neodymium magnets for mounting under the bottom of the car. They are in "sleep" mode and are activated only when moving, transmitting coordinates to a server via satellite.

Search trackers (such as Apple AirTag), despite their legal purpose, are often used to be thrown into bags, pockets or cars to covertly track a person's movements through a network of other people's smartphones.

A new challenge has become legal household devices that have vulnerabilities or are pre-configured to collect data. Smart TVs, robot vacuum cleaners with cameras and even modern "smart" air fryers with mobile applications collect audio data, room plans and usage statistics, sending them to manufacturers' servers, which can be hacked or controlled by third parties.

Detection of modern embedded devices requires a comprehensive approach and the use of professional equipment.

The legislation of Ukraine strictly restricts the circulation of special technical means of covert information acquisition, it is strictly forbidden to buy, sell, use or store such devices. The right to use them is exclusively reserved for authorized state bodies during operational-search activities by court decision. The circulation of such means is not limited in all countries, so it is possible to purchase them on foreign marketplaces (for example, AliExpress), but this also falls under the scope of the criminal code and is detained by customs authorities.

The modern market for covert information acquisition devices demonstrates a tendency to full integration into everyday things and digital ecosystems. The fight against this threat cannot be limited to attention alone. It requires regular technical audits of premises, the use of radio monitoring devices and strict adherence to information hygiene (restriction of the use of dubious devices). At the same time, the strict legal framework in Ukraine is a deterrent that protects citizens from mass uncontrolled surveillance.

Метельський Д. І.
Шейгас В. В.
Житомирський військовий інститут імені С. П. Корольова

РОЗРОБКА ТА ВПРОВАДЖЕННЯ АЛГОРИТМУ СКАНУВАННЯ Й МОНІТОРИНГУ СИСТЕМ ДЛЯ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВИТОКІВ ІНФОРМАЦІЇ ЧЕРЕЗ ПОБІЧНІ ЕЛЕКТРОМАГНІТНІ КАНАЛИ

У зв’язку з інтенсивним розвитком інформаційних систем, існує значний ризик витоку конфіденційної та службової через побічні канали, які формуються внаслідок електромагнітного випромінювання від електронних пристроїв. Традиційні методи захисту часто не враховують специфіку генерованих сигналів, тому навіть невеликі недоліки в дизайні або налаштуванні обладнання можуть стати вектором для шпигунських атак. Також, з постійним вдосконаленням технологій та збільшенням щільності електронних компонентів традиційні підходи можуть не забезпечувати належного рівня захищеності. Це створює небезпеку для цілісності систем та збережені важливої інформації від перехоплення противником.

Для подолання зазначених проблем пропонується розробка комплексного алгоритму інструментального контролю з наступними етапами:

1. Аналіз параметрів системи та виявлення критичних точок, тобто на першому етапі проводиться детальний аналіз архітектури системи із застосуванням методів моделювання роботи електронних пристроїв. Цей аналіз дозволяє ідентифікувати основні джерела формування побічних сигналів, визначити їх характеристику та виявити потенційно вразливі ділянки, з яких можуть відбуватися витоки.

2. Побудова вимірювального комплексу, відповідно для реєстрації електромагнітних сигналів впроваджуються сучасні засоби спектроаналізу, високочутливі датчики та інструменти для збору даних у режимі реального часу. Це дозволяє оперативно збирати інформацію про рівні випромінювання, які використовуються для подальшого аналізу в алгоритмі контролю.

3. Автоматизований процес сканування та аналізу, таким чином використання алгоритмів машинного навчання та сучасних статистичних

методів дає змогу проводити порівняльний аналіз отриманих даних з еталонними параметрами, встановленими нормативними документами. Автоматизований моніторинг забезпечує виявлення відхилень у спектральних характеристиках, що можуть свідчити про потенційний витік інформації через побічні канали.

4. Оцінка відповідності нормативним вимогам, тобто результати сканування порівнюються з вимогами стандартів безпеки (ДСТУ, ГОСТ, *ISO/IEC*). Це дозволяє оперативно виявити невідповідності та вчасно впровадити коригувальні заходи, що забезпечують додатковий рівень захисту.

Кожен із перелічених етапів спрямований на створення інтегрованої системи захисту, яка поєднує в собі як апаратні засоби збору даних, так і програмні рішення для їхнього аналізу. Такий підхід дозволяє максимально адаптувати систему до специфіки конкретного об’єкта інформаційної діяльності та умов експлуатації.

Системний підхід до контролю побічних електромагнітних каналів може бути значно розширений за рахунок впровадження новітніх технологій.

Перш за все, інтеграція засобів штучного інтелекту та алгоритмів машинного навчання дозволить здійснювати прогнозування потенційних загроз на основі аналізу історичних даних та поточних показників систем. Така інтеграція сприятиме виявленню нетипових змін у роботі обладнання ще на ранніх стадіях формування загрози, що дозволить оперативно вживати захисні заходи, коли противник тільки почне намагатися заволодіти інформацією.

Крім того, розробка портативних та мобільних версій систем моніторингу забезпечить можливість польового контролю та діагностики під час експлуатації в складних умовах, чи безпосередньо в зоні ведення бойових дій. Впровадження IoT-рішень дозволить інтегрувати систему у більшу мережу захисту, де кожен пристрій стане вузлом, що передає інформацію про потенційні загрози до центральної системи управління безпекою. Таким чином, центральний апарат того чи іншого військового формування, матиме змогу контролювати усі підпорядковані військові частини.

Запропонований алгоритмічний підхід до інструментального контролю побічних електромагнітних сигналів дозволяє забезпечити високий рівень захисту інформації на об’єктах інформаційної діяльності. Завдяки поєднанню ретельного аналізу параметрів, автоматизації процесів сканування і застосування сучасних

технологій моніторингу, ця методика сприяє своєчасному виявленню потенційних загроз і мінімізації ризиків витоку конфіденційної та службової інформації. Результатом є більш стійка система, здатна протистояти сучасним кібератакам навіть за умов швидкоплинних технологічних змін.

Рой І. М.
Шейгас В. В.
Житомирський військовий інститут імені С. П. Корольова

ПРОБЛЕМАТИКА ПОШУКУ ПРИХОВАНИХ ВІДЕОКАМЕР

Розвиток мікроелектроніки та бездротових технологій трансформував сферу відеоспостереження. Разом із корисними системами безпеки з’явився серйозний виклик — поширення засобів прихованого отримання інформації (шпигунських камер). Сьогодні камеру розміром з ґудзик або голівку гвинта можна без зусиль придбати через мережу інтернет. Їх незаконно встановлюють у готельних номерах, орендованих квартирах, роздягальнях, офісах та конференц-залах, об’єктах інформаційної діяльності, де циркулює (може циркулювати) інформація з обмеженим доступом.

Це створює серйозні ризики безпеки інформації (витік комерційної, банківської чи державної таємниці, персональних даних) та особистого життя громадян (порушення приватності). Пошук таких пристроїв став критично важливим завданням, яке щодня ускладнюється технологічним прогресом.

Сучасні об'єктиви типу «*Pin-hole*» (шпилькові вушка) мають діаметр вхідної зіниці менше 1 міліметра. Таку лінзу неможливо помітити неозброєним оком, якщо вона інтегрована в текстуровану поверхню, побутову техніку чи елементи інтер'єру. Камери для прихованого (негласного) спостереження зазвичай вмонтовують у:

датчики диму та руху на стелі чи стінах;

настінні годинники, будильники, нічники;

мережеві адаптери та блоки живлення (які постійно підключені до мережі);

кулькові (чорнильні) ручки, папки та інші канцелярські предмети.

Раніше шпигунські пристрої було легко виявити за допомогою радіочастотних сканерів, оскільки вони постійно випромінювали потужний сигнал. Сучасні пристрої використовують складніші алгоритми:

режим накопичення (*Store and Forward*) у якому камера записує відео на внутрішню карту пам'яті (*MicroSD*) і взагалі не випромінює радіохвиль. Вона активується і передає дані стислим пакетом через визначені проміжки часу (до однієї доби) або за командою зловмисника;

стиснення та маскування трафіку під стандартні протоколи *Wi-Fi* (2.4/5ГГц), *Bluetooth* або стільникових мереж зв'язку *LTE/5G*. У великому офісі чи готелі трафік від шпигунської камери легко губиться серед десятків легальних пристроїв користувачів.

Пристрої, підключені до електромережі 220 В або слабкострумових мереж, можуть працювати роками без обслуговування. Проте навіть акумуляторні моделі завдяки датчикам руху (*PIR*-сенсорам) переходять у режим очікування і споживають мікроампери, що унеможливлює їх фіксацію за тепловим випромінюванням, поки в приміщенні нікого немає.

Для пошуку використовуються три основні технічні підходи. Кожен з них має суттєві обмеження.

Оптичний метод - за якого пристрої випромінюють червоне світло, яке відбивається від матриці камери, створюючи відблиск. Ефективний лише за умови, що оператор дивиться на камеру під прямим кутом. Якщо об'єктив закритий спеціальним напівпрозорим склом (фільтром), вібдлиску не буде. Метод вимагає багато часу та ретельного огляду кожного сантиметра приміщення.

Радіочастотний моніторинг - за якого пристрої фіксують випромінювання під час передачі даних. Безсилий проти камер, які записують на карту пам'яті без трансляції. Також вони дають багато хибних спрацьовувань через роботу легальних роутерів, смартфонів та інших засобів та пристроїв.

Використання тепловізорів, камера під час роботи нагрівається (процесор та матриця виділяють тепло). Сучасні мікросхеми виділяють мінімум тепла. Якщо камера захована глибоко всередині стіни або меблів, тепловий малюнок розсіюється і стає непомітним для тепловізорів.

Найслабша ланка в пошуку прихованих камер — кваліфікація персоналу та відсутність регулярності. Одноразова перевірка приміщення (наприклад, перед важливими переговорами) гарантує безпеку лише на момент самої перевірки. Камеру можуть встановити за п'ять хвилин до початку заходу під виглядом залишеного блокнота чи флешки.

Крім того, професійне обладнання для пошуку (нелінійні локатори, спектроаналізатори) коштує тисячі доларів і вимагає глибоких знань з

радіотехніки від оператора. Дешеві "детектори" з маркетплейсів створюють лише ілюзію безпеки, реагуючи на будь-який побутовий шум.

Проблематика пошуку прихованих відеокамер полягає в технологічному асиметричному паритеті. Створити і заховати камеру сьогодні значно дешевше і простіше, ніж її знайти. Жоден технічний метод окремо не дає 100% гарантії захисту.

Для ефективної протидії необхідно застосовувати виключно комплексний підхід за якого поєднувати оптичний огляд, радіочастотний аналіз та суворий контроль доступу до приміщень. Тільки постійний моніторинг та розуміння психології зловмисника дозволяють мінімізувати ризики шпигунства.

Костерев Д. С.
Будзінська О. О.
Кулініч Ю. М.
Житомирський військовий інститут імені С. П. Корольова

ОСОБЛИВОСТІ ІМПЛЕМЕНТАЦІЇ СТАНДАРТНОГО ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ ОБРОБЛЮВАНОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В БАЗОВИЙ ПРОФІЛЬ БЕЗПЕКИ СИСТЕМИ

Сучасна законодавча база захисту інформації яка обробляється в автоматизованих системах різного типу (інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних) вимагає авторизації з безпеки таких систем, тобто прийняття рішення щодо можливості функціонування (експлуатації) відповідної інформаційної, електронної комунікаційної, інформаційно-комунікаційної, технологічної системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту, криптографічного захисту та кіберзахисту, що приймається у встановленому законодавством порядку. При цьому слід зазначити, що комплексні системи захисту інформації, системи управління інформаційною безпекою з підтвердженою відповідністю, створені до набрання чинності Законом України “Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури”,

застосовуються відповідно до умов їх створення та не потребують повторного підтвердження відповідності (авторизації).

Виходячи з наявних реалій, вибір засобів для застосування у якості комплексу засобів захисту інформації від несанкціонованого доступу (несанкціонованих дій), обмежений вимогами Закону України "Про захист інформації в інформаційно-комунікаційних системах" в частині які визначають обов'язковість використання для захисту інформації в системах засобів технічного та/або криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації або документу про відповідність (крім систем, об'єктів критичної інформаційної інфраструктури, в яких обробляється службова інформація або інформація, що становить державну таємницю), виданий органом з оцінки відповідності, який акредитовано національним органом України з акредитації або національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Перелік засобів технічного захисту інформації (ТЗІ), дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом містить операційні системи з вбудованим комплексом засобів захисту які мають дійсний експертний висновок в галузі ТЗІ та побудовані на основі Microsoft Windows 10 та Microsoft Windows 11, на базі яких в свою чергу були реалізовані комплексні системи захисту інформації, в тому числі й ті які підлягають авторизації з безпеки у відповідності до вимог постанови Кабінету Міністрів України від 18 червня 2025 р. № 712 "Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем".

В доповіді проаналізовано порядок формування комплексу засобів захисту інформації при реалізації заходів захисту визначених Базовим профілем безпеки системи, де обробляється відкрита або конфіденційна інформація та Базовим профілем безпеки системи, де обробляється службова інформація.

Наведений порядок співставлення функціональних критеріїв захищеності визначених нормативним документом НД ТЗІ 2.5-004-99 "Критерії оцінки

захищеності інформації в комп’ютерних системах від несанкціонованого доступу” з заходами захисту наведеними у нормативному документі НД ТЗІ 3.6-006-24 “Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем”.

Зауважено на необхідності вдосконалення “Принципу можливості розповсюдження та/або перетину окремих складових критеріїв, наведених у НД ТЗІ 2.5-004-99 та заходів захисту, що визначені в Каталозі заходів захисту інформації та персональних даних, наведених в НД ТЗІ 3.6-006-24”. Коригування таблиці співвідношення цих критеріїв рекомендовано зробити в зворотній відповідності, для того щоб виконавцю робіт з реалізації заходів захисту була зрозуміла деталізація відповідності функціональних послуг безпеки за кожним рівнем відповідним їм заходам захисту. Після розроблення такого співвідношення, буде одразу зрозуміло, який перелік заходів можна реалізувати застосуванням того чи іншого засобу ТЗІ спираючись на функціональні послуги які можуть їм бути реалізовані у відповідності до експертного висновку в галузі технічного захисту інформації.

Зубелевич Д. І.
Вандалович В. П.
Житомирський військовий інститут імені С. П. Корольова

ДЕМАСКУВАЛЬНІ ОЗНАКИ РОБОТИ ПУНКТУ УПРАВЛІННЯ: РИЗИКИ ТА ЗАХОДИ ЩОДО ЇХ ЗНИЖЕННЯ

Сучасна розвідка може отримувати значущу інформацію навіть без доступу до змісту повідомлень, а лише за самим фактом його наявності. Пункт управління виявляють не лише за прочитаним трафіком, а й за сукупністю ознак його роботи: радіовипромінюванням, ритмом обміну, переміщенням техніки та поведінкою особового складу. Криптографічний захист цю проблему не знімає, оскільки він приховує зміст, але не сам факт і не характер діяльності. Через це керування власними демаскувальними ознаками стає самостійним завданням захисту інформації, рівним за значенням захисту каналів зв'язку.

Для цілей цього дослідження ознаки роботи пункту управління доцільно умовно поділити на чотири групи. Перша охоплює радіоелектронні прояви:

випромінювання засобів зв'язку та абонентських терміналів супутникового зв'язку, роботу радіорелейних ліній, а також побічні електромагнітні випромінювання апаратури. Друга група це метадані обміну: обсяг, тривалість, періодичність сеансів і напрямки передавання. Третя охоплює поведінкові прояви: розпорядок роботи, маршрути підвезення, зміну варт, активність персональних пристроїв. Четверта група фізична: теплові та оптичні ознаки, енергоспоживання, сліди інженерного обладнання позиції. Джерела ознак, канали розвідки й відповідні заходи показано на рис. 1.

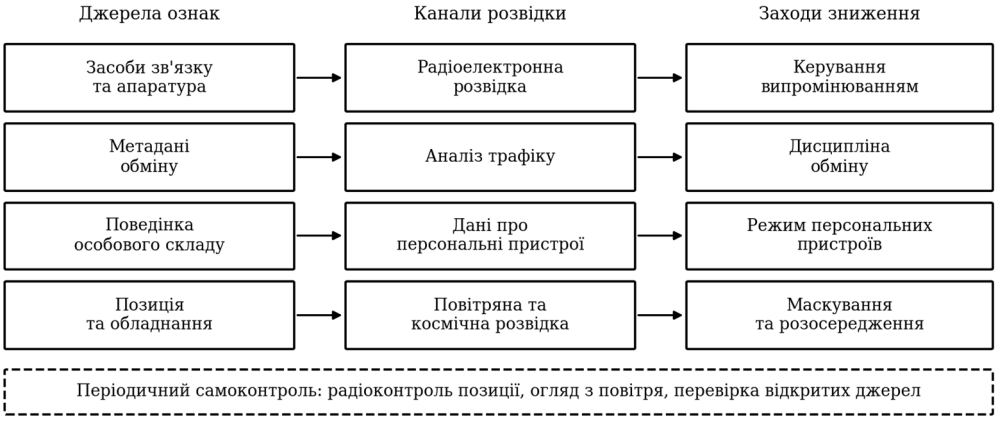


Рис. 1. Джерела демаскувальних ознак, канали розвідки та заходи зниження

Метадані обміну заслуговують окремої уваги, бо їх часто вважають другорядними. Навіть повністю зашифрований канал може розкривати окремі характеристики діяльності: зростання обсягу перед початком заходу, стабільні сеанси в ті самі години, характерні напрямки передавання. Аналіз трафіку є класичним методом радіоелектронної розвідки й не потребує розкриття шифру, тому дисципліна зв'язку за значенням не поступається стійкості алгоритмів.

Найбільш недооціненим джерелом ознак лишаються персональні пристрої. У листопаді 2024 року журналістське розслідування Databroker Files, виконане виданнями netzpolitik.org, Bayerischer Rundfunk і WIRED, показало масштаб проблеми. Безкоштовний демонстраційний зразок від брокера даних містив 3,6 мільярда записів про місцеперебування щонайбільше одинадцяти мільйонів пристроїв у Німеччині за період близько двох місяців. Лише на навчальному полігоні Графенвер у вибірці виявилося понад 190 тисяч сигналів і ідентифікатори 1257 пристроїв, на авіабазі Рамштайн понад 164 тисячі точок від щонайбільше 1275 пристроїв, а дані охоплювали також інші об'єкти. Автори розслідування застерігають, що частина ідентифікаторів і позначок часу в

наборі була некоректною, тому наведені числа є оцінкою згори. За цими записами простежувалися маршрути від казарм до місць проживання й режим змін. Ішлося про рекламні дані, зібрані звичайними застосунками, а не про результат спеціальної операції.

Окремий випадок становлять комерційні канали зв'язку, передусім абонентські термінали супутникових систем. Вони зручні й забезпечують потрібну пропускну здатність, проте залежно від типу системи та режиму роботи створюють періодичні або тривалі радіоелектронні ознаки, зокрема під час реєстрації в мережі, підтримання з'єднання та обміну службовою інформацією. Тобто радіоелектронна ознака може виникати й тоді, коли оператор не передає користувацьких даних. Зменшити ризик дозволяють винесення терміналів від місця розміщення особового складу, обмеження часу роботи, використання кількох рознесених точок доступу та відмова від постійно увімкненого обладнання там, де завдання цього не вимагає.

Наслідки розкриття ознак розрізняються за характером. Виявлення місця та часу роботи створює передумови для вогневого ураження. Розкриття структури обміну може сприяти визначенню того, який саме орган управління працює в цій точці, і відповідно розставити пріоритети цілей. Знання розпорядку може використовуватися для вибору часу впливу на об'єкт. Нарешті, встановлення персоналій відкриває шлях до впливу на конкретних осіб та їхні родини.

Заходи зниження ознак поділяються на кілька напрямів. Керування випромінюванням передбачає режими радіомовчання, роботу мінімально потрібною потужністю, винесення антен від місця роботи особового складу та надання переваги дротовим лініям там, де це можливо. Архітектурні заходи охоплюють розосередження елементів пункту управління, обмеження часу роботи з однієї позиції та застосування хибних позицій.

Дисципліна обміну спрямована проти аналізу трафіку. До неї належать рознесення сеансів у часі, уникнення сплесків обсягу перед заходами, а за наявності технічної можливості зменшення вираженості характерних змін інтенсивності обміну. Режим персональних пристроїв має бути однозначним: зберігання поза робочою зоною, а не вимкнення на місці, оскільки просте вимкнення не завжди є достатнім засобом контролю активності пристрою.

Фізичні заходи охоплюють теплове й оптичне маскування, керування освітленням, маскування енергетичного обладнання та зниження акустичних ознак роботи генераторів. Організаційні заходи передбачають варіювання розпорядку, контроль публікацій особового складу в мережі, інструктаж перед виходом на позицію та перевірку власних ознак у спосіб, у який їх бачить противник.

Слід ураховувати й ознаки, що виникають поза периметром позиції. Ідеться про відкриті відомості, які в сукупності дають змогу встановити район перебування особового складу, наприклад дописи в соціальних мережах, фотографії з геоданими або згадки про побутові потреби підрозділу в певному районі. Жодних технічних засобів розвідки для цього не потрібно, а результат такого зіставлення може створювати цілісну картину діяльності об'єкта, доповнюючи дані технічної розвідки. Протидія тут полягає в інструктажі, роз'ясненні правил родинам і регулярній перевірці того, що про підрозділ можна знайти у відкритих джерелах.

Останній пункт варто розгорнути, бо саме він найчастіше відсутній. Періодичний самоконтроль означає, що визначена група виконує радіоконтроль позиції наявними засобами, оцінює її вигляд із повітря, перевіряє відкриті джерела на згадки, публікації з геоданими та сліди персональних пристроїв, після чого складає перелік виявлених ознак. Як перспективні показники для майбутньої методики можуть розглядатися кількість ознак, виявлених за одну перевірку, і час, потрібний групі для встановлення місця розташування пункту управління від початку пошуку.

Отже, демаскувальні ознаки роботи пункту управління формують окремий клас інформаційних ознак, який не усувається засобами криптографічного захисту. Зниження цих ознак потребує поєднання керування випромінюванням, дисципліни обміну, режиму поводження з персональними пристроями, фізичного маскування та організаційних заходів, а також регулярної перевірки результату власними силами. Подальші дослідження доцільно спрямувати на розроблення методики оцінювання демаскувальних ознак пункту управління з урахуванням ваги кожного каналу розвідки противника.

Романчев А. М.
Боюка М. П., курсант
Житомирський військовий інститут імені С. П. Корольова

КОНТРОЛЬ ЦІЛІСНОСТІ ЕЛЕКТРОННОЇ ТЕЛЕГРАМИ ТА ЇЇ ВІДПОВІДНІСТЬ ОРИГІНАЛУ

Вихідну телеграму готують в електронному вигляді, друкують і подають на підпис уповноваженій особі. Після підписання виконавець приносить паперовий оригінал та електронний файл до підрозділу, який здійснює криптографічний захист і передачу адресату. На цьому етапі можливі розбіжності між двома примірниками: виконавець може помітити помилку й виправити її у Word-документі без повторного підписання. У підсумку може бути переданий текст, який посадова особа не погоджувала.

Працівник підрозділу криптографічного захисту інформації має звірити обидва примірники. За значного потоку телеграм читати кожну сторінку двічі складно, тому перевірка іноді зводиться до зіставлення абзаців і загального розміщення тексту. При цьому зміна дати, числа чи окремого слова майже не впливає на вигляд сторінки. Симетричне шифрування захищає документ під час передавання, однак не відповідає на запитання, чи відповідає електронний текст підписаному паперу.

Для розв’язання цієї задачі пропонується поєднати два способи контролю. Перший фіксує електронний файл у момент підготовки до підписання і виявляє його наступні зміни. Другий порівнює текст із зафіксованого файла з текстом, розпізнаним на скані підписаного оригіналу. Такий порядок залишає за працівником рішення у спірних випадках, але скорочує час на пошук можливих розбіжностей.

Перед друком виконавець остаточно зберігає Word-документ. Перевіряють, чи не залишилися в ньому невирішені виправлення, прихований текст і поля, значення яких змінюється під час відкриття або друку. Із збереженої версії друкують телеграму та обчислюють хеш її файла/ На вільному звороті аркуша з підписом окремою друкарською формою наносять цей хеш, ідентифікатор телеграми, назву файла, кількість сторінок і відомості про додатки. До перевірюваного Word-файла ці дані не додають.

Контрольне значення доцільно надрукувати символами та продублювати QR-кодом. Хеш обчислюють штатним засобом операційної системи

"Powershell", команди "Get-FileHash -Algorithm SHA256 –LiteralPath "Шлях до файлу"".., а QR-код формують вбудованим полем Word у допоміжному документі для друку командою "Displaybarcode "Хеш-значення" QR \q 3". За наявності вже встановленої NAPS2 такий порядок не потребує додаткового програмного забезпечення або онлайн-сервісів. Усі відмітки на звороті друкують до підписання. Уповноважена особа ознайомлюється з обома боками аркуша та засвідчує документ відповідно до встановленого порядку; за потреби візує контрольну відмітку на звороті. Якщо текст виправляють після підписання, фіксацію файла, друк і підписання проводять заново.

Контрольна відмітка залишається поза електронним файлом. Якщо хеш цілого Word-файла вписати в цей самий файл після обчислення, його вміст зміниться і наступне хешування дасть інше значення. Друк хешу з окремої форми на папері не змінює файл. У підрозділі криптографічного захисту інформації зчитують код зі звороту підписного аркуша й порівнюють із хешем наданого файла. За незбігу обробку зупиняють і повертають телеграму для уточнення розбіжностей.

Збіг хешів підтверджує незмінність електронного файла від моменту його фіксації, але сам по собі не відображає, що саме надруковано на папері. Для перевірки змісту необхідно сканувати лицьові сторони підписаного оригіналу із дотриманням порядку сторінок; зворот підписного аркуша зчитують окремо для контролю хешу. У досліджуваному варіанті для цього використалась безкоштовна програма NAPS2, яка створює PDF із розпізнаним текстовим шаром. Розпізнавання налаштовують для української мови; за потреби додають іншомовні пакети.

Важливим є локальна обробка. NAPS2 використовує встановлений на комп’ютері модуль розпізнавання, а потрібні мовні дані можна розмістити на ньому заздалегідь. Під час роботи з телеграмами сканування, розпізнавання та збереження результату виконуються на дозволеному робочому місці без виходу в Інтернет. Текст документа не передається до зовнішнього сервісу. Попереднє завантаження програми і мовних файлів слід організувати окремо від оброблення службових матеріалів.

Практична перевірка роботи NAPS2 на навчальному зразку дала добрий результат розпізнавання друкованого тексту. Це дозволяє використовувати одержаний текст для пошуку можливих відмінностей, хоча сама перевірка не може бути підставою говорити про безпомилковість програми на кожній телеграмі. Якість залежить від чіткості скану, стану паперу, шрифту та

складності таблиць. Тому перед широким застосуванням доцільно випробувати метод на різних за оформленням документах і зафіксувати типові помилки.

Із PDF, створеного NAPS2, розпізнаний текст переносять до Word для порівняння із зафіксованою електронною телеграмою. Функція порівняння Word показує вставлені, вилучені й замінені фрагменти в окремому документі. Розходження в перенесенні рядків або зайвих пробілах можна відділити від змістових змін. Особливу увагу приділяють числам, датам, адресатам і позначенням.

Розпізнавання допомагає працівникові знайти підозрілі місця, але не замінює огляду паперового оригіналу. Програма може пропустити слово, помилитися в таблиці чи неправильно визначити порядок читання колонок. Якщо знайдено змістову розбіжність, матеріали не передають на шифрування до її з’ясування. Після позитивної перевірки використовують саме той файл, для якого обчислено контрольний хеш.

Окремо слід перевірити, як система реагує на невеликі правки. У копіях, створених тільки для випробування, можна змінювати одну цифру в даті, літеру в прізвищі, рядок таблиці або прибирати сторінку. Контрольний хеш має виявити зміну файла, а порівняння зі сканом - указати на відмінність у видимому тексті. Такі випробування дадуть змогу відокремити помилки розпізнавання від справжніх розбіжностей і визначити час, потрібний працівникові для перевірки результату.

Запропонований порядок потребує перевірки в реальному документообігу. Доцільно порівняти час звичайного звіряння і звіряння з NAPS2, перевірити виявлення навмисно внесених змін та підрахувати помилкові позначки розпізнавання. Отримані дані допоможуть визначити, які дії варто автоматизувати повністю, а які залишити за відповідальним працівником. Поєднання контрольної відмітки хешу та локального розпізнавання створює практичний спосіб контролю відповідності електронної телеграми її паперовому оригіналу перед шифруванням та забезпечить цілісність інформації.

Росул Я. М., слухач
Павлюк Н. А.
Житомирський військовий інститут імені С. П. Корольова

ОРГАНІЗАЦІЯ ОПЕРАТИВНОГО ОБЛІКУ ТА КОНТРОЛЮ ФУНКЦІОНУВАННЯ СИСТЕМИ ДОПУСКУ ОСОБОВОГО СКЛАДУ ВІЙСЬКОВИХ ЧАСТИН (УСТАНОВ) ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

В умовах особливого періоду та правового режиму воєнного стану забезпечення своєчасного оформлення і переоформлення допусків до державної таємниці особового складу військових частин (установ) Збройних Сил України набуває особливого значення. Значна кількість посад у військових частинах та органах військового управління передбачає необхідність роботи із секретною інформацією, тому від належної організації системи допуску залежить можливість військовослужбовців своєчасно та в повному обсязі виконувати визначені службові обов'язки.

Відповідно до статті 21 Закону України “Про державну таємницю” у державних органах, установах та організаціях, які провадять діяльність, пов'язану з державною таємницею, створюються режимно-секретні органи (РСО). Вони функціонують як окремі структурні підрозділи та підпорядковуються безпосередньо керівнику відповідного органу або установи. До основних завдань РСО належать недопущення необґрунтованого допуску та доступу осіб до секретної інформації, розроблення і здійснення заходів щодо забезпечення режиму секретності та постійний контроль за їх додержанням.

Надання допуску починається з визначення обґрунтованої необхідності військовослужбовця працювати із секретною інформацією відповідно до його службових обов'язків. Статтею 22 Закону України “Про державну таємницю” встановлено, що допуск надається органами Служби безпеки України (СБУ) після проведення перевірки громадянина. Надання допуску передбачає визначення необхідності роботи із секретною інформацією, проведення відповідної перевірки, взяття особою письмового зобов'язання щодо збереження державної таємниці, отримання письмової згоди на встановлені законом обмеження та ознайомлення з відповідальністю за порушення законодавства про державну таємницю.

Законом передбачено три форми допуску залежно від ступеня секретності інформації. Після оформлення необхідних матеріалів вони у встановленому порядку направляються для проведення перевірки та прийняття відповідного рішення. Важливо розмежовувати поняття “допуск” та “доступ”: допуск є оформленням права громадянина на доступ до секретної інформації, тоді як доступ означає надання повноважною посадовою особою дозволу на ознайомлення з конкретною секретною інформацією відповідно до службової необхідності.

За загальним правилом перевірка громадянина у зв'язку з допуском здійснюється органами СБУ у строк до одного місяця. Водночас законодавством враховано специфіку функціонування військових формувань в особливий період. У разі оголошення мобілізації та/або введення воєнного стану громадянам, які призиваються на військову службу, а також військовослужбовцям і працівникам ЗС України, які переміщуються на посади, зайняття яких передбачає наявність допуску, він надається у десятиденний термін.

Окремим напрямом діяльності РСО є контроль за необхідністю переоформлення допусків. Відповідно до статті 26 Закону переоформлення здійснюється у разі закінчення строку дії допуску за необхідності подальшої роботи із секретною інформацією, необхідності підвищення форми допуску, а також необхідності проведення додаткової перевірки у передбачених законом випадках. Таким чином, забезпечення належного функціонування системи потребує постійного контролю стану оформлення допусків особового складу та своєчасного проведення заходів щодо їх переоформлення.

Разом з тим, в умовах особливого періоду практична реалізація встановленого порядку значно ускладнюється. Однією з основних проблем є часта зміна місць дислокації органів військового управління, штабів та військових частин. Підрозділи та окремі військовослужбовці можуть перебувати на значній відстані від пункту постійної дислокації та РСО своєї військової частини. Внаслідок цього ускладнюється своєчасний збір необхідних відомостей, оформлення документів, їх перевірка та подальше направлення для отримання допуску.

Не менш важливою проблемою є розосередженість особового складу. Постійні кадрові переміщення, довготривалі відрядження та виконання завдань військовослужбовцями у різних районах створюють додаткове навантаження на РСО. Працівникам необхідно одночасно контролювати значну кількість осіб,

строки дії їх допусків та необхідність оформлення або переоформлення відповідних документів. За таких умов особливої ваги набуває своєчасність отримання РСО інформації про кадрові зміни.

Наступною проблемою є ускладнення доставки оформлених документів до відповідних підрозділів СБУ. Необхідність дотримання встановленого порядку пересилання документів у поєднанні з частою зміною дислокації військових частин, значними відстанями та проблемами функціонування фельд'єгерсько-поштового зв'язку в умовах ведення бойових дій може призводити до збільшення фактичного часу слідування документів. У результаті навіть своєчасно підготовлений РСО комплект документів може надходити до відповідного органу із затримкою.

Суттєво впливають на функціонування системи допуску і часті ротації особового складу режимно-секретних органів. Відповідно до Закону на РСО покладається комплекс спеціальних завдань у сфері охорони державної таємниці, а передача цих функцій іншим структурним підрозділам не допускається. Тому зміна працівника РСО потребує забезпечення безперервності обліку: новопризначений військовослужбовець повинен своєчасно встановити, щодо яких осіб уже здійснюється оформлення чи переоформлення допуску, у кого закінчується строк його дії та щодо кого необхідно розпочати відповідні заходи.

Окремим проблемним питанням є комплектування РСО військовослужбовцями, призваними за мобілізацією, які можуть не мати достатнього рівня попередньої фахової підготовки та практичного досвіду роботи у сфері охорони державної таємниці. За умов високого навантаження недостатній практичний досвід може збільшувати вплив людського фактору на своєчасність виконання встановлених процедур.

Сукупність зазначених проблем – зміна місць дислокації, територіальна розосередженість особового складу, ускладнення доставки документів, ротація працівників РСО та різний рівень їх практичної підготовки – ускладнює оперативний облік і контроль стану оформлення та переоформлення допусків особового складу військових частин.

Одним із способів вирішення зазначеної проблеми є впровадження спеціалізованого програмного додатка для внутрішньої організації оперативного обліку та контролю. Його застосування може забезпечити

систематизацію відомостей про особовий склад і відповідні допуски, автоматизований контроль установлених строків та завчасне інформування відповідального працівника про наближення необхідності проведення відповідних заходів. При цьому програмний додаток не замінює встановленого законодавством порядку надання чи переоформлення допуску та має застосовуватися виключно з дотриманням установлених вимог щодо захисту інформації.

Таким чином, удосконалення оперативного обліку та контролю функціонування системи допуску особового складу до державної таємниці набуває особливої актуальності в умовах особливого періоду. Застосування програмного засобу як допоміжного інструменту діяльності РСО може зменшити вплив людського фактору, підвищити своєчасність контролю строків та забезпечити безперервність обліку під час кадрових ротацій, що сприятиме підвищенню ефективності роботи режимно-секретних органів військових частин та установ.

Поліщук Б. В., слухач
Буханевич С. В.
Житомирський військовий інститут імені С. П. Корольова

ЗАХИСТ ІНФОРМАЦІЇ ВІД ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ В УМОВАХ СУЧАСНИХ ВОЄННИХ ЗАГРОЗ

Захист інформації передбачає створення та підтримання необхідного рівня її безпеки шляхом реалізації визначених заходів. Одним із важливих напрямів є протидія витоку інформації технічними каналами. Технічний канал витоку можна розглядати як сукупність фізичного середовища, технічних засобів та умов, за допомогою яких інформація може бути отримана сторонньою особою. Джерелом небезпеки можуть бути електромагнітні випромінювання, акустичні сигнали, вібрації, побічні електромагнітні випромінювання та наведення, а також інші фізичні фактори, що виникають під час функціонування технічних засобів.

У сучасних умовах воєнних загроз ризик технічного витоку інформації посилюється використанням великої кількості електронних пристроїв, засобів бездротового зв'язку, систем відеоспостереження, мережевого обладнання та

автоматизованих інформаційних систем. Додаткову загрозу становить можливість застосування противником спеціальних технічних засобів для збору інформації. Для зниження таких ризиків необхідно насамперед визначити інформацію, яка підлягає захисту, встановити можливі загрози та оцінити технічні канали її витоку. На цій основі формуються вимоги до системи захисту інформації та визначається комплекс необхідних заходів. Важливим елементом захисту є контроль технічного стану приміщень та обладнання. Залежно від визначених загроз можуть застосовуватися екранування, фільтрація, заземлення, обмеження доступу до технічних приміщень, контроль використання електронних пристроїв, а також спеціальні організаційні та інженерно-технічні заходи.

Окрему увагу необхідно приділяти побічним електромагнітним випромінюванням і наведенням, які можуть виникати під час роботи засобів обробки інформації. Для протидії таким каналам використовуються технічні рішення, спрямовані на зменшення рівня небезпечних сигналів та ускладнення можливості їх перехоплення. Не менш важливим напрямом є захист акустичної інформації. У приміщеннях, де здійснюється обговорення інформації з обмеженим доступом, необхідно враховувати можливість її поширення через конструкції будівель, вентиляційні системи, вікна та інші елементи. Залежно від умов можуть використовуватися звукоізоляційні та звукопоглинальні матеріали, організаційні обмеження і спеціальні технічні засоби захисту.

В умовах воєнного стану система захисту інформації повинна бути не лише технічно спроможною, а й адаптивною до зміни загроз. Періодично необхідно проводити оцінювання стану захищеності, перевіряти ефективність застосованих заходів, контролювати дотримання встановлених вимог персоналом та своєчасно усувати виявлені недоліки. Ефективний захист повинен ґрунтуватися на своєчасному визначенні загроз, виявленні можливих каналів витоку та застосуванні комплексу організаційних і технічних заходів. Важливе значення мають контроль технічного стану обладнання, захист від побічних електромагнітних випромінювань і наведень, забезпечення акустичної безпеки та дотримання встановлених вимог ТЗІ.

Гриневич Б. Ю., слухач
Рачкінда В. А.
Житомирський військовий інститут імені С. П. Корольова

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ОЦІНЮВАННЯ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ НА ВІЙСЬКОВИХ ОБ’ЄКТАХ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Повномасштабне вторгнення в Україну та аналіз досвіду ведення російсько-української війни свідчить, що в ході бойових дій збройні сили російської федерації безперервно нарощують зусилля у веденні всіх видів розвідки: радіоелектронної, космічної, кібернетичної, агентурної та оптичної. Інформація про дислокацію підрозділів, наявність озброєння, плани застосування військ та системи управління є пріоритетною ціллю для ворога. Зростання інтенсивності розвідувальних заходів противника призводить до збільшення ризиків витоку інформації циркулюючої на військових об’єктах, що становить пряму загрозу для життя особового складу та успішності виконання бойових завдань. З позицій інформаційної безпеки, будь-який військовий об’єкт (штаб, вузол зв'язку, командний пункт) є середовищем, де циркулює інформація з обмеженим доступом . Витік цієї інформації може відбуватися через різні канали: перехоплення, прослуховування, мережеві кібератаки або через людський фактор (несанкціонований доступ). Тому своєчасна оцінка вразливостей та ідентифікація ризиків витоку є не лише превентивним, а й критично важливим завданням у сфері технічного захисту інформації далі – (ТЗІ). Практичний досвід діяльності підрозділів, на які покладено завдання із захисту інформації існує проблематика щодо великого навантаження на фахівців з ТЗІ, необхідності оперативного ухвалення рішень в умовах динамічної зміни обстановки, а також відсутність у військах зручного та мобільного автоматизованого інструментарію для швидкого моделювання загроз. Своєчасне виявлення потенційних каналів витоку, аналіз встановленого обладнання та наявних засобів захисту відіграє важливу роль у застосуванні дієвих заходів протидії. Зазвичай аудит інформаційної безпеки приміщень потребує тривалого ручного прорахунку математичних моделей ймовірності реалізації загроз. Для проведення всебічного і повного аналізу стану захищеності з метою мінімізації людської помилки доцільно розробити та

запровадити спеціалізований програмний застосунок, який буде допомагати в оцінюванні ризиків. Проблематика оцінювання ризиків витоку інформації в контексті інформаційної безпеки полягає у великій кількісті одночасних факторів (грифи секретності, тип обладнання, канали зв’язку) ускладнює швидкий ручний прорахунок загального рівня вразливості об'єкта; динамічність розгортання військових об'єктів (мобільних пунктів управління) унеможливлює проведення тривалих інструментальних перевірок, вимагаючи експрес-оцінки на місці; низький рівень обізнаності особового складу в розрізі знань про фізику поширення технічних каналів витоку послаблює загальний режим захисту інформації з обмеженим доступом; відсутність єдиної системи, яка б генерувала конкретні рекомендації та візуалізувала слабкі місця, що в свою чергу знижує оперативність реагування на загрози. З позицій інформаційної безпеки розроблений програмний застосунок має на меті виконувати такі функції як захист від розголошення даних – шляхом оперативної ідентифікації і вибору засобів захисту (екранування, генератори шуму, засоби та комплекси криптографічного захисту інформації); підтримка прийняття рішень та рекомендацій – щодо автоматичної генерація ризиків дозволяє раціонально розподілити ресурси; що унеможливить перехоплення підрозділами ворожих розвідок. Отже, автоматизація процесу оцінювання ризиків витоку інформації є критично необхідним кроком для підвищення стійкості систем управління військами в умовах сучасного збройного конфлікту. Впровадження спеціалізованого програмного застосунку дозволить трансформувати складний, тривалий та залежний від людського фактору процес аудиту з ТЗІ у швидкий, точний та надійний інструмент підтримки прийняття рішень. Це забезпечить не лише превентивне перекриття технічних каналів витоку, але й гарантуватиме безперебійний захист відомостей, що становлять державну таємницю, позбавляючи ворожі розвідки можливості здобути критично важливі дані.

