COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.099

УДК 004.75; 004.8

МЕТОДИ І ЗАСОБИ ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОСТІ ТА ЗАХИСТУ РАДІОЗВ'ЯЗКУ В УМОВАХ СКЛАДНОЇ ЕЛЕКТРОМАГНІТНОЇ ОБСТАНОВКИ

Р. Б. Кутень, О. Ю. Синявський

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: roman.b.kuten@lpnu.ua, orest.y.syniavskyi@lpnu.ua

Стаття містить огляд широкого спектру методів і засобів забезпечення стабільності зв'язку та захисту радіопередачі, зокрема шифрування, частотне переплутування, використання спрямованих антен, маскування та завадостійке кодування.

На основі проведеного огляду та аналізу було зроблено висновки про можливість застосування цих методів і засобів захисту у популярних нині безпілотних пристроях. Було виявлено аспекти захисту, які не перекривалися класичними методами захисту. Запропоновано метод покращення відмовостійкості і доступності каналу зв'язку БПЛА навіть для умов роботи під дією засобів радіоелектронної боротьби.

Зроблені висновки і рекомендації відкривають перспективи подальших досліджень у цьому напрямку і дають можливість значно підвищити "живучість" безпілотних пристроїв.

Ключові слова: захист каналів зв'язку, розподілені радіомережі, спрямовані антени, частотне переплутування, завадостійке кодування, моніторинг параметрів, РЕБ.

Вступ

У сучасному світі, де безперервне, завадостійке з'єднання стає все важливішим, проблема захищеного та стабільного радіозв'язку з низьким рівнем співвідношення сигнал/шум набуває особливого значення. Радіозв'язок є життєво важливим для багатьох застосувань, зокрема мобільного зв'язку, бездротових мереж, військових комунікацій та багато іншого. Однак збереження надійного з'єднання в умовах низького рівня співвідношення сигнал/шум є великим викликом, особливо в умовах штучного створення шумових завад зловмисником.

Особливо гостро потреба стабільного завадостійкого зв'язку постає саме тепер, коли технології набувають все більшого значення у бойових діях. Насамперед це стосується безпілотних літальних апаратів, або дронів, роль яких у воєнних конфліктах стає все важливішою, а їх вплив на стратегію та тактику ведення бою лише зростає і наразі складно навіть оцінити перспективи їх використання у майбутньому. Проведений у статті огляд допоможе покращити захищеність радіозв'язку за низького рівня співвідношення сигнал/шум, зокрема в умовах використання БПЛА під час активного електромагнітного протиборства з боку противника, що є дуже актуальним завданням за сучасного рівня використання безпілотних пристроїв.

1. Огляд літературних джерел

Основні та найбільш поширені методи захисту радіоканалу, як показує практика і які відображено у численній оглянутій нами літературі, становлять:

Шифрування: шифрування даних перед їх переданням може допомогти захистити інформацію від перехоплення.

Частотне переплутування: цей метод передбачає постійну зміну частоти передання, що ускладнює перехоплення та перешкоджання переданню сигналу.

Використання спрямованих антен: спрямовані антени дають можливість зосередити радіосигнал у певному напрямку, що зменшує ймовірність перехоплення сигналу.

Розподілена радіомережа: використання розподіленої радіомережі, де кожна станція може відігравати роль передавача та приймача, може збільшити стійкість радіомережі до атак.

Маскування: це метод, основною метою якого є приховування самого факту передання тієї чи іншої інформації.

Використання завадостійкого кодування високого порядку: це метод кодування інформації, який дає можливість виявляти та виправляти помилки, що виникають під час передання даних.

Шифрування

Методи шифрування та розшифрування, алгоритми, математичні їх основи описує криптографія – це така галузь науки, яка досліджує методи забезпечення таємниці та цілісності інформації. За допомогою криптографічних алгоритмів можна зашифрувати дані так, що їх можна розшифрувати тільки за наявності спеціального ключа [4].

Є такі два основні типи використовуваних криптографічних алгоритмів: симетричні й асиметричні. До найвідоміших та надійних симетричних алгоритмів належать AES, Serpent та Twofish [2]. Це є тривіальний і один із найбільш дієвих методів захисту інформації від розкриття її змісту у процесі її перехоплення під час передання каналом, до якого можливий несанкціонований доступ зловмисника (одним із яких, власне, і є радіоканал, оскільки радіохвиля поширюється відкритим простором і може бути вільно прийнята довільною антеною і приймачем), але водночас не передбачається захисту від модифікації (спотворення) інформації, чи повного знищення інформації і унеможливлення її прийому внаслідок просторового зашумлення.

