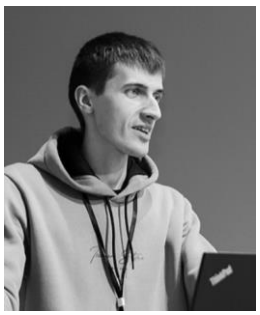
© Kuten R., Akhmedova A. Enhancing the level of protection and viability of unmanned aviation devices // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 88-94. ©

DOI: 10.18372/2225-5036.30.18609

ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ТАЖИТТЄЗДАТНОСТІ БЕЗПІЛОТНИХ АВІАЦІЙНИХ ПРИСТРОЇВ

Роман Кутень, Аліна Ахмедова

Національний університет «Львівська політехніка»



КУТЕНЬ Роман Богданович, аспірант
Рік та місце народження: 1996 рік, м. Львів, Львівська область, Україна.
Освіта: Національний університет «Львівська політехніка».
Посада: асистент кафедри «Захист інформації» Національного університету «Львівська політехніка».
Наукові інтереси: інформаційна безпека, вбудовані системи, мікропроцесорні пристрої, захист каналів бездротового зв'язку.
Публікації: більше 8 публікацій, серед яких наукові статті та тези і матеріали доповідей на конференціях.
E-mail: roman.b.kuten@lpnu.ua.
Orcid ID: 0000-0002-5688-2976.

АХМЕДОВА Аліна Самедівна, студентка
Рік та місце народження: 2004 рік, смт. Магерів, Львівська область, Україна.
Освіта: Національний університет «Львівська політехніка».
Посада: студентка спеціальності «Кібербезпека» Національного університету «Львівська політехніка».
Наукові інтереси: інформаційна безпека, вбудовані пристрої, захист каналів бездротового зв'язку.
E-mail: alina.akhmedova.kb.2021@lpnu.ua.
Orcid ID: 0009-0005-4743-7140.

Анотація. *За сучасного розвитку інформаційних технологій все більшого поширення набувають засоби із дистанційним керуванням. Їхнє поширення зумовлене в першу чергу їх основною перевагою – можливість ведення спостережень чи виконання якихось операцій в місцях, небезпечних або й зовсім не придатних для перебування там людини. Одним із таких застосувань є використання безпілотних пристроїв під час проведення військових операцій, що дозволяє оператору знаходитися у відносній безпеці. Таке використання безпілотних систем, в свою чергу, спонукає створення і розвиток методів протидії таким системам, виведенням з ладу каналів зв'язку та керування, або виявлення і локалізації розташування оператора. Для цього існує широкий спектр засобів радіоелектронної розвідки, радіоелектронної боротьби, пеленгаційні станції, тощо. Об'єктом даного дослідження є завдання підвищення рівня захищеності безпілотних засобів і комплексів проти засобів радіоелектронної боротьби противника та завдання відновлення зв'язку і працездатності апарату при збоях у його роботі внаслідок випадкових перешкод, чи дій зловмисника. Стаття містить стислий огляд сучасних методів і засобів, що використовуються для забезпечення захисту радіопередачі і аналіз можливості їхнього застосування у малогабаритних безпілотних авіаційних системах, які зараз найбільше використовуються військовими на поточному етапі протистояння ворогу. На основі чого було запропоновано спосіб реалізації заходів захисту зв'язку для відновлення працездатності безпілотного пристрою, описано принцип його функціонування. Основною актуальною проблемою, покладеною в основу дослідження є недостатня захищеність систем зв'язку та навігації у цивільних рішеннях та електронних пристроях, що зараз активно застосовуються для побудови використовуваних у військових та розвідувальних операціях безпілотних апаратів. Отримані результати дадуть змогу підвищити захищеність безпілотних систем за рахунок застосування засобів частотного переналаштування для покращення стабільності і надійності зв'язку у системах керування БПЛА.*

Ключові слова: *безпілотний пристрій, захист інформації в каналах зв'язку, частотне переплутування, пеленгація, радіо-електронна боротьба, «дрон»***.**

Постановка проблеми

За сучасних умов розвитку інформаційних технологій, та засобів бездротового зв'язку зокрема, радіозв'язок став життєво важливою ланкою для багатьох засобів та технологій якими користується людство. Особливо чутливими до питання захищеності і якості зв'язку є сучасні безпілотні пристрої із дистанційним керуванням, які в даний час стрімко розвиваються і займають все нові ніші у повсякденній людській діяльності, від моніторингу стану конструкцій і контролю території аграріїв, аж до пошуково-рятувальних та військових операцій [1-4].

Одним із видів таких дистанційно керованих апаратів є безпілотні авіаційні комплекси. Безпілотна авіація в теперішній час активно розвивається та інтегрується до глобальної авіаційної системи загалом. Розроблення, випробування та використання безпілотних авіаційних систем проводиться в наш час майже в усіх країнах світу.