Редько А. В., слухач

Кулініч Ю. М.

Житомирський військовий інститут імені С. П. Корольова

ПРОГРАМНА РЕАЛІЗАЦІЯ ПРОЦЕСУ ФОРМУВАННЯ АКТА ОБСТЕЖЕННЯ ОБ’ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЯК ЕЛЕМЕНТ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Інформація у сучасному світі є одним із найважливіших ресурсів. В умовах війни та збройних конфліктів її значення зростає у багато разів, адже саме від захищеності даних залежить ефективність управління військами, планування операцій та виконання бойових завдань. Повномасштабне вторгнення російської федерації в Україну стало переломним моментом, який продемонстрував критичну роль інформаційної безпеки у забезпеченні обороноздатності держави.

Захист інформації охоплює комплекс заходів, спрямованих на запобігання витоку ТКВІ, несанкціонованому доступу до неї неавторизованих та неідентифікованих осіб, модифікації чи знищенню даних.

У військовій сфері це питання має особливу вагу, адже будь-яка втрата чи компрометація інформації може призвести до серйозних наслідків. Саме тому система технічного захисту інформації (ТЗІ) є одним із ключових елементів сучасної оборонної інформаційної інфраструктури.

Разом із тим, процеси документування у сфері ТЗІ залишаються складними. Усталені способи складання актів обстеження, що базуються на ручному написанні даних, мають низку недоліків: вони потребують значних часових витрат, схильні до помилок та ускладнюють подальший аналіз. У військових умовах такі недоліки стають критичними, адже затримки чи неточності можуть вплинути на якість прийнятих рішень і поставити під загрозу правильність впроваджених способів захисту.

Один з варіантів вирішення цього завдання полягає у створенні програмних рішень, які дозволяють автоматизувати процес належного рівня захисту даних. Особливо це важливо у польових бойових умовах, де час і точність мають критичне значення. У ситуаціях, коли військові підрозділи діють

під тиском та в умовах обмежених ресурсів, ручне написання даних стає надто ризикованим: воно може призвести до затримок, невідповідности реальним даним та навіть втрати інформації. Автоматизований програмний додаток у таких умовах забезпечує швидке формування документів, зменшує вплив людського фактору та гарантує захищене зберігання й передачу даних.

Програмний додаток стає важливим елементом системи захисту інформації, який поєднує технічні та організаційні заходи. Його використання дозволяє не лише підвищити ефективність документування, а й забезпечити відповідність сучасним вимогам інформаційної безпеки.

Таким чином, робота в цьому напрямку спрямована на вирішення актуальної науково-практичної проблеми, що має значний вплив на ефективність та безпеку інформаційної діяльності у військовій сфері, яка поєднує теоретичні аспекти організації захисту інформації з практичними завданнями автоматизації процесів документування. Результати дослідження можуть бути використані для вдосконалення системи ТЗІ, підвищення рівня інформаційної безпеки у Збройних Силах України.

Розробка програмного додатку для автоматизації формування Акту обстеження ОІД є актуальним та необхідним кроком у розвитку системи інформаційної безпеки Збройних Сил України. Запропоноване рішення дозволяє підвищити ефективність, стандартизувати процес документування та забезпечити високий рівень захисту даних.

Міщенко Ю. В.
Науково-дослідний центр ракетних військ і артилерії

УДОСКОНАЛЕННЯ СКРИТОГО УПРАВЛІННЯ АРТИЛЕРІЙСЬКИМ ПІДРОЗДІЛОМ В УМОВАХ ТЕХНІЧНОЇ РОЗВІДКИ ПРОТИВНИКА

Сучасні бойові дії характеризуються широким застосуванням противником технічних засобів розвідки, спроможних здійснювати пошук, виявлення, ідентифікацію та визначення місцеположення елементів системи управління військами. Для артилерійських підрозділів ця проблема набуває особливого значення, оскільки функціонування пунктів управління, засобів зв’язку та інших елементів системи управління супроводжується формуванням

сукупності ознак, які можуть бути використані противником для визначення їх місцеположення та характеру діяльності.

У таких умовах скрите управління військами має розглядатися не лише як забезпечення захищеного передавання інформації, а як організація функціонування системи управління, за якої максимально ускладнюється її виявлення та ідентифікація противником при збереженні необхідної оперативності управління.

Одним із основних чинників, що впливає на скритність системи управління, є характер функціонування засобів зв’язку. Робота передавальних пристроїв створює електромагнітні ознаки, які можуть бути виявлені засобами радіоелектронної розвідки. Особливого значення набувають тривалість роботи засобів зв’язку, інтенсивність радіообміну, потужність випромінювання, структура та періодичність сеансів зв’язку. Тому організація управління повинна передбачати раціональне використання засобів зв’язку та недопущення формування стійких ознак, за якими противник може встановити місцеположення елементів системи управління.

Важливим напрямом є також раціональне просторове розміщення елементів системи управління. Концентрація пунктів управління, антенних систем, ретрансляційних та інших технічних засобів в одному районі може сприяти їх виявленню та ідентифікації. Застосування розосередженого розміщення окремих елементів, раціональне використання віддалених антенних систем та зміна їх просторового положення ускладнюють визначення структури системи управління.

Окрему проблему становить прогнозованість функціонування системи управління. Повторення однакових часових, просторових та інформаційних закономірностей може створювати додаткові можливості для технічної розвідки противника. У зв’язку з цим важливим напрямом удосконалення скритого управління є зменшення передбачуваності режимів роботи засобів зв’язку, порядку переміщення елементів системи управління та характеру інформаційного обміну.

Ефективність скритого управління також залежить від дисципліни використання технічних засобів. Порушення встановлених режимів роботи, необґрунтоване збільшення інтенсивності радіообміну або використання додаткових електронних пристроїв може формувати додаткові ознаки для технічної розвідки. Тому контроль за дотриманням встановленого порядку

функціонування системи управління має здійснюватися постійно та бути невід'ємною частиною організації управління.

Таким чином, удосконалення скритого управління артилерійським підрозділом доцільно здійснювати шляхом комплексного поєднання організаційних і технічних заходів, спрямованих на зниження демаскуючих ознак функціонування системи управління. Основними напрямами при цьому є зменшення електромагнітної помітності, раціональне просторове розміщення елементів системи управління, зниження передбачуваності її функціонування та постійний контроль за дотриманням встановлених режимів.

Висновки. У сучасних умовах скритість управління визначається не лише захищеністю інформації, що передається, а й спроможністю системи управління функціонувати без формування стійких ознак, які можуть бути використані противником для її виявлення та ідентифікації. Тому подальше вдосконалення скритого управління артилерійськими підрозділами доцільно пов'язувати з переходом від захисту окремих каналів зв'язку до комплексного управління ознаками функціонування всієї системи управління.

Додурич О. Б.
Ковзало І. Г.
Кулабухов О. М.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ СКРИТНОСТІ УПРАВЛІННЯ ВІЙСЬКАМИ В УМОВАХ ПРОТИДІЇ ТЕХНІЧНИМ ЗАСОБАМ РОЗВІДКИ ПРОТИВНИКА

Досвід широкомасштабної збройної агресії рф проти України засвідчив, що скритність управління військами стала одним із визначальних чинників успішного виконання бойових завдань. Противник застосовує розгалужену систему технічних засобів розвідки (ТЗР): комплекси радіоелектронної розвідки, безпілотні літальні апарати, космічні засоби спостереження. Будь-яке демаскувальне випромінювання чи використання незахищених каналів зв'язку призводить до швидкого виявлення та ураження пункту управління.

Скрите управління військами доцільно розглядати як комплекс організаційних, технічних і криптографічних заходів, спрямованих на приховування від противника змісту, факту та місця здійснення управління. Актуальними аспектами технічного захисту інформації є мінімізація потужності передавачів, застосування спрямованих антен, винесення антенних систем та контроль випромінювань абонентських терміналів супутникового і мобільного зв’язку. У сфері криптографічного захисту інформації першочерговими завданнями є перехід на цифрові засоби зв’язку з гарантованим шифруванням на основі національних алгоритмів та захищене управління ключовими даними.

Особливості сучасних форм і способів протидії ТЗР противника полягають у переході від пасивного приховування до активного управління власною електромагнітною обстановкою: розосередження та регулярна зміна місць розгортання пунктів управління, обмеження часу роботи на випромінювання, застосування сигналів із псевдовипадковою перебудовою робочої частоти, комплексне використання проводових, радіорелейних і супутникових ліній, створення несправжніх радіомереж.

Отже, комплексне застосування технічних, криптографічних та організаційних заходів суттєво обмежує можливості противника щодо виявлення та порушення системи управління військами.

Кулабухов О. М.
Додурич О. Б.
Коноваленко Б. О.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

НЕЙРОМЕРЕЖЕВИЙ КОНТРОЛЬ ТЕХНІЧНОГО СТАНУ КОМПЛЕКСУ ЗАСОБІВ АВТОМАТИЗАЦІЇ В СИСТЕМІ СКРИТОГО УПРАВЛІННЯ ВІЙСЬКАМИ

Протягом останніх років розвиток автоматизованих систем управління військами супроводжується ускладненням їх програмно-апаратної структури, збільшенням обсягів інформації, що обробляється, та підвищенням вимог до

надійності функціонування складових системи. Особливе місце серед них займають комплекси засобів автоматизації (КЗА), які забезпечують збір, передавання, накопичення, оброблення та відображення інформації, необхідної для підтримки процесів управління військами.

Технічний стан КЗА безпосередньо впливає на своєчасність прийняття та доведення управлінських рішень, стійкість функціонування пунктів управління і безперервність управління військами. Порушення роботи окремих технічних засобів може призвести до затримок в обробленні інформації, втрати окремих функціональних можливостей або зниження загальної готовності комплексу. У таких умовах особливого значення набуває своєчасне виявлення ознак погіршення технічного стану обладнання.

Досвід експлуатації КЗА показує, що значна частина відмов не виникає раптово, а формується внаслідок поступової зміни параметрів роботи окремих компонентів. Передвідмовний стан може проявлятися у підвищенні температури, нестабільності напруги живлення, збільшенні кількості помилок під час оброблення або передавання інформації, зростанні навантаження на обчислювальні засоби та інших відхиленнях. Своєчасне виявлення таких змін дозволяє провести додаткову перевірку обладнання та вжити необхідних заходів до виникнення відмови.

Традиційні методи технічного контролю переважно орієнтовані на визначення фактичного стану обладнання за результатами вимірювання окремих параметрів. При цьому не завжди враховується взаємний вплив декількох параметрів та характер їх зміни в часі. У результаті виникають труднощі з визначенням тенденції подальшого розвитку несправності та своєчасним прогнозуванням переходу обладнання до передвідмовного стану.

Одним із напрямів удосконалення технічної діагностики є використання методів машинного навчання та нейромережевих моделей. Їх застосування дає можливість аналізувати значні обсяги експлуатаційних даних і враховувати взаємозв'язки між параметрами, які характеризують роботу обладнання. Це створює можливість не лише виявляти поточні відхилення, а й визначати характер зміни технічного стану КЗА.

Серед різних типів нейронних мереж для такого завдання доцільним є використання багатошарового перцептрона. Його робота може ґрунтуватися на сукупності параметрів, отриманих під час експлуатації КЗА. До них належать

температура окремих вузлів, напруга та струм у колах живлення, завантаженість обчислювальних засобів, кількість помилок під час оброблення і передавання інформації, результати вбудованого контролю та інші характеристики, що відображають стан обладнання.

Особливість такого підходу полягає в тому, що оцінювання виконується не за одним показником, а за сукупністю параметрів та їх взаємними змінами. Це дає можливість виявляти характерні поєднання відхилень, які можуть свідчити про початок розвитку несправності. За результатами аналізу нейромережева модель може визначати поточний технічний стан обладнання та сигналізувати про ймовірне наближення передвідмовного режиму.

Практична цінність такого підходу полягає у можливості виявлення несправностей на ранньому етапі, до втрати працездатності окремих компонентів або комплексу в цілому. Для систем управління військами це має особливе значення, оскільки підтримання справного стану КЗА сприяє збереженню безперервності інформаційного обміну, своєчасному доведенню управлінської інформації та стійкості функціонування пунктів управління.

Гринчевський Я. В., слухач
Завірюха Д. О.
Житомирський військовий інститут імені С. П. Корольова

ВПЛИВ РАДІОПРОЗОРОСТІ МАСКУВАЛЬНИХ МАТЕРІАЛІВ НА ЕФЕКТИВНІСТЬ ВИКОНАННЯ ЗАВДАНЬ ПІДРОЗДІЛАМИ З АКТИВНИМИ ЗАСОБАМИ ПРОТИДІЇ ТЕХНІЧНИМ РОЗВІДКАМ

Аналіз досвіду ведення російсько-української війни свідчить, що в ході планування та проведення бойових дій (операції) на території України збройні сили російської федерації масштабують кількість безпілотних літальних апаратів та інтенсивність ведення повітряної оптичної розвідки, коригування вогню артилерії за допомогою цих апаратів із метою визначення об’єктів вогневого ураження. Крім того, неможливо обійти стороною велику кількість застосування БпЛА типу баражуючих боєприпасів та FPV-дронів, які також оснащені та є носіями засобів оптичної розвідки. Усі перераховані БпЛА створюють великі проблеми об’єктам протидії, які захищають підрозділи

(мобільні групи) протидії технічним розвідкам із активними засобами протидії, створюючи перешкоди каналам управління, телеметрії та передавання даних в електромагнітному середовищі.

Водночас необхідність захисту активних засобів протидії під час їх функціонування обумовлене значним впливом на перебіг та ефективність виконання завдань розвідувальними БпЛА противника. Візуальна, теплова помітність та потужне радіовипромінювання активних засобів ПДТР додатково створює демаскувальні ознаки в видимому, інфрачервоному та радіодіапазонах, які необхідно маскувати. Ефективне маскування цих засобів безпосередньо підвищує живучість як самих комплексів, так і екіпажів, які їх обслуговують, знижуючи ймовірність їх виявлення та ураження противником.

Проте маскувальні комплекти (маски) та інші підручні засоби маскування, антидроновий захист можна віднести до факторів, що знижують ефективність активних засобів ПДТР у площині виявлення та протидії БпЛА в радіодіапазоні за рахунок згасання та спотворення прийнятого та випромінюваного сигналу під час його проходження крізь маскувальні матеріали, що розгорнуті безпосередньо над приймально-передавальними антенами.

З аналізу ведення бойових дій Збройних Сил України маскування має здійснюватися у всіх видах бою, вдень і вночі, за будь-яких погодних умов та в будь-якій обстановці. Воно повинно мати активний характер дій - полягати не лише в пасивному злитті з ландшафтом, а й в активній протидії ворогу через демонстративні дії, тобто створення фальшивих позицій, розгортання макетів техніки та інших засобів.

Обов'язковою є комплексність, яка охоплює одночасний захист від оптичної, оптико-електронної, радіолокаційної, радіотехнічної, акустичної розвідки. Елементи маскування мають вирізнятися переконливістю та реалістичністю, повністю відповідаючи характеру місцевості та пори року, без неприродних форм чи додавання нових демаскувальних деталей. Повинні використовуватися камуфляжні сітки, маскувальні костюми; потрібно усунути будь-який блиск та розмити геометричні контури засобів і техніки.

Фізичні властивості середовища поширення радіохвиль свідчать про можливість згасання радіосигналів через застосування маскувальних комплектів, якими маскують активні засоби протидії технічним розвідкам. Маскувальні комплекти, які виготовлені з підручних матеріалів або

волонтерами, можуть мати різний матеріал, що суттєво впливає на радіопрозорість цих комплектів. Традиційні сітки, що містять провідні або металізовані елементи, часто повністю блокують або суттєво послаблюють радіосигнали. У реальних умовах сучасних бойових дій це змушує операторів виводити антени назовні маскувальних комплектів, що створює додаткові демаскувальні ознаки та збільшує вразливість активних засобів ПДТР.

Не слід також забувати про вологість маскувальних комплектів, які, як правило, виготовляються з текстильних, полімерних або композитних матеріалів. У сухий період згасання радіохвиль може бути не суттєвим, проте після дощу або в умовах високої вологості, характерних для осінньо-зимово-весняного періоду, згасання суттєво зростає, а втрати можуть сягати кількох децибел, а іноді й десятків децибел для багатошарових або щільних конструкцій. Особливо помітний цей ефект на вищих частотах, які активно використовують FPV-дрони та баражуючі боєприпаси противника. Тому при організації маскування засобів підрозділів протидії необхідно враховувати радіопрозорість матеріалів, щоб мінімізувати негативний вплив маскувальних комплектів на функціонування власних засобів ПДТР.

Таким чином, аналіз впливу погодних умов на радіопрозорість маскувальних комплектів у контексті російсько-української війни показує, що вологість, опади та температурні коливання є критичними факторами зниження ефективності активних засобів протидії технічним розвідкам. Для мінімізації цих негативних наслідків необхідно застосовувати матеріали з гідрофобними властивостями, забезпечувати можливість швидкого просушування сіток або передбачати конструктивні рішення, які зменшують накопичення вологи безпосередньо над приймально-передавальними антенами.

Одним із найбільш ефективних рішень є застосування маскувальних сіток з радіопрозорими поверхнями. У бойових умовах застосування таких маскувальних сіток усуває необхідність виводити антени назовні маскування, зберігаючи комплексний захист у видимому, інфрачервоному та радіолокаційному діапазонах. Практичне застосування подібних сіток суттєво знижує демаскувальні ознаки позицій підрозділів протидії.

Другим напрямом є конструктивне розв’язання проблеми шляхом оптимізації взаємного розташування антен і маскувального покриття. Антени активних засобів ПДТР доцільно піднімати над рівнем сітки або розміщувати в

спеціально обладнаних радіопрозорих “вікнах” - ділянках маскування з мінімальним вмістом провідних елементів. У польових умовах такі рішення часто реалізуються шляхом використання легких каркасів або щогл, які дозволяють підняти антени без втрати маскувальних властивостей.

Важливим способом є удосконалення матеріалів маскувальних комплектів. Застосування гідрофобних покриттів і тканин із низьким водопоглинанням суттєво зменшує вплив опадів і вологості на радіопрозорість. Уникнення або локальне обмеження використання металізованих і провідних волокон у зонах над антенами дозволяє знизити згасання сигналу. Перспективним напрямом є розробка комбінованих матеріалів, які поєднують низькі втрати в робочих частотних діапазонах активних засобів ПДТР.

Модульний принцип побудови маскування також дає практичний ефект. Окремі секції сітки над антенними системами можуть бути швидкознімними або відкидними, що дозволяє тимчасово покращувати радіопрозорість під час інтенсивної роботи засобів протидії, а потім відновлювати повне маскування. Такий підхід особливо актуальний для мобільних груп, які часто змінюють позиції в умовах інтенсивних ударів FPV-дронів і баражуючих боєприпасів противника.

У сукупності зазначені способи - радіопрозорі матеріали, конструктивна оптимізація розташування антен відносно маскувальних комплектів, удосконалення складу сіток, модульність і застосування спеціалізованих радіопрозорих елементів - дозволяють суттєво зменшити негативний вплив маскування на ефективність активних засобів протидії технічним розвідкам. Їх впровадження в умовах російсько-української війни підвищує живучість підрозділів і забезпечує більш стабільне виконання завдань з виявлення та протидії безпілотним літальним апаратам противника.

Отже, особливої актуальності набуває розроблення науково обґрунтованої методики оцінювання радіопрозорості маскувальних матеріалів у робочих діапазонах частот активних засобів ПДТР. Така методика має включати вимірювання коефіцієнта проходження сигналу, оцінку впливу вологості, температури та поляризації, а також визначення допустимих рівнів згасання, за яких зберігається ефективність виявлення та протидії.

Водночас необхідно сформувати практичні рекомендації щодо правильного маскування активних засобів ПДТР, орієнтовані на забезпечення живучості екіпажів. Вони мають передбачати оптимальне взаємне

розташування антен і маскувальних покриттів, правильне використання масок або маскувальних сіток, застосування гідрофобних матеріалів, а також дотримання модульного принципу маскування з можливістю швидкого відновлення повного приховування після інтенсивної роботи. Лише комплексне вирішення цих завдань дозволить одночасно зберегти ефективність засобів протидії технічним розвідкам і максимально підвищити живучість як техніки, так і особового складу в умовах сучасного бою.

Рупета Р. О.
Діденко А. П.
Житомирський військовий інститут імені С. П. Корольова

АКТУАЛЬНІ АСПЕКТИ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У сучасних воєнних конфліктах інформація перетворилася на стратегічний ресурс, від рівня захищеності якого залежить ефективність державного управління, діяльності органів влади та боєздатність військових формувань. Будь-яке незаконне втручання в інформаційні потоки — перехоплення, спотворення чи несанкціоноване використання — безпосередньо впливає на якість рішень і стабільність роботи критичних інфраструктур. Тому забезпечення інформаційної безпеки виходить далеко за межі суто технічних рішень і охоплює організаційні та правові механізми. Відповідно до Закону України «Про інформацію», захист інформації являє собою сукупність правових, адміністративних, організаційних, технічних та інших заходів, які забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

В умовах повномасштабної російсько-української війни ці аспекти набули особливої актуальності. Практичний досвід бойових дій підтверджує зростання ролі захищених ліній зв’язку та автоматизованих систем управління військами. Адже надзвичайно стрімко зростає кількість технічних засобів, каналів передачі та методів обробки даних, що, водночас, розширює спектр можливих способів несанкціонованого доступу до інформації.

Потреба в технічному захисті інформації визначається тим, що сучасні технічні засоби під час функціонування можуть випромінювати побічні електромагнітні випромінювання та інші фізичні поля, які потенційно

використовуються для отримання відомостей про їхню роботу. Технічний захист інформації являє собою комплекс заходів, спрямованих на запобігання її витоку через технічні канали.

У сфері технічного захисту інформації однією з найбільш актуальних проблем залишається витік інформації через побічні електромагнітні випромінювання та наведення (ПЕМВН). Сучасні технічні засоби обробки інформації під час функціонування генерують слабкі електромагнітні сигнали, спектральні характеристики яких корелюють з оброблюваними даними. Класична модель TEMPEST передбачала, що такі витоки мають практичне значення переважно в ближній зоні (до кількох метрів). Проте результати досліджень останнього десятиліття суттєво змінили оцінку ризику.

Одним із найбільш показових прикладів атак через побічні електромагнітні випромінювання на значних відстанях є так звані screaming channel атаки, детально досліджені Camurati та співавторами у 2018–2020 роках. Дослідники показали, що в сучасних мікросхемах, де процесор і радіопередавач розташовані на одному кристалі (зокрема в Bluetooth-пристроях), слабкі електромагнітні сигнали від роботи процесора під час шифрування AES-128 мимоволі потрапляють у радіосигнал і разом із ним випромінюються назовні. У результаті інформативний сигнал стає доступним на значно більших відстанях, ніж у класичних атаках ближнього поля. У лабораторних умовах (без зовнішніх перешкод) повний 128-бітний ключ AES вдалося відновити з відстані 10 метрів. У звичайному офісному середовищі з наявністю сторонніх джерел перешкод ключ успішно відновлювався з відстані 15 метрів, а сам інформативний сигнал фіксувався навіть на відстані до 60 метрів. Подальші дослідження 2025–2026 років підтвердили можливість успішного відновлення ключа вже на відстані 30 метрів. Ці результати суттєво змінюють уявлення про реальну дальність дії побічних електромагнітних каналів витоку інформації.

Аналогічно, методи модуляції випромінювання від шин пам’яті (RAM), процесорних ядер або ліній живлення дозволяють організовувати приховані канали витоку з ізольованих (air-gapped) систем. Активні атаки з використанням електромагнітного впливу використовують нелінійності апаратури і здатні переносити низькочастотні інформативні сигнали у високочастотний діапазон, долаючи традиційні засоби захисту інформації від витоку каналами ПЕМВН.

Характерною особливістю проблеми є суттєва відмінність між нормативними вимогами та емпіричними даними. В Україні досі зберігається

практика тотального захисту автоматизованих робочих місць від ПЕМВН відповідно до вимог, близьких до ТР ЕОТ-95. Водночас у відкритому науковому просторі майже відсутні підтверджені експерименти з успішного перехоплення інформативних сигналів на відстанях понад 10 м за допомогою сучасних засобів технічної розвідки. Традиційно вважається, що фізичні фактори — згасання поля, вплив екрануючих конструкцій, рівень електромагнітного шуму середовища — суттєво обмежують дальність пасивного перехоплення. Це створює ситуацію, коли значні ресурси витрачаються на захист від загрози, реальна ймовірність реалізації якої в конкретних умовах бойового застосування часто залишається недостатньо оціненою.

Науково обґрунтованим шляхом вирішення проблеми є перехід від універсального тотального захисту до диференційованого ризик-орієнтованого підходу. Він передбачає TEMPEST-профілювання конкретного обладнання, локальне екранування лише критичних вузлів з експериментальним контролем коефіцієнта екранування в широкому діапазоні частот, застосування активних засобів маскування (генераторів шуму) та фільтрацію ліній живлення відповідно до сучасних стандартів. Такий підхід дозволив би істотно знизити матеріальні витрати при збереженні прийнятного рівня захисту в умовах ведення бойових дій, забезпечивши би при цьому відповідний рівень захищеності інформації.

Соловей В. А.
Маковський І. Ю.
Житомирський військовий інститут імені С. П. Корольова

ВІДНОВЛЕННЯ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ INVISCOMM В УМОВАХ ПОРУШЕННЯ КАНАЛУ СКРИТОГО УПРАВЛІННЯ

Вступ. Порушення транспортного каналу в системах скритого управління може бути спричинене не лише фізичним руйнуванням або радіоелектронним подавленням, а й цілеспрямованим блокуванням, затримкою, перестановкою, повторним відтворенням чи модифікацією пакетів. У моделі D. Dolev та A. Yao (IEEE Transactions on Information Theory, 1983) противник може повністю контролювати транспорт, не маючи безпосереднього доступу до внутрішнього секретного стану кінцевих систем. За таких умов принциповим стає питання:

яким чином відновити інформаційну взаємодію після порушення обміну, не перетворюючи процедуру синхронізації на окремий канал передавання секретного компоненту.

У традиційних системах втрата частини службового обміну може вимагати повторної синхронізації лічильників, ключового контексту або іншої службової інформації. Для каналу скритого управління це створює додаткову вразливість, оскільки процедура відновлення виконується саме в середовищі, яке може контролювати противник. В архітектурі InvisComm (від. англ. Invisible Communication – приховані комунікації) запропоновано інший підхід: порушення поточної взаємодії не повинно автоматично змінювати останній підтверджений спільний стан комунікуючих систем. Відновлення розглядається не як узгодження двох уже незалежно змінених секретних станів, а як продовження або повторне завершення взаємодії від останньої підтвердженої всіма комунікативними системами (КС) симетричної точки.

Мета роботи. Формалізувати механізм відновлення інформаційної взаємодії InvisComm у разі втрати, модифікації, затримки або порушення порядку передавання шифрокодів; визначити умови збереження останнього підтвердженого симетричного стану, або протокольне використання резервної точки відновлення, та способи продовження фазової еволюції без передавання будь-якого секретного компоненту через порушений транспортний канал.

Основні результати. Повний внутрішній стан X_t кожної КС подамо як операційний стан S_t і подієву пам’ять обмеженої фазової глибини H_t:

$$X_t = (S_t, H_t) \quad (1)$$

Операційний стан (ОС) визначає поточний криптографічний контекст, а подієва пам’ять (ПП) акумулює лише ті результати взаємодії, які набули підтвердженого статусу відповідно до протоколу. Для задачі відновлення принциповим є розмежування підтвердженого повного стану та тимчасового локального контексту незавершеної фази. Отриманий шифрокод спочатку проходить логічну безпарольну автентифікацію (ЛБА) – локально-залежний внутрішній механізм InvisComm, що верифікує зовнішнє посилання не спираючись на семантику зашифрованого повідомлення, завдяки чому автентифікується система що сформувала цей шифрокод. Успішна локальна реконструкція навіть верифікованого шифрокоду не впливає автоматично на фазову еволюцію повного стану КС. До фазової еволюції допускається лише

впорядкований транскрипт взаємно підтверджених криптографічних подій (КП) – подієво-унікальне бінарне відображення усієї сукупності процесів що формували та реконструювали верифікований КС шифрокод.

Позначимо через Γ_t предикат завершення поточної фази, а через E_t^c – підтверджений фазовий транскрипт. Межа фіксації стану визначається правилом:

$$\Gamma_t = 1 \Rightarrow X_{t+1} = F_t(X_t, E_t^c) \quad (2)$$

До виконання умови $\Gamma_t = 1$ результати локально прийнятих, але ще не взаємно підтверджених шифрокодів можуть зберігатися лише у тимчасовому протокольному контексті. Вони не інтегруються до E_t^c і не визначають наступний підтверджений стан. Це формує ключовий інваріант відновлення: одинична втрата, пошкодження або затримка пакета може порушити завершення поточної фази або нівелювати відновлення повідомлення але не повинна сама по собі незворотно розвести підтверджені стани легітимних КС.

Нехай Θ_t^A та Θ_t^B – локальні тимчасові контексти систем A і B. Після порушення обміну можливий стан, за якого підтверджена симетрія зберігається, але незавершені локальні контексти вже відрізняються:

$$X_t^A = X_t^B = X_t^c,\ \Gamma_t = 0,\ \Theta_t^A \neq \Theta_t^B \quad (3)$$

Співвідношення (3) описує не компрометацію автентичності, а стан порушеної доступності: обидві КС мають одну й ту саму останню підтверджену криптографічну основу, однак різні уявлення про незавершену частину поточної взаємодії. Саме ця властивість відрізняє відновлення від класичного “пошуку правильнішого” з двох уже розбіжних секретних станів. В InvisComm відновлення повинно спиратися на збережену спільну точку, а не на передавання через транспорт одного з локальних станів іншій стороні.

Додатковим бар’єром є ЛБА. Модифікований, повторно відтворений у невідповідній фазі або зовнішньо сформований шифрокод не може вплинути на підтверджену еволюцію лише за фактом надходження. Для включення пов’язаної з ним КП $e_{t,j}$ до підтвердженого транскрипту необхідні одночасно структурна допустимість шифрокоду в поточному стані та завершення визначеного протоколом життєвого циклу цієї КП:

$$e_{t,j} \in E_t^c \Leftrightarrow V_{X_t}(C_{t,j}) = 1 \wedge L_t(e_{t,j}) = 1 \quad (4)$$

Тут V_{X_t} означає результат ЛБА, а L_t – предикат завершення життєвого циклу відповідної події. Якщо перша перевірка не пройдена, отримане зовнішнє

подання відхиляється. Якщо локальна ЛБА успішна, але взаємне підтвердження не завершене через втрату або блокування наступного пакета, результат залишається тимчасовим. Таким чином, механізм відновлення спирається на дворівневу межу безпеки: зовнішній транспорт не може безпосередньо керувати фазовою еволюцією, а незавершена взаємодія не перетворюється на підтверджену історію системи.

Першим і найпростішим режимом відновлення є відкладене підтвердження. Якщо транспортна можливість відновлюється до переходу від спільного підтвердженого стану, сторони можуть завершити незакінчений життєвий цикл подій у штатній послідовності. У цьому випадку додатковий механізм синхронізації не потрібний: відновлення полягає у завершенні вже розпочатого протокольного ланцюга.

Якщо штатне завершення фази неможливе, застосовується локально-імітаційний режим. Обидві КС, спираючись на один і той самий останній підтверджений стан та заздалегідь визначену умову відновлення ρ_t, локально відтворюють необхідну послідовність приймання і формування шифрокодів на основі імітаційних даних. Такі події не надходять із транспортного середовища і не можуть бути безпосередньо нав’язані зовнішнім пакетом. Непідтверджені розбіжні елементи Θ_t^A і Θ_t^B не використовуються як основа для формування нового підтвердженого стану. За тотожності початкової підтвердженої точки та правила відновлення локально сформовані послідовності є симетричними:

$$X_t^A = X_t^B = X_t^c \ \wedge \ \rho_t^A = \rho_t^B \ \Rightarrow \ E_t^A = E_t^B \ \Rightarrow \ X_{t+1}^A = X_{t+1}^B \qquad (5)$$

Формула (5) виражає основний принцип локального відновлення: симетрія відновлюється не шляхом обміну поточними секретними станами, а шляхом однакового локального відтворення передбаченої протоколом послідовності з уже спільної підтвердженої основи. Після завершення такого локально-імітаційного циклу обидві КС можуть сформувати тотожний підтверджений фазовий результат і продовжити подальшу еволюцію.

Другим архітектурним варіантом є перехід до заздалегідь підготовленого резервного симетричного стану – резервної точки відновлення, який раніше не використовувався у штатній взаємодії. Його безпековий сенс полягає у тому, що після порушення каналу сторони не намагаються передати одна одній поточний стан або “виправити” його через зовнішню інфраструктуру, а переходять до спільно визначеної резервної точки, з якої формується нова траєкторія еволюції.

Необхідною умовою такого режиму є однозначне локальне визначення обома КС необхідної кількості симетричних резервних станів, послідовності їх використання поповнення використаних та моменту переходу на основі попередньо узгодженого сценарію. Конкретний протокол синхронного вибору резервного стану та підтвердження переходу є окремою задачею реалізації і не повинен залежати від поточного секретного стану, від наслідків та причин порушення транспортного середовища.

З позицій скритого управління військами принциповою є саме відсутність “аварійного” винесення довіри у транспортну мережу. Порушник може блокувати доставку, змінювати порядок пакетів або тимчасово припиняти інформаційну взаємодію, однак це не повинно надавати йому можливості сформувати підтверджений стан легітимних КС. Відновлення виконується локально від синхронізованої спільної криптографічної основи, а не через отримання чи оновлення ключового матеріалу або будь-якого іншого секретного цифрового артефакту від зовнішнього постачальника. Це особливо важливо для тактичної ланки, де одна й та сама пара засобів може послідовно використовувати різні, у тому числі скомпрометовані або нестабільні, фізичні транспортні середовища, в умовах відсутності автентифікаційного каналу.

Водночас механізм не усуває проблему доступності. Якщо противник постійно блокує фізичний канал, жоден криптографічний механізм не може гарантувати доставку нової інформації. Запропонований підхід вирішує іншу задачу: не допустити, щоб тимчасове порушення доставки автоматично перетворилося на компрометацію автентичності або неконтрольоване розходження підтверджених секретних станів КС. Тому локальний механізм відновлення InvisComm слід оцінювати за двома незалежними критеріями – збереженням симетрії підтвердженого стану та часом і ймовірністю відновлення інформаційної взаємодії після припинення впливу.

Програмний PoC InvisComm, представлений J. A. Kamlofsky та J. F. Castro Tramontina у репозиторії JFCrypT/InvisComm (GitHub, 2026), уже реалізує двосторонню взаємодію через UDP/Wi-Fi, UART, LoRa та UDP/Ethernet, однак окремі експерименти з механізмом відновлення ще необхідні. Для кількісної перевірки доцільно контрольовано вводити втрати, затримки, перестановку та модифікацію шифрокодів і вимірювати: частку сценаріїв, у яких після припинення впливу сторони повертаються до симетричного підтвердженого

стану; тривалість відновлення; кількість непідтверджених подій, що не були інтегровані до еволюційного контексту; а також відсутність хибного переходу до нового стану під зовнішнім впливом.

Висновки. Відновлення інформаційної взаємодії InvisComm ґрунтується не на повторному передаванні секретного стану, а на збереженні останньої підтвердженої симетричної точки та відокремленні її від тимчасового контексту незавершеної фази. ЛБА і відкладене взаємне підтвердження не дозволяють непідтвердженому транспортному результату автоматично змінити еволюційний контекст. Після порушення каналу взаємодія може бути завершена після відновлення штатного обміну, локально відтворена за симетричними імітаційними правилами або, як резервний архітектурний режим, продовжена від заздалегідь підготовленого симетричного стану. Для систем скритого управління військами це створює передумови відновлення логічної взаємодії без передавання поточного секретного контексту через потенційно скомпрометований транспортний канал. Практична стійкість такого механізму до втрат, перестановки та тривалих переривань потребує окремого експериментального оцінювання.

Метельський Д. І, курсант
Умінський В. В., канд. техн. наук, ст. наук. співроб.
Житомирський військовий інститут імені С. П. Корольова

ЗАГРОЗА ДОВГОСТРОКОВІЙ КОНФІДЕНЦІЙНОСТІ ШИФРОВАНИХ ПОВІДОМЛЕНЬ В УМОВАХ РОЗВИТКУ КВАНТОВИХ ОБЧИСЛЕНЬ

Забезпечення довгострокової конфіденційності інформації з обмеженим доступом потребує врахування перспектив розвитку квантових обчислень. Особливу небезпеку становить модель «збережи зараз, розшифруй пізніше» (Harvest Now, Decrypt Later, HNDL), за якої противник може накопичувати перехоплені зашифровані повідомлення для їх подальшого розшифрування після появи достатньо потужного квантового комп’ютера. Тому для відомостей із тривалим строком секретності підготовка до постквантового захисту має розпочинатися до появи безпосередньої квантової загрози.

Для визначення пріоритетності переходу інформаційних систем військового призначення до постквантового захисту використано підхід Моски, який враховує три параметри: X – строк цінності інформації, Y – час запровадження квантово-стійких крипторафічних алгоритмів та Z – часовий горизонт появи квантової загрози. Критерій має вигляд:

$$X + Y > Z \quad (1)$$

Якщо нерівність виконується, існує ризик, що інформація, перехоплена сьогодні, може бути розкрита до завершення строку її секретності. Рівність лівої та правої частини у виразі (1) не зараховується як виконання критерію, оскільки не залишає запасу часу для реагування.

У роботі значення X і Y є сценарними припущеннями, призначеними для порівняння категорій військових повідомлень. Під час визначення Y враховано стандартизацію нових криптографічних алгоритмів, оновлення програмних та апаратних компонентів, тестування сумісності й сертифікацію. Результати оцінювання наведено в табл. 1.

Таблиця 1 – Приклад оцінювання пріоритетності інформації

Категорія	X **, років**	Y **, років**	$X + Y$	**Пріоритет**
Розвідувальні дані	15	5	20	1 - критичний
Плани бойових дій	10	5	15	2 - високий
Кадрові відомості	5	5	10	3 - середній
Оперативні накази	1	5	6	4 - плановий

Для Z використано три значення: 10, 15 і 20 років. Це не прогноз конкретної дати появи квантового комп’ютера, а часові горизонти для оцінювання стійкості результатів. Горизонт 20 років узято як додатковий, більш віддалений сценарій. За даними Quantum Threat Timeline Report 2025, експертна оцінка ймовірності появи криптографічно значущого квантового комп’ютера (Cryptographically Relevant Quantum Computer, CRQC) протягом наступних 10 років становить 28-49 %, а протягом 15 років – 51-70 %.

За прийнятими сценаріями нерівність (1) виконується для розвідувальних даних у всіх трьох випадках, для планів бойових дій – у двох, для кадрових відомостей – в одному, а для оперативних наказів – у жодному. Відповідно сформовано чотири рівні пріоритету за кількістю сценаріїв, у яких критерій

виконується: три – критичний, два – високий, один – середній, жодного – плановий. Підсумковий порядок має вигляд: розвідувальні дані, плани бойових дій, кадрові відомості, оперативні накази.

Аналіз чутливості показує, що рейтинг залежить від обґрунтованості X. Отже, сценарні припущення доцільно періодично переглядати під час планування переходу до постквантової криптографії.

Принципову зміну криптографічного ризику демонструє приклад RSA-2048. Класична факторизація такого модуля є обчислювально складною, тоді як алгоритм Шора дає змогу виконувати факторизацію цілих чисел на квантовому комп'ютері за поліноміальний час. Оцінка Gidney та Ekera показувала можливість факторизації RSA-2048 приблизно за 8 годин із використанням близько 20 млн шумних фізичних кубітів. У роботі Gidney 2025 року необхідний ресурс оцінено вже менш ніж у 1 млн шумних кубітів за часу виконання менше одного тижня. Ці результати не є прогнозом появи такого комп'ютера, але показують принципову зміну моделі загрози.