Частотне переплутування

Частотне переплутування – це метод захисту каналу зв'язку, який полягає в постійній зміні частоти передання сигналу, щоб ускладнити його перехоплення, придушення чи інше перешкоджання процесу його передання. Цей метод активно використовується в сучасних системах радіозв'язку із шумоподібними сигналами, які мають високу перешкодостійкість та прихованість [6–8].

Метод частотного переплутування дає змогу змінювати частоту передання сигналу відповідно до певного алгоритму або правила [7, 8]. Цей метод може бути реалізований за допомогою різних технік, таких як: псевдовипадкове переналаштування робочої частоти; частотне стрибання; частотне розподілення; частотне кодування. Частотне переплутування має низку переваг, таких як: зниження ймовірності перехоплення сигналу; зниження ймовірності перешкоджання передання сигналу; зниження ймовірності виявлення сигналу; зниження ймовірності локації сигналу; зниження ймовірності ідентифікації сигналу. Застосування методів зміни частоти, засобів зв'язку із шумоподібними сигналами дають змогу значно підвищити ефективність та безпеку радіозв'язку навіть в умовах бойових дій [6, 7].

Використання спрямованих антен

Спрямовані антени – це антени, які мають високу директорну дію, тобто вони зосереджують радіохвилі в певному напрямку, зменшуючи втрати потужності та збільшуючи дальність передання [1, 8–10]. Використання спрямованих антен для забезпечення надійності та захисту радіозв'язку має низку переваг, таких як: зниження ймовірності перехоплення сигналу; зниження ймовірності виявлення сигналу; зниження ймовірності локації джерела сигналу; зниження ймовірності ідентифікації сигналу. Ці антени можна сконструювати із застосуванням таких технологій, як: параболічні антени; решітчасті антени; антени з фазовим розподілом; антени з адаптивним формуванням діаграми спрямованості.

Сьогодні це питання особливо актуальне через постійну потребу у надійному польовому зв'язку у військових, зокрема, у документі [9] розглянуто характеристики і питання експлуатації

основних типів антен для ліній радіозв'язку під час виконання поставлених завдань підрозділами Національної гвардії України, зокрема спрямовані антени, антени з фазовим розподілом, антени з адаптивним формуванням діаграми спрямованості. На основі проведеного аналізу автори [9] обґрунтували, що як основний антенний елемент доцільно використовувати конструкцію кутової антени в поєднанні з іншими конструкціями, розглянутими у роботі, та застосовувати їх у складі об'єднаного комплексу разом зі штатними засобами забезпечення військового зв'язку.

Розподілена радіомережа

Розподілена радіомережа – це комплекс радіоелектронних пристроїв та споруд зв'язку, що належать певному користувачу. Вони використовують однакові частоти і мають здатність встановлювати безпосередній зв'язок між собою або через основний радіоелектронний пристрій. Всі ці елементи об'єднані в єдиний технологічний процес, що забезпечує обмін інформацією [11].

Розподілену радіомережу можна реалізувати за допомогою основних двох технологій:

- розподілена система керування (англ. Distributed Control System, DCS) – це системи керування техпроцесами, особливістю яких є децентралізована обробка даних, та розподіл між системами введення та виведення;
- розподілені обчислення (англ. Distributed Computing) – це спосіб, за якого для особливо складних і важких обчислень використовуються комп'ютери, що об'єднані в одну мережу.

В Сполучених Штатах Америки ведуться інтенсивні наукові дослідження та розробки, спрямовані на створення уніфікованої багатофункціональної інформаційно-управляючої системи. Ця система, відома як C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance), інтегрує в собі функції управління військами, зброєю, розвідкою, радіоелектронною боротьбою, а також зв'язку, навігації, орієнтування й впізнання [12].

Реалізація цієї системи здійснюється за допомогою фінансування програми створення інформаційної мережі поля бою (Warfighter Information Network-Tactical, WIN-T). Основною метою WIN-T є оптимізація бойового і чисельного складу підрозділів, водночас підвищуючи їхню бойову ефективність. Це досягається через збільшення мобільності, досягнення цілковитої переваги над противником в інформаційному забезпеченні і розвідувальних можливостях [12].

Використання маскування

Маскування передання інформації радіоканалом – це захист інформації від перехоплення, виявлення, локації та ідентифікації через зміну характеристик радіосигналу або використання спеціальних методів та засобів передання [13, 15].