Для протидії моделі HNDL першочерговими є облік криптографічних алгоритмів і ключових систем, визначення інформації з найбільшим строком конфіденційності та поетапний перехід найбільш критичних систем. Важливими є також криптографічна гнучкість, використання на перехідному етапі гібридних механізмів і впровадження стандартизованих постквантових алгоритмів. NIST FIPS 203 визначає ML-KEM як стандарт механізму інкапсуляції ключів, а FIPS 204 - ML-DSA для цифрових підписів.

Для симетричної криптографії квантова загроза має інший характер – алгоритм Гровера забезпечує квадратичне прискорення перебору, тому одним із заходів протидії є застосування ключів більшої довжини.

Отже, проведене оцінювання показало, що найвищий (критичний) пріоритет переходу до постквантового захисту мають системи, що обробляють інформацію з більш тривалим терміном цінності, який необхідно періодично переглядати. Загалом, запровадження постквантових механізмів захисту актуальне вже сьогодні, адже дозволить знизити ризик майбутнього розшифрування перехоплених повідомлень.

Мул Д. А., канд. техн. наук, доц.
Прокопенко Є. В., канд. техн. наук, доц.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ПОБУДОВА ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ ТАКТИЧНОЇ ЛАНКИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ В УМОВАХ АКТИВНОЇ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ТА РАДІОРОЗВІДКИ ПРОТИВНИКА

Сучасні бойові дії та виконання завдань із забезпечення недоторканності державного кордону України в умовах повномасштабної збройної агресії характеризуються високою динамічністю, просторовим розмахом та постійним застосуванням противником високотехнологічних засобів радіоелектронної боротьби (РЕБ) та радіоелектронної розвідки (РЕР). У цих умовах стійкість, безперервність, оперативність та прихованість управління підрозділами Державної прикордонної служби України (ДПСУ), які входять до складу Сил оборони України, значною мірою залежать від надійності функціонування спеціальних інформаційно-комунікаційних мереж (ІКМ) тактичної ланки.

Традиційні підходи до побудови мереж зв'язку, що базуються переважно на відкритому радіоефірі або на стандартних топологіях без урахування активного радіоелектронного придушення, виявилися недостатньо ефективними. Противник володіє розвиненими засобами пеленгації та автоматизованого аналізу спектра, що дозволяє йому в режимі реального часу визначати координати джерел випромінювання, наносити по них артилерійські та авіаційні удари, а також здійснювати навмисне радіозавадовий вплив на пункти управління та окремі елементи бойового порядку. З огляду на це, завдання розробки та впровадження інноваційних підходів до побудови захищених ІКМ тактичної ланки ДПСУ, які здатні функціонувати в умовах постійної радіоелектронної протидії та загрози деанонімізації, є надзвичайно актуальним.

Основною метою функціонування ІКМ тактичної ланки ДПСУ є забезпечення надійного та прихованого обміну інформацією між прикордонними нарядами, спостережними та опорними пунктами, мобільними вогневими групами та пунктами управління в умовах жорсткого часового

дефіциту та активних дій противника. Для досягнення цієї мети необхідно розв'язати комплекс науково-технічних та організаційно-тактичних завдань, спрямованих на підвищення завадозахищеності, криптографічного та технічного захисту інформації, а також забезпечення структурної адаптивності мережі.

Одним із ключових напрямків підвищення завадозахищеності та прихованості спеціального радіозв'язку є широке впровадження технологій з низькою ймовірністю перехоплення та виявлення (LPI/LPD). Це досягається за рахунок використання сигнально-кодових конструкцій із псевдовипадковою перебудовою робочої частоти (ППРЧ) з високою швидкістю стрибків, а також розширення спектра методом прямої послідовності (DSSS). Застосування таких режимів дозволяє розсіювати потужність сигналу у широкій смузі частот, роблячи його шумоподібним для засобів РЕР противника, що суттєво ускладнює виявлення фактів передачі даних та пеленгацію джерел випромінювання.

Разом із цим, використання виключно радіоліній не здатне повністю розв'язати проблему забезпечення стійкості управління в умовах масованого застосування засобів РЕБ. Оптимальним рішенням є створення гетерогенних (гібридних) інформаційно-комунікаційних мереж, які інтегрують різні середовища передачі даних: захищені радіолінії тактичного рівня, проводові та волоконно-оптичні лінії зв'язку, супутникові канали, а також спеціальні захищені безпроводові технології ближнього радіуса дії.

Особливе місце в системі зв'язку тактичної ланки ДПСУ посідають проводові та волоконно-оптичні лінії. На відміну від радіоефіру, вони абсолютно стійкі до впливу засобів радіоелектронного придушення противника та не випромінюють електромагнітне сигнал у простір, що робить їх повністю прихованими для радіоелектронної розвідки. Впровадження сучасних польових волоконно-оптичних кабелів підвищеної міцності у поєднанні з портативними медіаконвертерами та захищеними комутаторами дозволяє розгортати високошвидкісні та абсолютно завадозахищені лінії зв'язку між ротними та батальйонними пунктами управління, а також на стаціонарних об'єктах прикордонної інфраструктури.

Для забезпечення гнучкості та самовідновлення мережі в динамічних умовах бою перспективним є використання концепції мобільних радіомереж із довільною топологією (MANET — Mobile Ad-hoc Networks). У таких мережах кожен вузол (радіостанція прикордонного наряду або транспортного засобу)

виконує функції не лише кінцевого термінала, але й маршрутизатора. При виході з ладу окремих вузлів або придушенні завадами певних напрямків зв'язку, мережа MANET автоматично перебудовує маршрути доставки даних через альтернативні вузли. Це дозволяє зберегти зв'язок навіть у випадку часткового руйнування інфраструктури або інтенсивного локального завадового впливу.

Важливим аспектом забезпечення прихованості управління є суворе дотримання режимів радіомовчання та мінімізація часу роботи радіозасобів на передачу. Для реалізації цього принципу в ІКМ тактичної ланки застосовується технологія пакетної передачі даних короткими високошвидкісними сплесками (burst transmission). Замість безперервної передачі мовної інформації у відкритому ефірі, формалізовані текстові повідомлення, дані про обстановку, координати цілей та команди управління стискаються, кодуються та передаються короткою імпульсною посилкою за частки секунди. Засоби РЕР противника просто не встигають запеленгувати таке джерело та навести засоби ураження або завади.

Окрім радіофізичних аспектів, критично важливе значення має забезпечення технічного та криптографічного захисту інформації в мережах. Інформація, що циркулює у системі управління ДПСУ, має різний рівень обмеження доступу, проте вся вона вимагає гарантованого захисту від несанкціонованого доступу, модифікації або навмисного спотворення. Для цього на всіх рівнях ІКМ має застосовуватися надійне симетричне та асиметричне шифрування із використанням вітчизняних та апробованих міжнародних криптографічних стандартів.

Особлива увага повинна приділятися захисту каналів зв'язку при інтеграції спеціальних радіомереж із відомчими інформаційно-комунікаційними системами ДПСУ та Ситуаційними центрами. Використання захищених VPN-тунелів із криптографічним захистом за ГОСТ або алгоритмами AES-256 у поєднанні з апаратно-програмними засобами аутентифікації користувачів дозволяє виключити можливість проникнення противника в закритий інформаційний простір органу охорони державного кордону навіть у випадку захоплення ним окремих термінальних пристроїв.

Для оцінки стійкості та ефективності захищених ІКМ тактичної ланки ДПСУ пропонується використовувати інтегральний показник ефективності

мережі, який враховує ймовірність своєчасної та достовірної доставки інформації в умовах завадового впливу та радіоелектронного спостереження.

Нехай P_{del} — ймовірність успішної доставки пакета інформації від відправника до одержувача, яка залежить від відношення сигнал/завада на вході приймача та коефіцієнта структурної придатності маршруту. Якщо мережа складається з N можливих альтернативних маршрутів, а ймовірність придушення i-го маршруту завадами противника дорівнює $P_{jam}^{(i)}$, то підсумкова ймовірність доставки даних через самовідновлювану MANET-мережу визначається як:

$$P_{del} = 1 - \prod_{i=1}^{N} \left(1 - \left(1 - P_{jam}^{(i)} \cdot P_{succ}^{(i)}\right)\right), \quad (1)$$

де $P_{succ}^{(i)}$ — ймовірність безпомилкового прийому пакета в i-му маршруті за відсутності завад, що визначається параметрами завадостійкого кодування.

Водночас ймовірність розкриття структури мережі засобами РЕР противника P_{disc} суттєво знижується при використанні режимів LPI (Low Probability of Intercept — низька ймовірність перехоплення) та коротких сплескових передач:

$$P_{disc} = 1 - exp\left(-\lambda \cdot T_{trans} \cdot \frac{P_{rad}}{P_{sens}}\right), \quad (2)$$

де λ — щільність просторового розгортання засобів РЕР противника; T_{trans} — сукупний час роботи радіопередавача на випромінювання; P_{rad} — потужність випромінювання передавача; P_{sens} — порогова чутливість приймальних засобів РЕР.

Аналіз наведених співвідношень свідчить, що мінімізація часу випромінювання T_{trans} та зниження потужності P_{rad} за рахунок використання завадостійкого кодування та адаптивного керування потужністю дозволяють експоненційно зменшити ймовірність виявлення вузлів зв'язку ДПСУ противником, зберігаючи при цьому високий рівень ймовірності доставки критично важливої інформації.

Практична реалізація розглянутих підходів у підрозділах ДПСУ вимагає комплексного рішення, що включає переоснащення підрозділів сучасними засобами цифрового завадозахищеного зв'язку, розробку спеціалізованого програмного забезпечення для автоматизованої маршрутизації та керування мережевими ресурсами, а також удосконалення системи підготовки фахівців зв'язку та інформаційних систем.

Важливим напрямком є створення уніфікованих програмно-апаратних комплексів, які дозволяють автоматично обирати найбільш оптимальний та безпечний канал передачі даних (радіо, оптичний, супутниковий) залежно від поточної завадової обстановки, наявності покриття та рівня критичності інформації, що передається.

Таким чином, розбудова захищених інформаційно-комунікаційних мереж тактичної ланки ДПСУ на основі гетерогенних технологій, алгоритмів адаптивної маршрутизації, суворого дотримання режимів прихованості та надійного криптографічного захисту є гарантією забезпечення безперервного, стійкого та прихованого управління підрозділами під час виконання завдань з оборони державного кордону в складній радіоелектронній обстановці.

Новікова Є. В.
Діденко А. П.
Житомирський військовий інститут імені С. П. Корольова

ЗАСТОСУВАННЯ МЕРЕЖЕВОГО ФІЛЬТРА ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ НИЗЬКОЧАСТОТНИМИ КАНАЛАМИ

В умовах повномасштабної збройної агресії проти України захист конфіденційної інформації та службових даних на командних пунктах, в органах військового управління та на підприємствах критичної інфраструктури є питанням виживання держави. Діяльність технічних розвідок противника спрямована на перехоплення речової інформації будь-якими доступними методами, серед яких одне з провідних місць займають побічні електромагнітні випромінювання та акусто-електричні перетворення.

Низькочастотні канали витоку характеризуються здатністю малоамплітудних сигналів поширюватися на значні відстані провідними лініями без суттєвого згасання. Це створює сприятливі умови для їх перехоплення спеціальними технічними засобами. Відсутність комплексних методів протидії зумовлює актуальність дослідження фізичних механізмів формування таких каналів. Мережі електроживлення та заземлення неминуче пронизують усі захищені приміщення, виконуючи роль неконтрольованих антен або «провідників» інформаційного сигналу за межі контрольованої зони.

В умовах нестабільного енергопостачання, постійних обстрілів енергомережі та використання генераторів чи резервних джерел живлення, питання правильного вибору, проєктування та надійного застосування мережевих фільтрів набувають критичної гостроти. Класичні підходи до їх впровадження часто не враховують специфіку новітніх завад, високу інтенсивність розвідувальних атак та особливості роботи обладнання в надзвичайних режимах. Тому дослідження умов ефективного застосування таких фільтрів для блокування низькочастотних витоків є вкрай актуальним науково-практичним завданням.

В сучасному світі для забезпечення захисту від витоку інформації через систему електроживлення широко використовуються спеціалізовані TEMPEST-фільтри. Вони існують у різних форм-факторах: від компактних розеткових блоків до потужних систем на сотні ампер. Їх застосування гарантує відповідність міжнародним стандартам безпеки та захист критично важливих даних у військових, урядових і промислових середовищах. TEMPEST — міжнародний стандарт НАТО та NSA, що визначає вимоги до захисту обладнання від побічних електромагнітних випромінювань.

Фільтри живлення TEMPEST-класу сертифіковані за стандартами SDIP-27/29 (NATO) та NSTISSAM (США) та забезпечують:

– блокування передачі небажаних сигналів через електроживлення;

– багатоступеневу LC-фільтрацію;

– роботу у військових, урядових та фінансових системах

Метою роботи є теоретичне обґрунтування, аналіз та розробка схеми пристрою з покращеними характеристиками з використанням новітніх технологій для гарантованого запобігання витоку речової та конфіденційної інформації низькочастотними каналами в реальних умовах експлуатації на захищених об'єктах. Впровадження цифрових контролерів, які аналізують спектр шумів у реальному часі й автоматично змінюють параметри LC-ланцюгів. Це дозволить фільтру «підлаштовуватися» під конкретне середовище — наприклад, офіс, серверну чи польову станцію.

Вдосконалення та модернізація фільтрів живлення TEMPEST-класу дозволить вирішувати широкий спектр завдань:

1. Інтелектуальна адаптивна фільтрація

Впровадження цифрових контролерів, які аналізують спектр шумів у реальному часі й автоматично змінюють параметри LC-ланцюгів. Це дозволить

фільтру “підлаштовуватися” під конкретне середовище — наприклад, офіс, серверну чи польову станцію.

2. Гібридні фільтри з активними елементами

Поєднання пасивних LC-фільтрів із активними компенсаторами гармонік**.** Такі системи не лише пригнічують паразитні сигнали, а й генерують протифазні імпульси для їх нейтралізації — ефективно «гасить» витік на рівні джерела.

3. Модульна архітектура з багатоканальним екрануванням

Створення модульних TEMPEST-блоків, де кожен канал живлення має окремий екран і фільтр. Це зменшує взаємні наведення між лініями та підвищує рівень ізоляції.

4. Використання наноматеріалів у екранах

Нові композити на основі графену або феритових наночастинок можуть значно покращити поглинання електромагнітних хвиль у широкому діапазоні частот, зменшуючи витік через корпус фільтра.

5. Інтеграція з системами моніторингу безпеки

Додавання сенсорів електромагнітного поля та IoT-модулів, що передають дані про рівень шумів у мережі до централізованої системи безпеки. Це дозволить виявляти спроби перехоплення або аномальні сигнали.

6. Алгоритмічне маскування споживання

Розробка програмних алгоритмів, які змінюють профіль споживання енергії пристроїв, щоб зробити його статистично «плоским» — без характерних піків, що можуть нести інформацію.

Такі вдосконалення перетворюють TEMPEST-фільтри з пасивних елементів на активні системи кіберфізичного захисту, здатні реагувати на загрози в реальному часі. Запропоновані рекомендації та результати дослідження щодо практичного вдосконалення мережевих фільтрів можуть бути безпосередньо використані підрозділами технічного захисту інформації для підвищення рівня безпеки на критично важливих об'єктах сектору оборони України.

Метельська А. І.
Лутченко В. І.
Житомирський військовий інститут імені С. П. Корольова

АВТОМАТИЗАЦІЯ РОБОТИ РЕЖИМНО-СЕКРЕТНИХ ОРГАНІВ ВІЙСЬКОВИХ ЧАСТИН (УСТАНОВ) В УМОВАХ ВОЄННОГО СТАНУ

В умовах сучасних безпекових викликів та триваючої збройної агресії, збереження державної таємниці у військових формуваннях, правоохоронних органах і на об'єктах критичної інфраструктури відноситься до основних завдань системи національної безпеки. Надійність захисту секретної інформації безпосередньо залежить від дієвості режимно-секретних органів (далі – РСО), спрямованих підтримувати встановлений порядок доступу й безперервно відстежувати його дотримання. З початком збройної агресії рф проти України, розпочався процес масового формування нових військових частин та підрозділів. Це призвело до інтенсивного зростання обсягів документообігу та суттєвого збільшення кількості особового складу, який потребує процедур оформлення допуску та надання доступу до секретної інформації.

Однією з вагомих проблем існуючого підходу є традиційна система роботи, сфокусована на ручній обробці великих обсягів паперової документації, яка виявилася неготовою до таких навантажень. Необхідність щоденного опрацювання значної кількості матеріалів спричиняє часові витрати фахівців, сповільнює загальний темп прийняття управлінських рішень та ускладнює моніторинг дійсності допусків.

З огляду на стрімкий розвиток інформаційних технологій та актуалізовану вище проблему, виникає потреба у впровадженні спеціалізованого програмного забезпечення. Автоматизація режимно-секретної діяльності дозволить оптимізувати типові операції, мінімізувати вплив людського чинника та суттєво спростити виконання специфічних завдань із контролю за дотриманням режиму секретності.

Впровадження програмного застосунку для єдиного цифрового обліку суб'єктів режимно-секретної діяльності суттєво підвищить оперативність РСО. Автоматизація щоденних процедур прискорить обробку документів, знизить навантаження на фахівців та сформує надійний цифровий бар'єр для запобігання витоку інформації з обмеженим доступом.

Костерев Д. С.
Соловей В. А.
Житомирський військовий інститут імені С. П. Корольова

МЕТАДАНОНЕЙТРАЛЬНА ІНФОРМАЦІЙНА ВЗАЄМОДІЯ INVISCOMM

Вступ. Одним із суттєвих джерел розвідувальної інформації в сучасному інформаційному протиборстві є не лише зміст перехоплених повідомлень, а й спостережувана структура самого обміну. Навіть за умови криптографічного захисту змісту технічна розвідка може використовувати часові характеристики, інтенсивність, довжини й напрямки пакетів, повторюваність подій та сталі зв’язки між транспортними кінцевими точками для побудови моделей діяльності системи управління.

Дослідження у сфері ідентифікації вебресурсів за профілем зашифрованого трафіку (website fingerprinting) демонструють, що шифрування змісту не усуває можливості класифікації інформаційної взаємодії за зовнішньо спостережуваними характеристиками. Огляд P. Liu, L. He та Z. Li «A Survey on Deep Learning for Website Fingerprinting Attacks and Defenses» (IEEE Access, 2023) систематизує методи машинного та глибокого навчання, здатні використовувати часові, напрямні та структурні закономірності зашифрованих потоків без розкриття змісту повідомлень. Для прихованого управління це означає необхідність захищати не тільки зміст команд і донесень, а й характеристики реального інформаційного навантаження всередині спостережуваного каналу.

Мета роботи. Обґрунтувати метаданонейтральну інформаційну взаємодію архітектури InvisComm (від. англ. Invisible Communication – приховані комунікації) як засіб підвищення скритності інформаційної взаємодії та визначення структури реального обміну корисними даними, що мають залишатися прихованими від зовнішнього спостерігача в межах активного сеансу зв’язку.

Основні результати. Формальна модель InvisComm розглядає повний внутрішній стан комунікативної системи (КС) як синхронізований секретний криптографічний контекст, що фазово еволюціонує та складається з операційного стану і подієвої пам’яті:

$$X_t = (S_t, H_t) \quad (1)$$

Операційний стан визначає контекст поточної фази, а подієва пам'ять є агрегованим внутрішнім станом обмеженої фазової глибини. У межах фази операційний стан залишається незмінним, тоді як робочі стани окремих компонентів подієвої пам'яті можуть змінюватися внаслідок криптографічних і геометричних подій. Після завершення фазового розкладу накопичений подієвий вплив агрегується, а перехід до наступного операційного стану виконується одноразово на основі поточного повного стану та впорядкованого фазового транскрипту.

Повний внутрішній стан визначає конфігурацію віртуального простору, операційні домени, тимчасові правила асоціації та інші фазово залежні параметри формування й реконструкції шифрокодів. Фазовий транскрипт утворюється з верифікованих криптографічних подій (КП) і локально реалізованих геометричних подій. За тотожних початкових станів, операторів і таких транскриптів забезпечується збереження симетрії повних станів взаємодіючих КС.

Для формування одного шифрокоду послідовність із k слів відкритого тексту (ВТ) опрацьовується у k різних операційних доменах (ОД). Кожен ОД має власну підмножину активних об'єктів і тимчасове бієктивне правило, яке однозначно асоціює допустиме значення слова ВТ з одним активним об'єктом. Кожен об'єкт віртуального координатного простору змінює свої координатні параметри у процесах фазової еволюції операційного стану, який складається із сталої кількості ОД. Унікальні в межах фази координатні параметри асоційованого активного об'єкта, після параметризації, перетворюються на раундовий бінарний опис. У результаті k слів ВТ тригерують k раундових бінарних описів із k ОД. Стано- та подієзалежний оператор формує з упорядкованої послідовності таких описів шифрокод – зовнішню бінарну проєкцію відповідної КП. Тому однакове значення слова ВТ не має сталого раундового бінарного еквівалента в інших ОД поточної або наступних фаз. Жоден ОД не використовується у поточній фазі більше одного разу, натомість він змінює координати всіх своїх об'єктів у наступній фазі відносно поточної.

Для метаданонейтральності принциповими є два взаємопов'язані механізми. Перший – використання станозалежних імітаційних даних: за відсутності відповідного слова реального повідомлення його позиція заповнюється

проіндексованим імітаційним словом, яке є повноцінним тригером відповідної доменної події та бере участь у формуванні КП на тих самих умовах, що й слово ВТ. Другий – протокольно визначений послідовний обмін шифрокодами однакової структури і фіксованої в межах фази довжини незалежно від того, сформовані вони з реальних, імітаційних даних або їх поєднання. Тому наявність транспортного пакета сама по собі не означає наявності корисного інформаційного навантаження.

Для прикладної інтерпретації введемо узагальнене зовнішнє спостереження O за активним сеансом як упорядковану послідовність доступних противнику ознак:

$$O_{1:T} = (o_1, \dots, o_T), \;\; o_i = (\tau_i, d_i, \ell_i, C_i), \;\; i = 1, \dots, T \qquad (2)$$

де для кожного передавання відповідно фіксуються часова мітка спостереження τ_i, фізичний напрямок руху пакета d_i, його довжина ℓ_i та спостережуваний шифрокод C_i як доступне зовнішнє представлення КП. Таке спостереження може бути достатнім для встановлення самого факту прямого транспортного з’єднання та його кінцевих точок. Предметом метаданонейтральності InvisComm є інше: у межах активного сеансу узагальнене зовнішнє спостереження $O_{1:T}$ не повинно дозволяти визначати момент, обсяг і фактичний напрямок передавання саме корисного інформаційного навантаження.

Для формального опису цієї властивості позначимо через $Z = (\tau_{\text{info}}, V_{\text{info}}, D_{\text{info}})$ сукупність прихованих характеристик корисного інформаційного навантаження, де τ_{info} – момент його фактичного передавання, V_{info} – обсяг, а D_{info} – фактичний напрямок передавання корисного інформаційного навантаження. Тоді метаданонейтральність у межах прийнятої моделі зовнішнього спостереження можна інтерпретувати як обмеження інформації, яку спостереження $O_{1:T}$ містить щодо Z:

$$I(Z; O_{1:T}) \le \varepsilon \qquad (3)$$

де $I(\cdot;\cdot)$ – взаємна інформація, а ε – допустима залишкова інформативність зовнішнього спостереження щодо характеристик корисного навантаження. У цій роботі умова (3) задає цільовий інформаційно-теоретичний критерій метаданонейтральності, а не доведену властивість довільної реалізації InvisComm. В ідеалізованому теоретичному випадку $\varepsilon \to 0$, тобто накопичення зовнішнього транскрипту не повинно забезпечувати стійкого приросту знань

про момент, обсяг або фактичний напрямок реального інформаційного обміну. Тобто зовнішнє спостереження не містить інформації про визначені характеристики корисного навантаження. У практичній реалізації метою є забезпечення достатньо малого ε для заданої моделі спостерігача. Така умова не означає невидимості самого транспортного сеансу: зовнішній спостерігач може встановлювати факт активного з'єднання, його кінцеві точки та фізичні напрямки руху пакетів, але ці ознаки не повинні надавати достатньої інформації для реконструкції прихованої структури корисного управлінського навантаження.

Це розмежування є принциповим для приховування інформаційної взаємодії у системах управління військами. Фізичний напрямок руху пакета не тотожний фактичному напрямку команди або донесення. Двосторонній обмін шифрокодами може тривати незалежно від того, чи передає сторона реальну команду, отримує відповідь, чи обидві КС опрацьовують лише імітаційні дані в активному сеансі без корисного інформаційного навантаження. Отже, у межах задачі метаданонейтральності критерій захищеності полягає не у приховуванні самого транспортного обміну, а в обмеженні можливості зовнішнього спостерігача відновлювати за ним приховані характеристики реального управлінського обміну.

З позицій протидії технічній розвідці це розширює об'єкт захисту. Поряд зі змістом повідомлень захисту потребує також зв'язок між спостережуваною транспортною активністю та реальним процесом управління. Традиційне криптографічне шифрування спрямоване насамперед на захист змісту повідомлення, тоді як тривале спостереження за зовнішньою структурою трафіку може накопичувати непряму інформацію про ритм управління, інтенсивність бойової роботи та взаємозв'язок дій вузлів. Для метаданонейтрального режиму доцільно формулювати цільову вимогу як відсутність стійкого приросту знань про корисне інформаційне навантаження зі збільшенням тривалості спостереження. Захисний ефект полягає не у «невидимості» каналу, а у зменшенні розвідувальної інформативності його зовнішнього транскрипту щодо реального процесу управління.

Попередня експериментальна перевірка окремих статистичних проявів цієї властивості виконувалася аргентинською дослідницькою групою J. A. Kamlofsky та J. F. Castro Tramontina у програмному PoC InvisComm (2026). Згідно з офіційним звітом, у порівнянні досліджених вибірок Info та Noise не

було підстав відхилити нульову гіпотезу про відсутність статистично значущих відмінностей ($p > 0,05$). Окремо зафіксовано однаковий характер тактування і ритму обміну в обох напрямках; за дослідженими часовими характеристиками зовнішній спостерігач не міг визначити сторону, яка ініціювала реальну інформаційну взаємодію. Ці результати не є універсальним доказом нерозрізнюваності будь-якої реалізації InvisComm і не дозволяють стверджувати про відсутність усіх можливих побічних ознак. Їх доцільно розглядати як попереднє експериментальне свідчення зменшення статистичної розрізнюваності реального та імітаційного інформаційного навантаження за перевіреними характеристиками. Подальше оцінювання має охоплювати незалежні запуски, різні транспортні середовища та посилену модель зовнішнього спостерігача, здатну спільно аналізувати часові, напрямні й доступні структурні ознаки переданих представлень.

Практичне значення підходу полягає у зменшенні можливості противника пов’язувати транспортну активність із конкретними моментами прийняття рішень, появою команд, обсягом донесень або фактичним напрямком корисного інформаційного потоку. Це особливо важливо за тривалого радіо- та мережевого спостереження, коли навіть слабкі непрямі ознаки можуть агрегуватися у розвідувальну модель поведінки системи. InvisComm не приховує факт активного прямого з’єднання та його транспортні кінцеві точки, але доповнює захист змісту механізмами зменшення інформативності зовнішніх ознак реального управлінського обміну.

Висновки. Метаданонейтральність у моделі InvisComm доцільно розглядати як цільову прикладну властивість каналу прихованої взаємодії, що підвищує скритність управління. Спостереження за транспортним середовищем не повинно розкривати момент, обсяг і фактичний напрямок корисного інформаційного навантаження.

Інформаційно-теоретичний критерій (3) дозволяє формалізувати цю властивість як обмеження інформативності зовнішнього спостереження щодо прихованих характеристик реального управлінського обміну.

Попередні результати PoC архітектури InvisComm узгоджуються з такою інтерпретацією в межах перевірених характеристик, але не замінюють подальшого багатофакторного експериментального оцінювання.

Отже, InvisComm доцільно розглядати як засіб зниження розвідувальної інформативності спостережуваного обміну щодо реального процесу управління військами, як протидію засобам технічної розвідки.

Варишнюк В. О.
Казєв О. В.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ОСОБЛИВОСТІ ФОРМ ТА СПОСОБІВ ПРОТИДІЇ ТЕХНІЧНИМ ЗАСОБАМ РОЗВІДКИ ПРОТИВНИКА

Сучасні бойові дії характеризуються насиченістю простору різнорідними технічними засобами розвідки (далі ТЗР): безпілотними літальними апаратами (далі - БпЛА), засобами радіо та радіотехнічної розвідки, оптико-електронними, тепловізійними й радіолокаційними станціями, а також засобами розвідки в кіберпросторі. Їх комплексне застосування дає противнику змогу майже безперервно спостерігати за районом дій, виявляти елементи систем управління та в стислі строки наносити по них вогневе ураження. За таких умов скритність управління військами стає не другорядною вимогою, а необхідною умовою збереження боєздатності пунктів управління (далі - ПУ) і безперервності управління підпорядкованими підрозділами.

Протидію ТЗР противника доцільно розглядати як сукупність взаємопов’язаних заходів, спрямованих на ускладнення виявлення, розпізнавання та визначення місцезнаходження елементів системи управління, а також на зниження достовірності відомостей, які отримує противник. Форми такої протидії різняться за часом проведення. Завчасні заходи охоплюють вибір та інженерне обладнання районів розгортання, підготовку резервних і запасних ПУ, розроблення порядку обміну інформацією та сигналів управління. У ході виконання завдань здійснюються маскування, регулювання режимів роботи засобів зв’язку, чергування засобів виявлення повітряних цілей. Реагувальні заходи застосовуються після виявлення розвідувальної активності і передбачають зміну розташування, перехід на резервні канали та введення противника в оману.

Підґрунтям ефективної протидії є знання демаскувальних ознак, за якими ТЗР розкривають систему управління. Вони поділяються на візуальні (форма й контури техніки, антенні системи, сліди колісної та гусеничної техніки), теплові (нагрів двигунів, генераторів, обігрівачів і місць перебування особового складу), радіоелектронні (випромінювання радіозасобів, їх частота,

інтенсивність і періодичність роботи), акустичні, а також ознаки діяльності - інтенсивність руху транспорту й кур’єрів, концентрація людей, регулярність виходів на зв’язок. Практика свідчить, що найбільшу небезпеку становлять радіоелектронні ознаки та ознаки фізичної діяльності, оскільки їх важче приховати засобами лише візуального маскування, а аналіз у динаміці дає змогу противнику відновити структуру управління навіть без прямого спостереження за ПУ.

Основою радіоелектронної скритності є свідоме обмеження випромінювання. До способів її забезпечення належать скорочення часу роботи радіозасобів на передавання, використання мінімально необхідної потужності та спрямованих антен, винесення антен від ПУ, застосування короткого формалізованого обміну повідомленнями, своєчасна зміна частот і позивних. Там, де обстановка дозволяє, слід віддавати перевагу проводовим і волоконно-оптичним лініям, кур’єрському зв’язку та передаванню розпоряджень за заздалегідь визначеними сигналами. Доцільним є запровадження режимів обмеження роботи радіозасобів, що змінюються залежно від етапу підготовки й ведення дій: від повного радіомовчання до роботи лише на прийом. Окремої уваги потребує контроль особистих електронних пристроїв військовослужбовців, які можуть унеможливлювати навіть ретельно сплановані заходи маскування.

Протидія розвідці з повітря потребує поєднання пасивних і активних способів. До пасивних належать використання природних укриттів і рельєфу, багатошарове маскування з урахуванням видимого та теплового діапазонів, розосередження елементів ПУ, дотримання маскувальної дисципліни під час руху та роботи, ліквідація слідів діяльності. До активних – організація постів спостереження, виявлення БпЛА за допомогою спеціальних засобів, радіоелектронне подавлення каналів керування й передавання даних, а також вогневе ураження повітряних цілей підготовленими екіпажами. Жоден із цих способів не є універсальним, тому їх слід поєднувати в єдину систему прикриття ПУ з визначеними відповідальними особами та порядком дій за сигналами оповіщення.

Важливе значення має імітація та дезінформування. Створення хибних ПУ, імітаторів радіовипромінювання, макетів техніки й видимої активності спрямоване на розпорошення сил розвідки противника, виснаження його ресурсу та формування хибних уявлень про розташування й структуру управління. Однак імітація буде результативною лише тоді, коли хибні об’єкти за сукупністю ознак узгоджені з реальними: некоректна імітація легко

розпізнається і навіть допомагає противнику уточнити справжнє розташування. Поряд з цим застосовується принцип мобільності: ПУ не повинен перебувати в одному місці довше, ніж це необхідно для виконання завдань управління. Практичну реалізацію забезпечують розосередження елементів ПУ, підготовка резервних позицій і здатність швидко передавати управління між ними без втрати контролю над підрозділами.

Не менш значущими є організаційні та морально-психологічні чинники. Навіть найдосконаліші технічні рішення втрачають ефективність через порушення дисципліни: невиправдане виходження в ефір, використання мобільних телефонів із геолокацією, публікація інформації в соціальних мережах, недбале маскування під час тривалого перебування на позиції. Тому система підготовки командирів, штабів і підрозділів зв'язку має передбачати регулярні тренування в умовах імітованого впливу розвідки противника, систематичний контроль за дотриманням вимог скритності та використання власних засобів радіотехнічного контролю для виявлення витоків демаскувальної інформації.

Ефективність протидії ТЗР доцільно оцінювати не за окремими заходами, а за результатом для системи управління загалом. Основними критеріями можуть бути зниження ймовірності виявлення ПУ, тривалість їх безперервного функціонування, час відновлення управління після зміни розташування, кількість зафіксованих порушень режимів скритності та частка підрозділів, що виконали завдання без втрати управління.

Отже, протидія ТЗР противника при забезпеченні скритного управління військами має бути комплексною, адаптивною та постійною. Вона повинна поєднувати зниження демаскувальних ознак, регулювання радіоелектронної активності, захист від розвідки з повітря, імітацію та дезінформування, мобільність ПУ й високий рівень дисципліни особового складу. Реалізація цих положень у практиці підготовки командирів і штабів, зокрема підрозділів Державної прикордонної служби України, що діють у складі Сил оборони, сприятиме збереженню стійкого управління та зменшенню втрат за умов активної розвідувальної діяльності противника.

Гурковський М. Ю.
Житомирський військовий інститут імені С. П. Корольова

МЕТОД ЗАХИЩЕНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ НА ФЛЕШ-НАКОПИЧУВАЧАХ

Захист інформації з обмеженим доступом (ІзОД) є головною задачею підрозділів охорони державної таємниці. В підрозділах, де передбачена робота з ІзОД, вона зберігається на попередньо облікованих флеш-накопичувачах у відкритому вигляді, що може створювати передумови до її витоку та в подальшому завдати шкоди державі. Саме тому для підвищення рівня безпеки зберігання ІзОД та, відповідно, зменшення ризиків можливого її витоку та доступності стороннім особам, у разі втрати флеш-накопичувача або його викрадення, пропонується створити програмний застосунок шифрування флеш-накопичувачів.

Метою роботи буде створення програми, яка дозволить мати захищене зашифроване сховище на стандартному флеш-накопичувачі. Вона має гарантувати захист від несанкціонованого доступу до даних, навіть якщо стороння особа отримає фізичний доступ до накопичувача.

Основою програми буде створення багаторівневого криптографічного алгоритму захисту даних. Пароль, введений користувачем, буде лише однією зі складових всього алгоритму захисту. До пароля додається унікальна випадкова послідовність байтів - «сіль», після чого за допомогою алгоритму формування ключів і хешування паролів Argon2id пароль в комбінації з «сіллю» перетворюється на ключ шифрування ключа (КШК). Алгоритм AES-256-GCM у системі застосовуватиметься двічі: спочатку КШК захищає ним окремо згенерований ключ шифрування даних (КШД), а вже КШД цим самим алгоритмом безпосередньо шифрує вміст файлів. Завдяки такому розподілу ключів зміна пароля не потребує перешифрування всіх даних. Великі файли обробляються блоками, тож їх не потрібно повністю завантажувати в оперативну пам'ять. Графічний інтерфейс відокремлений від криптографічного ядра.

У результаті отримаємо модульний програмний застосунок, де кожна підсистема відповідає лише за своє завдання. Криптографія виконує зашифрування та розшифрування даних. Автентифікація перевіряє пароль, введений користувачем, та правильність похідного ключа, а підсистема керування контейнером формує структуру сховища з розподіленням інформації

на ту, яка має бути відкритою для коректної роботи застосунку, і ту, яка обов’язково має бути захищеною шифруванням. Тому без успішної автентифікації неможливо дізнатися ні імена файлів, ні структуру збережених даних. Також передбачена обробка нештатних ситуацій: від'єднання носія під час зашифрування чи розшифрування, пошкодження контейнера чи невдалу перевірку тега автентичності. У таких випадках повідомлення про помилку не має розкривати внутрішнього змісту інформації.

Основна цінність в тому, що дана програма дає змогу зробити захищеним носієм будь-який флеш-накопичувач без використання спеціального обладнання. Це підвищує рівень безпеки в повсякденній роботі, зменшує ризики витоку ІзОД, якщо носій буде втрачено, викрадено або захоплено. Вона доповнює всі заходи захисту ІзОД, відповідаючи за захист даних, що зберігаються фізично.

Васянович В. В.
Житомирський військовий інститут імені С. П. Корольова

ФУНКЦІОНАЛЬНА СТРУКТУРА ПРОГРАМНОГО ЗАСТОСУНКУ УПРАВЛІННЯ ДОСТУПОМ ДО ЕЛЕКТРОННИХ НОСІЇВ ІНФОРМАЦІЇ

Сучасні інформаційні системи характеризуються постійним збільшенням обсягів інформації, що зберігається та обробляється на електронних носіях. До таких носіїв належать USB-накопичувачі, зовнішні твердотільні та магнітні накопичувачі, карти пам’яті, оптичні диски та інші пристрої, здатні забезпечувати зберігання або перенесення цифрових даних. Використання знімних носіїв є зручним з погляду обміну інформацією, однак одночасно створює додаткові ризики несанкціонованого доступу, копіювання, модифікації, втрати або винесення інформації за межі контрольованого інформаційного середовища.

Особливої актуальності набуває завдання забезпечення контрольованого використання електронних носіїв інформації (ЕНІ) у системах, де обробляється інформація з обмеженим доступом. Застосування лише системних засобів операційної системи не завжди забезпечує необхідний рівень централізованого контролю, журналювання та адаптації політики доступу до конкретних умов

функціонування організації. Тому доцільним є створення спеціалізованого програмного застосунку, який реалізує єдиний механізм ідентифікації носія, автентифікації користувача, перевірки його повноважень, прийняття рішення щодо доступу та реєстрації відповідних подій.

Метою роботи є обґрунтування структури та принципів функціонування програмного застосунку управління доступом до ЕНІ, який забезпечує контроль підключення носіїв, розмежування прав користувачів, реєстрацію операцій та централізоване застосування політики інформаційної безпеки.

Для досягнення мети проаналізовано основні етапи використання ЕНІ в складі інформаційної системи: його підключення до робочої станції, ідентифікацію, визначення користувача, перевірку політики безпеки, надання або блокування доступу та подальше фіксація дій. В основу запропонованого підходу покладено принцип мінімальних повноважень, відповідно до якого користувачеві надається лише той обсяг прав, який необхідний для виконання визначених завдань.

Функціональну структуру програмного застосунку доцільно подати у вигляді декількох взаємопов’язаних модулів. Модуль ідентифікації носія, який визначає підключений пристрій за його технічними параметрами та унікальними ідентифікаторами. Модуль автентифікації користувача – встановлює особу суб’єкта доступу з використанням визначеного організацією механізму автентифікації. Модуль авторизації – порівнює отримані ідентифікаційні дані з установленою політикою доступу та визначає дозволені операції. Модуль журналювання – реєструє факти підключення, відключення, дозволу, блокування та інші значущі події.

Запропонована логіка прийняття рішення може бути представлена послідовністю: «виявлення носія, ідентифікація носія, ідентифікація та автентифікація користувача, перевірка політики, прийняття рішення, надання/блокування доступу, журналювання події». Такий підхід дає змогу розглядати доступ не як одноразову операцію операційної системи, а як контрольований процес, у якому рішення залежить одночасно від властивостей носія, суб’єкта доступу та встановлених правил.

Політика доступу може містити перелік дозволених і заборонених носіїв, групи користувачів, типи дозволених операцій, часові обмеження та вимоги до реєстрації подій. Для підвищення керованості системи доцільно застосовувати

рольову модель розмежування доступу. У такому випадку права визначаються не безпосередньо для кожного користувача, а для відповідної ролі, після чого користувач отримує необхідні повноваження через належність до цієї ролі.

Важливим результатом дослідження є визначення вимог до журналу подій. Для кожної контрольованої операції доцільно зберігати щонайменше час події, ідентифікатор користувача, ідентифікатор електронного носія, тип операції, прийняте рішення та результат виконання операції. Наявність таких відомостей створює основу для подальшого аналізу подій безпеки, виявлення порушень установленої політики та проведення службових перевірок.

Для програмної реалізації доцільним є використання клієнтського компонента на робочій станції та централізованого компонента керування політиками. Клієнтський компонент здійснює моніторинг подій підключення носіїв, виконує локальні перевірки та застосовує отримані правила. Центральний компонент забезпечує зберігання політик, облікових даних і журналів та надає адміністратору засоби налаштування. Така архітектура забезпечує відокремлення функцій контролю від функцій адміністрування.

У межах дослідження визначено основні сценарії роботи застосунку. До базових сценаріїв віднесено: дозволене підключення зареєстрованого носія; блокування невідомого носія; дозвіл доступу користувачу з відповідними повноваженнями; відмову в доступі користувачу без необхідних прав; фіксацію спроб порушення політики; формування журналу подій для подальшого аналізу. Отримані результати можуть бути використані як основа для створення програмного прототипу та його подальшого функціонального розширення.

З погляду захисту інформації застосунок має забезпечувати не тільки механізм дозволу або заборони доступу, а й контрольованість усіх критичних дій. Для цього необхідно передбачити захист журналів від несанкціонованої зміни, розмежування адміністративних повноважень, перевірку коректності політик, оброблення помилок та контроль цілісності конфігураційних даних. Реалізація цих положень дає змогу підвищити керованість використання електронних носіїв та зменшити ризик неконтрольованого переміщення інформації.

Отже, у результаті проведеного дослідження обґрунтовано доцільність застосування спеціалізованого програмного засобу для управління доступом до ЕНІ. Визначено основні функціональні компоненти такого застосунку. Запропонована послідовність прийняття рішення забезпечує комплексний контроль доступу та дає змогу враховувати одночасно характеристики носія, повноваження користувача й установлені правила безпеки.

Березюк К. О.
Житомирський військовий інститут імені С. П. Корольова

АКТУАЛІЗАЦІЯ НОРМАТИВНИХ ДОКУМЕНТІВ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ЗА ДОСВІДОМ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ рф ПРОТИ УКРАЇНИ

Нормативна база у сфері охорони державної таємниці та технічного захисту інформації (ТЗІ) формується з урахуванням надійного захисту інформації з обмеженим доступом (ІзОД). В той же час повномасштабна збройна агресія рф проти України призвела до необхідності перегляду підходів до захисту ІзОД. Умови розгортання об’єктів інформаційної діяльності в зонах (районах) ведення бойових дій, а також переміщення технічних засобів створюють ситуації, які не завжди враховані керівними документами, розробленими раніше.

Одним із важливих напрямків для оновлення має бути актуалізація вимог до захисту ІзОД від витоку через технічні канали. ТЗІ передбачає виявлення та блокування каналів, через які інформація може потрапляти до противника без прямого доступу до фізичного носія. Реальність витоку інформації через технічні канали безпосередньо пов’язана з існуванням технічного каналу для розповсюдження інформації та реалізацією таких заходів захисту, щоб відповідати вимогам ТЗІ. У наш час це питання має враховуватися на режимних об'єктах. При оновленні нормативних документів важливо враховувати використання сучасного обладнання, електронних засобів, систем зв’язку та будь-яких технологій, які можуть бути на місці, де здійснюється робота з секретною інформацією. Водночас вимоги повинні включати не лише саме обладнання, але й враховувати його розміщення, експлуатацію.

Другим важливим напрямком є модернізація режимних об’єктів та приміщень, де здійснюється робота з державною таємницею. Постійне місцезнаходження військової установи або частини в умовах бойових дій може змінюватися. Тому нормативна база повинна враховувати можливість розміщення режимних приміщень у тимчасових місцях та мінімальні вимоги до їх обладнання та безпеки. Своєчасний перегляд керівних документів системи ТЗІ є дуже важливим. Нормативний документ не повинен залишатися

незмінним протягом тривалого часу, якщо технічні засоби, методи обробки інформації та характер загроз значно змінюються. Сучасне нормативне забезпечення вже передбачає процедури оновлення документів у сфері ТЗІ. Зокрема, зміни були внесені до Положення про державну експертизу у сфері ТЗІ.

Важливою частиною такого коригування є удосконалення державної експертизи у сфері ТЗІ. Це – вивчення, перевірка, аналіз та оцінка об'єктів для забезпечення їх відповідності нормативним документам ТЗІ та можливості їх експлуатації.

З досвідом сучасної війни дуже важливо мати підхід з експертизою, яка враховує не лише формальне дотримання системою встановлених норм, але й реальні умови експлуатації об’єкта. Для військових установ це особливо важливо, оскільки одна й та ж система ТЗІ може працювати в різних умовах – у будівлі, на тимчасовому майданчику або навіть під час переміщення військової частини.

Окрему увагу слід приділити актуалізації Зводу відомостей, що становлять державну таємницю, з урахуванням сучасних умов оборонної діяльності. Відомості, що включені до Зводу, мають відповідати сучасним умовам оборонної діяльності та враховувати характер інформації, розголошення якої може створювати загрозу національній безпеці. Звід наразі має чинну редакцію, і деякі зміни вже були внесені до нього. Між тим, оновлення Переліку не повинно здійснюватися шляхом необґрунтованого розширення обсягу секретної інформації, а шляхом постійної оцінки, яка інформація на сьогодні може становити загрозу національній безпеці у разі її розголошення. Такий підхід відповідає Закону України «Про державну таємницю», який передбачає обґрунтування можливого збитку національній безпеці при віднесенні інформації до державної таємниці.

Таким чином, досвід сучасної війни слід використовувати як практичну основу для перегляду керівних документів ТЗІ та захисту державної таємниці. Особливу увагу слід приділити режимним об’єктам, засобам ТЗІ, каналам витоку інформації, процесу контрольних заходів.

Гладич Р. І.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДОЛОГІЧНІ ЗАСАДИ МАСКУВАННЯ ТЕЛЕМЕТРИЧНИХ КАНАЛІВ РОБОТИЗОВАНИХ СИСТЕМ ПІД РАДІОЕЛЕКТРОННІ СИГНАТУРИ ШТАТНИХ ЗАСОБІВ ЗВ’ЯЗКУ ТАКТИЧНОЇ ЛАНКИ В УМОВАХ АКТИВНОЇ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ПРОТИВНИКА

Сучасний досвід ведення бойових дій Сил оборони України демонструє, що масове впровадження безпілотних авіаційних, наземних та морських роботизованих систем стало вирішальним фактором забезпечення ситуаційної обізнаності та вогневого ураження на тактичному рівні. Проте висока інтенсивність насичення передової лінії бойового зіткнення різнорідними безпілотними комплексами породила критичну технічну вразливість, пов'язану з демаскуванням пунктів управління та наземних екіпажів. Головна проблема сучасного радіоефіру полягає в глибокому технологічному розриві між штатними засобів зв'язку Збройних Сил України та каналами керування роботизованими платформами. Якщо цифрові тактичні радіостанції іноземного виробництва (зокрема, Falcon серій III та IV від корпорації L3Harris) володіють високим рівнем завадозахищеності та скритності завдяки режиму швидкісної псевдовипадкової перебудови робочої частоти (ППРЧ), то телеметрія та відеопотоки більшості розвідувальних і ударних безпілотників транслюються через комерційні або спеціалізовані цифрові протоколи broad-band типу, що працюють у фіксованих частотних діапазонах. Автоматизовані комплекси радіоелектронної розвідки (РЕР) та радіоелектронного придушення (РЕБ) противника, такі як «Житель», «Торн-М» або «Леер-3», миттєво ідентифікують характерну структуру пакетів телеметрії дронів. Навіть за умови повного шифрування змісту трафіку, регулярні цифрові заголовки, специфічна щільність розподілу бітів та інтервали випромінювання дозволяють ворогу з точністю до кількох метрів вирахувати координати екіпажу операторів БПЛА, після чого по них завдається прицільний артилерійський удар. Захищений Harris у бліндажі залишається неушкодженим, але особовий склад КСП та оператори знищуються через демаскувальний профіль дрона. У межах реалізації концепції багатосферних операцій НАТО виникає гостра потреба розробки неординарних

методів протидії технічним засобам розвідки, здатних штучно змінювати фізичні параметри сигналів роботизованих систем безпосередньо в ефірі. Перспективним вирішенням цієї задачі є метод динамічної модифікації структури телеметрії з метою її маскування під легітимні, звичні для противника радіоелектронні сигнатури штатних засобів зв'язку типу Harris.

Сутність і наукова новизна пропонованого підходу в межах технічного та криптографічного захисту інформації полягає в розробці методології динамічного перекодування інформаційних потоків на рівні структури кадру даних (Frame Structure Mitigation). Замість класичного шифрування змісту повідомлень, яке залишає статистичний портрет пакетів незмінним, пропонується використання проміжного програмно-визначеного радіомодуля (Software-Defined Radio — SDR) з інтегрованими алгоритмами штучного інтелекту. Цей модуль встановлюється між кінцевим терміналом оператора і передавачем роботизованого комплексу. Алгоритм ШІ в реальному часі аналізує поточний радіопрофіль тактичного підрозділу, фіксуючи параметри роботи рацій Harris (інтенсивність обміну, тривалість пакетів, затримки між циклами ППРЧ). Після цього SDR-модуль штучно фрагментує потік телеметрії безпілотника, накладає на мікропакети фальшиві цифрові заголовки (Headers) військового зразка, викривлює статистичну щільність бітів та синхронізує часові інтервали випромінювання із тактами роботи штатних радіостанцій. У результаті такого перекодування сигнал керування роботизованою платформою повністю втрачає унікальні демаскувальні сигнатури безпілотної авіації. Для комплексів РЕР противника цей трафік змішується із загальним легітимним фоном радіообміну батальйону і класифікується як стандартна військова рація Harris, яку ворог не здатний ефективно пеленгувати через надшвидкісний режим зміни частот, що забезпечує повну скритність управління БПЛА на рівні фізичного сигналу.

Математичний апарат забезпечення стійкості запропонованої методики базується на алгоритмах стохастичного впровадження маркерів та нелінійного кодування завадостійких кодів Ріда-Соломона, адаптованих до умов інтенсивного радіоелектронного придушення. Задача криптографічного приховування сигнатур полягає у мінімізації відстані Кульбака-Лейблера між статистичними розподілами реального сигналу телеметрії та еталонного профілю військової радіостанції. Для досягнення цієї мети застосовується

математична модель динамічної інкапсуляції, де кожен кадр телеметрії БПЛА стискається за допомогою вейвлет-перетворень і «розчиняється» всередині випадково згенерованої надлишкової цифрової матриці, що імітує пакет передачі даних стандарту STANAG. Щоб зняти виклик різниці частотних діапазонів (УКХ-діапазон Harris проти гігагерцових частот дронів), пропонується метод віртуального зміщення спектра, за якого SDR-передавач роботизованого комплексу використовує псевдовипадкові сплески випромінювання на гармоніках тактичних частот зв'язку. Обчислювальна складність такого процесу на борту безпілотної платформи зведена до мінімуму завдяки використанню матричних обчислень фіксованої розрядності, що дозволяє виконувати перекодування сигнатур за наносекунди на стандартних бортових мікропроцесорах без додаткового навантаження на польотні акумулятори.

З точки зору протидії технічним засобам розвідки противника, впровадження методу штучного маскування під сигнатури Harris дозволяє радикально знизити уразливість пунктів управління БПЛА та КСП підрозділів. Російські станції автоматизованого радіомоніторингу орієнтовані на виявлення специфічних частотно-часових матриць, характерних саме для каналів керування безпілотниками (наприклад, протоколів ELRS чи Crossfire), оскільки знищення операторів дронів є пріоритетним завданням артилерії. Модифікований сигнал, що повністю копіює радіопрофіль Harris, сприймається ворожими пеленгаторами як постійний, рутинний обмін даними між штабними машинами. Оскільки на даній ділянці фронту одночасно працюють десятки легітимних радіостанцій Сил оборони, ворожа РЕР втрачає можливість виокремити координати конкретного оператора безпілотника з-поміж загального фону. Водночас суттєво нівелюється дія прицільного РЕБ: противник не може активувати вузькосмугове придушення на частоті телеметрії, оскільки система маскування постійно трансформує структуру випромінювання, змушуючи ворожі глушилки працювати по захищеному алгоритму ППРЧ, марно витрачаючи свій енергетичний ресурс.

Підсумовуючи, слід зазначити, що розробка методологічних засад маскування телеметричних каналів під радіоелектронні профілі штатних засобів зв’язку ланки Harris є ефективним і безальтернативним кроком для підвищення живучості військ. Перехід від концепції звичайного шифрування змісту даних до концепції повного приховування типу і призначення сигналу в радіоефірі

дозволяє ефективно протидіяти передовим системам радіоелектронної розвідки противника, надійно захищає екіпажі операторів від пеленгування та запобігає вогневому ураженню пунктів управління.

Мякішев Н. В., курсант
Баратюк В. І., канд. військ. наук, доц.
Корчев В. Б., канд. військ. наук, ст. наук. співроб.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ОРГАНАХ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ: СПІВВІДНОШЕННЯ ОПЕРАТИВНОСТІ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Використання електронного документообігу в органах Державної прикордонної служби України доцільно розглядати як засіб прискорення управлінських процедур за одночасного забезпечення юридичної достовірності та захищеності інформації. Електронна форма дає змогу скоротити час передавання документів між територіально віддаленими підрозділами, забезпечити контроль строків виконання доручень і встановити персональну відповідальність за погодження та прийняття рішень. Однак саме переведення документа в цифровий формат ще не гарантує його належного правового статусу. Стаття 5 Закону України «Про електронні документи та електронний документообіг» визначає електронний документ через поєднання електронних даних та обов’язкових реквізитів, стаття 7 установлює вимоги до його оригіналу, а стаття 8 забороняє заперечувати юридичну силу документа виключно через його електронну форму. Звідси випливає необхідність розмежовувати електронний оригінал, електронну копію паперового документа та звичайне інформаційне повідомлення: фотографія підписаного наказу, надіслана через канал комунікації, сама по собі не набуває статусу електронного оригіналу. Додаткове значення має стаття 18 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», яка прирівнює юридичну силу кваліфікованого електронного підпису до власноручного. Водночас підтвердження підпису не доводить автоматично наявності у підписувача

повноважень на прийняття конкретного рішення і не забезпечує конфіденційності його змісту. Наприклад, належно підписаний кадровий документ залишається неправомірно розкритим, якщо його передано особам, які не мають права ознайомлюватися з відповідними відомостями. Тому юридична надійність електронного документообігу потребує окремої перевірки автентичності документа, компетенції посадової особи та правомірності доступу одержувачів.

Організаційною основою електронного документування управлінської діяльності є постанова Кабінету Міністрів України від 17 січня 2018 року № 55, якою затверджено, зокрема, Типову інструкцію з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну. Її значення для органів ДПСУ полягає у формуванні загальних правил роботи з управлінськими документами, які мають конкретизуватися у відповідних відомчих процедурах з урахуванням спеціального законодавства. Прискорення документообігу доцільно забезпечувати через усунення зайвого дублювання, визначення послідовності погодження, автоматичне інформування виконавців та контроль проходження документа. Натомість скорочення обов’язкових перевірок або поширення практики користування чужими обліковими записами створює ризик втрати персональної відповідальності. Наприклад, під час погодження заявки на матеріальне забезпечення паралельне опрацювання різними підрозділами може скоротити строк прийняття рішення, якщо предмет їхньої перевірки не залежить від попередніх висновків інших учасників. Однак усі погодження повинні стосуватися визначеної версії документа: зміна змісту після погодження потребує встановленої процедури повторного розгляду. Окремого регулювання потребує робота під час перебоїв електропостачання, зв’язку або недоступності інформаційної системи. Доцільно заздалегідь визначати дозволені резервні процедури, порядок реєстрації документів після відновлення роботи та спосіб усунення дубльованих записів. При цьому терміновість документа не повинна тлумачитися як універсальний дозвіл на його передавання через особисту пошту чи інший канал, не дозволений для відповідної категорії інформації. Оперативність варто оцінювати за часом доведення належно оформленого документа до уповноваженого виконавця, а не лише за швидкістю пересилання файла.

Специфіка органів ДПСУ зумовлює необхідність розмежування правових режимів інформації, що міститься в електронних документах. Сам факт створення документа прикордонним органом не означає, що весь його зміст є таємним або службовим. Статті 6 і 9 Закону України «Про доступ до публічної інформації» встановлюють правові підстави обмеження доступу та визначають ознаки службової інформації; під час вирішення питання про надання інформації на запит необхідно враховувати законну мету обмеження, істотність можливої шкоди та співвідношення цієї шкоди із суспільним інтересом в отриманні відомостей. При цьому правила публічного доступу не слід механічно ототожнювати з порядком внутрішнього службового обміну, який потребує самостійного визначення повноважень і потреб одержувачів. Порядок поводження з документами, що містять службову інформацію, деталізує Типова інструкція, затверджена постановою Кабінету Міністрів України від 19 жовтня 2016 року № 736. Її застосування означає, що електронний формат не скасовує вимог до обліку, зберігання, використання та знищення таких матеріалів. Самостійне значення має захист персональних даних. Стаття 6 Закону України «Про захист персональних даних» вимагає відповідності обсягу даних визначеній меті обробки та забороняє їх надмірність, а стаття 24 установлює обов’язок забезпечувати захист від незаконної обробки й несанкціонованого доступу.

Технічний і організаційний захист електронного документообігу має ґрунтуватися на Законі України «Про захист інформації в інформаційно-комунікаційних системах» та застосовних підзаконних вимогах. У сучасному регулюванні необхідно враховувати також механізм авторизації з безпеки, порядок якої затверджено постановою Кабінету Міністрів України від 18 червня 2025 року № 712: оцінювання захищеності системи не можна зводити до факту встановлення окремого програмного засобу або використання електронного підпису. Застосовні вимоги визначаються характеристиками системи, категоріями оброблюваної інформації та відповідними процедурами забезпечення безпеки. Для органів ДПСУ доцільною є модель, за якої права користувачів відповідають посадовим обов’язкам, переглядаються після переведення чи звільнення, а дії з документами фіксуються для подальшої перевірки. Захищати необхідно не лише текст і додатки, а й відомості про документ: його назва, перелік адресатів або інші реєстраційні дані також можуть розкривати інформацію з обмеженим доступом. В умовах воєнного

стану особливого значення набуває доступність документів для законних користувачів, тому резервне копіювання слід поєднувати з перевіркою можливості відновлення, а резервні примірники – захищати відповідно до режиму інформації. Стаття 13 Закону України «Про електронні документи та електронний документообіг» пов’язує зберігання електронних документів із можливістю перевірки їхньої цілісності та подальшого використання, що потребує збереження юридично значущих електронних реквізитів, а не лише візуального зображення документа.

Отже, удосконалення електронного документообігу в ДПСУ доцільно спрямувати на поєднання швидкого проходження документів із контрольованим доступом, підтвердженням їх походження, належним зберіганням та відновленням після збоїв. Показниками ефективності мають бути одночасно строки опрацювання, кількість помилок адресування, повнота обліку дій і здатність забезпечити безперервність роботи без порушення встановленого режиму інформації.

Будзінська О. О.
Соловей В. А.
Житомирський військовий інститут імені С. П. Корольова

ЛОГІЧНА БЕЗПАРОЛЬНА АВТЕНТИФІКАЦІЯ INVISCOMM У ЗАХИЩЕНИХ СИСТЕМАХ УПРАВЛІННЯ

Вступ. Сучасні безпарольні механізми зменшують ризики слабких або повторно використовуваних паролів, але продовжують спиратися на криптографічні ключі, автентифікатори та захищене середовище їх виконання. Це узагальнено в огляді M. I. M. Yusop та ін. (IEEE Access, 2025). Дослідження C. Catalano, A. Chezzi, V. S. Barletta та F. Tommasi щодо атак на FIDO2/CTAP2/WebAuthn (Journal of Computer Virology and Hacking Techniques, 2025) додатково показує, що стійкість протоколу не усуває ризиків компрометації середовища взаємодії.

Для захищених систем управління окремий автентифікаційний об’єкт, його носій або інфраструктура перевірки утворюють самостійні об’єкти захисту та можуть ставати додатковими точками атаки. Тому становить інтерес модель,

у якій належність отриманого зовнішнього подання до поточного захищеного контексту перевіряється структурно і не потребує використання окремого автентифікаційного об'єкта.

Мета роботи. Формалізувати логічну безпарольну автентифікацію (ЛБА) метаданонейтральної архітектури InvisComm (від. англ. Invisible Communication – приховані комунікації), як структурно вбудований механізм перевірки кожного отриманого шифрокоду та визначити її зв'язок із верифікацією криптографічних подій (КП) і фазовою еволюцією внутрішнього стану комунікативних систем (КС).

Основні результати. У InvisComm секретним криптографічним контекстом є синхронізований повний внутрішній стан КС, який містить операційний стан S_t і подієву пам'ять H_t обмеженої фазової глибини:

$$X_t = (S_t, H_t). \qquad (1)$$

Операційний стан (ОС) визначає поточну конфігурацію віртуального координатного простору та правила оброблення даних, а подієва пам'ять (ПП) агрегує результати попередніх взаємодій і зберігає їх обмежений вплив у межах визначеної фазової глибини. Для пояснення принципу ЛБА достатньо розглянути віртуальний простір V_t фази t як сукупність активних і пасивних об'єктів, що мають стале розташування протягом однієї фази:

$$V_t = A_t \cup P_t, \qquad A_t \cap P_t = \varnothing, \qquad |P_t| \gg |A_t|. \qquad (2)$$

Активні об'єкти можуть бути використані для формування шифрокоду, пасивні – ні. Множина A_t розподіляється на неперетинні доменно-залежні підмножини $A_t^{(r)}$, кожна з яких належить відповідному операційному домену $D_t^{(r)}$, де r – індекс операційного домену (ОД). Один ОД призначається для опрацювання одного слова відкритого тексту (СВТ) $M_{i,j}$. Визначену кількість k СВТ, фіксованої довжини l використовують у k різних ОД для формування j-того шифрокоду $C_{t,j}$.

Для i-го слова $M_{i,j}$, що належить множині допустимих n-бітових слів W_n, позначимо активну підмножину $A_{t,i,j}$ у відповідному ОД $D_t^{(r_i)}$ із множині доменів призначених для шифрокоду $C_{t,j}$. У кожному ОД діє власне унікальне фазово-залежне бієктивне правило асоціації:

$$\varphi_{t,i,j}: W_n \leftrightarrow A_{t,i,j}, \forall M_{i,j} \in W_n \ \exists!\ a_{t,i,j} \in A_{t,i,j}:\ a_{t,i,j} = \varphi_{t,i,j}(M_{i,j}). \qquad (3)$$

Отже, кожне допустиме значення СВТ може бути асоційоване лише з одним активним об’єктом свого ОД. Координатні параметри вибраного об’єкта відображаються у раундовий бінарний компонент $b_{t,i,j}$, а стано- та подієзалежний оператор $\Gamma_{t,j}$ формує з упорядкованої послідовності k таких компонентів шифрокод:

$$C_{t,j} = \Gamma_{t,j}\left(b_{t,1,j}, b_{t,2,j}, \dots, b_{t,k,j}\right). \quad (4)$$

На стороні отримувача застосовується відповідний обернений оператор $\Gamma_{t,j}^{-1}$, після чого з кожного відновленого координатного компонента реконструюється об’єкт $\hat{a}_{t,i,j}$ у призначеному йому ОД.

Зміст ЛБА полягає в тому, що отриманий шифрокод $C_{t,j}$ у поточному внутрішньому стані КС виконує функцію координатної навігаційної інструкції: після оберненого перетворення його k компонентів система реконструює k об’єктів у k призначених ОД. Оскільки під час легітимного формування шифрокоду кожне i-те СВТ могло бути асоційоване з об’єктом виключно у відповідному i-му домені, належність усіх реконструйованих об’єктів активним множинам саме своїх ОД є структурним критерієм ЛБА для верифікації отриманого шифрокоду $C_{t,j}$:

$$V_{X_t}\left(C_{t,j}\right) = \begin{cases} 1, & \forall i \in \{1, \dots, k\}:\ \hat{a}_{t,i,j} \in A_{t,i,j}, \\ 0, & \exists i \in \{1, \dots, k\}:\ \hat{a}_{t,i,j} \notin A_{t,i,j}. \end{cases} \quad (5)$$

Значення $V_{X_t}\left(C_{t,j}\right) = 1$ означає успішну ЛБА, тобто повну структурну допустимість отриманого шифрокоду в поточному криптографічному контексті. Після цього допускається подальша реконструкція шифрокоду до рівня визначення СВТ згідно унікальних доменних правил асоціації, що були сформовані саме для цього j-го шифрокоду. Якщо хоча б один із реконструйованих у призначених ОД об’єктів належить до пасивної підмножини $P_{t,i,j}$ відповідного ОД $D_t^{(r_i)}$, шифрокод відхиляється, а реконструкція відкритого повідомлення не виконується. Таким чином, автентифікаційна перевірка здійснюється не за семантикою повідомлення і не за окремим переданим автентифікатором, а за структурною відповідністю отриманого подання поточному секретному стану. Ймовірність випадкового хибного прийняття $V_{X_t}(C^*) = 1$ ЛБА визначається часткою активних об’єктів у призначених ОД $D_t^{(r_i)}$ та кількістю k незалежно перевірюваних компонентів

шифрокоду. За спрощеної моделі незалежного й рівномірного потрапляння реконструйованого компонента до будь-якого об'єкта відповідного ОД ця ймовірність оцінюється як:

$$Pr\left[V_{X_t}(C^*) = 1\right] \approx (|A_t|/(|A_t| + |P_t|))^k = \prod_{i=1}^{k} \left(\left|A_{t,i,j}\right|/\left|D_t^{(r_i)}\right|\right) \quad 6)$$

Успішну ЛБА необхідно відрізняти від завершеної верифікації КП. КП індукується відправником під час формування $C_{t,j}$; успішна ЛБА на стороні отримувача не починає, а продовжує її життєвий цикл і створює умову для подальшого взаємного підтвердження. Верифікованою вважається КП, що пройшла визначений протоколом цикл взаємного підтвердження і може бути включена до впорядкованого фазового транскрипту E_t. За тотожності повних станів і таких транскриптів сторін та застосування однакового оператора фазової еволюції зберігається симетрія їх подальшої фазової еволюції:

$$X_t^A = X_t^B \ \wedge \ E_t^A = E_t^B \ \Rightarrow \ X_{t+1}^A = X_{t+1}^B. \quad (7)$$

Отже, успішна ЛБА є умовою, необхідною для формування узгодженого верифікованого подієвого контексту, але сама по собі не означає завершення життєвого циклу КП і не є достатньою умовою фазового переходу. На відміну від схем, у яких автентифікаційне рішення залежить від перевірки окремого переданого або пред'явленого цифрового об'єкта, ЛБА не потребує передавання чи перевірки окремого пароля, сертифіката, токена, статичного ключового ідентифікатора або іншого самостійного автентифікаційного об'єкта. Для виконання ЛБА шифрокод не потребує включення окремого автентифікаційного ідентифікатора відправника: його структурна належність визначається поточним внутрішнім контекстом отримувача.

Термін «безпарольна» при цьому не означає відсутності секретного матеріалу. Повний стан X_t залишається секретним криптографічним контекстом і функціональним аналогом ключового матеріалу, що еволюційно оновлюється. Відмінність полягає в тому, що для ЛБА конкретного шифрокоду не формується і не перевіряється окремий багаторазово використовуваний автентифікаційний фактор. За умови збереження секретності та синхронності станів успішна ЛБА свідчить про структурну сумісність отриманого шифрокоду з поточним криптографічним контекстом легітимної взаємодії.

Для захищених систем управління це означає, що фізичне отримання транспортного пакета саме по собі не надає його вмісту статусу допустимої

команди. ЛБА формує дискретну тригерну логіку прийняття: конкретний шифрокод або структурно відповідає поточному криптографічному контексту й допускається до реконструкції, або відхиляється як недопустимий. Блокування, затримка, перестановка, повторне відтворення чи модифікація мають різну фізичну природу, однак структурно недопустимі або контекстно невідповідні подання не повинні формувати прийнятий системою результат лише внаслідок факту їх надходження через транспортний канал.

З позицій протидії активному нав’язуванню це зменшує ризики, пов’язані з компрометацією окремого автентифікаційного об’єкта. Для формування структурно допустимого шифрокоду порушник має відтворити релевантний поточний контекст або іншим способом сформувати подання, яке після оберненого перетворення відновить активні об’єкти у всіх призначених доменах. Водночас ЛБА не є універсальним доказом стійкості до всіх активних атак: імовірність хибного прийняття, стійкість до цілеспрямованого підроблення, виснаження ресурсів і наслідки компрометації кінцевого пристрою залежать від конкретної реалізації. Розкриття повного поточного стану компрометує відповідний криптографічний контекст.

Практичне значення підходу полягає у структурному поєднанні автентифікаційної перевірки з процесом координатної реконструкції та у відсутності необхідності передавати окремий автентифікаційний об’єкт. Це скорочує клас ситуацій, у яких компрометація одного багаторазово використовуваного фактора автоматично дозволяє формувати прийнятні системою команди, а розмежування успішної локальної ЛБА і завершеного взаємного підтвердження відокремлює структурно прийняте подання від інформації, уже інтегрованої у спільний еволюційний контекст.

Програмний PoC архітектури метаданонейтральної інформаційної взаємодії InvisComm, розроблений J. A. Kamlofsky та J. F. Castro Tramontina і представлений у відкритому репозиторії JFCrypT/InvisComm (GitHub, 2026), демонструє практичну реалізовність станозалежного двостороннього обміну через UDP/Wi-Fi, UART, LoRa та UDP/Ethernet. Проведені випробування були спрямовані переважно на статистичні й часові характеристики потоків Info і Noise, тому не становлять кількісної перевірки ЛБА. Для її експериментального оцінювання необхідно контрольовано вводити модифіковані, повторно відтворені та контекстно невідповідні шифрокоди, окремо фіксувати випадки

коректного відхилення та визначати частоту хибного прийняття. Такий експеримент має встановити практичну ймовірність того, що зовнішньо сформований шифрокод, який не відповідає поточному внутрішньому контексту, помилково буде класифікований механізмом ЛБА як структурно допустимий.

Висновки. ЛБА архітектури InvisComm є структурно вбудованим станозалежним механізмом перевірки отриманого шифрокоду в поточному синхронізованому секретному криптографічному контексті. Її принцип полягає у перевірці доменно-залежної належності всіх реконструйованих координатних об’єктів активним множинам саме тих ОД, у яких відповідні компоненти могли бути легітимно сформовані. Така перевірка не залежить від семантики повідомлення і не потребує передавання окремого пароля, токена, цифрового ідентифікатора чи іншого самостійного автентифікаційного об’єкта. Для захищених систем управління це дає змогу поєднати реконструкцію інформації та перевірку структурної належності кожного отриманого зовнішнього подання до актуального криптографічного контексту в межах єдиної процедури. У практичних сценаріях це означає усунення автентифікаційного об’єкта як самостійного об’єкта фішингової атаки.

Нікора І. В.
Лях І. Ю.
Мукосій Д. В.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

АНАЛІЗ МЕТОДІВ КОМБІНОВАНОГО ДЕТЕКТУВАННЯ КІБЕРАТАК НА АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З БОКУ ВЗАЄМОДІЮЧИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сучасні автоматизовані системи управління (АСУ) авіації та протиповітряної оборони функціонують у тісній взаємодії з іншими інформаційними системами: засобами розвідки, систем управління суміжних угруповань, систем ситуаційної обізнаності. Така інтеграція скорочує цикл управління, але розширює область вразливості. Досвід широкомасштабної

збройної агресії рф проти України свідчить, що противник цілеспрямовано атакує інформаційні системи, в першу чергу через менш захищені місця.

Сукупність взаємодіючих систем утворює неоднорідну мережу що поєднує різні системи: її елементи мають різні принципи побудови, протоколи обміну, моделі безпеки та засоби захисту інформації, є територіально розподіленими, а характеристики трафіку в ній неоднорідні. Засоби контролю, орієнтовані на однорідні мережі, у таких умовах не забезпечують своєчасного виявлення атак. Крім того, шкідливі дані надходять від формально достовірного джерела штатним каналом обміну та не блокуються периметровим захистом.

Існуючі підходи мають принципові обмеження. Криптографічний захист каналу виявляє модифікацію повідомлень, але безсилий, якщо скомпрометована сама взаємодіюча система, оскільки вона формує хибні дані з коректним підписом. Системи виявлення аномалій здатні виявити нетипову поведінку, проте дають значну кількість хибних спрацювань, а централізований аналіз усього трафіку неможливий через обмежену пропускну здатність каналів спеціального призначення.

Метою аналізу є розроблення методу комбінованого детектування кібератак на АСУ спеціального призначення з боку взаємодіючих інформаційних систем, який поєднує криптографічний та аналітичний контроль на основі поетапного розподіленого моніторингу.

Метод передбачає розміщення інтелектуальних агентів у точках взаємодії АСУ спеціального призначення з суміжними системами та сервера моніторингу на рівні АСУ. Виявлення атаки здійснюється поетапно. На першому етапі агент за локальною інформацією виконує криптографічний контроль цілісності й автентичності повідомлень (імітовставка, мітки часу, порядкові номери) та перевірку їх формату. Повідомлення, що пройшли перевірку і не мають ознак аномальності, приймаються без обміну даними з іншими вузлами.

Лише підозрілі повідомлення передаються на наступні етапи, де із залученням додаткових незалежних ознак уточнюються тип атаки та скомпрометоване джерело. Аналізуються фізична правдоподібність параметрів, статистичні характеристики потоку та узгодженість даних з іншими джерелами, для чого застосовуються методи машинного навчання. Фактично реалізується принцип змінної апертури: у штатному режимі мережа контролюється широким полем з малою деталізацією, а в разі виявлення порушення аналіз звужується до відповідного вузла і поглиблюється.

Рішення на кожному етапі приймається шляхом порівняння відношення правдоподібності з порогом. Пороги обираються за критерієм Неймана–Пірсона: за фіксованої ймовірності хибної тривоги мінімізується ймовірність пропуску атаки, яка для автоматизованих систем управління є значно небезпечнішою. У процесі функціонування пороги уточнюються шляхом навчання на накопиченій інформації.

Поетапна процедура забезпечує точність виявлення не гіршу за байєсову, оскільки на кожному етапі використовує незалежні ознаки, і водночас суттєво скорочує обсяг службової інформації, що передається між вузлами, адже більшість рішень приймається вже на першому етапі. Метод не потребує зміни архітектури АСУ та протоколів обміну.

Таким чином, запропонований метод дозволяє виявляти як атаки на канал передачі, так і атаки з боку скомпрометованої довіреної системи, що підвищує захищеність АСУ спеціального призначення. Подальші дослідження спрямовані на формування набору ознак для кожного етапу та експериментальну оцінку ефективності методу на імітаційній моделі.

Новацька М. І.
Катеринчук І. С., д-р техн. наук, проф.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

АКТУАЛЬНІ АСПЕКТИ У СФЕРІ ТЕХНІЧНОГО ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У сучасній науковій дискусії криптографія нерідко помилково сприймається як статичний інструмент забезпечення безпеки, де застосування стійкого алгоритму гарантує абсолютний захист. Однак аналіз практичної безпеки свідчить, що теоретико-числові алгоритми рідко є найслабшою ланкою системи. Основні вразливості виникають на перетині математичних моделей, засобів їх програмно-апаратної реалізації, процедур управління ключовим матеріалом, а також людського чинника. На сучасному етапі ключовим викликом для криптографічних систем є забезпечення їхньої резилієнтності в умовах динамічного середовища загроз, зокрема, розвитку постквантових

обчислень, атак на ланцюги постачання, міграції до хмарних інфраструктур, гібридних кіберконфліктів та посилення регуляторних вимог до захисту персональних даних.

Головна тема останніх років – постквантова криптографія. Класичні асиметричні схеми (RSA, еліптичні криві, обмін ключами за Діффі-Геллманом) спираються на складність факторизації та дискретного логарифма. Алгоритм Шора дає змогу достатньо потужному квантовому комп'ютеру розв'язати обидві задачі за поліноміальний час. Такої машини поки немає, і прогнози строків розходяться, але чекати неможливо. Супротивник уже зараз збирає трафік, який вдалося перехопити, щоб згодом його розкрити. Для даних із довгим терміном таємності (державні секрети, медичні та біометричні відомості, дипломатичне листування, промислова власність) ця загроза існує сьогодні. У 2024 році NIST затвердив перші стандарти: ML-KEM для обміну ключами, ML-DSA та SLH-DSA для електронного підпису. Згодом до них додали ще одну схему інкапсуляції ключів на основі кодів. Тепер починається міграція, і вона складніша, ніж здається. Нові ключі та підписи значно більші, вимоги до пам'яті й пропускної здатності інші, тож протоколи, смарт-картки, вбудовані пристрої та ланцюжки сертифікатів доведеться переробляти. Постквантові схеми молодші за класичні й пройшли менше років атак, а розумна відповідь на це – гібридні рішення. У них класичні і постквантові механізми працюють разом, і зламування одного не руйнує захист.

З міграцією пов'язана криптоагільність. Історія знає багато алгоритмів, які вважали надійними, а потім відкинули: DES, MD5, SHA-1. Найбільших витрат щоразу завдавала не сама заміна, а незнання того, де саме використовується алгоритм. Першим кроком я вважаю повну інвентаризацію криптографічних активів: протоколів, бібліотек, сертифікатів, апаратних модулів і залежностей. Далі системи слід будувати так, щоб алгоритм був параметром конфігурації, а не припущенням, закладеним у код назавжди.

Не менш гостра проблема полягає в реалізації. Реальні інциденти спричиняють здебільшого не теоретичні атаки на шифри, а помилки в бібліотеках, слабкі генератори випадкових чисел, повторне використання одноразових значень, хибна перевірка сертифікатів і витоки через побічні канали: час виконання, споживання енергії, поведінка кеш-пам'яті, спекулятивне виконання в процесорах. Тут потрібні реалізації з постійним

часом виконання, формальна верифікація коду, безпечні мови програмування та незалежні аудити. Для постквантових алгоритмів це особливо важливо, бо їхні реалізації ще молоді, а захист від побічних каналів для них тільки напрацьовується.

Керування ключами залишається місцем, де найчастіше ламається вся конструкція. Найстійкіший алгоритм марний, якщо приватний ключ лежить у відкритому файлі на сервері, обмінюється месенджерами або роками не змінюється. Потрібні апаратні модулі безпеки, чіткі політики ротації та відкликання, розподіл ключа між кількома сторонами й жорсткий контроль адміністраторів. У хмарі частину контролю тримає провайдер, і тому зростає роль конфіденційних обчислень, де дані залишаються захищеними навіть під час обробки, та схем, у яких ключем володіє клієнт.

Криптографія працює лише в парі з технічним захистом. Модель із безпечним периметром і довірою до всього, що всередині, застаріла. Віддалена робота, хмари, мобільні пристрої та партнерські інтеграції стерли межі мережі, тож нульова довіра стала інженерною необхідністю: кожен запит, пристрій і користувач проходить перевірку незалежно від місця в мережі. Поруч стоять атаки на ланцюг постачання, коли шкідливий код потрапляє в легітимне оновлення або залежить від відкритої бібліотеки. Проти них допомагають підписування збірок, відтворювані збирання, перелік компонентів програмного забезпечення та суворий контроль довіри до постачальників. Для критичної інфраструктури додається захист технологічних мереж, які проєктували десятиліття тому, не замислюючись про кіберзагрози.

Український досвід війни дає практичні уроки. Держава-агресор має ресурси для тривалих прихованих проникнень, і робочим принципом проєктування має бути припущення, що компрометація вже відбулася. З цього випливають сегментація мереж, резервні копії поза основною інфраструктурою, швидке відновлення та виявлення аномалій. Наскрізне шифрування зв'язку – тут питання безпеки людей, а не зручності. Електронний підпис і довірчі послуги стали критичною інфраструктурою держави.

Перспективним напрямом залишається криптографія, що зберігає приватність: докази з нульовим розголошенням, багатосторонні обчислення, гомоморфне шифрування. Вона дає змогу довести твердження або отримати результат без розкриття вхідних даних, наприклад, підтвердити повноліття чи громадянство без передавання всього документа. Такі технології складні, дорогі

й чутливі до помилок проєктування, тож їх варто застосовувати там, де вони вирішують конкретну проблему.

Штучний інтелект діє з обох боків. Він здешевлює для атакуючих пошук вразливостей, фішинг і підробку голосу та відео, а для захисників допомагає аналізувати журнали, виявляти аномалії й перевіряти код. Самі моделі та їхні дані теж потребують захисту, і ця тема ще лише формується.

Головний виклик галузі полягає в зміні мислення: від вибору надійного алгоритму до побудови системи, яка залишається безпечною попри зміни. Це означає готовність до постквантової міграції, криптоагільність, якісні реалізації, зрілу культуру керування ключами, нульову довіру та тверде припущення, що частину захисту рано чи пізно подолають. Математика дає фундамент, а безпеку створює інженерна дисципліна й організаційна культура.