Є чимало способів, які можуть допомогти приховати факт передання, які описані у літературі [6–8, 13–15], серед них такі як:

- Використання хаотичних сигналів, які мають широкий спектр та непередбачувану динаміку, що ускладнює їх виявлення та розпізнавання [15].
- Використання спектрального маскування, яке полягає в тому, що інформаційний сигнал передається на двох сусідніх довжинах хвиль, а на приймальній стороні одна з них відкидається [14].

У дослідженні [15] було розглянуто маскування передання цифрового сигналу засобом радіозв'язку із використанням хаотичного маскування. Як несучий сигнал для передання даних було використано хаотичне коливання, згенероване за схемою Чуа [16]. Проведений у цій роботі аналіз імітаційної моделі системи передавання цифрової інформації, що застосовує схему хаотичного маскування, свідчить про її широкий потенціал для практичної реалізації у системах зв'язку. Хоча розуміємо, що, як у будь-якій системі зв'язку, відновлення інформації ускладнюється наявністю шумів значного рівня у каналі зв'язку, а також метод має свою складність, зумовлену перехідним процесом під час зміни бітів повідомлення.

Використання завадостійкого кодування високого порядку

Цей метод дає змогу виявити та у разі достатньої кодової відстані виправити помилки, що можуть виникати у реальних каналах зв'язку під час передання даних [17].

Сучасні наукові роботи значною мірою присвячені “балансуванню” між завадостійкістю коду і його надлишковістю, зокрема у дослідженні [18] представлено метод забезпечення надійності інформації в бездротових системах передання даних, який базується на адаптації різноманітних кодових структур. Особливість цього методу, яка відрізняє його від наявних, полягає у застосуванні різних за структурою завадостійких кодів за різної ситуації у приймально-передавальному тракті. Відповідно до відношення сигнал-шум у каналі використовуються коди, що варіюються від простих до складних. Це сприяє досягненню визначених характеристик надійності інформації та забезпеченню оптимального використання обчислювальних ресурсів, у тому числі в умовах нестаціонарних навмисних завад.

2. Постановка завдання

Першим завданням цієї статті був огляд джерел із описом сучасних методів і засобів у сфері захисту каналів радіозв’язку від перебоїв у роботі та забезпечення стабільного зв’язку з акцентом на можливі виклики в умовах активного інформаційного протиборства. Наступні завдання дослідження можна сформулювати так: провести подальший порівняльний аналіз та оцінку можливості застосування розглянутих методів, а також навести пропозиції можливих способів покращення стабільності зв’язку з врахуванням сучасних умов його застосування силами оборони України. Основною із таких умов для цього дослідження є врахування потенційної можливості використання того чи іншого засобу у пристроях невисокого рівня обчислювальної продуктивності, зокрема безпілотних пристроїв із автономним живленням та малого розміру БПЛА.

3. Основна частина

Аналіз вищенаведених джерел і публікацій доводить, що різні методи захисту каналу зв’язку, зокрема шифрування, переплутування частот, використання шумоподібних сигналів, спрямованих антен, кодування, що стійке до помилок, та розподілені радіомережі, мають значний потенціал для забезпечення надійного та безпечного зв’язку, особливо в складних умовах, таких як активний радіошум у бойових ситуаціях або одночасна робота кількох пристроїв на суміжних частотах. Хоча кожен метод має свої переваги, вони також мають обмеження і потребують ресурсів для обробки даних, потенційно знижуючи ефективну швидкість передання даних. Вибір найбільш відповідних методів захисту залежить від конкретних умов і завдань каналу зв’язку, а також можливості їх застосування в бойових умовах, ресурсомісткості цих методів, можливості їх впровадження як вбудованого пристрою або елемента безпілотних систем.

З огляду на теперішню поширеність використання БПЛА у військових операціях, останній пункт є найбільш значущим і важливим, саме тому він був обраний як якісний критерій оцінки можливості застосування тих чи інших методів захисту у безпілотних пристроях. Враховуючи цей критерій, можна одразу констатувати, що методи маскування сигналу та використання спрямованих антен на сучасному етапі мало придатні для використання у безпілотних пристроях. Методи маскування сигналу потребують значних ресурсів, що неможливо в умовах автономного пристрою з акумулятором. Спрямовані антени своєю чергою мають інший недолік: окрім того, що зазвичай вони мають більші габарити і їх складно розмістити на БПЛА невеликих розмірів, такі антени потребують точного настроювання і спрямування на іншого абонента. Враховуючи маневрування літальних апаратів під час роботи, це є критичним обмеженням, адже зміна просторового положення апарату спричинить втрату зв’язку.