Варламова І. Є.
Військовий інститут Київського національного університету
імені Тараса Шевченка

АДАПТАЦІЯ СИСТЕМ ТА ЗАСОБІВ КОМУНІКАЦІЇ МАЛОЧИСЕЛЬНИХ ПІХОТНИХ ГРУП ПІД ЧАС КАСКАДНОГО ПЕРЕСУВАННЯ: ДОСВІД ЗБРОЙНИХ СИЛ УКРАЇНИ

Швидка зміна обстановки на полі бою вимагає стрімких дій та модернізації сучасної техніки пересування та методів ведення бою загалом. Лінія бойового зіткнення (лбз) характеризується високою щільністю та суцільним покриттям безпілотними авіаційними комплексами тепловізійної та радіоелектронної розвідки (РЕР), високоточного ураження живої сили противника та технічних засобів, озброєння, позицій ворога за допомогою дронів, артилерії, баражуючих боєприпасів (дронів камікадзе). Така нова тактика ведення бою повністю витіснила принцип застосування класичних атак бронетехнікою та суттєво зменшила їх ефективність.

Основний елемент, який використовується для виконання наступальних та оборонних завдань є піхотна група малої чисельності (кількість може варіюватися від 6-10 осіб). Проте класичні методи пересування, які описані в бойових статутах, та стандартні процедури НАТО без адаптації до умов

використання засобів радіоелектронної боротьби (РЕБ) призводять до дезорганізації всередині підрозділу і на вищих рівнях та, як наслідок, втрат. Постає гостра потреба у об’єднанні національного бойового досвіду ЗСУ із закордонними доктринальними стандартами (зокрема Бундесверу) та створенні децентоалізованого методу пересування, зв’язку та управління.

Використання традиційного голосового радіозв'язку у відкритому або зашифрованому ефірі під час виконання штурмових завдань демаскує власні позиції та наміри дій малої тактичної групи. Засоби радіоелектронної розвідки (РЕР) противника здатні запеленгувати джерело, яке здійснює випромінення, за 3-5 секунд. Це можуть бути радіо частоти, або сигнали мобільних телефонів тощо. Точність перехоплення сигналу є достатньою для наведення ворогом засобів високоточного ураження (наприклад, FPV-дронів, баражуючих боєприпасів, ствольної артилерії тощо). З огляду на це, виникає потреба в комплексному перегляді та адаптації засобів і способів комунікації під час застосування модифікованих способів пересування, зокрема, каскадного методу в поєднанні з класичними методами пересування у складі двійок та трійок.

На реальному досвіді Збройних Сил України було проведення оцінки ефективності синтезу німецької концепції каскадного просування із динамічною та стійкою внутрішньою структурою українського методу просування двійками і трійками. Проте ключовою умовою успіху такого маневру є створення стійкої, багатоальтернативної, безперервної та безпечної системи зв’язку.

При поділі штурмового відділення (малої тактичної групи) на дві рівноцінні підгрупи, наприклад, підгрупу “Альфа”, яку очолюватиме командир відділення та підгрупу “Бета”, очолювану заступником командира відділення система зв’язку адаптується. По-перше відмовившись від тривалих голосових перемовин, підрозділи переходять на використання цифрових малопотужних радіостанцій із технологією Mesh, яка працює за принципом P2P-мереж або застосування режиму відсутності радіоефірів до моменту виявлення противником. Передача команд між командиром відділення та заступником командира відділення здійснюється короткочасними імпульсними тоновими сигналами, тобто короткими чіткими вказівками, або за допомогою заздалегідь кодованих цифрових текстуальних/сигнальних повідомлень. Це зводить до мінімуму час активної роботи передавача та унеможливлює його пеленгацію засобами РЕР.

Під час безпосереднього вогневого контакту та каскадного перекату (з німецької "sprung" – "стрибків") основне навантаження припадає на невербальну та жестову комунікацію. Стандартна система жестів, затверджена стандартами НАТО, адаптується для дій із заниженим силуетом (з позицій: “лежачи”, “з коліна”, в умовах тісних окопів та урбанізованої місцевості). Команди на зміну сторони, яка прикриває або переміщується, початок каскадного перекату для двійки чи виявлення повітряної загрози дублюється візуально кожним по ланцюжку всередині бойової групи.

В умовах обмеженої видимості або бою вночі основним каналом зв'язку та орієнтуванням між підгрупами командиром відділення та заступником командира відділення стає інфрачервоний-спектр (довжина хвилі сягатиме 850/940 нм), невидимий без спеціальних приладів або обладнання. Використання активних інфрачервоних-маркерів на шоломах або екіпіруванні у поєднанні з приладами нічного бачення дозволяє командиру відділення та заступнику командира відділення миттєво оцінювати взаємне розташування та відстежувати переміщення підгруп під час каскаду. Вказування рубежів та напрямку маневру для двійок/трійок здійснюється короткочасним підсвічуванням цілей вузькоспрямованими інфрачервоними-лазерами, що виключає необхідність довгого пояснення голосом по радіомовленню.

Для координації дій між підгрупою вогневої підтримки та тиловими підрозділами під час підготовки до чергового "стрибка" або у разі перегрупування застосовуються надтонкі оптоволоконні лінії зв'язку або тактильні пейджери малої дальності. Це дає змогу передавати критично важливі сигнали стану справ у підрозділі (“Готовий”, “Починаю рух”, “Затримка”) в умовах застосування противником засобів радіоелектронної боротьби.

Таким чином, адаптована система комунікації при веденні комбінованого методу пересування каскадами та двійками-трійками, забезпечуватиме безперервність управління військами (силами) при децентралізованій структурі, оскільки командир відділення та заступник командира відділення, окрім того, що здійснюють управління, також безпосередньо беруть участь у бою. Основна ціль ведення каскадного бою – зберегти високу щільність вогневого прикриття та стрімкість пересуванн такий спосіб комунікації мінімізує ризик виявлення засобами ворожих засобів радіоелектронної розвідки.

Застосування адаптованих засобів зв'язку та жестових методів комунікації підвищує живучість військ (зокрема малих тактичних груп) на 40–60%, забезпечує гнучкість маневру та мінімізує втрати особового складу під час виконання штурмових дій.

Першин О. В.
Клабан І. Ю.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ СПОВІЩЕНЬ КІБЕРБЕЗПЕКИ НА ОСНОВІ ЛОКАЛЬНИХ МОВНИХ МОДЕЛЕЙ

Постійна еволюція кіберзагроз вимагає від систем захисту інформації підвищення чутливості до потенційних атак і скорочення часу реагування на інциденти. Для забезпечення моніторингу мережевої інфраструктури ключовим інструментом залишаються системи виявлення вторгнень, які спроможні здійснювати глибокий аналіз пакетів у режимі реального часу та здатні фіксувати найменші аномалії та сигнатури шкідливої активності. Попри це, саме зростання ефективності засобів виявлення створило парадоксальну проблему: швидкість і обсяги генерації сповіщень безпеки суттєво перевищили фізичну спроможність людини їх проаналізувати.

На рівні первинної аналітики в центрах моніторингу безпеки це призводить до критичного інформаційного перевантаження операторів. Оператори першої лінії щодня стикаються з тисячами сповіщень, більшість з яких виявляються хибними спрацюваннями (False Positives), спричиненими специфікою мережевих конфігурацій або легітимними системними процесами. Необхідність рутинної перевірки кожного такого випадку породжує феномен «Alert Fatigue» — хронічну втомлюваність від сповіщень. У результаті монотонної роботи увага аналітика розсіюється, а першорядні сигнали про реальні атаки губляться у фоновому «шумі», що безпідставно збільшує час реакції на інциденти та створює вікно можливостей для зловмисників.

Намагаючись вирішити цю проблему, сучасний ринок пропонує комерційні Security Orchestration, Automation and Response – платформи та хмарні AI-сервіси. Проте їхнє практичне застосування зіштовхується з низкою фундаментальних бар’єрів. Традиційні засоби автоматизованого реагування спираються на жорсткі, статичні сценарії «If-Then», які вимагають постійного ручного оновлення й втрачають ефективність при найменшій зміні формату логів. З іншого боку, інтеграція хмарних мовних моделей створює неприпустимі ризики витоку даних: передавати деталі внутрішньої мережевої інфраструктури,

IP-адреси та інциденти у зовнішній хмарний контур заборонено з міркувань регуляторної відповідності та корпоративної безпеки. До того ж, висока вартість ліцензування комерційних продуктів робить їх недоступними для багатьох організацій.

Саме тому виникає гостра потреба у формуванні альтернативного підходу — побудові автономної та локальної системи підтримки прийняття рішень. Поєднання відкритих інструментів оркестрації для первинної збірці й нормалізації файлів подій, векторних баз знань (технологія RAG) та локальних мовних моделей дозволяє створити інтелектуальне «сито». Таке рішення збагачує сповіщення необхідним контекстом та формує первинний аналітичний висновок безпосередньо всередині захищеного контуру підприємства.

Застосування автономного інтелектуального конвеєра дозволяє зняти з аналітиків рутинне навантаження з первинного розбору файлів подій, мінімізувати час обробки критичних загроз та зберегти повну конфіденційність системних даних, що й зумовлює високу актуальність та практичну цінність цього напряму досліджень

Шило С. Г., канд. техн. наук, доц.
Руденко В. А.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

РОЗРОБКА КОМБІНОВАНОГО МЕТОДУ ГЕШУВАННЯ ДАНИХ НА ОСНОВІ ДВОВИМІРНОЇ МОДЕЛІ ІЗІНГА ТА ГЕШ-ФУНКЦІЇ КУПИНА ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ Й КОНТРОЛЮ ДОСТУПУ ОПЕРАТОРІВ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

Розвиток сучасних інформаційних систем і засобів автоматизованого управління зумовлює підвищення вимог до захисту інформаційних ресурсів, зокрема забезпечення цілісності даних і надійності механізмів контролю доступу операторів. Одним із базових інструментів криптографічного захисту є гешування, яке дає змогу отримувати значення фіксованої довжини для повідомлень довільного розміру та виявляти їх несанкціоновану модифікацію. Водночас актуальним напрямом досліджень залишається розроблення

комбінованих методів гешування, що поєднують властивості стандартизованих криптографічних алгоритмів з альтернативними математичними моделями для дослідження ефективності перетворення даних.

Однією з таких моделей є двовимірна модель Ізінга, яка описує взаємодію спінів у вузлах ґратки та зміну її стану під впливом визначених параметрів. Для моделювання переходів між конфігураціями системи може використовуватися алгоритм Метрополіса, який передбачає ймовірнісний вибір нових станів відповідно до зміни системи. Особливості динаміки моделі Ізінга становлять інтерес для дослідження процесів формування псевдовипадкових послідовностей і перетворення двійкових даних. Водночас для використання цієї моделі в криптографічних конструкціях необхідно враховувати відтворюваність обчислень, залежність результату від початкових умов і можливість статистичного аналізу вихідних послідовностей.

Перспективним напрямом є дослідження комбінованого методу, у якому двовимірна модель Ізінга використовується як додатковий механізм перетворення даних, а геш-функція Купина використовується для формування кінцевого геш-значення. Такий підхід передбачає визначення правил кодування вхідного повідомлення, параметрів ініціалізації спінової ґратки та послідовності виконання операцій гешування. Результативність запропонованої конструкції доцільно оцінювати за швидкодією, чутливістю геш-значення до зміни вхідних даних, рівномірністю розподілу вихідних бітів і стійкістю до відомих криптографічних атак. Необхідно здійснити порівняння з базовою геш-функцією Купина, оскільки додавання нових етапів перетворення не гарантує підвищення криптографічної стійкості.

Застосування такого методу може досліджуватися в контексті контролю цілісності інформаційних ресурсів автоматизованих систем управління авіацією та протиповітряною обороною, де важливими є виявлення змін даних і захист інформації від несанкціонованої модифікації. Використання геш-значень у процедурах контролю доступу операторів потребує інтеграції з окремими механізмами автентифікації та розмежування повноважень. Що дає змогу розглядати комбінований метод як один із можливих компонентів комплексної системи криптографічного захисту інформації.

Клімчук О. А., курсант
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

КОНЦЕПТУАЛЬНА АРХІТЕКТУРА АВТОМАТИЗОВАНОЇ СИСТЕМИ ПРОТИДІЇ ТЕХНІЧНІЙ РОЗВІДЦІ ШЛЯХОМ УПРАВЛІННЯ ЦИФРОВИМ СЛІДОМ ПІДРОЗДІЛУ

У цих тезах піднімається питання витоку даних через неконтрольований цифровий слід підрозділу – це слабке місце для систем прихованого управління військами. Автор пропонує загальну ідею програмно-апаратного комплексу, який би автоматично перевіряв метадані, фільтрував трафік і створював фейкову мережеву активність, щоб збити з пантелику технічні засоби розвідки супротивника.

Під час активних бойових дій прихованість управління військами – один із основних факторів для успішного виконання задач. Можливості розвідки супротивника суттєво змінилися: окрім класичної радіоелектронної розвідки (РЕР), масово використовують автоматизовані OSINT-системи, аналізують мережеві аномалії й перехоплюють незахищені пакети даних. Необережність при користуванні комерційними каналами зв'язку, надсилання фото чи відео з невидимими метаданими (EXIF, геомітки), або просто хаотична активність по локальних мережах залишає "цифровий слід", що демаскує позиції та плани набагато швидше, ніж банальний радіообмін.

Більшість сучасних методів захисту інформації робить акцент на шифруванні каналів зв'язку чи апаратному обмеженні випромінювання (наприклад, використання виносних антен або перевірених терміналів). А от системного контролю за цифровим слідом саме на рівні тактичної ланки майже немає. Такий пробіл потребує нових підходів і рішень для протидії технічним засобам розвідки супротивника.

Для вирішення цієї проблеми пропонується програмно-апаратний комплекс під робочою назвою "Цифрова тінь", який працює за принципом "Zero Trust" – жодної довіри до середовища передачі даних. Архітектура умовно складається з трьох пов'язаних модулів, які можна встановити прямо на захищений термінал зв'язку або окремий сервер:

Модуль пасивного моніторингу. Виконує сканування радіоефіру й цифрового середовища навколо підрозділу. Що входить: виявлення пристроїв

особового складу, які "фонять" через Bluetooth чи Wi-Fi, автоматичний моніторинг відкритих джерел (наприклад, регіональних Telegram-каналів) по ключових словах для швидкого виявлення витоку інформації про переміщення сил.

Модуль фільтрації та санітаризації трафіку. По суті, це фільтр між пристроєм і каналом зв'язку. Алгоритм сканує всі вихідні файли (фото, документи, логи), автоматично видаляє приховані EXIF-дані, GPS-координати, службову інформацію, імена авторів, MAC-адреси. Тобто якщо противник навіть перехопить і розшифрує дані, вони будуть анонімізовані та не дадуть нічого корисного.

Модуль активної протидії. Найцікавіша частина: система вже не просто захищається, а навмисно створює фейки. Алгоритм генерує масиви неправдивої мережевої активності: програмно емулює підключення до базових станцій у випадкових місцях, надсилає фіктивні запити до серверів, напускає "паразитний" трафік. Це перевантажує аналітику OSINT-систем супротивника зайвими даними та робить відбір справжніх цілей серед десятків фейкових набагато складнішим.

Вже зрозуміло - класичного маскування недостатньо. Автоматизоване керування цифровим слідом дає змогу:

1. Збити людський фактор у витоках чутливої інформації до мінімуму;
2. Автоматизувати контррозвідувальний захист на рівні підрозділів без залучення додаткових фахівців;
3. Ефективніше протистояти і РЕР, і автоматизованим пошуковим системам ворога.

Подальші дослідження будуть спрямовані на створення софт-прототипу модуля санітаризації метаданих на Python та тестування його у моделюванні роботи захищеного термінала.

СЕКЦІЯ 8
Спеціальний радіозв’язок

Гребняк В. С., слухач
Папуш О. Г.
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ ЗАГРОЗ ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ ТА КОМПЛЕКСНІ МЕТОДИ ЇХ НЕЙТРАЛІЗАЦІЇ

Сучасний сектор безпеки значною мірою залежить від інформації, цифрових технологій та інформаційних систем. Використання автоматизованих систем управління, електронного документообігу, цифрових засобів зв’язку та обробки даних створює нові можливості для підвищення ефективності роботи, однак одночасно призводить до появи нових загроз. В умовах активного розвитку цифрового середовища, інформація стає одним із важливих ресурсів, від якого залежить своєчасність прийняття управлінських рішень, ефективність виконання завдань та стійкість функціонування складових сектору безпеки. Саме тому технічний захист інформації набуває особливої актуальності, як основа забезпечення конфіденційності, цілісності та доступності даних у державних і оборонних структурах.

Однією з основних проблем залишається постійне вдосконалення кіберзагроз та способів їх реалізації. Кібератаки можуть бути спрямовані на отримання несанкціонованого доступу до інформаційних систем, викрадення або знищення даних, порушення роботи інформаційних ресурсів та компрометацію облікових записів користувачів. Особливу небезпеку для сектору безпеки становлять атаки, спрямовані не лише на окремі комп’ютери, а й на інформаційні системи, від яких залежить управління, обмін інформацією та взаємодія між підрозділами. У таких умовах технічний захист інформації повинен протидіяти витоку через побічні канали.

Практичним прикладом такої загрози є використання противником фішингових повідомлень для атак на державні органи, Сили оборони України та підприємства оборонно-промислового комплексу. Фішингові повідомлення можуть маскуватися під службове листування, документи, повідомлення від знайомих користувачів або іншу інформацію, яка викликає довіру. Перехід за

шкідливим посиланням або відкриття зараженого файлу може призвести до встановлення шкідливого програмного забезпечення та подальшої компрометації пристрою. У результаті зловмисники зможуть отримати можливість викрадення облікових даних, доступу до інформаційних ресурсів та інформації, яка зберігається на скомпрометованому пристрої. Технічні засоби захисту, зокрема системи виявлення аномалій і контролю цілісності програмного забезпечення, у поєднанні з криптографічними механізмами автентифікації та шифрування локальних сховищ дозволяють суттєво обмежити наслідки таких інцидентів.

Окрему увагу слід звернути на використання противником публічно доступних каналів комунікації, зокрема електронної пошти та соціальних мереж. Відкриті або недостатньо захищені поштові скриньки та акаунти в соціальних мережах можуть використовуватися для встановлення контакту з військовослужбовцями та подальшого проведення цілеспрямованих фішингових атак. Інформація, яку самі користувачі публікують у відкритому доступі, може використовуватися для підготовки більш переконливих повідомлень. Зловмисники можуть враховувати місце служби, характер діяльності, коло спілкування та інші доступні відомості, щоб замаскувати шкідливе повідомлення під звичайний службовий або особистий контакт. У цьому контексті технічний захист передбачає застосування засобів фільтрації трафіку та контролю цілісності, а криптографічний – використання захищених протоколів передачі даних і надійного шифрування вмісту повідомлень, що унеможливлює їх прочитання сторонніми особами навіть у разі перехоплення.

Таким чином, соціальні мережі та публічні електронні скриньки можуть стати одним із початкових елементів ланцюга кіберзагрози: від збору інформації про користувача та встановлення контакту, до надсилання фішингового посилання, зараження комп’ютера шкідливим програмним забезпеченням і подальшого несанкціонованого доступу до інформації. Особливу небезпеку це становить для військовослужбовців, оскільки компрометація одного пристрою або облікового запису потенційно може створити умови для подальшого поширення атаки та отримання доступу до інших інформаційних ресурсів. Ефективна протидія таким сценаріям неможлива без комплексного застосування технічних засобів захисту від витоку інформації та криптографічних алгоритмів, які забезпечують конфіденційність даних на всіх етапах їх життєвого циклу.

Важливим фактором ризику залишається людський фактор. Навіть сучасна система технічного та криптографічного захисту може бути недостатньо ефективною, якщо користувач не дотримується встановлених вимог інформаційної безпеки. Використання слабких паролів, повторне використання однакових паролів, передача облікових даних іншим особам, відкриття підозрілих файлів або перехід за неперевіреними посиланнями можуть створити умови для компрометації інформаційної системи. Тому підготовка особового складу та формування культури безпечної роботи з інформацією мають бути невід’ємною складовою системи захисту, доповнюючи технічні та криптографічні заходи.

Окремого значення набуває захист інформації з обмеженим доступом. У сучасних умовах значний обсяг такої інформації обробляється, зберігається та передається в цифровому середовищі. Це потребує особливої уваги до організації доступу, зберігання, передачі та резервного копіювання інформації. Для сектору безпеки особливо важливим є недопущення розголошення відомостей, які можуть становити державну таємницю або іншим чином бути використані противником для отримання переваги. Саме криптографічні засоби забезпечують гарантований захист таких даних шляхом шифрування, а технічні – запобігають їх витоку через фізичні та електромагнітні канали.

Вирішення зазначених проблем потребує комплексного підходу. Насамперед необхідно забезпечувати своєчасне оновлення програмного забезпечення, виявлення та усунення вразливостей, застосування багатофакторної автентифікації, антивірусного захисту, систем виявлення підозрілої активності, шифрування та резервного копіювання інформації. Важливим є також розмежування прав доступу, де кожен користувач отримує лише ті повноваження, які необхідні для виконання його службових завдань. Криптографічні механізми, зокрема симетричне та асиметричне шифрування, електронний підпис і захищені протоколи обміну ключами, мають застосовуватися на всіх рівнях обробки інформації.

Значну увагу необхідно приділяти навчанню особового складу. Регулярне проведення занять із питань кібергігієни, розпізнавання фішингових повідомлень, безпечного використання електронної пошти та соціальних мереж дозволить зменшити ризик помилкових дій користувачів. Важливо сформувати у військовослужбовців розуміння того, що інформаційна безпека залежить не лише від технічних і криптографічних засобів захисту, а й від особистої відповідальності кожного користувача.

Перспективним напрямом розвитку систем захисту інформації є використання сучасних інформаційних технологій, зокрема штучного інтелекту, для аналізу великих обсягів даних, виявлення нетипової активності та швидкого реагування на потенційні загрози. Водночас використання таких технологій повинно супроводжуватися контролем за достовірністю отриманих результатів, захистом даних і визначенням відповідальності за прийняття відповідних рішень. Не менш важливим є забезпечення стійкості інформаційних систем до можливих порушень їх функціонування. Для цього необхідно передбачати резервне копіювання критично важливих даних, дублювання інформаційних ресурсів і каналів зв'язку, можливість оперативного відновлення систем та розроблення алгоритмів реагування на інциденти. Це дозволяє мінімізувати наслідки атак і забезпечити безперервність виконання завдань.

Отже, сучасний етап розвитку інформаційних систем у секторі безпеки характеризується зростанням складності загроз, що зумовлює необхідність системного вдосконалення технічних і криптографічних механізмів захисту інформації. Актуальними залишаються ризики, пов'язані з компрометацією каналів зв'язку, використанням вразливостей програмно-апаратних засобів, а також атаками, що ініціюються через відкриті джерела інформації та соціальні мережі і призводять до впровадження шкідливого програмного забезпечення з подальшим несанкціонованим доступом до захищених ресурсів. Ефективна протидія таким загрозам потребує комплексного застосування засобів технічного захисту інформації, спрямованих на блокування побічних каналів витоку, контролю цілісності середовищ функціонування та фільтрації мережевого трафіку, у поєднанні з криптографічними методами забезпечення конфіденційності, автентичності та цілісності даних. Ключове значення мають алгоритми симетричного та асиметричного шифрування, протоколи захищеного обміну ключами, механізми електронного підпису, багатофакторна автентифікація та системи криптографічного управління доступом. Обов'язковою складовою є також організаційно-технічні заходи з розмежування повноважень користувачів, регулярного оновлення засобів захисту та підвищення рівня компетентності особового складу. Лише інтегроване впровадження зазначених технічних і криптографічних рішень здатне забезпечити необхідний рівень стійкості інформаційних систем, безперервності критично важливих процесів у секторі безпеки.

Прокопенко Є. В., канд. техн. наук, доц.
Мул Д. А., канд. техн. наук, доц.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ПІДХОДИ ДО ІНТЕГРАЦІЇ РІЗНОРІДНИХ СИСТЕМ РАДІОЗВ’ЯЗКУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАВДАНЬ СПЕЦІАЛЬНОЇ РОЗВІДКИ ПІДРОЗДІЛАМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ З ВИКОРИСТАННЯМ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ «ГАРТ»

Повномасштабна збройна агресія російської федерації проти України суттєво змінила умови виконання розвідувальних завдань і вимоги до їх інформаційно-комунікаційного забезпечення. Фізичне руйнування інфраструктури, порушення енергоживлення, радіоелектронний вплив, кібератаки, деградація або знищення мереж загального користування та швидка зміна оперативної обстановки безпосередньо впливають на своєчасність передавання розвідувальної інформації. За таких умов стійкість управління залежить не від наявності одного надійного каналу, а від можливості використовувати сукупність технологічно різнорідних засобів зв’язку та оперативно переходити між ними без втрати критичних інформаційних сервісів.

У межах цих тез спеціальна розвідка розглядається як діяльність, що передбачає добування, первинне опрацювання, передавання та доведення розвідувальної інформації в інтересах прийняття управлінських рішень і виконання визначених завдань. Радіозв’язок у цьому процесі є не окремим видом розвідки, а складовою її інформаційно-комунікаційного забезпечення. Тому предметом інтеграції мають бути не «системи радіозв’язку спеціальної розвідки» як ізольований клас техніки, а різнорідні засоби зв’язку, через які передаються голосові повідомлення, координатна, телеметрична, текстова, графічна та відеоінформація між виконавцями, технічними засобами, пунктами управління та споживачами розвідувальної інформації.

Практична діяльність підрозділів Державної прикордонної служби України (далі – ДПСУ), залучених до виконання розвідувальних завдань, об’єктивно потребує одночасного використання різних за призначенням і

технологічною реалізацією комунікаційних ресурсів. До них можуть належати засоби тактичного УКХ- і КХ-радіозв'язку, цифрові системи професійного мобільного радіозв'язку, радіорелейні та супутникові канали, відомчі IP-мережі, ресурси мобільних мереж LTE/5G, а також канали передавання даних від технічних засобів спостереження та інших джерел інформації. Така різнорідність підвищує потенційну живучість системи, але одночасно створює проблеми сумісності, маршрутизації, пріоритезації трафіку, ідентифікації користувачів і реалізації єдиних вимог до захисту інформації.

Для вирішення зазначеної суперечності Інтегровану інформаційно-комунікаційну систему «Гарт» (далі – ІІКС «Гарт») доцільно розглядати як інтеграційний рівень, через який забезпечується узгоджене використання різнорідних комунікаційних контурів ДПСУ. Йдеться не про фізичне об'єднання всіх радіостанцій і каналів в одну мережу, а про інтеграцію інформаційних сервісів, правил доступу, маршрутизації та обміну даними поверх різних транспортних середовищ. У такій моделі конкретний канал виступає ресурсом доставки інформації, а його роль – основна, резервна або додаткова – визначається поточною обстановкою, критичністю повідомлення, доступністю та якістю зв'язку.

Структурно гетерогенну систему доцільно формувати за багаторівневим принципом: джерела та споживачі розвідувальної інформації; рівень радіодоступу; транспортний рівень; інтеграційний рівень ІІКС «Гарт»; відомчі інформаційні сервіси та органи управління. На першому рівні формуються й приймаються повідомлення, дані, координатна, телеметрична або відеоінформація. Рівень радіодоступу може поєднувати УКХ-, КХ- та цифрові професійні радіосистеми, а транспортний рівень – відомчі IP-мережі, радіорелейні, проводові, волоконно-оптичні, мобільні та супутникові канали. ІІКС «Гарт» у запропонованій моделі виконує функцію логічного узгодження інформаційного обміну між цими рівнями.

Забезпечення стійкості такої системи доцільно здійснювати за багатоконтурним принципом. Для кожного критичного інформаційного сервісу мають бути завчасно визначені основний, резервний та, за потреби, аварійний способи передавання. Тактичний радіоконтур доцільно використовувати для оперативного голосового обміну й коротких повідомлень; широкосмуговий – для передавання значних масивів даних, відео та телеметрії; транспортний – для

зв’язку між районами виконання бойових завдань і пунктами управління; резервний – для підтримання мінімально необхідного обміну за деградації або знищення основних ресурсів. Перехід між ними має здійснюватися з урахуванням фактичної доступності, затримки, пропускної здатності, захищеності та впливу радіоелектронної обстановки.

Ресурси цивільних комунікаційних мереж доцільно залучати як додатковий транспортний контур, а не як заміну відомчої системи зв’язку. Публічні LTE/5G-мережі можуть розширювати доступність і забезпечувати резервування, однак передавання відомчої інформації повинно здійснюватися через контрольовані механізми доступу та захисту. Інтеграція різнорідних засобів потребує уніфікації класів критичності повідомлень, правил адресації та маршрутизації, розмежування прав доступу, ідентифікації користувачів і пристроїв, а також централізованого моніторингу стану доступних каналів. Технологічна сумісність при цьому не повинна призводити до неконтрольованого поширення розвідувальної інформації між сегментами системи.

Процес інтеграції доцільно реалізовувати поетапно: визначити критичні інформаційні сервіси й категорії користувачів; провести інвентаризацію доступних систем і каналів; установити правила їх взаємодії через ІІКС «Гарт»; сформувати основні та резервні маршрути; визначити пріоритетність інформаційних потоків; перевірити працездатність у сценаріях часткової деградації або знищення; організувати постійний моніторинг і коригування конфігурації відповідно до оперативної, кібернетичної та електромагнітної обстановки. Отже, перспективним напрямом забезпечення підрозділів ДПСУ під час виконання завдань спеціальної розвідки є інтеграція різнорідних засобів зв’язку навколо ІІКС «Гарт» як інтеграційного рівня відомчих сервісів. Такий підхід розглядає зв’язок як інфраструктурну основу своєчасного передавання й доведення розвідувальної інформації та створює передумови для підвищення сумісності, стійкості й адаптивності інформаційного обміну.

Якименко В. С.
Печерська В. І., курсант
Житомирський військовий інститут імені С. П. Корольова

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ MESH–СИСТЕМ

У сучасній війні поле бою не закінчується дальності ураження озброєння, а переходить в електромагнітне середовище. Підрозділи зв’язку будують інформаційну систему, підрозділи радіоелектронної боротьби та радіоелектронної розвитки противника намагаються зруйнувати або отримати контроль над інформаційною системою. Управління без сучасної інформаційної системи як снайпер без зору. Сучасні бойові дії характеризується застосуванням засобів радіоелектронної боротьби (РЕБ), радіоелектронної розвідки (РЕР) та високою динамікою зміни обстановки на лінії бойового зіткнення (ЛБЗ). Війська ворога здійснюють руйнування цивільної інфраструктури (стільникового зв’язку, провідних ліній), системи військового зв’язку (“станція — ретранслятор — станція”), що повністю паралізує управління підрозділом. Станції супутникового зв’язку StarLink показали вразливість у разі певних “політичних” або технічних рішень, що призводить до зупинки передачі даних. Відсутність власної системи супутникового зв’язку не дозволяє організувати якісний надійний канал передачі даних.

У зв'язку з цим особливої актуальності набуло впровадження самоорганізуючих комірчастих мереж (MANET/MESH), які забезпечують високу децентралізацію, стійкість до завад та можливість передачі даних на тактичному рівні.

Сутність та переваги технології MESH у тактичній ланці.

MESH-архітектура передбачає, що кожен приймач-передавач (радіостанція, безпілотник чи мобільний вузол) виконує роль не лише кінцевого термінала, а й ретранслятора даних для інших учасників мережі.

MESH система має наступні властивості:

(Self-Healing) автоматична реконфігурація забезпечує у разі виходу з ладу або знищення одного чи кількох вузлів мережа миттєво перераховує маршрути та продовжує передачу пакетів через інші доступні радіоточки;

(Multi-hop) багатострибкова передача дозволяє обходити складний рельєф місцевості, міську забудову чи складні складки рельєфу без застосування високорослих щогл або спеціальних ретрансляторів;

масштабованість здійснює швидке додавання нових вузлів (піхотинців, БПЛА, НРК) без додаткового налаштування мережевої інфраструктури.

Застосування MESH-систем у Збройних Силах України.

Збройні Сили України підійшли до побудови тактичного MESH-зв’язку комбінованим шляхом, поєднуючи професійні стандарти NATO з масштабуванням бюджетних систем.

Офіційні рішення професійного рівня:

застосування військових цифрових радіостанцій (SDR) фірми Harris (L3 Harris) та Silvus Technologies (технології MN-MIMO), які забезпечують високошвидкісну передачу даних, відеопотоків та сигналів управління в умовах жорсткої дії РЕБ;

використання технології MESH для побудови тактичної мережі BWA (Broadband Wireless Access) на рівні батальйон — бригада з використанням радіомостів.

Масовий низовий та волонтерський рівень:

впровадження портативних радіостанцій із прошивками та протоколами MESH (Meshtastic на базі LoRa, радіостанції Retevis, Hyt, рішення на базі DMR із функцією Pseudo Trunking / IP Multi-Site Connect);

впровадження від окремих переносних радіостанцій до комплексних рішень Himera G1 Pro;

MESH на БПЛА та НРК: використання повітряних та наземних дронів як динамічних ретрансляторів для пробиття ліній РЕБ та збільшення радіуса дії FPV-дронів і систем розвідки;

інтеграція з ситуаційними системами: MESH-мережі забезпечують каналом зв'язку планшети з системами ситуаційної обізнаності (на кшталт «Кропива», «Дельта») безпосередньо в окопах та бронетехніці.

Застосування MESH-систем підрозділами ЗС рф.

Збройні сили рф демонструють дещо інший вектор розвитку, де офіційні концепції зіштовхнулися з реальністю бойових дій.

Штатні військові системи:

у рамках концепцій МКС (багатоканальних комплексів зв'язку) рф намагалася впроваджувати радіостанції серії «Азарт» (Р-187П1), які декларували підтримку режимів ППРЧ та елементів Mesh-мереж. Проте через проблеми (постачання, складність налаштувань, корупцію та відсутність навченого персоналу) повноцінне MESH-покриття на базі «Азартів» у масштабах підрозділів реалізувати не вдалося.

Адаптація та інші рішення:

для компенсації дефіциту штатного зв’язку ворог перейшов на активне використання цивільних цифрових систем DMR (Hytera, Motorola, TYT) із налаштуванням ретрансляторів та спрощених комірчастих топологій;

проведення власної розробки та масового впровадження спеціалізованих модулів MESH-зв'язку для FPV-дронів та розвідувальних БПЛА (передавачі діапазонів 868/915 МГц та 2.4 ГГц) з метою протидії українським засобам РЕБ;

Ключові виклики та тенденції подальшого розвитку.

Для ефективної роботи MESH-мережі потребують активного обміну службовими пакетами для підтримки топології. Це створює постійний радіовипромінювальний слід, що вимагає впровадження режимів ППРЧ (стрибкоподібного перелаштування частоти), низької ймовірності перехоплення (LPI/LPD) та спрямованих антен. Основним чинником якісної MESH системи – це кількість нод (вузлів), які розгортаються в даній системі. Чим вища кількість тим надійніша MESH система. Постає питання, чому не закупити всім дані радіостанції та сформувати єдину MESH мережу? Чим більше нод — це краще покриття та надійність, але лише до межі пропускної спроможності радіоканалу! Для низькошвидкісних систем (LoRa/Meshtastic) межа настає вже на кількох десятках вузлів, тоді як професійні військово-промислові SDR MESH-системи спроможні тримати сотні вузлів за рахунок широкої смуги та складних алгоритмів часового розділення. Тут і постає основне питання створення ієрархії даної системи.

Майбутні MESH-системм повинні розгортатися відповідно визначеній ієрархії підпорядкування. Організацію створення гібридних мереж «наземний бієць — наземний робот — повітряний дрон-ретранслятор», де втрата одного з елементів автоматично компенсується іншим.

Захист від спуфінгу та впровадження вузлів ворога потребує постійного моніторингу розгорнутих систем, захист передбачає надійного шифрування (AES-256) та автентифікації кожного нового вузла в комірчастій мережі.

Висновок: розвиток та застосування MESH-систем у російсько-українській війні довів їхню перевагу. Незамінність для забезпечення безперервного та стійкого управління в низовій тактичній ланці за рахунок малопотужних радіозасобів (0,25Вт). Збройні Сили України зберігають технологічну гнучкість та оперативність у впровадженні сучасних MESH-рішень (від західних професійних SDR до народних LoRa-мереж), тоді як ЗС рф

намагаються компенсувати провали у штатному військовому зв'язку за рахунок централізованої закупівлі китайських цифрових систем та власної адаптації MESH-каналів для безпілотної авіації. Домінування на полі бою отримує той, хто швидше інтегрує MESH-мережі з автономними роботизованими комплексами та забезпечить їхню стійкість до завад РЕБ в розгорнутій ієрархічній MESH системі.

Лейко О. М.
Житомирський військовий інститут імені С. П. Корольова

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ТА ЗАСОБІВ ЗВ’ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З УРАХУВАННЯМ ВПРОВАДЖЕННЯ МЕРЕЖ LTE

1. Вступ та актуальність дослідження

Сучасний етап трансформації Збройних Сил України та досвід протистояння повномасштабній агресії висувають принципово нові вимоги до життєдайності інформаційних просторів. Модернізація системи зв'язку спеціального призначення Сил оборони України перебуває у прямій залежності від оперативного впровадження передових технологій та глибокого аналізу реального бойового досвіду.

У сучасних реаліях ключовим завданням є не просто номінальний вибір новітніх стандартів комунікації, а комплексне вивчення механізмів їх адаптації та функціонування в умовах високоінтенсивних бойових дій. Особливо гострою ця проблема постала під час проведення масштабних наступальних та контрнаступальних операцій. Практика довела, що війська змушені виконувати завдання на абсолютно непідготовлених у комунікаційному плані територіях, або в районах, де цивільна та критична телекомунікаційна інфраструктура зазнала тотального або часткового руйнування внаслідок вогневого впливу.

В таких ситуаціях надзвичайно перспективним напрямком є інтеграція у систему військового управління технологій стільникового зв’язку стандартів 3G та 4G (LTE). Даний матеріал присвячений теоретичному та практичному обґрунтуванню впровадження мереж Private LTE, спираючись на досвід забезпечення зв'язку підрозділам у Сумській області та безпосередньо на лінії бойового зіткнення (ЛБЗ) під час деокупації східних регіонів України.

2. Комплексна постановка проблеми

Аналіз дій Сил оборони України на полі бою виявив системні труднощі під час організації стабільного зв'язку в умовах динамічного руху. Коли стаціонарна опорна транспортна мережа повністю знищена, а розгортання класичних кабельних ліній потребує значних часових витрат, основним інструментом забезпечення управління стають радіозасоби. Проте розгортання польових вузлів зв'язку тягне за собою комплекс супутніх викликів:

Необхідність оперативного розподілу та передачі обмежених телекомунікаційних ресурсів.

Організація автономного електроживлення в польових умовах.

Забезпечення життєдіяльності особового складу підрозділів зв’язку, а також безпосередня охорона та оборона об’єктів зв’язку від диверсійно-розвідувальних груп противника та ударних БПЛА противника.

Ситуація критично ускладнюється в умовах складної електромагнітної обстановки на передовій. Постійне використання засобів РЕБ противником суттєво знижує ефективність стандартних каналів зв’язку. Також існують географічні та технічні зони (включаючи прикордонні райони та території РФ), де використання звичних мобільних супутникових терміналів типу Starlink – не можливе. Отже, організація та впровадження альтернативних мобільних високошвидкісних мереж зв'язку спеціального призначення є стратегічною потребою.

3. Негативні фактори та критичні виклики при розгортанні Private LTE на ЛБЗ

Практична експлуатація виділених стільникових мереж у безпосередній близькості до лінії бойового зіткнення (ЛБЗ) супроводжується низкою жорстких обмежень. Специфіка бойового застосування виявила чотири ключові проблеми:

Висока радіолокаційна та радіоелектронна помітність (Radio Signature): Класичне комерційне радіообладнання стільникового зв'язку проєктується для всеспрямованого випромінювання (у секторі 360°). Постійна робота та випромінення базових станцій перетворюють їх на помітні радіовипромінювальні пристрої. Для засобів радіоелектронної розвідки (РЕР) противника така станція стає пріоритетним об'єктом пеленгації, що неминуче призводить до виведення з ладу або фізичного знищення артилерією чи ракетно-бомбовими ударами.

Уразливість стандартних стеків протоколів до завад РЕБ: Базові алгоритми LTE розроблялися без розрахунку на навмисне інтелектуальне придушення. Спрямований загороджувальний або прицільний шум в робочих

діапазонах частот — особливо атаки на пілотні сигнали й канали синхронізації — здатний повністю дезорганізувати роботу мережі та призвести до втрати зв'язку між абонентами мережі.

Вимогливість до топології та централізації комутаційного ядра (Core Network): Функціонування LTE критично залежить від працездатності ядра мережі — EPC (Evolved Packet Core). За традиційної схеми, коли EPC розгорнуто віддалено у тилу, стабільність тактичного сегмента прив'язана до магістральних каналів (радіорелейних ліній або супутникових терміналів Starlink). У разі фізичного переривання чи придушення цього магістрального каналу, базова станція на передовій втрачає зв'язок із ядром, ізолюючи абонентів на місці, попри фізичну наявність сигналу.

Жорстка ієрархічність та обмеження мобільності (Neighbor Discovery): На відміну від децентралізованих військових систем типу MANET або Mesh, де кожна радіостанція є ретранслятором, архітектура LTE побудована на принципі «клієнт-сервер». За відсутності динамічного перенаправлення трафіку між терміналами, вихід військовослужбовця або рухомої платформи за межі радіуса покриття конкретної базової станції означає миттєве та повне розірвання інформаційного обміну.

5. Перспективні технологічні рішення та вектори розвитку (Perspectives)

Для нівелювання зазначених негативних факторів у Силах оборони України реалізується комплекс системно-технічних та інженерних модифікацій архітектури Private LTE.

Архітектурна децентралізація на основі концепції «Tactical Bubble»

Для усунення ризиків, пов'язаних із втратою зв'язку з тиловою інфраструктурою, впроваджуються рішення класу "Core-on-a-Box" та "Core-on-the-Edge".

Віртуалізоване програмне ядро (EPC) інтегрується безпосередньо в обчислювальні модулі (промислові міні-комп’ютери), конструктивно об'єднані з мобільною базовою станцією (eNodeB/gNodeB). Це дозволяє сформувати повністю автономну локальну систему зв'язку — «тактичну бульбашку». За умов повної ізоляції від зовнішнього інтернету чи вищих штабів, всередині батальйону зберігається повноцінний високошвидкісний обмін даними: трансляція відеострімів із БПЛА, внутрішня координація в ІКС («Дельта», «Кропива») та робота локальних месенджерів.

Протидія РЕБ/РЕР через інтеграцію SDR та технологій Beamforming

Зниження демаскуючих ознак та підвищення завадозахищеності досягається завдяки переходу на програмно-визначені радіосистеми (SDR) та активні фазовані антенні решітки (АФАР):

Динамічне формування променів (Beamforming): Базова станція відмовляється від кругового випромінювання на користь формування вузькоспрямованих просторових променів, орієнтованих суворо на конкретні термінали бійців чи техніки. Це зменшує дальність радіоелектронного виявлення станції ворогом у 5–10 разів.

Просторове занулення (Spatial Nulling): У разі фіксації активної завади з боку ворожого комплексу РЕБ, адаптивна антенна система вираховує вектор джерела випромінювання та програмно створює «нуль» (зону максимального затухання) у цьому напрямку. Це дозволяє нівелювати заваду, продовжуючи стабільно приймати корисний сигнал від своїх абонентів.

Розгортання повітряного ешелону зв'язку (Airborne LTE)

Подолання проблем складного рельєфу, щільної міської забудови та лісистої місцевості реалізується через підняття полегшених базових станцій (вагою до 2–3 кг) на повітряні платформи — важкі БПЛА-ретранслятори або мобільні аеростати. Функціонування станції на висотах 300–500 метрів дозволяє забезпечити стійке широкосмугове покриття в радіусі до 15–20 км. Така повітряна базова станція є недосяжною для стандартного артилерійського вогню, а її висока мобільність дозволяє оперативно змінювати позицію у разі виникнення загрози знищення.

Криптографічний захист та радіомаскування

Для запобігання перехоплення даних та ускладнення аналізу радіоелектронного середовища ворогом, застосовуються специфічні заходи безпеки:

Наскрізне шифрування (End-to-End VPN): Поверх базових алгоритмів шифрування LTE (AES-128/256) розгортається додатковий транспортний криптографічний рівень. Він базується на сертифікованих в Україні алгоритмах та національних стандартах захисту інформації.

Адаптація частотного спектра: Робота систем Private LTE переводиться на нестандартні частотні діапазони, що не використовуються комерційними операторами. Це суттєво ускладнює роботу засобів РЕР противника.

6. Перспективи масштабування: перехід від Private LTE до систем 5G спеціального призначення

Логіка розвитку сучасних воєнних конфліктів доводить, що Private LTE є базовим, але не кінцевим етапом цифровізації. Наступним стратегічним кроком для Сил оборони України є поступова інтеграція та адаптація технологічного стека п'ятого покоління (5G). На відміну від цивільного сектору, у військовій сфері ця технологія здійснює фундаментальний архітектурний переворот.

Гнучке програмне керування та створення віртуальних мереж

Традиційні системи зв'язку спеціального призначення історично залежали від спеціалізованого, апаратного та монолітного обладнання (критична прив'язка до вендорів, складність конфігурації). Технологія 5G пропонує повністю програмно-визначений підхід (Software-Defined Networking — SDN). Ключові мережеві функції (оркестрація, комутація та управління ресурсами) піддаються глибокій віртуалізації. Військовим органам управління це надає:

Радикальне зниження фінансових витрат на розгортання інфраструктури.

Зменшення фізичних масо-габаритних параметрів комплексів зв'язку.

Можливість гнучкого та динамічного переналаштування параметрів мережі безпосередньо під час виконання бойових завдань.

Ефективність спектра та нові радіочастотні можливості

Впровадження 5G дозволяє Силам оборони не лише оптимізувати роботу у звичних частотних діапазонах нижче 6 ГГц (Sub-6 / FR1), але й освоїти міліметрові хвилі (mmWave / FR2) у межах частот 26, 28 та 39 ГГц. Задіяння FR2 відкриває безпрецедентні канали пропускної здатності. Велика пропускна здатність дозволяє миттєво обмінюватися гігантськими масивами даних у захищених локальних системах.

Ефективність використання цього спектра досягається завдяки технологіям Massive MIMO та цифрового формування променів (Beamforming). Замість неефективного всеспрямованого випромінювання система 5G генерує точкові, сфокусовані просторові промені, які слідують за динамічними об'єктами. Це не лише мінімізує взаємні радіоперешкоди, але й критично знижує енергоспоживання базових станцій у польових умовах.

Тріада послуг IMT-2020 в інтересах мережецентричної війни

Відповідно до глобальної рамкової моделі ITU IMT-2020, архітектура 5G розгортає три базові класи послуг в межах єдиної фізичної інфраструктури. Кожен з кластерів закриває конкретну операційну потребу військ:

1.eMBB (покращений мобільний широкосмуговий доступ): Гарантує передачу надважкого контенту, роботу геоінформаційних систем та трансляцію багатоканального відео високої роздільної здатності з розвідувальних БПЛА.

2.URLLC (наднадійний зв'язок із низькою затримкою): Забезпечує миттєвий відгук мережі (затримки менше 1 мілісекунди), що є критично важливим для систем управління ППО/ПРО, дистанційного оперування роботизованими вогневими точками та координації роїв автономних БПЛА.

3.mMTC (масивний машинний зв'язок): Дозволяє одночасно підключати мільйони недорогих датчиків з низьким рівнем споживання енергії. Це закладає основу для створення «Військового Інтернету речей» (IoMT) — суцільного сенсорного поля, де кожен елемент (від датчика руху в лісосмузі до сенсора життєдіяльності на бронежилеті бійця) інтегрований у загальну систему.

7. Міжнародний досвід та стандартизація: кейс PROTEAS та нормативна база НАТО

Практичний вектор інтеграції широкосмугових мереж нового покоління у військову сферу чітко простежується в межах проєктів Європейського оборонного фонду (EDF). Найбільш показовим прикладом є ініціатива PROTEAS, спрямована на створення перспективного Командного пункту управління Сил спеціальних операцій (SOFCP C2) для спільних операцій ЄС.

У межах PROTEAS розгорнуто автономну непублічну мережу стільникового зв'язку нового покоління — SNPN (Standalone Non-Public Network) за даними консорціуму 3GPP. Даний простір виділено для забезпечення стійкого функціонування Системи безпеки периметра (PSS) командного пункту.

Архітектура SNPN PROTEAS створює захищену та повністю ізольовану комунікаційну «бульбашку», яка об'єднує різнорідне користувацьке обладнання (UE):

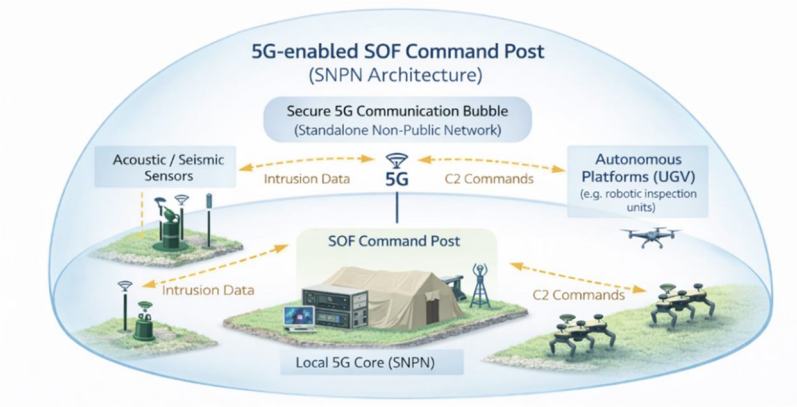
Акустичні та сейсмічні наземні датчики, що фіксують спроби проникнення або висування техніки противника в режимі реального часу.

Роботизовані безпілотні платформи (зокрема автономні чотириногі роботи — «робособаки»), які автоматично висуваються для розвідки та зачистки зони, одразу після спрацювання сенсорів.

Цей досвід підтверджує можливість повної автоматизації ланцюжка «виявлення — зв'язок — реагування» на базі стільникових технологій.

Важливим кроком на шляху узаконення цих технологій у військовому середовищі стало оприлюднення 11 лютого 2026 року першої редакції угоди зі

стандартизації НАТО — STANAG 5665 (Cellular Communications for Defence). Цей документ заклав нормативний фундамент для забезпечення оперативно-технічної сумісності мереж 5G між збройними силами держав-членів Альянсу, що підтверджує незворотність переходу глобальних оборонних систем на комерційні стільникові стандарти із військовою надбудовою.



Концептуальне представлення автономної непублічної мережі 5G (SNPN) компанії PROTEAS, що підтримує систему безпеки периметра (PSS) командного пункту SOF

8. Висновки та практичні пропозиції

1.Неминучість технологічної інтеграції:

Подальший розвиток та забезпечення стійкості системи зв’язку Збройних Сил України в умовах зруйнованої або відсутньої стаціонарної інфраструктури неможливі без залучення цивільних стандартів широкосмугового зв'язку (LTE та 5G). Досвід бойових дій у Сумській області та під час наступальних операцій на Сході України довів високу ефективність стільникового радіообладнання для швидкої організації зв'язку там, де інші канали заблоковані або знищені.

2.Подолання викликів безпеки:

Головним бар'єром на шляху повного впровадження LTE/5G у ЗСУ залишається відсутність спеціалізованих військових сертифікацій для COTS-обладнання (готових комерційних рішень) та вразливість перед цілеспрямованим впливом засобів РЕБ/РЕР. Перспективним шляхом вирішення є обов'язкове розгортання додаткових рівнів наскрізного криптографічного захисту інформації (End-to-End VPN) за національними стандартами поверх базових протоколів 3GPP (на кшталт TS 33.501). Перехід на нестандартні частотні діапазони.

3.Архітектурна автономія:

Для зменьшення ризиків ураження комутаційних вузлів, військові мережі стільникового зв'язку повинні будуватися за децентралізованим принципом «Tactical Bubble» на базі рішень Core-on-a-Box (віртуалізоване ядро EPC/5GC безпосередньо на борту мобільної базової станції). Це гарантує живучість внутрішнього зв'язку підрозділу навіть за умов повної втрати супутникових чи радіорелейних каналів.

4.Впровадження повітряного ешелону:

Результати практичних досліджень вказують на високу доцільність інтеграції полегшених базових станцій LTE/5G з безпілотними авіаційними комплексами (концепція Airborne LTE). Підняття ретрансляторів на висоту дозволяє ігнорувати складний рельєф місцевості та оперативно маневрувати зонами покриття під час наступу.

5.Практична значущість:

Сформовані у статті пропозиції та технічні висновки є критично важливими для органів військового управління під час планування майбутніх деокупаційних операцій. Обґрунтування закупівель новітнього комунікаційного обладнання та розробки перспективних форм і способів застосування підрозділів зв’язку Сил оборони України з урахуванням стандартів НАТО (зокрема STANAG 5665).

Стасєв Ю. В., д-р техн. наук, проф.
Новічков В. О.
Карамушка М. І.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

АЛГОРИТМ ПІДВИЩЕННЯ НЕЛІНІЙНОСТІ КЕРУЮЧИХ ПОСЛІДОВНОСТЕЙ У СИСТЕМАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Сучасні системи управління військами та засоби спеціального зв’язку функціонують в умовах активної радіоелектронної та кібернетичної протидії противника, що висуває підвищені вимоги до криптографічного захисту

інформації, яка передається каналами зв’язку. Захист має забезпечувати високу стійкість і водночас не створювати помітних затримок та не знижувати пропускну здатність каналів. Цим вимогам найкраще відповідають потокові шифри, швидкість формування гами яких у перспективних алгоритмах досягає сотень мегабіт за секунду, що робить їх оптимальними для динамічних каналів передачі даних, зокрема супутникових, мобільних і широкосмугових.

Водночас досвід експлуатації показує, що навіть широко застосовувані потокові алгоритми можуть мати суттєві вразливості, прикладом чого є відомі недоліки шифру A5 стандарту GSM. Криптографічна стійкість потокового шифру визначається насамперед якістю псевдовипадкових керуючих послідовностей, що формують гаму шифру. Передбачення або часткове відновлення гами призводить до компрометації всієї системи незалежно від складності вищих рівнів обробки, у тому числі інтелектуальних методів адаптивного управління. Тому розроблення математично обґрунтованих способів формування криптографічно стійких керуючих послідовностей залишається актуальним науково-прикладним завданням.

До керуючих послідовностей висувається комплекс вимог: забезпечення необхідної імітостійкості на фізичному рівні; оптимальність процедур формування з погляду обчислювальних витрат; можливість синтезу послідовностей довільної тривалості; реалізованість формувачів із прийнятною технічною складністю, зокрема на мікропроцесорній техніці; відповідність розподілу символів критерію псевдовипадковості.

Найпоширенішим підходом до побудови генераторів керуючих послідовностей є використання лінійних рекурентних регістрів зі зворотним зв’язком на основі примітивних поліномів. При потоковому методі елементи послідовності задовольняють рекурентному співвідношенню

$$m_{n+j} = a_0 m_j + a_1 m_{j+1} + \ldots + a_{n-1} m_{j+n-1}, \quad j = 0, 1, \ldots$$

де m_i, a_i – елементи поля Галуа $GF(p)$.

На теперішній час в криптосистемах використовують послідовності, побудовані над полем GF(2).

Проведений аналіз показав, що чисто лінійні схеми мають фундаментальні недоліки: короткі повторювані цикли, лінійну залежність між елементами, недостатній баланс нулів і одиниць, низьку структурну скритність та низьку лінійну складність, що робить їх вразливими до криптоаналітичних

атак. Крім того, регістри над полем GF(2) малоефективні у програмній реалізації, особливо коли довжина регістра перевищує розмір машинного слова, і генерують лише один біт за такт.

Нелінійність в алгоритм формування керуючих послідовностей доцільно вводити такими способами: нелінійною фільтрацією на виході регістра; комбінаційним перемішуванням виходів кількох регістрів нелінійною функцією; введенням нелінійної функції безпосередньо у схему зворотного зв'язку; комбінацією зазначених способів. При цьому надмірне ускладнення структури може погіршити загальну стійкість, тому введення нелінійності має супроводжуватися аналізом статистичних, кореляційних і структурних властивостей отриманої послідовності.

Для усунення зазначених недоліків запропоновано використовувати лінійні рекурентні регістри, побудовані над розширеним полем $GF(2^q)$. Такий регістр математично еквівалентний q паралельним регістрам зсуву над $GF(2)$ з різними початковими станами, кожний довжиною

$$L = qn,$$

де n – ступінь утворюючого примітивного полінома. Період послідовності такого регістра дорівнює

$$T = 2^L - 1,$$

а її лінійна складність

$$\lambda(z) = qL.$$

Перевагами регістрів над $GF(2^q)$ є: видача за один такт блоку бітів довжиною машинного слова q; незалежність швидкодії від виду утворюючого полінома (проріджeного чи щільного); можливість використання відомих проріджених примітивних поліномів; значне збільшення періоду послідовності, що зменшує частоту перезавантаження ключової інформації.

Для подальшого підвищення лінійної складності вихід регістра піддається блоковим нелінійним перетворенням (S-блокам), які здійснюють відображення $\{0,1\}^n \rightarrow \{0,1\}^q$. Верхня границя лінійної складності вихідної послідовності z визначається як

$$\lambda(z) \le C^1_L + C^2_L + \ldots + C^d_L,$$

де d – алгебраїчний ступінь нелінійної функції. Оскільки для узагальненого регістра L є складеним числом, при фіксованому L підвищення складності

досягається вибором функцій з максимальним d, а ступінь полінома n підбирається для забезпечення великої довжини регістра.

Як нелінійне перетворення запропоновано використовувати каскад 8-бітових підстановок у блоках Z0, Z1, …, Z31. Ключ підстановки генерується за алгоритмом, що використовує просте число довжиною 256 біт і первісний елемент поля GF(p), а ключі наступних блоків формуються циклічними зсувами базового ключа. Додатково застосовуються блоки нелінійної фільтрації на основі булевих функцій (кон’юнкції, диз’юнкції, елементів Пірса і Шеффера, вузлів вибірки, трійки та перестановки), які забезпечують необхідну еквівалентну лінійну складність і вирівнюють імовірності появи нулів і одиниць. У програмній реалізації такий блок подається масивом, у якому 8-розрядна адреса елемента є вхідним символом, а значення елемента – вихідним бітом, що дозволяє заздалегідь записувати таблиці у пам’ять і досягати високої швидкодії.

Отже, для досягнення високої криптографічної стійкості керуючі послідовності мають наближатися за статистичними характеристиками до випадкових, забезпечувати рівноймовірний розподіл символів і мати період, що суттєво перевищує тривалість сеансу зв’язку. Найбільш ефективним рішенням є гібридний підхід – поєднання лінійних рекурентних регістрів над розширеним полем $GF(2^q)$ з блоковими нелінійними перетвореннями (S-блоками, таблицями підстановок і булевими функціями високого алгебраїчного ступеня). Він дозволяє одночасно суттєво збільшити період і лінійну складність послідовності та забезпечити стійкість до диференціального, лінійного та кореляційного криптоаналізу. Блоки нелінійної фільтрації доцільно проєктувати з розміром, кратним машинному слову (8, 16 біт і більше), а замість єдиного блоку підстановки комбінувати кілька нелінійних перетворень із застосуванням техніки “забілювання”.

Отримані результати можуть бути використані під час створення криптографічно стійких засобів потокового шифрування для систем скритого управління військами та захисту інформації в телекомунікаційних мережах військового призначення.

Ваврічен О. А.
Бібік А. В.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ЗАГРОЗИ НЕСАНКЦІОНОВАНОГО ЗНІМАННЯ ІНФОРМАЦІЇ З ВОЛОКОННО-ОПТИЧНИХ ЛІНІЙ ЗВ'ЯЗКУ

Сучасні інформаційно-комунікаційні системи значною мірою базуються на використанні волоконно-оптичних ліній зв'язку, які забезпечують високу пропускну здатність, низьке загасання сигналу, стійкість до електромагнітних завад та можливість передавання значних обсягів інформації на великі відстані. Особливого значення така інфраструктура набуває у відомчих інформаційно-комунікаційних системах та мережах спеціального призначення.

Волоконно-оптичні лінії традиційно вважаються більш захищеними від несанкціонованого перехоплення порівняно з металевими лініями зв'язку. Це зумовлено тим, що передавання інформації відбувається у вигляді оптичного випромінювання всередині світловода та практично не супроводжується утворенням зовнішнього електромагнітного поля, придатного для дистанційного знімання інформації. Водночас фізичний рівень оптичної мережі не є абсолютно захищеним. За наявності доступу до кабельної траси, оптичних муфт, кросів, розподільчих шаф або іншого телекомунікаційного обладнання існує можливість прихованого відведення частини оптичної потужності та подальшого отримання інформації, що передається каналом.

Найбільшу небезпеку становлять пасивні способи перехоплення, оскільки вони можуть не призводити до припинення роботи каналу та тривалий час залишатися непоміченими. Одним із найбільш характерних фізичних механізмів, що може бути використаний для несанкціонованого знімання інформації, є відведення частини оптичного випромінювання шляхом локального вигину волокна. За нормальних умов світловий потік поширюється у серцевині волокна завдяки явищу повного внутрішнього відбиття. У разі надмірного вигину частина оптичної енергії може виходити за межі серцевини. За наявності відповідного приймального обладнання така енергія може бути зафіксована та використана для відновлення сигналу.

До інших можливих способів фізичного відгалуження належать використання оптичних розгалужувачів, спеціальних відгалужувальних пристроїв та втручання у штатні елементи оптичної інфраструктури. Якщо частка відібраної оптичної потужності є незначною, внесені втрати можуть залишатися в межах допустимого енергетичного бюджету, а канал зв’язку продовжуватиме функціонувати без очевидних ознак втручання.

Найбільш уразливими є оптичні муфти, кросові шафи, патч-панелі, розподільчі вузли та інші місця фізичного доступу до волокна. Для відомчих інформаційно-комунікаційних систем це особливо важливо, оскільки кабельні траси можуть проходити через підземні комунікації, технічні колодязі та зовнішні вузли, де постійний фізичний контроль ускладнений.

Одним із важливих напрямів технічного захисту інформації є контроль цілісності оптичного тракту. Для цього широко застосовується оптична рефлектометрія у часовій області. Її принцип базується на введенні в оптичне волокно тестових імпульсів та аналізі відбитого і розсіяного випромінювання. За результатами вимірювання формується рефлектограма, яка дає змогу визначити характер загасання вздовж лінії, виявити неоднорідності, пошкодження, місця з’єднань, надмірні вигини та інші зміни параметрів оптичного тракту.

Для систем спеціального призначення доцільно формувати еталонну рефлектограму після введення лінії в експлуатацію. Подальші вимірювання можуть порівнюватися з еталонним станом, а поява нових неоднорідностей, локального збільшення загасання або зміни характеру відбиття може свідчити як про технічну несправність, так і про стороннє втручання.

Водночас періодичний рефлектометричний контроль не завжди дає змогу своєчасно виявити малопомітне втручання. За незначного відведення оптичної потужності зміни можуть бути співмірними з природними коливаннями параметрів лінії. Тому для критично важливих систем доцільно застосовувати комплексний моніторинг фізичного рівня.

Такий моніторинг може передбачати контроль прийнятої оптичної потужності, загасання, співвідношення сигнал/шум, частоти бітових помилок і параметрів відбиття. Сукупний аналіз цих показників підвищує ймовірність виявлення нетипових змін, що можуть свідчити про стороннє втручання.

Протидія несанкціонованому зніманню інформації з волоконно-оптичних ліній повинна здійснюватися за принципом багаторівневого захисту. Перший

рівень має включати фізичну охорону кабельної інфраструктури, контроль доступу до телекомунікаційних приміщень, оптичних кросів, муфт, розподільчих шаф та інших технологічних точок. Доступ до таких об’єктів доцільно надавати лише визначеному персоналу з обов’язковою реєстрацією виконаних робіт.

Другий рівень повинен включати технічний контроль стану лінії: періодичну або постійну оптичну рефлектометрію, контроль потужності сигналу, моніторинг параметрів обладнання та автоматичне формування повідомлень про відхилення від штатного режиму роботи.

Третім рівнем має бути криптографічний захист інформації. Фізичний захист волоконно-оптичної інфраструктури ускладнює отримання сигналу, однак не може повністю виключити можливість компрометації кабельної мережі. Використання стійкого шифрування забезпечує додатковий рівень захисту, за якого навіть у разі успішного фізичного відгалуження оптичного сигналу отримані дані не повинні бути придатними для безпосереднього використання.

Для відомчих інформаційно-комунікаційних систем особливо важливим є поєднання засобів технічного та криптографічного захисту. У таких мережах доцільно забезпечувати шифрування інформаційних потоків між територіально рознесеними вузлами, взаємну автентифікацію обладнання, контроль цілісності переданих даних, захищене управління мережевими пристроями та суворий контроль фізичного доступу до елементів транспортної інфраструктури.

Таким чином, використання волоконно-оптичних ліній зв’язку саме по собі не гарантує абсолютної конфіденційності інформації. За наявності фізичного доступу до оптичної інфраструктури існує можливість відведення частини сигналу без повного порушення працездатності каналу. Найбільшу небезпеку становлять малопомітні пасивні способи перехоплення.

Ефективний захист волоконно-оптичних ліній у відомчих інформаційно-комунікаційних системах та мережах спеціального призначення повинен ґрунтуватися на поєднанні фізичного захисту кабельних трас, контролю доступу до вузлів мережі, рефлектометричного та параметричного моніторингу, автоматизованого виявлення аномалій і криптографічного захисту інформаційних потоків.

Дідух Л. І.
Бовсуновський В. Ю., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАВАДОСТІЙКИХ КОДІВ ДЛЯ КАНАЛУ ДЕКАМЕТРОВОГО РАДІОЗВ'ЯЗКУ

Переважна більшість систем радіозв’язку використовує відповідні сигнально-кодові конструкції для забезпечення завадостійкості зв’язку в радіоканалі з визначеними властивостями.

Впровадження нових видів сигналів, видів передач в системи радіозв’язку декаметрового діапазону потребує обґрунтування доцільності застосування завадостійких кодів з урахуванням специфіки інформації, яка буде передаватися в каналі радіозв’язку та особливостей його функціонування.

Зазначена проблема може бути вирішена за рахунок розробки методики оцінювання ефективності завадостійких кодів для каналу декаметрового радіозв'язку. яка повинна враховувати такі критерії:

мінімальну кодова відстань, що визначає здатність виявляти та виправляти помилки в радіоканалі;

швидкість кодування, (ефективність використання пропускної спроможності каналу).

ймовірність виникнення помилок (ризик появи невиправлених помилок після декодування).

складність реалізації (обчислювальні витрати, апаратні ресурси та затримка обробки).

Для вирішення зазначеного завдання традиційно використовують ймовірнісний (аналітичний) та геометричний методи, імітаційне моделювання, а також спектральний аналіз. Окреме використання зазначених методів не дозволяє вирішити поставлене завдання повністю та потребує застосування комплексного підходу.

Для подолання зазначеного протиріччя розроблено методику оцінювання ефективності завадостійких кодів для каналу декаметрового радіозв'язку, яка являє сукупність етапів і розрахункових процедур для визначення доцільності застосування коду в конкретному каналі зв'язку як компромісу між коригувальною здатністю, швидкістю та складністю.

Запропонована методика складається з п'яти етапів:

1. Визначення вхідних параметрів і моделі каналу (тип каналу, ймовірність помилки, вид модуляції).

2. Збір та розрахунок структурних характеристик (розмірність, швидкість коду, мінімальна кодова відстань, коригувальна здатність коду).

3. Оцінювання технічних критеріїв (енергетична ефективність, достовірність, частотно-часова швидкість).

4. Оцінювання складності реалізації (апаратні затрати у вентилях програмованої логічної інтегральної схеми, часова затримка декодування).

5. Комплексний порівняльний аналіз (побудова матриць зважених оцінок для остаточного оцінювання ефективності та вибору оптимального коду).

Застосування запропонованої методики забезпечує можливість вибору завадостійкого коду оптимального з точки зору функціонування каналу декаметрового радіозв'язку та особливостей інформації, яка передається у радіоканалі.

Чіпєра В. В.
Поливаний С. В.
Житомирський військовий інститут імені С. П. Корольова

SOFTWARE COGNITIVE RADIO ТА SSDF-АТАКИ: ПРИНЦИПИ РОБОТИ, ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ ЇМ

Нині розвиток бездротових технологій супроводжується дефіцитом доступного радіочастотного спектра. За традиційного підходу, заснованого на жорсткому ліцензуванні, частоти закріплюються за визначеними користувачами, хоча в окремі проміжки часу частина виділеного ресурсу може не використовуватися. Саме цю проблему покликані вирішити технології Cognitive Radio та її програмна еволюція — Software Cognitive Radio.

Cognitive Radio (CR) — це інтелектуальна система бездротового зв'язку, здатна оцінювати стан радіосередовища, навчатися на отриманих даних і автоматично адаптувати робочі параметри, зокрема частоту, потужність, вид модуляції та протокол обміну.

Software Cognitive Radio (SCR) розвиває концепцію CR на базі Software-Defined Radio (SDR). SDR забезпечує програмне керування функціями радіосистеми, тоді як SCR доповнює цю гнучкість засобами аналізу

радіосередовища та адаптивного прийняття рішень. У SCR обробка сигналів, вибір параметрів і переналаштування виконуються переважно програмним забезпеченням, що зменшує залежність функціональності від спеціалізованої апаратної реалізації.

Головна мета SCR полягає у реалізації динамічного доступу до спектра. Система в режимі реального часу шукає тимчасово вільні частоти і використовує їх, не створюючи перешкод користувачам.

Робота SCR ґрунтується на безперервному циклі з трьох послідовних етапів: спостереження за радіосередовищем, аналізу отриманих даних і програмного переналаштування трансивера.

Машинне навчання розширює адаптивні можливості SCR додаючи змогу виявляти закономірності використання частот, ураховувати попередні помилки та поступово оптимізувати параметри роботи для конкретного радіосередовища й умов поширення сигналу.

Сфери застосування SCR охоплюють, військовий зв’язок, управління безпілотними літальними апаратами та інше.

Основними перевагами SCR є максимальна ефективність використання радіочастотного ресурсу, універсальність апаратної платформи та високий рівень автономності системи.

Водночас впровадження SCR ускладнюють апаратні обмеження, високе енергоспоживання, проблема “прихованого вузла” та вразливість до Spectrum Sensing Data Falsification (SSDF).

Безпека циклу залежить від достовірності даних спектрального зондування: якщо вхідні відомості спотворено, система може ухвалити неправильне рішення щодо доступності каналу. Саме цю вразливість використовують атаки SSDF.

SSDF атака спрямована на спотворення процесу кооперативного спектрального зондування, який є основою функціонування CR та SCR.

Суть SSDF-атаки полягає в тому, що зловмисний вузол надсилає іншим вузлам мережі хибні результати спектрального зондування. Мета полягає у спотворенні спільного рішення про наявність або відсутність первинного користувача в частотному каналі. Унаслідок цього система може помилково визнати зайнятий канал вільним або, навпаки, вільний канал — зайнятим.

Дана атака може призвести до:

збільшення ймовірність хибної тривоги, змусивши користувачів відмовлятися від використання вільних частот;

збільшення ймовірність пропуску сигналу первинного користувача, створюючи йому перешкоди;

захоплення зловмисником контроль над окремими частотними ресурсами для власного використання.

У найбільш складних випадках кілька зловмисників можуть координувати свої дії, реалізуючи кооперативну SSDF-атаку.

Успішна SSDF-атака спотворює рішення про стан частотних каналів. Хибне визначення зайнятого каналу як вільного створює ризик перешкод для ліцензованих користувачів, а помилкове визначення вільного каналу як зайнятого знижує ефективність використання спектра. Сукупно ці помилки погіршують якість роботи когнітивної мережі та підривають довіру до кооперативного зондування. У військових і критичних системах наслідком може стати втрата зв’язку або порушення роботи засобів радіоелектронної боротьби.

Для протидії SSDF застосовують кілька взаємодоповнювальних підходів. Репутаційні механізми присвоюють кожному вузлу рейтинг довіри на основі історії його повідомлень і дають змогу не враховувати дані від вузлів із низькою репутацією. Статистичні методи та кластеризація допомагають виявляти аномальні звіти, кворумні правила зменшують вплив окремого зловмисного вузла на спільне рішення, а криптографічні засоби захищають цілісність переданих даних. Перспективним напрямом є застосування машинного навчання для виявлення аномальної поведінки вузлів у реальному часі.

SCR є важливою технологією підвищення ефективності використання радіочастотного спектра в умовах зростання навантаження на бездротові мережі та сучасних конфліктів. Водночас залежність адаптивних рішень від результатів спектрального зондування робить SSDF однією з основних загроз для когнітивних радіосистем. Тому захист має поєднувати репутаційні, статистичні та криптографічні механізми з алгоритмами штучного інтелекту, щоб одночасно перевіряти достовірність даних, виявляти аномалії та зменшувати вплив зловмисних вузлів.

Ткач О. С., слухач
Кудряшов Ю. О.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СПЕЦІАЛЬНОГО РАДІОЗВ’ЯЗКУ ДЕКАМЕТРОВОГО ДІАПАЗОНУ ЗА РАХУНОК ПРОСТОРОВОЇ СЕЛЕКЦІЇ СИГНАЛІВ

Надійність спеціального радіозв’язку декаметрового діапазону має особливе значення за умов, коли прокладання кабельної інфраструктури або використання супутникових каналів ускладнене. Радіохвилі цього діапазону дають змогу організовувати зв’язок на значних відстанях завдяки поширенню земною хвилею та відбиттю від іоносфери. Водночас параметри такого каналу змінюються під впливом стану іоносфери, часу доби, сезону й сонячної активності. Багатопроменеве поширення спричиняє завмирання та частотно-селективні спотворення, а природні й навмисні завади можуть суттєво погіршувати приймання. Тому для забезпечення стійкого зв’язку важливо використовувати методи, які враховують не лише часові й частотні, а й просторові властивості сигналів.

Одним із таких методів є просторова селекція сигналів. Її сутність полягає у використанні відмінностей між корисним сигналом і завадою, що спостерігаються у просторі: напрямку приходу, фазових співвідношень, рівнів і кореляційних властивостей на різних приймальних елементах. На відміну від приймання однією антеною, багатоканальна система надає змогу зіставляти кілька копій електромагнітного поля та формувати результуючий сигнал із підвищеним внеском корисної складової. Просторова селекція є основним методом обробки, а рознесення антен створює фізичну основу для отримання просторово різних спостережень.

Відстань між антенами, їхні діаграми спрямованості, поляризацію, взаємне екранування та характеристики фідерів потрібно враховувати під час проєктування. Величину просторового рознесення доцільно визначати з урахуванням робочої частоти, умов поширення та доступного майданчика, а його ефект оцінювати за взаємною кореляцією сигналів у приймальних каналах. Відмінності між цими сигналами створюють додаткову інформацію для

селекції; якщо ж канали мають подібні характеристики, виграш від рознесення може бути обмеженим. Тому конфігурацію антенної системи слід добирати й перевіряти для характерних напрямків приходу корисного сигналу та завади.

Для перевірки методики пропонується порівняти базовий одноканальний прийом із прийманням на рознесену антенну систему та спільною обробкою її виходів. Моделювання має відображати основні особливості декаметрового каналу: змінність амплітуди, багатопроменевість, можливі часові затримки, доплерівські зсуви, шуми та завади з різними напрямками приходу. Окремі сценарії можуть передбачати одну домінантну заваду, кілька завад, зміну її потужності, а також зміну параметрів каналу в часі. Порівняння конфігурацій за кількістю антен, взаємним рознесенням і характером обробки дасть змогу визначити, за яких умов додаткові приймальні канали створюють практичний виграш.

Основним показником якості доцільно обрати відношення потужності корисного сигналу до сумарної потужності завад і шуму (SINR) на виході системи. Додатковим показником пропонується обрати — доступність каналу зв’язку, тобто частка часу або ймовірність, за якої параметри приймання відповідають установленому критерію працездатності. Числові значення цих показників мають бути отримані за результатами моделювання або експерименту, а не задаватися наперед.

Очікується, що дослідження дасть змогу встановити залежність ефективності просторової селекції від числа антен, їх геометричного розміщення, статистичної незалежності прийнятих компонентів і співвідношення потужностей сигналу та завади. Важливо також оцінити складність реалізації: кількість приймальних трактів, вимоги до синхронізації, обчислювальні витрати й чутливість до похибок калібрування. Ці чинники визначають, чи може обраний алгоритм працювати в реальному часі та зберігати ефективність за змінних умов поширення.

Практичне значення методики полягає у можливості підвищити стійкість приймання без зміни передавальної інфраструктури, використовуючи додаткові просторові спостереження на приймальному пункті. Рознесені антени можуть бути інтегровані з цифровим приймачем, який налаштовує спільну обробку відповідно до поточної завадової обстановки. Водночас реальний виграш залежатиме від умов розміщення антен, характеристик каналу та точності оцінювання. Розроблена й перевірена методика може стати основою для вибору

конфігурації приймальної системи спеціального радіозв’язку декаметрового діапазону та обґрунтування доцільності впровадження просторової селекції у визначених умовах експлуатації.

Vasylenko S. V., Cand. Sc. (Tech.), Senior Research.
Yerokhin V. F., Dr. Sc. (Tech.), Prof.
Institute of Special Communications and Information Protection
of National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”

A COGNITIVE APPROACH TO HIGH-FREQUENCY RADIO LINK ADAPTATION

Limited time-frequency resources, channel non-stationarity, and a complex electromagnetic environment significantly reduce the operational efficiency of modern high-frequency (HF) radio communication systems. Under such conditions, conventional electronic counter-countermeasures, such as space-time filtering or increasing the signal-to-noise ratio (SNR), prove insufficiently effective, necessitating the search for novel solutions, including those based on adaptive cancellation procedures.

At the same time, the challenge arises of adapting modern deterministic protocols under STANAG and MIL-STD specifications, which strictly regulate the sequence and set of operational procedures across time intervals, frequency bandwidths, and modulation and coding schemes of HF radio links.

It is proposed, alongside conventional HF radio channel adaptation methods, to employ a cancellation loop that – by leveraging standard interference libraries and time-adaptive procedures – enables interference parameter determination and replica generation for subsequent cancellation at the receiver input or directly within the demodulation chain. The cancellation processing chain can be implemented by integrating the following components:

an interference parameter measurement and extraction module that determines the time-frequency dynamics of the radio spectrum;

a reference model repository of potential unintentional interference based on ITU-R Recommendations;

a suite of cancellation processing algorithms (Successive Interference Cancellation, Maximum Likelihood detection, adaptive filtering);

a decision selector that, based on MIL-STD and STANAG specifications, defines a constrained solution space regarding allowable signal parameters (modulation and coding scheme, frequency bandwidth, frame size, etc.).

The essence of the proposed approach lies in transitioning from reactive interference management to predictive control based on feature analysis and subsequent interference classification. This enables radical optimization of receiver parameters towards the implementation of time-adaptive cancellation procedures.

Герус О. І., слухач
Прокопович В. Д.
Житомирський військовий інститут імені С. П. Корольова

РОЗРОБКА АНТЕНИ СПРЯМОВАНОЇ ДІЇ ДО РАДІОСТАНЦІЇ HARRIS RF7850M-HH

Сучасні системи радіозв'язку потребують підвищення ефективності використання радіочастотного ресурсу, забезпечення необхідної дальності зв'язку та зменшення впливу зовнішніх електромагнітних завад. Одним із способів підвищення ефективності радіоканалу є застосування антен спрямованої дії, які концентрують електромагнітну енергію в заданому напрямку.

Радіостанція Harris RF-7850M-HH є програмно визначуваною багатодіапазонною портативною радіостанцією, що охоплює частотний діапазон 30–512 МГц. Для її антенного тракту характерний хвильовий опір 50 Ом. Радіостанція підтримує як вузькосмугові, так і широкосмугові режими роботи.

Тому створення сумісної спрямованої антени є актуальним завданням, особливо для випадків, коли необхідно підвищити енергетичну ефективність радіоканалу без збільшення потужності передавача.

Мета роботи — розробити та дослідити конструкцію спрямованої антени, призначеної для роботи з радіостанцією Harris RF-7850M-HH, з оптимізацією її електричних характеристик та узгодження з 50-омним антенно-фідерним трактом.

З огляду на це, антена повинна:

мати вхідний опір, близький до 50 Ом;

забезпечувати прийнятний коефіцієнт стоячої хвилі в заданому робочому піддіапазоні;

забезпечувати необхідну спрямованість;

мати механічну міцність і невелику масу;

бути сумісною з відповідним антенним роз'ємом та фідером;

забезпечувати допустимий рівень втрат у фідерному тракті.

Водночас охоплення всього діапазону 30–512 МГц однією високоефективною вузькосмуговою спрямованою антеною є складним завданням. Тому доцільним є розгляд багатодіапазонної конструкції або окремих антенних рішень для визначених піддіапазонів.

Результатом роботи має стати обґрунтована конструктивна схема спрямованої антени та її електромагнітна модель. Критеріями оцінювання запропонованої конструкції можуть бути:

відповідність 50-омному антенному тракту;

забезпечення заданої ширини робочої смуги;

отримання необхідної спрямованості;

прийнятний коефіцієнт підсилення;

мінімізація втрат у фідері та узгоджувальному пристрої;

відповідність масо-габаритним і механічним вимогам.

Розробка спрямованої антени для Harris RF-7850M-HH є комплексним завданням, у якому необхідно враховувати широкий частотний діапазон радіостанції, 50-омний антенний тракт, вимоги до спрямованості та обмеження портативного застосування.