Інші з розглянутих методів мають свої переваги і хиби, але в межах нашого дослідження можна резюмувати, що жоден із методів не убезпечує оператора апарату від повної втрати зв’язку з пристроєм, і жоден із методів не пропонує шляхи відновлення зв’язку після його втрати внаслідок впливу ворожих засобів радіопридушення та радіоелектронної боротьби. Тому основним результатом роботи є пропозиція розв’язання такого завдання: враховуючи особливості функціонування БПЛА та їх можливість самостійно переміщуватися у просторі, було розроблено концепцію методу

"останнього порятунку" для відновлення зв'язку, якщо його втрата відбулася під час зальоту в зону роботи засобів РЕБ, інших пристроїв або в зону, де сигнал пульта недосяжний через фізичні умови середовища.

4. Результати

Основна ідея розробленої і запропонованої концепції ґрунтується на тому, що ми маємо враховувати координати переміщення БПЛА як один із параметрів, що впливає на стабільність і захищеність зв'язку безпосередньо. Це зумовлено тим, що безпілотні пристрої мають можливість переміщуватися у просторі, а у разі безпілотної авіації це може відбуватися ще й на великі відстані і з великою швидкістю. І в різних місцях розміщення апарату рівень його захищеності буде різний, незважаючи на той факт, що методи його захисту, протоколи обміну даними й інші його параметри залишилися незмінними. Для обґрунтування цієї теорії розглянемо на схематичному рисунку потенційні умови і ситуації, які можуть виникнути під час роботи безпілотних пристроїв у тих чи інших випадках.

На цій схемі ми бачимо модель, згідно з якою може працювати безпілотний апарат в умовах його використання як засобу розвідки у зоні бойових дій. Схематично зображені розташування траншей противника, його засоби вогневого ураження (у схемі для прикладу зображено два міномети), розташування особового складу, а також зображені умовні місця розташування засобів радіоелектронної боротьби, призначення яких – якраз боротьба із нашим безпілотником, також колами зображено орієнтовні зони роботи ворожого РЕБ: зона, у якій погіршується якість зв'язку, але бортових систем забезпечення стабільності і захисту цілісності каналу зв'язку все ще достатньо для задовільної роботи, відповідає синьому колу, а червоному колу відповідає зона, у якій потужність випромінювання сигналу РЕБ значно перевищує можливості протидії нашого апарату і зв'язок із ним повністю втрачається.

Розглянемо три окремі випадки, можливі під час роботи цього апарату, і для кожного випадку приймаємо, що використовується один і той самий БПЛА з однаковими параметрами.

Під час польоту оператором дрону траєкторією, позначеною літерою "А", оператор матиме можливість безперешкодно розвідати передню лінію траншей і їхнє обладнання, а на підльоті до позицій мінометного підрозділу він уже потрапляє у зону дії РЕБ і може спостерігати погіршення роботи пристрою, але все ще керувати ним і мати можливість завершити роботу поверненням на базу.

Під час польоту оператором дрону траєкторією, позначеною літерою "Б", оператор розвідає передню і другу лінію оборонних траншей, водночас він оминає всі засоби РЕБ і не відчує жодних перешкод чи збоїв у роботі апарату, внаслідок чого успішно виконає завдання і повернеться на базу.