Найбільш раціональним підходом є визначення конкретного робочого піддіапазону, вибір відповідного типу широкосмугової або вузькосмугової антени, її електромагнітне моделювання та подальша експериментальна перевірка.

Практична цінність роботи полягає у створенні методики вибору та оцінювання антенної системи, яка дозволяє підвищити ефективність радіоканалу за рахунок спрямованого випромінювання, не змінюючи основні параметри самої радіостанції.

Островська – Бугайчук І. М., канд. пед. наук, доц.
Земський В. О., курсант
Житомирський військовий інститут імені С. П. Корольова

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ СПЕЦІАЛЬНОГО ВІЙСЬКОВОГО ЗВ'ЯЗКУ

Бойові дії в Україні довели: що пункти управління та засоби військового зв’язку змушені постійно переміщуватися і розосереджуватися через загрозу їх виявлення та ураження противником, тому вони змушені постійно маневрувати й розосереджуватися. Таким чином системи спеціального зв'язку мають не просто надійно шифрувати дані, а й оперативно розгортатися, змінювати конфігурацію, використовувати резервні канали та швидко відновлювати функціонування після кіберінцидентів або фізичного ураження, особливу загрозу становлять БПЛА противника.

Раніше захист будували за класичною комплексною системою захисту інформації (КСЗІ), яка включала суворий, багатоетапний бюрократично-технічний процес виконуючи встановлений перелік технічних та організаційних правил. У 2025 році підхід оновили: з'явилися механізми авторизації з безпеки, а також базові, галузеві й цільові профілі безпеки. Завдяки цьому вимоги можна визначати індивідуально — з огляду на призначення техніки та оцінку ризиків. Проте на практиці ці норми ще треба адаптувати під рухомі військові станції, де конфігурація апаратури постійно змінюється прямо в польових умовах.

Правове регулювання захисту інформації та кібербезпеки визначається Законами України «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про Державну службу спеціального зв’язку та захисту інформації України» та іншими нормативно-правовими актами.

Важливим кроком стало оновлення статті 8 Закону «Про захист інформації в інформаційно-комунікаційних системах» та прийняття постанови Кабміну від 18 червня 2025 року № 712, якою визначено порядок авторизації та розробки профілів безпеки. Це дозволяє гнучко підходити до кожного комплексу. Для армії такий механізм потрібно розвивати далі, створивши чіткі правила саме для мобільних польових систем з урахуванням фронтових реалій.

Окреме питання — цивільні технології, передусім комерційні термінали супутникового зв'язку. Вони допомагають швидше налагодити обмін даними, проте їх застосування потребує чітких нормативних правил оцінки ризиків та перевірки надійності шифрування за державними стандартами.

Важливим є також забезпечення сумісності з нормативами НАТО. Зокрема, STANAG 4606 стосується SHF військового супутникового зв’язку (MILSATCOM) та EPM waveform для послуг Class B. Тому під час впровадження відповідних технологій необхідно одночасно забезпечувати технічну сумісність із стандартами НАТО та виконання національних вимог щодо захисту інформації.

Отже, головна проблема полягає не у відсутності законів, а в тому, що наявні норми треба пристосувати до швидкого темпу бойових дій. Нові механізми профілів безпеки та авторизації дають для цього всі правові підстави. Створення окремого профілю для мобільних машин зв'язку та легалізація перевірених комерційних рішень допоможуть військовим оперативно розгортати мережі, не порушуючи правил секретності та зберігаючи взаємосумісність зі стандартами НАТО.

Логічним є формування спеціального профілю безпеки для мобільних військових систем, визначення критеріїв використання комерційних технологій та чітке розмежування повноважень суб’єктів кібербезпеки, швидкість розгортання, покращення та відновлення військових систем. Це дозволить поєднати оперативність розгортання і покращення військових систем із належним рівнем захисту інформації та забезпеченням сумісності з відповідними стандартами НАТО.

Мордюк В. І.
Науково-дослідний інститут воєнної розвідки
Мишлевич В. В.
Житомирський військовий інститут імені С. П. Корольова

НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЧАСТОТНОГО ПЛАНУВАННЯ ДЕКАМЕТРОВИХ РАДІОЛІНІЙ

Одним із типових завдань систем радіозв’язку в декаметровому (ДКМ) діапазоні є формування переліку робочих частот, на яких за заданих

просторово-часових умов існує висока ймовірність установлення стійкого радіозв'язку. Актуальність цього завдання зумовлена специфікою поширення радіохвиль у ДКМ-діапазоні, де можливість зв'язку на значних відстанях визначається переважно умовами іоносферного поширення радіохвиль, а характеристики радіоканалу на визначеній частоті істотно змінюються залежно від часу доби, сезону, географічного положення кореспондентів і поточного стану іоносфери.

Традиційне визначення придатної частоти ДКМ-радіоліній лише за прогнозованими межами робочого діапазону або за значенням максимально використовуваної частоти не забезпечує повного врахування реальних умов функціонування цифрової радіолінії.

Проведений аналіз існуючих підходів до визначення робочих частот ДКМ-радіоліній показав, що підвищення обґрунтованості їх вибору потребує комплексного врахування поточного стану іоносфери, особливостей поширення звичайної (О) та незвичайної (Х) магнітоіонних мод, багатопроменевої структури каналу, енергетичних характеристик окремих шляхів поширення та вимог конкретного режиму передавання.

За результатами проведеного дослідження *визначено такі напрями підвищення ефективності частотного планування ДКМ-радіоліній:*

Актуалізація просторово-часового опису іоносфери за доступними оперативними та модельними даними. Доцільним є формування просторово-часового поля електронної концентрації на основі поєднання фонової моделі іоносфери з доступними оперативними даними спостережень.

Тривимірне трасування радіохвиль з окремим урахуванням звичайної (О) та незвичайної (Х) магнітоіонних мод. На відміну від спрощеного подання каналу однією траєкторією або однією магнітоіонною модою, доцільно окремо визначати можливі шляхи поширення О- та Х-мод з урахуванням одно- і багатострибкових траєкторій.

Енергетичне оцінювання каналів поширення радіохвиль окремо для кожної магнітоіонної моди. Для кожної фізично допустимої траєкторії доцільно окремо визначати інтегральне іоносферне поглинання, геометричні втрати, вплив характеристик передавальної та приймальної антен, втрати під час взаємодії із земною поверхнею, рівень прийнятого сигналу, шумову потужність та відношення сигнал/шум.

Модемно-орієнтоване оцінювання придатності та формування множини допустимих робочих частот. Запропоновано оцінювання придатності робочих частот на основі узагальнених характеристик багатопроменевого каналу, сформованих за сукупністю фізично відмінних О- та Х-модових шляхів. Для кожної частоти враховуються енергетичні, часові та доплерівські характеристики шляхів, а також доступна смуга каналу, після чого вони зіставляються з вимогами конкретного режиму передавання.

Оцінювання та формування переліку рекомендованих робочих частот. Для частот, що увійшли до множини допустимих, доцільно виконувати додаткове багатокритеріальне оцінювання з урахуванням запасу за основними параметрами відносно граничних вимог режиму передавання. На основі інтегрального показника придатності формується впорядкований перелік рекомендованих робочих частот.

Таким чином, результатом проведеного дослідження є визначення та обґрунтування взаємопов’язаних напрямів підвищення ефективності частотного планування ДКМ-радіоліній, реалізація яких має забезпечити перехід від вибору частот переважно за умовою існування іоносферної траси та її енергетичним показником до комплексного оцінювання багатопроменевого каналу поширення радіохвиль з окремим урахуванням звичайної (О) та незвичайної (Х) магнітоіонних мод, а також вимог конкретного режиму передавання.

Гнатюк В. О.
Котенко В. М., канд. техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова

АНАЛІЗ ЧАСТОТНО-ЧАСОВОЇ СТРУКТУРИ РАДІОСИГНАЛІВ ПЕРСПЕКТИВНИХ ЗАВАДОЗАХИЩЕНИХ ТА СКРИТИХ СИСТЕМ ЗВ’ЯЗКУ

Розглянуто частотно-часовий аналіз радіосигналів як метод дослідження їхніх параметрів у системах радіозв’язку, визначення інформативних часових, частотних і частотно-часових характеристик сигналів та з’ясування можливостей їх використання для оцінювання впливу радіозавад. Розглянуто застосування короткочасного перетворення Фур’є та спектрограми, а також

особливості вибору тривалості аналізувального вікна. Показано, що поєднання часових і частотних характеристик дає змогу повніше описати сигнал, параметри якого змінюються під час передавання.

Радіочастотний спектр є обмеженим ресурсом, який використовують різні системи радіозв'язку. Одночасна робота багатьох радіозасобів може спричиняти взаємні завади та погіршувати якість приймання інформації. Тому під час дослідження радіосигналів важливо визначати не лише їхні загальні спектральні характеристики, а й зміни параметрів у часі.

Для сигналів, частота, амплітуда або інші характеристики яких змінюються під час передавання, одного аналізу в часовій чи частотній області може бути недостатньо. Частотно-часове представлення дає змогу встановити, у який момент виникають окремі частотні складові та як змінюється їхній розподіл. Це робить його корисним інструментом аналізу сигналів у змінному радіочастотному середовищі.

Одним із поширених методів частотно-часового аналізу є короткочасне перетворення Фур'є (КПФ; англ. Short-Time Fourier Transform, STFT). Під час його застосування сигнал послідовно аналізують у коротких часових вікнах, для кожного з яких визначають частотний склад. Результат часто подають у вигляді спектрограми, де відображено розподіл інтенсивності сигналу за часом і частотою.

Важливою умовою застосування КПФ є правильний вибір тривалості вікна. Коротке вікно дає змогу точніше визначити момент зміни сигналу, проте знижує частотну роздільну здатність. Довше вікно, навпаки, допомагає краще розрізняти близькі частотні складові, але ускладнює визначення швидких змін у часі. Отже, параметри аналізу слід добирати з урахуванням властивостей сигналу та завдання дослідження.

Для опису сигналу доцільно використовувати три групи характеристик. Часові характеристики охоплюють тривалість сигналу, тривалість його окремих елементів та інтервали між ними. Частотні характеристики включають центральну частоту, ширину спектра й рівні спектральних складових. Частотно-часові характеристики описують зміну частоти в часі, тривалість перебування сигналу на певній частотній ділянці та розподіл його енергії.

Такі характеристики дають змогу послідовно описати структуру сигналу та порівнювати її за різних умов приймання. Зокрема, за наявності радіозавад можуть спостерігатися зміни співвідношення сигнал/шум, погіршення

виділення окремих спектральних складових або поява додаткових компонентів у спектрограмі. Водночас самі ці ознаки не доводять наявності конкретної завади: їх потрібно оцінювати разом з іншими параметрами та умовами вимірювання.

Частотно-часовий аналіз також застосовують для дослідження сигналів, параметри яких змінюються за визначеним алгоритмом, наприклад під час перебудови робочої частоти. У таких випадках важливо враховувати послідовність появи частотних складових, тривалість окремих ділянок і характер переходів між ними. Проте результати аналізу залежать від параметрів вимірювального обладнання, рівня шуму та обраного методу оброблення.

Отже, короткочасне перетворення Фур’є та спектрограма є інструментами, що доповнюють традиційний часовий і частотний аналіз. Їх використання дає змогу отримати наочніше уявлення про зміни структури радіосигналу та сформувати набір характеристик для подальшого порівняння й класифікації. Для обґрунтованого оцінювання завадостійкості ці характеристики потрібно доповнювати результатами вимірювання якості приймання.

Встановлено, що основна перевага частотно-часового аналізу радіосигналів полягає в одночасному відображенні частотного складу сигналу та змін цього складу в часі. Короткочасне перетворення Фур’є дає змогу отримувати спектрограми, однак вибір тривалості аналізувального вікна потребує компромісу між часовою та частотною роздільною здатністю. Для опису сигналів доцільно спільно використовувати часові, частотні й частотно-часові характеристики. Такий підхід може бути основою подальшого аналізу сигналів і дослідження їхньої поведінки за наявності радіозавад.

Воронін В. О., курсант
Площик А. С.
Національна академія Державної прикордонної служби України

ІННОВАЦІЙНІ ПІДХОДИ ДО РОЗРОБЛЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМ СПЕЦІАЛЬНОГО РАДІОЗВ’ЯЗКУ В УМОВАХ АКТИВНОГО РАДІОЕЛЕКТРОННОГО СПОСТЕРЕЖЕННЯ

Практика останніх місяців на передовій остаточно довела, що старі армійські настанови зі зв'язку більше не рятують. Якщо раніше радіостанцію намагалися захистити від глушіння, то зараз стоїть куди жорсткіше завдання -

взагалі не дати ворогу зрозуміти, що в секторі хтось вийшов на передачу. Противник повністю автоматизував свій радіоелектронний контроль. На передньому краї та в ближньому тилу розгорнуті десятки SDR-комплексів, які сканують весь УКХ-діапазон цілодобово. Люди там часто взагалі не слухають ефір вухами - усе роблять цифрові спектроаналізатори. Щойно десь на позиції чи в лісосмузі натискають тангенту, на пульті ворожого оператора одразу вискакує спектральний пік. За кілька хвилин по цьому місцю вже летить пакет ствольної артилерії, мінометний залп або черговий дрон-камікадзе.

Найбільше проблем створюють розподілені системи радіопеленгації часових методів. Їм не потрібні громіздкі обертові антени. Достатньо розставити по флангах три або чотири синхронізованих приймачі, які фіксують мікросекундну різницю в приході сигналу. Цьому алгоритму байдуже, чи зашифрований наш канал, чи є там ППРЧ або маскування голосу. Якщо передавач дає випромінювання хоча б одну-дві секунди поспіль, софт автоматично малює на планшеті ворожого артилериста чітку точку перетину гіпербол. Через це малі розвідувальні групи, яким треба передавати координати з глибини або з нейтральної смуги, опиняються у пастці, коли вийдеш на зв'язок - демаскуєш район.

Спроби перекричати цю систему через підсилювачі потужності чи задирання довгих антен на дерева - це вірна загибель. Чим сильніше ми світимо в ефір, тим швидше прилітає відповідь. Треба йти від зворотного: переходити на протоколи з наднизькою ймовірністю виявлення та перехоплення. Головний принцип тут дуже простий: різко скоротити час виходу в ефір, прибрати радіостанцію подалі від людей і перестати ганяти сигнал по передбачуваних прямих лініях.

Насамперед треба повністю вибити з практики живий голос під час передачі бойових донесень. Голосовий зв'язок - це секунди й хвилини випромінювання. Замість цього використовується пакетна стрільба даними. Розвідник сидить в укритті та спокійно набиває на захищеному планшеті короткий звіт за заздалегідь прописаною формою. Вказав координати, тип цілі, кількість броні, час фіксації. Спеціальний софт стискає весь цей масив разом із дрібними графічними мітками в крихітний пакет на пару сотень байт. Далі передавач викидає його в повітря одним коротким імпульсом - десь за 20–40 мілісекунд. Ворожа апаратура такий сплеск просто відсікає. Порогові фільтри

їхніх пеленгаторів налаштовані ігнорувати надкороткі клацання, списуючи їх на грозові розряди, роботу системи запалювання транспорту чи звичайні індустріальні перешкоди.

Наступна критична річ - фізичний рознос антени та самого особового складу. Роками людей вчили тримати радіостанцію на бронежилеті або ставити щоглу прямо над дахом бліндажа. Сьогодні це гарантована братська могила. Навіть якщо ворожий комплекс засіче сигнал, у точці випромінювання не повинно бути жодної живої душі. Для цього ми виносимо передавальний блок на 500–1200 метрів убік. Між укриттям розвідгрупи та випромінювачем розмотується тонкий польовий оптоволоконний дріт. Оптика копійчана за вагою, не гниє у воді, а головне - не випромінює жодного стороннього поля, на відміну від звичайної крученої пари чи коаксіального кабелю. Антену підвішують десь у кроні високого дерева або на зруйнованій споруді на нейтралці. Розвідники працюють із глибокої нори, а сигнал вилітає з порожньої точки. Якщо туди й прилетить снаряд за пеленгом - група спокійно живе далі.

Далі - робота через малогабаритні асинхронні ретранслятори, які більшу частину часу «сплять». Пряма видимість між групою в яру та базовим пунктом буває рідко. Щоб не лупити на повну потужність через пагорби, на маршруті руху скидають автономну коробку-ретранслятор розміром трохи більше пачки від сигарет. Цей блок лежить у траві в режимі мертвої тиші. Він узагалі не світить генератором і нічого не сканує, поки не почує специфічну цифрову преамбулу від своєї групи. Отримавши пакет, ретранслятор робить штучну паузу в кілька хвилин, щоб розірвати часову прив'язку для ворожих аналізаторів, і лише потім перекидає пакет далі. Найкраще скидати цей сигнал не по землі, а вгору - на черговий БпЛА-ретранслятор, який висить на двох тисячах метрів у нашому тилу. З землі цей вертикальний промінь ворожий РЕР засікти практично не здатен.

І нарешті, радикальний спосіб обнулити ворожу радіорозвідку - взагалі піти з радіодіапазону в атмосферну оптику. Лазер не має радіохвилі, тому всі російські комплекси РЕР проти нього просто безпорадні залізяки. Але тут вилазить інший нюанс: дешеві цивільні лазери на 850–940 нм розсіюються в тумані й пилу, і їх чудово видно у звичайні нічники покоління 2+ чи 3.

Щоб закрити цю дірку, потрібно переходити в діапазон SWIR - на довжину хвилі 1550 нм. Фізика тут працює на нас: звичайні кремнієві матриці камер і оптичні трубки до цієї хвилі абсолютно сліпі. Щоб побачити промінь

1550 нм, ворогу потрібні рідкісні та наддорогі охолоджувані камери на основі InGaAs, яких на спостережних пунктах просто немає. Якщо такий випромінювач заховати в глибоку трубку-бленду з чорними ребрами, натягнути стільникову сітку від бліків і тримати потужність на мінімумі, лазерний міст стає повністю невидимим ні для радіоелектронних, ні для оптичних приладів противника.

У підсумку маємо простий висновок: виживати під сучасним РЕР-ом можна лише за рахунок мізків і гнучких алгоритмів, а не зайвих ватів у антені. Поєднавши мілісекундні цифрові посилки, винесення передавачів на оптичному дроті, приховані ретранслятори та лазерний зв'язок на 1550 нм, ми отримуємо реальну живучість зв'язку. Це дає можливість розвідці вчасно скидати координати на артилерію та виходити з завдань живими.

Дубовський Ю. В.
Сторчаєва А. С.
Карамушка М. І.
Василишин В. І., д-р техн. наук, проф.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба

КОНЦЕПЦІЯ РОЙОВОЇ КОГНІТИВНОЇ РАДІОМЕРЕЖІ З ПРОСТОРОВО-АДАПТИВНИМ ФОРМУВАННЯМ ПРОМЕНЯ ДЛЯ ПОВІТРЯНОГО ЕШЕЛОНУ ТАКТИЧНОГО ЗВ’ЯЗКУ В УМОВАХ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ

Досвід бойових дій під час відсічі збройної агресії рф проти України свідчить, що радіоелектронна боротьба (РЕБ) є одним із визначальних чинників ведення бойових дій тактичного рівня. Радіоелектронне подавлення каналів управління, передачі даних і навігації безпілотних літальних апаратів (БпЛА) спричиняє порушення зв’язку з повітряними ретрансляторами та втрату зв’язності повітряного ешелону системи зв’язку.

Наявні засоби тактичного радіозв’язку з технологією мобільних самоорганізованих мереж (MANET), наприклад радіостанції з формою сигналу ANW2C (до 30 абонентів, швидкість від 85 кбіт/с до 2,36 Мбіт/с у смузі 1,2 МГц), використовують всеспрямовані антени, а їх завадозахищеність забезпечується переважно частотно-часовими методами – псевдовипадковим

перебудуванням робочої частоти та завадостійким кодуванням. В умовах загороджувальних завад, що перекривають усю робочу смугу, ефективність цих методів суттєво знижується, а завада з будь-якого напрямку приймається з тим самим коефіцієнтом підсилення, що й корисний сигнал. При цьому не використовується просторовий ресурс – відмінність напрямків приходу корисних сигналів і завад.

Отже, наукове завдання полягає в обґрунтуванні способу підвищення завадостійкості повітряного ешелону зв’язку за рахунок просторової селекції сигналів, причому не лише на окремому вузлі, а в масштабі угруповання БпЛА-ретрансляторів (рою).

Пропонується концепція ройової когнітивної радіомережі, у якій кожен БпЛА-ретранслятор оснащується цифровою антенною решіткою з N елементів, кожен з яких має власний приймально-передавальний тракт, а рій розглядається як сукупність просторово рознесених решіток, що обмінюються інформацією про радіоелектронну обстановку. Розміщення на борту БпЛА решітки з міжелементною відстанню близько половини довжини хвилі можливе лише в дециметровому та сантиметровому діапазонах хвиль, тому концепція орієнтована саме на ці діапазони. Вектор сигналів на виходах елементів решітки має вигляд

$$\mathbf{x}(t) = \mathbf{a}(\varepsilon_0, \varphi_0)s(t) + \mathbf{a}(\varepsilon_1, \varphi_1)j_1(t) + \ldots + \mathbf{a}(\varepsilon_K, \varphi_K)j_K(t) + \mathbf{n}(t), \qquad (1)$$

де $s(t)$ – корисний сигнал; $j_k(t)$ – сигнал k-ї завади; K – кількість джерел завад; $\mathbf{n}(t)$ – вектор власних шумів; $\mathbf{a}(\varepsilon, \varphi)$ – вектор просторової характеристики решітки для напрямку з кутом місця ε та азимутом φ, n-й елемент якого

$$a_n(\varepsilon, \varphi) = \exp[j(2\pi/\lambda)(x_n \cos\varepsilon \cos\varphi + y_n \cos\varepsilon \sin\varphi + z_n \sin\varepsilon)], \qquad (2)$$

де x_n, y_n, z_n – координати n-го елемента; λ – довжина хвилі. Урахування кута місця принципово важливе для повітряних вузлів, оскільки кореспонденти, наземні термінали та засоби РЕБ розташовані на різних висотах.

Цифрове діаграмоутворення (Beamforming) полягає у ваговому підсумовуванні сигналів елементів решітки

$$y(t) = \mathbf{w}^{\mathrm{H}}\mathbf{x}(t), \qquad (3)$$

де $\mathbf{w}$ – вектор вагових коефіцієнтів; H – ермітове спряження. За критерієм мінімуму потужності завад і шумів на виході за незмінного коефіцієнта підсилення в напрямку кореспондента оптимальний вектор має вигляд

$$\mathbf{w} = \mathbf{R}^{-1}\mathbf{a}_0 / (\mathbf{a}_0^{\mathrm{H}}\mathbf{R}^{-1}\mathbf{a}_0), \qquad (4)$$

де $\mathbf{R}$ – кореляційна матриця завад і шумів; $\mathbf{a}_0 = \mathbf{a}(\varepsilon_0, \varphi_0)$. Рішення (4) формує нулі діаграми спрямованості в напрямках джерел завад (Null-steering), зберігаючи головний пелюсток у напрямку кореспондента. Решітка з N елементів здатна сформувати нулі не більше ніж для $N - 1$ незалежних джерел завад, а завада, що потрапляє в головний пелюсток, просторовою обробкою не подавляється. Ці обмеження окремого вузла компенсуються на рівні рою, як показано нижче.

Широкосмугові завади, багатопроменеве поширення радіохвиль і маневрування носія знижують ефективність суто просторової обробки, оскільки фазові зсуви між елементами залежать від частоти, а кутові координати джерел змінюються в часі. Тому пропонується просторово-часова обробка сигналів: до кожного з N елементів підключається лінія затримки з M відводами, а оптимальний вектор вагових коефіцієнтів розмірністю NM визначається як

$$\mathbf{w}_{\text{пч}} = \mathbf{R}_{\text{пч}}^{-1}\mathbf{v} \,/\, (\mathbf{v}^{\text{H}}\mathbf{R}_{\text{пч}}^{-1}\mathbf{v}), \quad \mathbf{v} = \mathbf{b} \otimes \mathbf{a}(\varepsilon_0, \varphi_0), \tag{5}$$

де $\mathbf{R}_{\text{пч}}$ – просторово-часова кореляційна матриця розміром $NM \times NM$; $\mathbf{b}$ – часовий вектор, що відповідає частоті корисного сигналу; $\otimes$ – добуток Кронекера. Для оцінювання $\mathbf{R}_{\text{пч}}$ з втратами не більше 3 дБ потрібно близько $2NM$ незалежних вибірок, що в умовах динамічної зміни радіоелектронної обстановки потребує неприйнятно тривалого часу накопичення. Подолання цього обмеження покладається на бортовий модуль штучного інтелекту (ШІ), який класифікує завади за видом (шумові загороджувальні, прицільні, імпульсні, з перебудуванням частоти), відбирає навчальні вибірки, вільні від корисного сигналу, прогнозує зміну кутових координат завад з урахуванням маневру БпЛА за даними інерціальної навігаційної системи та обирає кількість відводів M залежно від ширини спектра завад. Отже, ШІ не замінює класичну обробку (5), а забезпечує її адаптацію до динамічної зміни радіоелектронної обстановки.

Коректна робота просторової обробки потребує виконання двох технічних умов. Перша – урахування взаємного впливу елементів решітки: під час керування променем змінюється вхідний опір кожного елемента, що призводить до втрат потужності, перевантаження підсилювачів і зменшення глибини нулів. Тому вагові коефіцієнти доцільно обчислювати з урахуванням виміряної матриці розсіювання решітки, а в передавальних трактах застосовувати автоматичне узгодження вихідного каскаду з антенним елементом для поточного режиму роботи. Друга – часова синхронізація вузлів,

яка в сучасних MANET здійснюється переважно за сигналами супутникової навігації. Для її збереження доцільно застосовувати навігаційні антени з керованою діаграмою прийому (англ. Controlled Reception Pattern Antenna), які за тим самим принципом формують нулі в напрямках джерел навігаційних завад.

Якщо засоби динамічного доступу до спектра не знаходять вільної від завад ділянки, застосовується розширення спектра корисного сигналу псевдовипадковою послідовністю з виграшем обробки $G_p = W_s/R_b$, де W_s – ширина спектра розширеного сигналу, R_b – інформаційна швидкість. Сигнал зі спектральною густиною потужності нижче рівня шумів має нижчу ймовірність виявлення засобами радіорозвідки, а під час стиснення спектра на приймальній стороні відношення потужності завади до потужності сигналу зменшується в G_p разів. Допустиме відношення завада/сигнал на вході приймача (у децибелах) з урахуванням просторової обробки становить

$$(J/S)_{\text{доп}} = G_p + G_{\text{под}} - (E_b/N_0)_{\min} - L, \qquad (6)$$

де $G_{\text{под}}$ – глибина подавлення завад просторово-часовою обробкою; $(E_b/N_0)_{\min}$ – мінімальне відношення енергії біта до спектральної густини шуму для заданої ймовірності помилки; L – втрати в системі. З (6) випливає, що просторова і спектральна складові захисту додаються. Різниця між допустимим і фактичним відношенням завада/сигнал є запасом завадостійкості лінії, за яким для кожної лінії окремо обирається сигнально-кодова конструкція: за великого запасу – високошвидкісна, за малого – зі збільшеною базою сигналу та стійкішою модуляцією.

Основу концепції становить використання результатів просторової обробки на рівні рою. Вузли обмінюються пеленгами завад і значеннями запасу завадостійкості своїх ліній, що дозволяє визначати місцеположення засобів РЕБ методом тріангуляції; формувати маршрути передачі через лінії з найбільшим запасом завадостійкості, виключаючи з маршрутів вузли, на які діє більше джерел завад, ніж здатна подавити їхня решітка; у разі втрати вузла перераховувати топологію мережі та параметри променів; за наявності такої можливості коригувати взаємне розташування вузлів так, щоб кутова відстань між напрямками на кореспондента і на джерело завад перевищувала ширину головного пелюстка.

Новизна запропонованого підходу полягає в тому, що на відміну від відомих рішень, у яких просторова обробка виконується автономно кожною

радіостанцією, її результати (пеленги завад, глибина подавлення, запас завадостійкості лінії) використовуються на мережевому рівні для маршрутизації та керування взаємним розташуванням вузлів, тобто просторовий ресурс розподіляється в масштабі угруповання БпЛА.

Запропонована концепція створює основу для побудови завадостійкого повітряного ешелону зв'язку тактичної авіації та угруповань БпЛА в умовах радіоелектронного подавлення. Кількісне оцінювання ефективності концепції потребує імітаційного моделювання з урахуванням реальних діаграм спрямованості решіток, маневру БпЛА та сценаріїв застосування засобів РЕБ. Перспективними напрямами подальших досліджень є розроблення алгоритмів ШІ для оцінювання просторово-часових кореляційних матриць за обмеженої кількості вибірок, оцінка обмежень за масою, енергоспоживанням і обчислювальними ресурсами бортових решіток, а також забезпечення взаємодії ройової мережі з наявними MANET через мережеві шлюзи.

Стечишин С. В.
Городиський Р. О.
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького

ІНТЕГРАЦІЯ МІКРОПРОЦЕСОРНИХ МОДУЛІВ ТА ЗАСОБІВ БЕЗДРОТОВОГО ЗВ'ЯЗКУ В СИСТЕМАХ ДИСТАНЦІЙНОГО МОНІТОРИНГУ

Забезпечення охорони державного кордону потребує безперервного контролю значних за протяжністю ділянок, значна частина яких є важкодоступною та віддаленою від пунктів управління. Постійне перебування особового складу на всіх ділянках неможливе, тому актуальним є застосування автономних технічних систем, здатних самостійно збирати інформацію про обстановку та передавати її на віддалений пункт моніторингу. Ефективність таких систем визначається не лише характеристиками окремих датчиків, а насамперед тим, наскільки узгоджено поєднано засоби збору, обробки та передавання даних.

Роль мікропроцесорних засобів. Основою сучасних систем дистанційного моніторингу є мікропроцесорні пристрої (мікроконтролери), які виконують

первинну обробку сигналів датчиків, фільтрацію хибних спрацювань, формування службових повідомлень і керування каналом зв’язку. Первинна обробка безпосередньо на об’єкті дозволяє суттєво зменшити обсяг даних, що передаються, і тим самим знизити навантаження на радіоканал та енергоспоживання вузла. Це особливо важливо для автономних пристроїв, що живляться від акумуляторів чи малогабаритних сонячних панелей.

Модульна архітектура передбачає поділ системи на функціонально завершені блоки: сенсорний модуль, модуль обробки на базі мінроконтролера, модуль зв’язку, модуль живлення та пункт моніторингу. Уніфіковані інтерфейси між модулями дають змогу замінювати чи нарощувати їх без перероблення всієї системи, наприклад, додавати нові типи датчиків (сейсмічні, інфрачервоні, акустичні) або змінювати тип каналу зв’язку залежно від умов місцевості. Такий підхід спрощує обслуговування, ремонт і масштабування системи на різні за протяжністю ділянки.

Інтеграція модуля зв’язку з мікропроцесорним вузлом є ключовим етапом побудови системи. Для віддалених ділянок використовують радіоканали малої потужності з великою дальністю дії (зокрема технології класу LoRa), стільникові мережі та, за потреби, супутникові канали. Вибір засобу визначається дальністю зв’язку, пропускною здатністю, енергоспоживанням і стійкістю до перешкод. Через невеликі обсяги службових повідомлень (стан вузла, факт спрацювання, координатна прив’язка) вимоги до пропускної здатності є помірними, тоді як надійність доставки та своєчасність повідомлення залишаються пріоритетними.

Дані системи охорони кордону мають підвищену чутливість, тому канал зв’язку має бути захищений від перехоплення, підміни та несанкціонованого втручання. З цією метою доцільно застосовувати шифрування повідомлень, автентифікацію вузлів, контроль цілісності даних і періодичну перевірку працездатності каналу. Також необхідно враховувати можливість навмисного радіоелектронного впливу на канал, а отже, передбачати резервні канали та режими накопичення даних у пам’яті вузла до відновлення зв’язку.

Розглянутий підхід може бути покладений в основу системи дистанційного моніторингу ділянок державного кордону, у якій розподілені вузли на основі мікроконтролерів формують мережу, що передає інформацію про події на пункт управління в режимі, наближеному до реального часу.

Модульність дозволяє адаптувати склад системи до рельєфу, кліматичних умов і рівня загроз на конкретній ділянці.

Інтеграція мікропроцесорних модулів із засобами бездротового зв'язку створює технологічну основу для побудови гнучких, масштабованих та енергоефективних систем дистанційного моніторингу. Застосування модульної архітектури, алгоритмів первинної обробки даних і захищених каналів передавання інформації сприяє підвищенню автономності, надійності та стійкості таких систем до зовнішніх впливів. Використання зазначених технічних рішень дозволяє підвищити ефективність контролю віддалених і важкодоступних ділянок державного кордону та забезпечити своєчасне надходження інформації про зміни обстановки до пунктів управління.

Нікітченко І. В.
Кудряшов Ю. О.
Житомирський військовий інститут імені С. П. Корольова

ФОРМУВАННЯ ІНТЕГРАЛЬНОГО КРИТЕРІЮ ВИБОРУ РАЦІОНАЛЬНОГО РЕЖИМУ РОБОТИ СПЕЦІАЛЬНОЇ РАДІОЛІНІЇ ДЕКАМЕТРОВОГО ДІАПАЗОНУ

Планування режиму роботи спеціальної радіолінії декаметрового діапазону потребує одночасного врахування кількох вимог: завадозахищеності, безпеки та пропускної здатності. Ці характеристики залежать від параметрів передавання, що налаштовуються в радіостанції, та вибраного режиму її роботи. Зміна параметрів може по-різному впливати на кожну характеристику, тому поліпшення одного показника не обов'язково забезпечує прийнятний рівень інших. Це зумовлює необхідність розглядати вибір режиму як багатокритеріальну задачу.

На попередньому етапі дослідження сформовано часткові функції штрафу, що описують завадозахищеність, пропускну здатність і безпеку радіолінії залежно від керованих параметрів сигналу. Наступним етапом є розроблення способу об'єднання цих часткових оцінок для порівняння допустимих режимів роботи радіостанції.

Мета дослідження — сформувати методичний підхід до вибору раціонального режиму роботи спеціальної радіолінії декаметрового діапазону

на основі спільного оцінювання часткових критеріїв з урахуванням їхньої відносної важливості.

Для досягнення мети передбачається:

узгодити шкали та напрям часткових функцій;

використати вагові коефіцієнти критеріїв, визначені на попередньому етапі дослідження за результатами експертного оцінювання;

дослідити можливість застосування нелінійної згортки критеріїв, зокрема згортки Вороніна;

сформувати алгоритм розрахунку узагальненої оцінки для множини допустимих режимів.

Окрему увагу планується приділити перевірці отриманого підходу на розрахункових прикладах і аналізу впливу зміни пріоритетів на вибір режиму.

Вагові коефіцієнти мають відображати відносну значущість завадозахищеності, пропускної здатності та безпеки в узагальненій оцінці. Для їх визначення використовуються результати експертного оцінювання, узагальнені методом аналізу ієрархій Сааті, узгодженість експертних суджень оцінюється за відповідним показником конкордації Кендалла. Передбачається, що застосування цих ваг дасть змогу враховувати пріоритети критеріїв під час порівняння різних режимів роботи радіостанції.

Очікуваним результатом дослідження є методичний підхід, який дасть змогу для кожного допустимого режиму формувати узагальнену оцінку на основі часткових критеріїв і вагових коефіцієнтів. Перевірка підходу має показати, як вибір раціонального режиму залежить від налаштувань радіостанції, значень часткових оцінок і пріоритетів критеріїв. Отримані результати можуть стати основою для подальшого створення програмного засобу підтримки прийняття рішень.

Отже, оскільки завадозахищеність, безпека та пропускна здатність залежать від налаштувань радіостанції, вибір режиму потребує комплексного врахування цих характеристик. Запланований підхід до їх згортання з урахуванням вагових коефіцієнтів має дати змогу порівнювати допустимі режими та обирати раціональний відповідно до пріоритетів конкретного завдання.

Кашпур І. Р.
Самонюк О. В.
Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА АНАЛІЗУ ЕНЕРГЕТИЧНИХ ХАРАКТЕРИСТИК АНТЕННО-ФІДЕРНИХ ПРИСТРОЇВ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ КОРОТКОХВИЛЬОВОГО ДІАПАЗОНУ

Актуальність теми. У сучасних умовах збройних конфліктів забезпечення безперервного та стійкого управління підрозділами тактичної ланки є критично важливим завданням. Зважаючи на вразливість супутникових систем зв’язку та систем УКХ-діапазону до засобів радіоелектронної боротьби (РЕБ), короткохвильовий (КХ) радіозв'язок (3–30 МГц).

Постановка проблеми. Геометричні розміри антенно-фідерних систем, якими комплектуються переносні та мобільні радіостанції тактичної ланки управління, комплектуються геометрично скороченими антенно-фідерними системами. Це зумовлює зниження коефіцієнта корисної дії (ККД), складність узгодження з вихідним каскадом передавача. Відповідно, виникає потреба в комплексній методиці аналізу енергетичних характеристик АФП, яка б враховувала як електродинамічні параметри самих антенно-фідерних систем.

Мета роботи. Розробка комплексної методики оцінки та аналізу енергетичних характеристик антенно-фідерних пристроїв КХ-діапазону для оптимізації радіоліній тактичної ланки управління в умовах впливу дестабілізуючих факторів.

Основний зміст методики

Запропонована методика базується на системному підході та складається з трьох взаємопов'язаних етапів:

1. Електродинамічне моделювання АФП. На першому етапі здійснюється побудова математичної моделі антени за допомогою чисельних методів (наприклад, методу моментів – МоМ). Аналізу підлягають такі первинні параметри:

Вхідний імпеданс антени в заданому діапазоні частот.

Коефіцієнт спрямованої дії (КСД).

Діаграма спрямованості у вертикальній та горизонтальній площинах (особливо для зенітного випромінювання NVIS, де максимум випромінювання має бути спрямований під кутами 70–90 градусів до горизонту).

2. Розрахунок енергетичних характеристик, що визначають дальність та якість зв'язку:

Коефіцієнт стоячої хвилі за напругою (КСХН): Визначає ступінь узгодження антени з фідером та передавачем. Аналізується ефективність роботи автоматичних антенних тюнерів.

Коефіцієнт корисної дії (ККД): Розраховується як відношення опору випромінювання до суми опору випромінювання та опору втрат (враховуючи втрати в провідниках антени та пристроях узгодження).

Еквівалентна ізотропно-випромінювана потужність (ЕІВП) (англ. *EIRP — Equivalent Isotropically Radiated Power*) — це потужність, яку повинна була б випромінювати ідеальна антена (яка світить однаково в усі сторони), щоб створити у приймача такий самий рівень сигналу, який створює ваша реальна антена у напрямку свого найкращого випромінювання.

$$EIRP = P_{tx} - L_c + G_a$$

Де:

- P_{tx} — вихідна потужність самого передавача (радіостанції).
- L_c — втрати енергії в кабелі (фідері), роз'ємах та тюнері (чим довший кабель, тим більше втрат).
- G_a — коефіцієнт підсилення антени відносно ізотропної (в дБі).

Рис. 1

3. Експериментальна верифікація та оптимізація. Теоретичні розрахунки підтверджуються польовими вимірюваннями за допомогою портативних векторних аналізаторів кіл (VNA). Вимірюється реальний КСХН та комплексний опір при налаштування. На основі розбіжностей між моделлю та експериментом здійснюється коригування схем узгодження (вибір оптимальної топології LC-ланок).

Висновки

Запропонована методика аналізу дозволяє з високою точністю прогнозувати реальні енергетичні характеристики антенно-фідерних пристроїв КХ-діапазону, що використовуються в тактичній ланці управління.

Встановлено, що ключовим резервом підвищення енергетичної ефективності електрично малих АФП є не стільки збільшення вихідної потужності передавача, скільки мінімізація втрат в АФС.

Практичне застосування даної методики дозволяє підвищити стійкість та дальність радіозв'язку та забезпечити надійне управління підрозділами.

ЗМІСТ

Вітальне слово начальника Житомирського військового інституту імені С. П. Корольова доктора історичних наук, професора **Слюсаренка Андрія Віталійовича**…… 3

СЕКЦІЯ 1. Застосування безпілотних систем Силами оборони України 4

Зубелевич Д. І., Охріменко Д. В. Стійкість моделей комп'ютерного зору автономних безпілотних систем до цілеспрямованих збурень зображень та фізичних маскувальних візерунків…… 4

Раєвський О. В., Вигівська О. В. Роботизація бронетехніки радянського походження як напрям збереження особового складу (на прикладі модернізації БРДМ-2)…… 9

Зиков В. Г., Черняхівський І. В. Розвиток і перспективи застосування безпілотних систем у сучасному військовому мистецтві…….. 12

Вінник В. В., Москалик С. В. Аналіз комплексного застосування безпілотних систем…… 15

Добровінський В. П., Приймачук О. В. Проблеми мотивації та добору студентів до навчання за програмою підготовки офіцерів запасу високотехнологічних спеціальностей……... 17

Бондаренко О. О., Чередніченко Є. В., Давлетов А. Р. Вплив якості відновлення зображення в умовах активних шумових завад на ефективність застосування ударних і розвідувальних безпілотних комплексів…… 20

Омельчук О. В. Шляхи вирішення питання збільшення запасу ходу безпілотних наземних комплексів…… 23

Колодницький В. В., Михайловський В. П. Обґрунтування практичної та теоретичної складових підготовки фахівців безпілотних систем…… 26

Лиходєєв О. С., Георгієв Ю. В., Василенко Р. В. Розвиток бортового комплексу безпілотних літальних апаратів військового призначення та перспективні вимоги до нього…… 28

Мошаренков В. В., Мошаренкова Т. В., Рогуля О. В. Застосування безпілотних систем: аналіз досвіду та організаційні виклики…… 30

Коваленко І. О., Заіченко А. В., Мошаренков В. В. Застосування гібридної моделі штучного інтелекту для аналізу відеопотоку безпілотних літальних апаратів у реальному часі…… 32

Піонтківський П. М. Багатовимірна модель оцінювання автономності безпілотних систем в умовах збройного конфлікту…… 36
Дзіковський А. П. Автономні функції російських безпілотних літальних апаратів…….. 41
Іщенко Д. А., Стрінада В. В. Аналіз особливостей робіт із військової стандартизації в аспекті наукової підтримки набуття спроможностей у сфері військової техніки з високою динамікою розвитку……... 42
Мірошніченко С. І., Пількевич І. А. Забезпечення запуску безпілотних літальних апаратів з водної поверхні…….. 47
Дзюбчук Р. В., Перфілов А. Ю. Система відбору й підготовки операторів безпілотних систем: психологічний аспект…….. 52
Осадчук Р. М., Коровайний Є. О. Методологія оцінювання ймовірності виявлення та розпізнавання військової техніки на знімках із безпілотних літальних апаратів……. 56
Салій Д. В., Бедрій Н. А. Перспективи застосування технологій штучного інтелекту в безпілотних системах…… 58
Солошенко Ю. В., Куровська Т. Ю. Архітектурні принципи та перспективи інтеграції технологій штучного інтелекту в безпілотні авіаційні комплекси Сил оборони України…… 60
Чуканов А. І., Щерблюк В. А. Перспективи застосування технологій штучного інтелекту для підвищення автономності безпілотних систем Сил оборони України……. 63
Казєв О. В., Курилін Я. В. Наземні роботизовані комплекси як засіб зниження ризиків для особового складу під час логістичного забезпечення та евакуації……... 66
Петров В. М., Афанасьєв В. В., Крук Б. М., Кудрявцев А. Ф., Марченко О. М. Трансформація форм та способів застосування безпілотних авіаційних систем на основі впровадження бойового досвіду…. 71
Лазакович М. С., Лех А. І. Застосування безпілотних літальних апарататів під час виконання завдань хімічного, біологічного, радіологічного та ядерного захисту…….. 74
Рибчинський Д. А. Метод багатокрокової оптимізації маршруту розвідувальних безпілотних літальних апаратів в умовах просторово-часових загроз…….. 77
Краснодубець А. І. Удосконалення способів застосування безпілотних систем на основі інтеграції бойового досвіду, технологій штучного інтелекту та адаптивного захисту від безпілотних літальних апаратів…. 79

Гаєвський С. О., Піонтківський П. М. Нові підходи до об'єднаної підготовки фахівців безпілотних систем на основі бойового досвіду….. 81
Гаврилюк В. В., Селезенєв А. П. Застосування наземних роботизованих комплексів спільно із безпілотними літальними апаратами для евакуації поранених в умовах вогневого впливу противника…….. 85
Павленко В. О., Сокальський І. М. Сучасні технології у формуванні компетентностей здобувачів вищої освіти з основ національного спротиву… 88
Петраш С. В., Зелінський О. В., Коваль М. В. Пропозиції щодо усунення неоднозначності виміру координат наземних об'єктів у безпілотних літальних апаратах…… 90
Горбач В. Я., Горбач Т. П. Вплив геометричних характеристик об'єкта на вибір оптимального кута спостереження з безпілотного літального апарата… 92
Оверчук С. П., Пількевич І. А. Підвищення точності навігації безпілотних літальних апаратів в умовах радіоелектронного подавлення шляхом нейромережевої компенсації похибок…… 94
Соломатін Д. О., Седляр А. А. Аналіз особливостей застосування та можливостей ударних FPV-дронів і мультикоптерів зі скидами…… 96
Луцевят О. І., Попков С. Б. Трансформація форм і способів бойового застосування ударних безпілотних літальних апаратів відповідно до еволюції їх елементної бази……... 101
Засядько А. А., Стригун В. В., Барвінок Р. Д., Швець С. І. Тестування антен із керованою діаграмою спрямованості за допомогою лабораторних випробувальних стендів……. 102
Винту А. О., Волощук Т. Ю. Оптимізація структури та технологічного оснащення рухомого комплексу обслуговування та ремонту безпілотних авіаційних комплексів…….. 104
Майборода Ю. М. Трансформація безпілотних систем Сил оборони України: інтеграція штучного інтелекту та перехід до автономності…… 106
Стрінада В. В., Іщенко Д. А. Оцінювання ефективності бойового застосування підрозділів безпілотних наземних комплексів……. 109
Наумчак Л. М. Визначення координат наземних об'єктів за даними безпілотного літального апарата І класу в умовах подавлення GNSS….. 112
Демидюк М. О., Кухарчук І. В. Реактивні безпілотні літальні апарати-перехоплювачі як засіб протидії ворожим реактивним повітряним цілям…. 115
Мукосій Д. В., Лях І. Ю., Новічков В. О. Ключова роль засобів автоматизації в сучасних збройних конфліктах…….. 117

Trokhymenko V. O., Malakhov O. V. Specific of Confined Flow Departure from the Body with Contour Break…… 118
Зуєв Т. Є., Котвицький М. М. Технології штучного інтелекту в безпілотних системах…….. 120
Сисоєнко С. В., Аркушенко П. Л., Кузьміч О. Є. Підвищення надійності навігаційно-керуючої системи безпілотних літальних апаратів шляхом комплексного контролю сенсорних даних…….. 123
Кузнецов В. О., Засядько А. А., Орлов С. В. Порівняння нових військових стандартів лабораторних випробувань безпілотних авіаційних комплексів щодо впливу механічних факторів…….. 126
Засядько А. А., Юла О. В., Рижков О. В., Братко В. В. Аналіз методів тестування антен із керованою діаграмою спрямованості……... 128
Засядько А. А., Цуря Е. І., Гусак М. Ю., Кот О. Б. Особливості використання антен із керованою діаграмою спрямованості для геодезичної прив'язки радіолокаційного поста……... 130
Верголяс О. О. Відеоконтент із безпілотних літальних апаратів у відкритому інформаційному просторі: комунікаційний ефект, канали демаскування та відбір перед оприлюдненням…… 132
Пулеко І. В., Бородуліна М. В. Технології доповненої реальності під час вивчення елементів безпілотних авіаційних систем……. 136
Данилюк А. М. Застосування наземних роботизованих комплексів та безпілотних авіаційних систем у завданнях медичної евакуації, порятунку цивільного населення та вивезення тіл загиблих для подальшого обміну……. 138
Говтва Д. С. Застосування безпілотних авіаційних комплексів у завданнях дистанційного мінування та розмінування місцевості……. 140
Виговська О. О. Повітряне десантування наземних роботизованих комплексів безпілотними літальними апаратами…… 142
Марич О. В. Обґрунтування способів застосування роти безекіпажних наземних комплексів у складі загальновійськової бригади…… 144
Староконь Є. Г. Лідерство та командна взаємодія в екіпажі безпілотного літального апарата……... 146
Омельчук І. А., Пількевич І. А. Аналіз переваг сервоприводів електромагнітної системи…… 148
Музичак А. З., Чернов Є. В. Функції штучного інтелекту в системах керування розвідувальними безпілотними наземними комплексами…… 153

Островська – Бугайчук І. М., Міскарян Д. С. Міжнародно-правові аспекти застосування безпілотних систем у сучасних збройних конфліктах……. 157
Островська – Бугайчук І. М., Пензюр К. В. Правові аспекти застосування автономних безпілотних систем та технологій штучного інтелекту у військовій сфері…….. 159
Островська – Бугайчук І. М., Стецюк М. Є. Аналіз правових норм щодо регулювання застосування автономних безпілотних систем та технологій штучного інтелекту у військовій діяльності: сучасний стан та перспективи розвитку…… 162
Хмелевський С. І., Большакова І. М. Нечіткі моделі оцінювання в умовах невизначеності: автономність та інтелектуальні технології в безпілотних системах……. 164
Токар А. М., Попик В. І. Каскадний осьовий імпелерний рушій з ефектом Вентурі для компактних електричних безпілотних авіаційних комплексів……... 168
Конечний М. Д. Застосування імпедансних антен у безпілотних системах Сил оборони України……. 172
Жук І. С. Досвід застосування та напрями вдосконалення безпілотних систем у сучасних бойових діях…… 174
Островська – Бугайчук І. М., Кобилянський Н. О. Правове регулювання застосування штучного інтелекту в системах військового призначення: виклик та перспективи…… 176
Островська – Бугайчук І. М., Федоришена О. В. Міжнародно-правові обмеження застосування безпілотних систем для дистанційного мінування територій……... 178
Козмуляк О. А., Васильєв В. П. Впровадження та використання інтерактивних карт під час виконання бойових завдань……. 180
Колотуша Я. В. Перспективи розвитку автономних безпілотних систем на основі технологій штучного інтелекту…… 181
Бубнов Т. Ю., Гаєвський С. О. Досвід застосування наземних роботизованих комплексів у наступальній операції та напрями його впровадження в освітній процес…… 185
Голдобін С. М., Ленський М. М. Методи навігації та оцінювання прохідності наземних роботизованих комплексів в урбанізованій місцевості…… 187

Березовський А. І., Сухар В. В., Махнюк О. В. Шляхи покращення експлуатації наземних логістичних роботизованих комплексів з урахуванням бойового досвіду застосування Силами оборони України.. 192
Майданюк В. А., Вознюк В. В. Еволюція застосування наземних роботизованих комплексів у російсько – українській війні…… 193
Маковський В. Ю. Автономність та технології штучного інтелекту в безпілотних системах: можливості, перспективи, обмеження…… 198
Омельчук І. А., Карпухін Р. Т. Аналіз стану вторинної переробки пластику на сировину для 3D – друку в Збройних Силах України……. 200
Первак І. В., Бондарчук В. Д., Тимчук Г. М. Інтеграція MESH-мереж для забезпечення завадостійкого зв'язку ударних разових стратегічних безпілотних літальних апаратів під час виконання завдань із вогневого ураження противника……. 203
Грунович В. О., Маліка А. А. Розвиток способів застосування наземних роботизованих комплексів з урахуванням конструктивних можливостей ходової частини……... 205
Бондарчук В. Д., Первак І. В., Галепа О. Г. Навігація безпілотних літальних апаратів в умовах подавлення GNSS на основі візуально-інерційних методів…. 210
Пилипчук Т. І., Площик А. С. Інформаційні системи ситуаційної обізнаності про повітряну обстановку в тактичній ланці Сил оборони України…… 212
Крутієнко О. В., Площик А. С. Особливості використання автономних безпілотних літальних апаратів в умовах активного подавлення сигналів супутникової навігації…… 216
Кудрявцева А. П. Захищена MESH-мережа для забезпечення радіозв'язку малих безпілотних літальних апаратів в умовах щільної міської забудови……. 220
Лемішко Л. С., Ейдельштейн Г. Б. Розробка рекомендацій щодо підвищення оперативності оброблення даних повітряної розвідки з використанням згорткових нейроних мереж…… 224
Пасічнюк І. А., Льова О. І., Гром В. А. Шляхи підвищення ефективності виявлення об'єктів оптико-електронними системами безпілотних літальних апаратів в умовах зниження температурного контрасту об'єктів та впливу атмосферних явищ…… 226

Чоларія Р. Г., Стус А. В., Слюсарєв М. Ф. Використання моделей YOLO для автоматизованого виявлення об'єктів інтересу у відеопотоці безпілотних авіаційних систем…….. 227
Сотніков О. М., Тюріна В. Ю. Метод сегментації зображень для систем навігації безпілотних літальних апаратів в умовах дефіциту інформативних ознак…….. 229
Перегуда О. М., Ушаков С. І. Інтеграція безпілотних систем та традиційних зразків озброєння в єдині інноваційні розвідувально-ударні контури Сил оборони України…… 231
Ушаков С. І., Гаврилюк О. С. Розвиток тенденцій масованого застосування наземних роботизованих комплексів у ході сучасної збройної боротьби…….. 233
Бондаренко А. Ю. Побудова циклу бойового застосування бригади безпілотних систем в операціях угруповання військ…….. 237
Круковський І. А., Александров А. К., Сімаков В. Л. Про доцільність використання консалтингових матеріалів компаній IDC, GARTNER, FORRESTER RESEARCH для реалізації систем підтримки рішень на основі Business Intelligence в Силах безпеки і оборони України…….. 241

СЕКЦІЯ 2. Протидія безпілотним авіаційним системам противника 246
Джемула О. М., Черниш О. В., Удовицький В. В., Предчук В. А. Досвід підготовки фахівців із протидії безпілотним авіаційним комплексам противника……. 246
Адаменко А. А., Порохончук О. М., Григоренко Є. О. Підсистема інформаційного забезпечення застосування підрозділів радіоелектронної боротьби…… 250
Лаврик С. В. Шляхи вдосконалення системи захисту артилерійських підрозділів від ураження ударними безпілотними авіаційними системами….. 252
Гусаківський А. В., Мазур В. П., Уваров Ю. Г. Шляхи вдосконалення методики підготовки особового складу зі знищення FPV-дронів зі стрілецької зброї……. 254
Баталов М. А. Методичний підхід до оцінювання ефективності функціонування комплексної системи захисту артилерійського підрозділу… 256
Телегін В. В., Кошкін М. А., Шульга В. В. Дослідження продуктивності систем обробки радіолокаційної інформації на базі операційної системи Linux в умовах інтенсивного потоку даних…….. 259

Пасічник В. М., Слюсаренко М. О. Аналіз особливостей застосування та можливостей баражуючих боєприпасів (типу “Ланцет-1” (“Ланцет-3”), “Молнія”, “КУБ-БЛА”)……..…….... 261
Коростельов В. А. Протидія безпілотним авіаційним системам противника…. 262
Задорожний І. С., Байцурак С. І., Швиденко А. В., Шинкаренко О. М. Трансформація повітряних загроз та формування нових вимог до систем активного захисту наземних виробів озброєння та військової техніки….. 265
Королюк Н. О., Рудь Б. С. Особливості побудови ешелонованої системи протиповітряної оборони від ударів повітряного противника…. 270
Ушаков С. І., Костиря О. О., Черкес О. П., Тіора В. А., Зубелевич Д. І. Тенденції вдосконалення засобів протидії ударним безпілотним літальним апаратам типу FPV…….. 272
Чорномаз О. А. Комплексний підхід до протидії безпілотним літальним апаратам-перехоплювачам для підвищення живучості багаторазових ударних безпілотних авіаційних комплексів…….. 277
Савчук Д. В., Шостак Р. С. Комплексна система захисту артилерійських підрозділів за досвідом ведення бойових дій…… 279
Варава В. В. Рекомендації щодо функціонування комплексної системи захисту артилерійських підрозділів під час планування та ведення бойових дій……... 283
Храпач Д. О. Протидія безпілотним авіаційним комплексам противника…….. 287
Балакірева С. М., Ковзало І. Г., Додурич О. Б. Аналіз програмних засобів підвищення ситуаційної обізнаності про повітряну обстановку в протидії ударним безпілотним апаратам…….. 288
Малишев О. А., Арасланов М. Р., Примак Р. Є. Підвищення завадостійкості оглядових радіолокаційних станцій L-діапазону за рахунок удосконалення діаграми спрямованості антени……. 289
Королюк Н. О., Бутенко А. Ю. Аналіз методів управління вогневими засобами підрозділів зенітних ракетних військ на основі порівняння багатокритерійних альтернатив…… 291
Королюк Н. О., Чопенко Я. Р., Луценко А. С. Підвищення ефективності розпізнавання повітряного противника в умовах ведення бойових дій…… 293
Стеценко С. М., Дорохов О. М. Досвід підготовки фахівців артилеристів із протидії безпілотним авіаційним комплексам противника……. 295

Кошкін М. А., Телегін В. В., Першин О. В. Розробка мережевої системи імітації джерела радіолокаційних повідомлень із використанням протоколу ASTERIX…… 298
Мирончук Ю. А. Формування вимог до безпілотних перехоплювачів реактивних ударних безпілотних літальних апаратів противника……. 299
Заєць Ю. О., Ольшанський М. А., Солопій І. А. Науково-методичні засади модернізації 70-мм некерованих авіаційних ракет для підвищення ефективності ураження безпілотних літальних апаратів…….. 304
Maidaniuk V. A., Vahnin O. V. High-Power Microwave Weapons as a Means of Countering Enemy UAVs……... 307
Дроздов М. О., Шкурпіт О. М., Небесний С. О. Перспективи персонального захисту від FPV–безпілотного літального апарата на полі бою.. 312
Парфенюк В. Г., Григорєв І. С. Цифрове переналаштування частоти у FHSS-системах із застосуванням SDR-технології……... 314

СЕКЦІЯ 3. Засоби ураження безпілотних систем 316
Черняєв С. І., Павленко К. І. Засоби розвідки та ураження безпілотних авіаційних комплексів противника механізованих підрозділів…… 316
Білоус Г. П., Смоляр О. І. Удосконалення форм і способів протидії масовому застосуванню ударних безпілотних авіаційних систем противника з урахуванням досвіду бойових дій на півдні України…….. 317
Брановицький В. В. Застосування безпілотних літальних апаратів для залистування території противника як спосіб психологічного впливу на цільову аудиторію…….. 320
Пількевич І. А., Лобода Р. І. Особливості застосування боєприпасів для безпілотних літальних апаратів із модулем коригування траєкторії польоту.. 322
Онищенко В. М., Терещенко О. П., Долинюк В. В. Моделювання збуренного руху та навантаження конструкції безпілотного літального апарата під час стрільби……. 325
Третяк Д. А., Яромій А. В. Особливості застосування ударних безпілотних літальних апаратів та типи боєприпасів для їх оснащення…….. 327
Тучемський В. С., Лобода Р. І. Застосування підривачів із затримкою спрацювання……... 330
Пантєлєєва Н. М., Лайське Є. В., Хуторна М. Е. Експериментальна апробація інтеграції "Вертоліт – безпілотний авіаційний комплекс" для протидії безпілотним повітряним загрозам…….. 331
Синявський А. А. Засоби ураження безпілотних систем…….. 336

СЕКЦІЯ 4. Космічна підтримка дій військ (сил) 339

Болобан С. І., Мельничук М. В. Методика дешифрування нафтохімічних підприємств за даними космічного знімання……. 339

Болобан С. І., Портовой М. І. Виявлення руйнувань об’єктів за даними космічного знімання середнього та малого просторового розрізнення…. 340

Гордієнко Ю. О., Лобода В. В. Моніторинг іноземних ядерних випробувальних полігонів засобами сейсмічного групування з урахуванням форми очікуваного сигналу…… 341

Якименко В. С., Андрющенко К. О. Стан та перспективи розвитку систем супутникового зв’язку…… 342

Самчишин О. В. Особливості підготовки військових фахівців із дешифрування матеріалів космічної видової розвідки в умовах війни росії проти України……. 346

Бобай Ю. Ю., Магалецький О. О. Трансформація військового застосування космічних апаратів під впливом досвіду російсько-української війни 2014–2026 рр……... 348

Болобан С. І., Шмуйло О. П. Фасетна класифікація шумів даних космічного знімання……... 353

Корнієнко І. В., Попов М. О., Андрощук Р. А. Мобільна сейсмічна група для виконання завдань розвідки……. 358

Николюк О. М., Пивовар П. В. Війна як фактор трансформації земного покриву України……... 359

Топольницький П. П., Ковальчук М. О. Особливості впровадження ГІС–технологій у навчальний процес……. 363

Пивовар П. В., Савчук А. В., Топольницький П. П., Франжі О. В. Дводіапазонна станція приймання наукової інформації з космічних апаратів дистанційного зондування Землі…… 366

Завада А. А., Франжі О. В., Беспалко І. А., Випорханюк Д. М. Автоматизоване виявлення маневрів космічних апаратів і відображення орбітальної обстановки на основі формату ОММ в інтересах Сил оборони України…….. 367

Наумчак О. М., Марцинкевич О. С. Штучний інтелект у життєвому циклі космічних апаратів: світовий досвід і перспективи для космічної підтримки дій військ (сил)……. 370

Рибачук О. І., Борцова М. В. Ефективне планування застосування наземних роботизованих комплексів із залученням спроможностей космічних систем дистанційного зондування Землі…… 374
Беспалко І. А, Випорханюк Д. М., Завада А. А., Пекарєв Д. В. Проблеми актуалізації термінологічної бази космічної підтримки дій військ (сил)……. 376
Sysoienko S. V., Vovchanivska N. M. Information and Analytical Provision of Space Support of Troops in Conditions of Counteraction and Limited Access to Space Resources……... 379
Романчук М. П., Наумчак О. М., Денисюк Ю. Р. Надійнісний критерій якості зображення для планування знімання оптико-електронним космічним апаратом…….. 380
Лящук О. І., Андрущенко Ю. А., Осадчий В. І. Комплексний геоінформаційний моніторинг високоенергетичних вибухових подій…. 383
Лящук О. І., Парновський О. С., Андрущенко Ю. А., Осадча Н. Ю., Довбиш С. В. Організація використання інформації про космічну погоду у Збройних Силах України……. 384
Миклуха В. А. Особливості використання інфрачервоних космічних знімків для виявлення прихованих об'єктів……. 388

<u>СЕКЦІЯ 5.</u> Радіоелектронна розвідка 390

Єгоров В. О., Запорожченко Ю. І. Радіочастотні відбитки як інструмент ідентифікації радіоелектронних засобів у системах радіотехнічної розвідки…….. 390
Єгоров В. О., Андрущенко І. С. Інноваційні технології та перспективні напрями розвитку систем радіотехнічної розвідки: когнітивні, розподілені та квантові підходи……. 393
Тимчук С. В., Тарасенко В. О. Оцінювання меж застосовності півтонового тензорного подання спектрограм у ході розпізнавання вузькосмугових радіосигналів……... 394
Тарасенко В. О., Шишкін Ю. Д. Застосування штучного інтелекту в радіоелектронній розвідці: можливості автоматизації та роль оператора-аналітика…….. 397
Єгоров В. О., Гайка Ю. А. Застосування глибоких нейронних мереж для класифікації радіолокаційних сигналів в умовах інтенсивних завад та низького відношення сигнал / шум…….. 400

Бугайов М. В. Топологія системи радіомоніторингу з використанням групи безпілотних літальних апаратів…… 403
Данилюк І. А., Куцаєв В. В., Матвієнко В. М. Визначення позиційних районів розгортання оперативно-тактичного ракетного комплексу “Іскандер” за даними багатоканальної радіотехнічної розвідки…….. 404
Дзігора О. М., Яровий С. В., Красношапка І. В. Технологічні можливості конструювання твердотільного підсилювача потужності радіолокаційного призначення S-діапазону…… 409
Радушинський О. П. Особливості виявлення та спектрального аналізу радіовипромінювань MESH / MANET-мереж у завданнях радіоелектронної розвідки…… 413
Гайка Ю. А., Єгоров В. О. Оптимізація та перспективи застосування засобів радіорозвідки на базі безпілотних авіаційних платформ…….. 417
Сидорчук О. Л., Залевський В. Й. Дослідження коефіцієнтів відбиття електроманітних хвиль від позамежних перерізів опромінювачів фазованих антенних решіток…… 420
Мельник С. В. Сучасний стан використання інформаційно-комунікаційних систем підрозділами радіоелектронної розвідки…… 422
Остапчук О. М. Застосування технологій штучного інтелекту та машинного навчання для автоматизованої класифікації джерел радіовипромінювання в сучасних комплексах радіоелектронної розвідки… 424
Красношапка І. В., Садовий К. В., Чепурний В. П. Обґрунтування структури апаратно-програмного комплексу пасивного виявлення безпілотних літальних апаратів на основі SDR-технологій…… 427
Гребенюк О. О., Гребенюк О. П. Обґрунтування вибору математичної моделі для розпізнавання джерел радіовипромінювання в умовах складної радіоелектронної обстановки…… 428
Андрущенко І. С., Єгоров В. О. Метод циклостаціонарного аналізу сигналів у завданнях радіомоніторингу…… 430
Козюра І. В. Обґрунтування методики перевірки достовірності розвідувальної інформації в умовах складної оперативної обстановки…. 433
Любиченко В. П. Оцінювання стану групових об’єктів спостереження в умовах обмеженої апріорної інформації…… 434
Пінчук О. А., Тимчук С. В. Математичні моделі поведінки радіомереж для прогнозування дій підрозділів противника…… 436

Нікітін А. І., Площик А. С. Перспективи створення постів радіоелектронної розвідки з елементами штучного інтелекту в підрозділах охорони державного кордону України…….. 437
Вода Ю. Л. Актуальні питання розвитку радіоелектронної розвідки як виду артилерійської розвідки в умовах сучасних високотехнологічних конфліктів…. 439
Ставісюк Р. Л., Каменчук А. В. Обґрунтування актуальності виявлення та оцінювання параметрів сигналів технології "Несуча – в – Несучій"…….. 441
Бондаренко Д. М., Стефанишин Я. І., Липський О. А. Використання штучного інтелекту під час проєктування спеціальної техніки на FPGA.. 442
Kononova O. A. Application of Radio Frequency Identification Systems for Target Identification by Radio-Technical Units of Air Defence of The Air Force of The Armed Forces of Ukraine During Electronic Reconnaissance…. 444
Іванов В. К. Бойова ефективність та архітектурна живучість аеростатного комплексу радіотехнічної розвідки…….. 445
Сапронова С. М., Запорожченко Ю. І. Спектральні методи оцінювання кутових параметрів джерел випромінювання в адаптивних антенних системах…….. 449
Ставісюк Р. Л., Сікан Ю. В. Перспективи розроблення способів динамічного планування завдань силам і засобам радіоелектронного моніторингу на основі мультиагентного навчання з підкріпленням……. 453
Луніна К. В. Сучасні методи виявлення та локалізації джерел радіовипромінювання…… 454
Колос Ю. О., Маслов О. А. Обґрунтування напрямів розвитку експериментальної бази для проведення навчання та наукових досліджень антенно-фідерних пристроїв в умовах російсько-української війни…… 456
Рибалка А. О. Конструктивні та теплові особливості польової радіоелектронної апаратури: аналіз зразків ADEX 2026…… 460

<u>СЕКЦІЯ 6.</u> Радіоелектронна боротьба 465

Шельвестер В. Я., Шейгас В. В. Контроль характеристик антен засобів радіоелектронної боротьби як фактор забезпечення їх ефективності в умовах сучасної війни…….. 465
Іщенко Д. А. Варіант класифікації засобів у системі загальних технічних вимог до техніки радіоелектронної боротьби……. 468
Журавський С. В., Чолпанов В. О., Назарчук Я. Ю. Удосконалений алгоритм виявлення та подавлення відеоканалів безпілотних авіаційних апаратів із системою FPV……... 472

Брановицький В. В., Фриз В. П. Застосування спрямованої антени для підвищення дальності та радіоелектронної стійкості FM-радіомовлення в інтересах психологічного впливу…….. 477
Філіппов М. О., Пак Д. Є. Забезпечення стійкості навігації безпілотних систем в умовах порушення та недоступності супутникових навігаційних сигналів…… 480
Рихальський О. Р., Борисов П. С., Дем'яненко Є. О. Дослідження впливу узгодження широкосмугової антени для техніки радіоелектронної боротьби на робочу смугу частот…… 483
Лазуріна Н. П. Стратегічні пріоритети інтеграції вищої освіти України до європейського освітнього простору……. 485
Ільченко М. О., Бібік А. В. Сучасний стан та перспективи розвитку систем і засобів радіоелектронної боротьби: удосконалення форм і способів ведення радіоелектронної боротьби Силами оборони України.. 487
Делех В. А., Висоцький О. В. Розробка пропозицій щодо протидії радіотехнічних підрозділів засобам технічної розвідки та радіоелектронної боротьби противника…….. 492
Ничипорчук В. М., Чернишов Л. В. Технічні аспекти радіоелектронного впливу на низькоорбітальну систему широкосмугового зв'язку «Рассвет»……. 494
Нагорнюк О. А., Журавський С. В. Методика дослідження засобів виявлення радіосигналів безпілотних літальних апаратів у лабораторних умовах……. 497
Нагорнюк О. А., Борисов П. С., Зелінський А. В. Вимірювальний стенд для дослідження перешкодостійкості адаптивних антенних решіток із керованою діаграмою спрямованості…….. 499
Галяс А. В., Біховський О. В. Застосування оптико-електронних засобів подавлення для прикриття критичних об'єктів шляхом впливу на системи комп'ютерного зору безпілотних літальних апаратів…….. 502
Трохименко О. В. Електромагнітний та кіберпростір. Тенденції та перспективи подальшої інтеграції…… 505
Столяренко М. П. Радіоелектронний захист радіолокаційних станцій артилерійської розвідки……. 510
Сухотеплий М. В., Гота О. С. Особливості застосування децентралізованих MESH-мереж для забезпечення стійкості зв'язку Сил оборони України з урахуванням досвіду війни…… 512

Цимбалюк В. М., Поліщук Д. О. Застосування штучного інтелекту для підвищення ефективності систем радіоелектронної боротьби…… 513
Дубина О. Ф., Авсієвич Р. О., Дацько Д. В. Автоматизація систем радіоелектронної боротьби: сучасний стан та перспективи розвитку….. 515
Сергієнко А. Я. Особливості забезпечення електромагнітної сумісності засобів радіоелектронної боротьби та радіозв'язку в сучасних умовах…. 518
Глущенко О. О., Біховський О. В. Прикриття об'єктів інфраструктури засобами радіоелектронної боротьби…… 521
Ковтонюк Д. В. Використання штучного інтелекту для підготовки фахівців із радіоелектронної боротьби…… 524
Трачук Є. С. Алгоритм розрахунку ефективності засобу радіоелектронної боротьби…… 526
Загорулько К. М., Коваленко К. А. Аналіз недоліків використання MESH-мережі та модемів у передачі даних безпілотних літальних апаратів.. 527
Гулюк Д. С., Біховський О. В. Зміна тактики застосування російськими ударними безпілотними літальними апаратами використання MESH-мереж.... 529
Колот В. В. Використання засобів радіоелектронної боротьби на наземних роботизованих платформах з інерціальною системою…….. 532
Верховцев Ю. Ю., Шостачук А. М. Стан і перспективи використання методів та засобів радіоелектронної боротьби в умовах сучасної війни… 534
Smyrynska N. B. Analysis of Failure Mechanisms in UAV Onboard Electronic Systems Under Intentional High-Power Electromagnetic Exposure…… 538
Червоненко Д. В., Площик А. С. Технічні та організаційні шляхи вдосконалення радіоелектронної боротьби з безпілотними літальними апаратами…….. 540
Солдатенко А. О., Хіжнюк О. А. Обґрунтування напрямків модернізації станції оптико-електронного подавлення вертольота з урахуванням стандартів НАТО…… 542
Сушко О. Ю. Розробка та застосування ультраширокосмугової антени для роботи на високих потужностях…… 545

<u>СЕКЦІЯ 7.</u> Скрите управління військами 550

Sheihas V. V., Vasiyk P. S. Modern Devices for Covert Information Acquisition….. 550
Метельський Д. І., Шейгас В. В. Розробка та впровадження алгоритму сканування й моніторингу систем для виявлення та попередження витоків інформації через побічні електромагнітні канали…….. 552
Рой І. М., Шейгас В. В. Проблематика пошуку прихованих відеокамер. 554

Костерев Д. С., Будзінська О. О., Кулініч Ю. М. Особливості імплементації стандартного функціонального профілю захищеності оброблюваної інформації від несанкціонованого доступу в базовий профіль безпеки системи…….. 556
Зубелевич Д. І., Вандалович В. П. Демаскувальні ознаки роботи пункту управління: ризики та заходи щодо їх зниження…… 558
Романчев А. М., Боюка М. П. Контроль цілісності електронної телеграми та її відповідність оригіналу…… 562
Росул Я. М., Павлюк Н. А. Організація оперативного обліку та контролю функціонування системи допуску особового складу військових частин (установ) до державної таємниці…….. 565
Поліщук Б. В., Буханевич С. В. Захист інформації від технічних каналів витоку в умовах сучасних воєнних загроз…… 568
Гриневич Б. Ю., Рачкінда В. А. Автоматизація процесу оцінювання ризиків витоку інформації на військових об’єктах в умовах збройного конфлікту… 570
Редько А. В., Кулініч Ю. М. Програмна реалізація процесу формування акта обстеження об’єкта інформаційної діяльності як елемент системи інформаційної безпеки Збройних Сил України……. 572
Міщенко Ю. В. Удосконалення скритого управління артилерійським підрозділом в умовах технічної розвідки противника…… 573
Додурич О. Б., Ковзало І. Г., Кулабухов О. М. Особливості забезпечення скритності управління військами в умовах протидії технічним засобам розвідки противника…… 575
Кулабухов О. М., Додурич О. Б., Коноваленко Б. О. Нейромережевий контроль технічного стану комплексу засобів автоматизації в системі скритого управління військами…….. 576
Гринчевський Я. В., Завірюха Д. О. Вплив радіопрозорості маскувальних матеріалів на ефективність виконання завдань підрозділами з активними засобами протидії технічним розвідкам…….. 578
Рупета Р. О., Діденко А. П. Актуальні аспекти у сфері технічного захисту інформації……... 582
Соловей В. А., Маковський І. Ю. Відновлення інформаційної взаємодії INVISCOMM в умовах порушення каналу скритого управління……... 584

Метельський Д. І, Умінський В. В. Загроза довгостроковій конфіденційності шифрованих повідомлень в умовах розвитку квантових обчислень…….. 589
Мул Д. А., Прокопенко Є. В. Побудова захищених інформаційно-комунікаційних мереж тактичної ланки Державної прикордонної служби України в умовах активної радіоелектронної боротьби та радіорозвідки противника…….. 592
Новікова Є. В., Діденко А. П. Застосування мережевого фільтра для захисту інформації від витоку низькочастотними каналами…….. 596
Метельська А. І., Лутченко В. І. Автоматизація роботи режимно-секретних органів військових частин (установ) в умовах воєнного стану…….. 599
Костерев Д. С., Соловей В. А. Метаданонейтральна інформаційна взаємодія INVISCOMM…….. 600
Варишнюк В. О., Казєв О. В. Особливості форм та способів протидії технічним засобам розвідки противника…….. 605
Гурковський М. Ю. Метод захищеного зберігання інформаціїї з обмеженим доступом на флеш-накопичувачах…… 608
Васянович В. В. Функціональна структура програмного застосунку управління доступом до електронних носіїв інформації…… 609
Березюк К. О. Актуалізація нормативних документів у сфері охорони державної таємниці за досвідом повномасштабної збройної агресії рф проти України…….. 612
Гладич Р. І. Методологічні засади маскування телеметричних каналів роботизованих систем під радіоелектронні сигнатури штатних засобів зв'язку тактичної ланки в умовах активної радіоелектронної розвідки противника…….. 614
Мякішев Н. В., Баратюк В. І., Корчев В. Б. Використання електронного документообігу в органах Державної прикордонної служби України: співвідношення оперативності та захисту інформації... 617
Будзінська О. О., Соловей В. А. Логічна безпарольна автентифікація INVISCOMM у захищених системах управління…… 620
Нікора І. В., Лях І. Ю., Мукосій Д. В. Аналіз методів комбінованого детектування кібератак на автоматизовані системи управління спеціального призначення з боку взаємодіючих інформаційних систем.. 625

Новацька М. І., Катеринчук І. С. Актуальні аспекти у сфері технічного та криптографічного захисту інформації…….. 627
Варламова І. Є. Адаптація систем та засобів комунікації малочисельних піхотних груп під час каскадного пересування: досвід Збройних Сил України…… 630
Першин О. В., Клабан І. Ю. Інтелектуальний аналіз сповіщень кібербезпеки на основі локальних мовних моделей…… 633
Шило С. Г., Руденко В. А. Розробка комбінованого методу гешування даних на основі двовимірної моделі Ізінга та геш-функції Купина для забезпечення цілісності інформації й контролю доступу операторів автоматизованих систем управління…… 634
Клімчук О. А. Концептуальна архітектура автоматизованої системи протидії технічній розвідці шляхом управління цифровим слідом підрозділу…… 636

СЕКЦІЯ 8. Спеціальний радіозв'язок 638

Гребняк В. С., Папуш О. Г. Аналіз загроз витоку інформації технічними каналами та комплексні методи їх нейтралізації……. 638
Прокопенко Є. В., Мул Д. А. Підходи до інтеграції різнорідних систем радіозв'язку для забезпечення завдань спеціальної розвідки підрозділами Державної прикордонної служби України з використанням інтегрованої інформаційно-комунікаційної системи «Гарт»…….. 642
Якименко В. С., Печерська В. І. Стан та перспективи розвитку MESH–систем …… 645
Лейко О. М. Перспективи розвитку системи та засобів зв'язку спеціального призначення з урахуванням впровадження мереж LTE….. 648
Стасєв Ю. В., Новічков В. О., Карамушка М. І. Алгоритм підвищення нелінійності керуючих послідовностей у системах криптографічного захисту інформації……. 655
Ваврічен О. А., Бібік А. В. Загрози несанкціонованого знімання інформації з волоконно-оптичних ліній зв'язку…….. 659
Дідух Л. І., Бовсуновський В. Ю. Методика оцінювання ефективності завадостійких кодів для каналу декаметрового радіозв'язку…….. 662
Чіпєра В. В., Поливаний С. В. Software Cognitive Radio та SSDF-атаки: принципи роботи, загрози та методи протидії їм…… 663

Ткач О. С., Кудряшов Ю. О. Методика підвищення завадостійкості спеціального радіозв'язку декаметрового діапазону за рахунок просторової селекції сигналів…… 666
Vasylenko S. V., Yerokhin V. F. A Cognitive Approach to High-Frequency Radio Link Adaptation …… 668
Герус О. І., Прокопович В. Д. Розробка антени спрямованої дії до радіостанції HARRIS RF7850M-HH……. 669
Островська – Бугайчук І. М., Земський В. О. Правове забезпечення кібербезпеки та захисту інформації в системах спеціального військового зв'язку.. 671
Мордюк В. І., Мишлевич В. В. Напрями підвищення ефективності частотного планування декаметрових радіоліній…… 672
Гнатюк В. О., Котенко В. М. Аналіз частотно-часової структури радіосигналів перспективних завадозахищених та скритих систем зв'язку…. 674
Воронін В. О., Площик А. С. Інноваційні підходи до розроблення та застосування систем спеціального радіозв'язку в умовах активного радіоелектронного спостереження……... 676
Дубовський Ю. В., Сторчаєва А. С. Карамушка М. І., Василишин В. І. Концепція ройової когнітивної радіомережі з просторово-адаптивним формуванням променя для повітряного ешелону тактичного зв'язку в умовах радіоелектронного подавлення…… 679
Стечишин С. В., Городиський Р. О. Інтеграція мікропроцесорних модулів та засобів бездротового зв'язку в системах дистанційного моніторингу…… 683
Нікітченко І. В., Кудряшов Ю. О. Формування інтегрального критерію вибору раціонального режиму роботи спеціальної радіолінії декаметрового діапазону…… 685
Кашпур І. Р., Самонюк О. В. Методика аналізу енергетичних характеристик антенно-фідерних пристроїв тактичної ланки управління короткохвильового діапазону…… 687

Н А У К О В Е В И Д А Н Н Я

ІННОВАЦІЙНІ ПІДХОДИ ЩОДО ФОРМ ТА СПОСОБІВ ЗАСТОСУВАННЯ ВИСОКОТЕХНОЛОГІЧНИХ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ СИЛАМИ ОБОРОНИ УКРАЇНИ

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

Тези доповідей
Частина 1

Видавничий оригінал виготовлений
у науково-організаційному відділі ЖВІ

Відповідальний за випуск
Середюк Сергій Анатолійович

Комп'ютерна верстка та макетування **І. В. Голуб**
Дизайн і макет обкладинки **О. Ю. Тофанчук**

Свідоцтво про реєстрацію серія ДК № 7355 від 9 червня 2021 року
Підписано до друку 22.10.2026. Формат 60 × 84 / 16
Ум. друк. арк. 41,15. Зам. 757ц.

Друкарня ЖВІ

Просп. Миру, 22, м. Житомир, 10004



Застосування безпілотних систем Силами оборони України



Протидія безпілотним авіаційним системам противника



Засоби ураження безпілотних систем



Космічна підтримка дій військ (сил)



Радіоелектронна розвідка



Радіоелектронна боротьба



Скрите управління військами



Спеціальний радіозв'язок