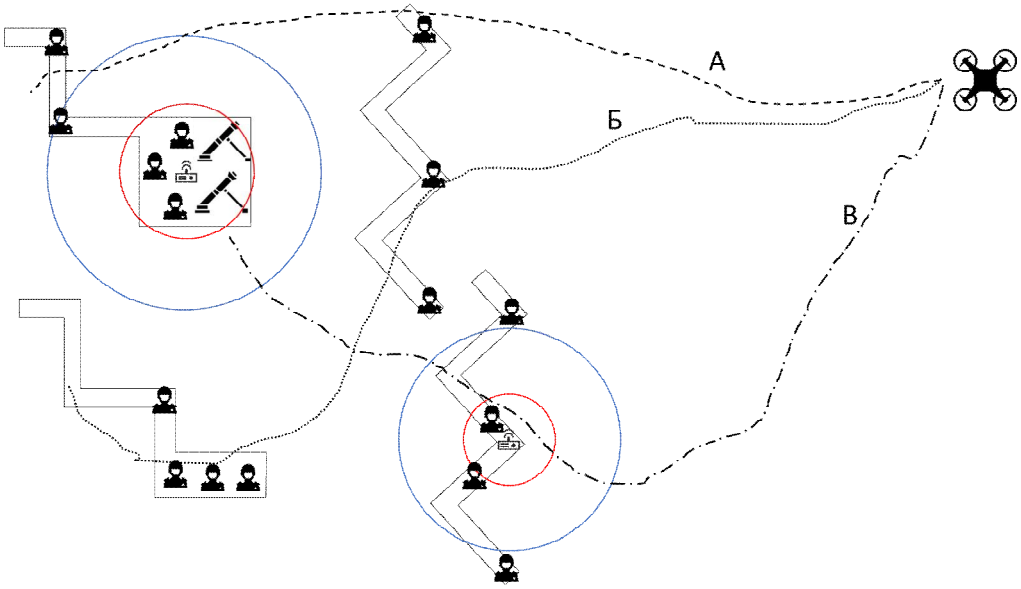
Під час польоту оператором дрону траєкторією, позначеною літерою "В", оператор на прямій ділянці маршруту, під час підльоту до переднього краю траншей потрапляє у зону дії першого РЕБу. І якщо він вчасно не відчує проблем з управлінням чи не встигне вжити потрібних заходів, він залітає у ближню зону ураження засобу радіоелектронної боротьби і повністю втрачає зв'язок з апаратом і можливість керувати ним. Якщо у цьому БПЛА використовуються лише класичні, описані в огляді джерел, засоби забезпечення захисту каналу зв'язку, це буде означати неодмінну втрату безпілотного апарату і, найвірогідніше, неуспішне завершення операції із втратою обладнання.

Тут також можемо зазначити кілька важливих моментів, які можна зауважити із схеми і моделювання даних трьох різних ситуацій і які доводять актуальність та перспективність пропонованого нами методу захисту.

Перший із них – поліпшення параметрів класичних методів захисту каналу зв'язку БПЛА, такі як збільшення потужності передавачів пульта, збільшення коефіцієнту підсилення приймача апарату, збільшення потужності завадостійкого коду тощо, покращить стійкість безпілотника до ворожих засобів лише на якийсь певний рівень. Це змінить конфігурацію зон ураження засобу РЕБ

для цього безпілотника, вони стануть меншими завдяки деякому підвищенню завадостійкості каналу зв'язку, що дасть змогу підлітати до захищених ним позицій ближче, але завжди існуватиме така зона дії, залетівши за межу якої апарат втратить зв'язок зі станцією, і оператор не зможе передбачити, коли цей момент настане.

Другий важливий момент – оператор дрону, особливо під час розвідувального польоту, не має такої схеми, як зображено на рисунку, тобто в нього немає інформації ні про конфігурацію оборонних рубежів противника, ні про розташовані там засоби, і оператор не знає наперед, де є чи можуть бути засоби РЕБ противника, тому дуже часто втрата зв'язку із дроном відбувається непередбачено і стрімко, що в більшій частині випадків означає втрату обладнання.



Можливі варіанти роботи БПЛА в умовах складної електромагнітної обстановки

Для цієї схеми були використані такі умовні позначення:

 – особовий склад противника

 – певні засоби противника (наприклад, міномет)

 – засоби РЕБ противника

 – наш керований безпілотний літальний апарат

 – ближня зона дії РЕБ (повний вивід із ладу каналу зв'язку БПЛА)

 – дальня зона дії РЕБ (перебої і завади у каналі зв'язку БПЛА)

Тому для розв'язання цих проблем і виходу з критичної ситуації, коли ми втратили зв'язок з апаратом, що вже відлетів на значну відстань або перебуває на підконтрольній ворогу території, пропонується такий метод захисту стійкості каналу зв'язку як повернення апарату під час зникнення зв'язку із пультом за зворотним маршрутом, таким самим, як той, за яким наш апарат залетів у зону, де зник зв'язок. Він полягає в тому, що під час польоту бортова система БПЛА з певною визначеною частотою відстежує переміщення апарату і записує маршрут у пам'ять як дискретну вибірку.

Щоб реалізувати такий метод, для кожної із можливих осей переміщення записуємо координати в певний момент часу як функцію від часу x(t), y(t), z(t). Другий параметр моніторингу – якість зв'язку. Потрібно також фіксувати якість зв'язку у тій чи іншій координаті і фіксувати, коли є факт зниження якості зв'язку для того, щоб розуміти, коли ми потрапили під вплив засобу придушення і треба переключатися із моніторингу на алгоритм повернення назад. Для цього потрібно вести запис параметрів зв'язку як дискретної функції. Тут вже є два можливі варіанти: можна записувати якість зв'язку як функцію від координат f(x,y,z) або записувати якість зв'язку як функцію від часу f(t) із наступною синхронізацією в часі між функціями запису координат і запису якості зв'язку. Враховуючи особливості функціонування запам'ятовувальних пристроїв у цифрових системах, а також принцип роботи арифметично-логічного пристрою, на яких базуються мікропроцесори (чи, наприклад, мікроконтролер із вбудованою пам'яттю), більш доцільним і оптимальним у реалізації виглядає другий варіант запису даних розміщення і якості зв'язку – як двох функцій часу із синхронізацією за часом. Таку синхронізацію дуже легко організувати – достатньо запустити алгоритм моніторингу і запису одночасно та зберігати їх в одному масиві даних. Наприклад, можна організувати сховище польотних даних в умовний масив значень "flight_data[]", який матиме такі параметри:

flight_data[time] flight_data[x] flight_data[y] flight_data[z] flight_data[link_q].

Тоді дані, збережені у ньому, матимуть такий вигляд:

Приклад організації запису даних для методу повернення

flight_data[time]	flight_data[x]	flight_data[y]	flight_data[z]	flight_data[link_q]
0,1	1	2	1	95 %
0,2	2	5	2	95 %
0,3	2	9	3	85 %
0,4	2	13	3	90 %
…	…	…	…	…
T_n	X_n	Y_n	Z_n	Q_n

Таким способом ми отримаємо масив даних за певний останній час польоту і зможемо аналізувати його або в режимі реального часу, або з невеликою затримкою задля виявлення таких позаштатних ситуацій як, наприклад, значне зниження якості зв'язку чи раптове повне зникнення зв'язку. Якщо така ситуація виникне, маючи такий масив даних, ми зможемо передавати дані польоту і координат у зворотному порядку на контролер управління безпілотним апаратом та ініціювати його повернення у зворотному порядку.

Такий підхід має низку переваг – у звичайному режимі алгоритм не втручається у роботу безпілотного апарату, а тільки здійснює моніторинг його параметрів і записує потрібні з них у пам'ять, що дає можливість зберегти продуктивність системи керування БПЛА і не викликати затримок і збоїв у його роботі. Друга перевага – якщо ми записуватимемо параметри польоту апарату за його інерційними показниками, без прив'язки до зовнішніх параметрів та сигналів, які можуть бути скомпрометовані, наш метод буде стійким до будь-яких засобів радіоелектронної боротьби, в тому числі GPS-спуфінг, оскільки опиратиметься на фізичні показники польоту. Третя перевага – повернення зворотною траєкторією, аналогічною траєкторії підльоту, дає можливість дістатися точки задовільного зв'язку найкоротшим шляхом, порівняно із стандартною процедурою "повернення додому", яка інколи наявна у базовому програмному забезпеченні польотних контролерів і полягає у поверненні прямою траєкторією до точки запуску, ігноруючи всі маневри і рухи до цього.

Такі переваги і можливості пропонованого методу доводять його високу перспективність впровадження і доцільність подальшої роботи та практичних розробок щодо розвитку і реалізації цієї ідеї у фізичний пристрій для покращення його характеристик.

Висновки

У статті проведено огляд та аналіз методів і засобів захисту радіопередачі та забезпечення стабільності зв'язку. Розглянуто шифрування, частотне переплутування, використання спрямованих антен, розподілені радіомережі, маскування передання даних та завадостійке кодування.

Внаслідок аналізу можливостей використання тих чи інших методів захисту радіозв'язку в контексті їхнього застосування у БПЛА на основі наведених публікацій можна зробити висновки, що для забезпечення стабільності та захисту радіозв'язку в умовах складної електромагнітної обстановки, зокрема захисту зв'язку від електромагнітного придушення, найбільш доцільно використовувати комплексний підхід до питання захисту радіозв'язку. Основними методами покращення доступності та підвищення відмовостійкості систем керування БПЛА є використання оператором спрямованих антен із високим коефіцієнтом підсилення, застосування надійного завадостійкого кодування та методів переналаштування частоти. Поряд з цим було виявлено такий аспект, що у деяких випадках вказаних заходів недостатньо за будь-яких умов, тому є гостра потреба у створенні методу для відновлення втраченого зв'язку.

Для випадків повної і раптової втрати зв'язку, непередбачуваності електромагнітної обстановки в потенційній зоні роботи БПЛА було розроблено, обґрунтовано і рекомендовано метод і алгоритм для відновлення працездатності систем зв'язку і керування БПЛА, який полягає у поверненні апарату в зону, де був зв'язок задовільної якості по тій самій траєкторії, що й траєкторія підльоту у зону його зникнення. Для цього здійснюється моніторинг якості зв'язку і запис польотних даних з інформацією про пройдену апаратом траєкторію, а під час виявлення втрати зв'язку записана траєкторія польоту передається у польотний контролер і задіюється алгоритм зворотного повернення аж до моменту, коли БПЛА не прийме стабільний сигнал від пульта керування свого оператора.

Запропонований метод має значні переваги перед наявними і буде основою для подальших досліджень та створення покращених засобів забезпечення стабільності і захисту радіозв'язку в умовах складної електромагнітної обстановки.

Список літератури

1. Burlyai I. V. Systems of Radio Communication and Their Application by the Emergency Rescue Service / I. V. Burlyai, B. B. Orel, O. M. Dzhulai: Guide. Chernihiv: RVK "Desnianska Pravda", 2007. 288 p. ISBN 978-966-502-351-7. Available at: https://www.academia.edu/10574082/Системи_радіозв'язку_та_їх_застосування_оперативно_рятувальною_службою (Accessed: 20 February 2024).

2. Lyashuk O. M. MHED – Highly Effective Data Protection Method Based on Multilayer Hybrid Encryption // Bulletin of the National Technical University of Ukraine "KPI". 2014. Issue 56. P. 144–151. DOI: 10.20535/RADAP.2014.56.144-151

3. Hryb D. A. Principles, Methods and Technologies of Conducting Armed Struggle, Managing Forces and Means in Conditions of Active Information Confrontation of the Conflicting Parties / D. A. Hryb, B. O. Demidov, Yu. F. Kucherenko, A. M. Tkachov, T. V. Kuleshova // Science and Technology of the Air Forces of the Armed Forces of Ukraine. 2019. Volume 1, No. 43. P. 12—22. DOI:10.30748/nitps.2019.34.02

4. Mao V. Modern Cryptography: Theory and Practice. M.: Publishing House "Williams", 2005. 763 p. ISBN 5-8459-0847-7

5. Hudaverdova A. O. Information War Today and Possible Methods of Fighting. Information Aggression of the Russian Federation Against Ukraine: materials of the scientific seminar of KhNU PS named after I.Kozhedub, 21.10.2020. Kharkiv: KhNU PS named after I. Kozhedub, 2020. P. 1—5. Available at: https://www.hups.mil.gov.ua/assets/doc/science/stud-conf/suchasna-vijna-gumanitarnij-aspekt-21-10-2020/24.pdf (Accessed: 20 February 2024).

6. Kubrak O. M. Methodology of Radio Suppression of Radio Communication Systems with Noise-Like Signals / O. M. Kubrak, P. S. Borisov // Bulletin of ZHDTU. Series: Technical Sciences. 2014. No. 2. P. 37–41. ISSN 1728-4260. Available at: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/2181/15.pdf?sequence=1&isAllowed=y (Accessed: 20 February 2024).

7. Dzyaylo V. V. Improvement of characteristics of radio communication channels with frequency multiplexing: author's abstract. master's degree: 8.05090103 – radio electronic devices, systems and complexes / V. V. Dzyaylo; Ternopil National Technical University named after Ivan Puluj. Ternopil: TNTU, 2017. 7 p. Available at: https://elartu.tntu.edu.ua/bitstream/123456789/19322/1/aref_dziailo.pdf (Accessed: 20 February 2024).

8. Vasylenko S. V. Radio communication systems with pseudorandom retuning of the operating frequency // Electronic scientific professional publication-journal Problems of Telecommunications. 2016. No. 1 (18). P. 91–100. Available at: https://pt.nure.ua/wp-content/uploads/2020/01/161_vasilenko_pprch.pdf (Accessed: 20 February 2024).

9. Belokurskyi Yu. P. Principles of Building a Radio Electronic Protection System for Units of the National Guard of Ukraine During the Execution of Tasks / Yu. P. Belokurskyi, O. Yu. Iokhov, V. E. Kozlov, O. O. Shcherbina // Systems of Armament and Military Equipment. 2017. Volume 4, No. 52. P. 73–80. ISSN 1997-9568. Available at: https://www.hups.mil.gov.ua/hups/periodic-app/article/18377 (Accessed: 20 February 2024).

10. Ilyinov M. D., Gursky T. G., Borisov I. V., Grytsenok K. M. Lines of radio communication and antenna devices: educational manual. Kyiv: Military Institute of Telecommunications and Informatization, 2018. 249 p. ISBN 978-966. Available at: https://sprotyvg7.com.ua/wp-content/uploads/2023/05/антениілінії.pdf (Accessed: 20 February 2024).

11. Ivanenko S. A. Determination of unoccupied frequency channels in cognitive radio networks by methods of detection and recognition of signals under conditions of a priori uncertainty: dissertation of candidate of technical sciences: 05.12.17 / Kharkiv National University of Radio Electronics. Kharkiv, 2019. 156 p. Available at: https://nure.ua/wp-content/uploads/2018/Dissertation/dyssertatsyia-yvanenko-21.03.19-ukr.pdf (Accessed: 20 February 2024).

12. Dumitrash V., Bondarenko O., Dumitrash O., Hetman A. Analysis of the development directions of NATO radio communication systems: electronic journal Ukrainian Military Page. 2020. Available at: https://www.ukrmilitary.com/2020/08/signal.html (Accessed: 20 February 2024).

13. Shishatsky A. V. Methodology for managing parameters of multi-antenna systems with noise-like signals / A. V. Shishatsky, K. N. Grytsenok, V. K. Chumak, A. A. Zavada // Systems of management, navigation and communication. Collection of scientific works. 2017. Volume 3, No. 43. P. 143–145. ISSN 2073-7394. Available at: https://journals.nupp.edu.ua/sunz/article/view/344/311 (Accessed: 20 February 2024).

14. Karpukov L. M., Shchekotykhin O. V., Savchenko D. K. Improved method and device for masking confidential information. Radio technical fields, signals, devices and systems: materials of the International scientific-practical conference. Zaporizhzhia: ZNTU, 2019. P. 213–215. Available at: https://ela.kpi.ua/bitstream/123456789/35805/1/RTPSAS_2019_s8_t01.pdf (Accessed: 20 February 2024).

15. Vovchuk D. A. Simulation of a digital information transmission system using chaotic masking. Information technologies and control systems. 2013. Issue 13. P. 55–57. DOI: https://doi.org/10.15587/2312-8372.2013.18416

16. Politansky L. F. Continuous and pulse synchronization of Chua's generators [Text] / S. D. Galyuk, O. M. Eliashiv, L. F. Politansky, N. Ya. Kushnir, V. S. Tanasyuk // Technology and design in electronic equipment. 2012. No. 1. P. 21–26. Available at: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/51644/05-Eliyashiv.pdf?sequence=1 (Accessed: 20 February 2024).

17. Banket V. L., Ivashchenko P. V., Ishchenko M. O. Noise-resistant coding in telecommunication systems: educational manual. Module 4. 2011. 254 p. Available at: https://duikt.edu.ua/uploads/l_265_53269880.pdf (Accessed: 20 February 2024).

18. Horlynskyi B. V. Methods of ensuring the reliability of information in wireless data transmission devices due to adaptive coding: author's abstract. dis. candidate of technical sciences: 05.03.06. Kyiv, 2019. 20 p. Available at: https://itgip.org/wp-content/uploads/2020/01/aref1487.pdf (Accessed: 20 February 2024).

METHODS AND MEANS OF ENSURING STABILITY AND PROTECTION OF RADIO COMMUNICATIONS IN A COMPLEX ELECTROMAGNETIC ENVIRONMENT

R. Kuten, O. Syniavskyi

Lviv Polytechnic National University,
Department of Information Protection

The article contains a review of a wide range of methods and means to ensure the stability of communication and protection of radio transmissions, including encryption, frequency hopping, the use of directional antennas, masking, and interference-resistant coding.

Based on the conducted review and analysis, conclusions were made about the possibility of applying these methods and means of protection in popular unmanned devices today. Aspects of protection that were not covered by classical protection methods were identified. A method for improving the fault tolerance and availability of the UAV communication channel is proposed, even for working conditions under the influence of electronic warfare means.

The conclusions and recommendations made open up prospects for further research in this direction and will significantly increase the "survivability" of unmanned devices.

Keywords: communication channel protection, distributed radio networks, directional antennas, frequency hopping, interference-resistant coding, parameter monitoring, EW.