Актуальність дослідження питання захисту систем керування і зв'язку із БПЛА зумовлює також той факт, що саме зараз, зокрема під час захисту України від нападу агресора безпілотні технології набувають все більшого значення у бойових діях. Кожного дня у зведеннях новин і подій із фронту можна спостерігати роботу як ударних, так і розвідувальних дронів, з чого можна зробити висновок про багатократне підвищення їхньої ролі у сучасних воєнних конфліктах і безумовно такі апарати зараз мають значний вплив на тактику ведення сучасних бойових дій, при цьому цей вплив лише збільшується і в даний час складно дати точну оцінку перспективам їхнього розвитку та використання у майбутньому.

Хоча в даний час вже існує низка потужних ударних і розвідувальних безпілотних комплексів, найвідоміші з яких вітчизняні БПЛА «Лелека», «Фурія», «Валькірія», легендарний турецький «TB-2 Bayraktar», нажаль, кількість а інколи й можливість використання таких потужних засобів промислового рівня, порівняно із запитами на них у українського війська є недостатньою. Подекуди є потреба у компактних безпілотних комплексах або в максимально недорогих засобах, призначення яких доставка корисного навантаження «в один кінець». Тому переважна більшість безпілотних засобів розвідки і ураження являє собою малогабаритні і малопотужні комплекси, складені ентузіастами із запчастин, призначених в першу чергу для цивільного використання, таких як SpeedyBee, Arduino, тощо. Прикладом таких БПЛА є ударні FPV-дрони, що виготовляються за програмою «Народний дрон» від Міністерства цифрової трансформації України. В таких реаліях перед нами постає проблема недостатньої захищеності таких засобів, а також певного обмеження їхніх характеристик у визначених цивільним законодавством межах. Ця проблема гостро потребує вирішення, оскільки це призводить до значних втрат безпілотної техніки і засобів у випадку використання противником навіть компактних і простих засобів РЕБ.

Аналіз останніх досліджень і публікацій

На актуальність даного питання вказують і інші автори і дослідники, зокрема Станіслав Слободяник, та співавтори у роботі [5] висвітлили поточне зростання і приватного і державного інтересу до БПЛА-систем, зокрема у військовій сфері, де держава виступає основним замовником, споживачем і інвестором. Висвітлюється також стрімкий історичний розвиток та оцінені перспективи майбутнього розвитку використання БПЛА, включаючи автономні системи та рої дронів.

Одними із найбільш актуальних напрямків сучасних досліджень з метою покращення характеристик стійкості роботи як самого апарату, так і його систем навігації є розробки систем навігації на основі штучного інтелекту, моделей нечіткої логіки, тощо. [3-6]. Такі системи дозволяють працювати апарату в автономному режимі і виконувати певні задачі в автономному режимі польоту. Такі засоби частково задовольняють виконання поставлених перед БПЛА задач, та підвищують можливості управління безпілотними апаратами, в тому числі у випадку втрати зв'язку. Але ці рішення не задовольняють задачу захисту самого каналу зв'язку із апаратом і не забезпечують виконання завдань, які потребують постійного моніторингу отримуваних від БПЛА параметрів чи своєчасного коригування його роботи оператором, що є дуже суттєвим обмеженням для використання БПЛА у військовій сфері, оскільки більшість військових застосувань БПЛА все ж не є автономними, а майже повністю керованими оператором. [7]

Варто також вказати, що активна робота по виготовленню, розробці і вдосконаленню безпілотних систем проводиться постійно, про що свідчить ряд нових розроблених українських БПЛА, включаючи такі моделі як "Берегиня", "Грім", "Фурія", RAM UAV, "Демон-Е", "Демон-Т", "Велика Химера", F-2M, "Горлиця", "Мисливець", "Сокіл-300" – описані розробки включають в себе як розвідувальні дрони, так і навіть ударні їх варіанти. Українські БПЛА мають чималий інноваційний потенціал, який багато чим зумовлений здатністю адаптуватися до складних метеоумов та змін електромагнітної обстановки, а також можливістю виконувати різноманітні функції, від розвідки до ударних операцій.

Мета та постановка завдання

Таким чином, мета роботи – покращення рівня захищеності каналу зв'язку БПЛА від завад та навмисного придушення його зловмисником, та покращення життєздатності безпілотних пристроїв та систем. Завдання дослідження, яке забезпечить досягнення поставленої мети – аналіз можливості застосування сучасних методів і засобів в області захисту каналів радіозв'язку у поширених зараз безпілотних пристроях невеликих розмірів, побудованих на базі рішень для цивільного або подвійного призначення шляхом виявлення потенційних механізмів оптимального їхнього застосування у таких малогабаритних БПЛА. У результаті це дасть змогу підвищити ефективність використання БПЛА, дозволить зменшити втрати апаратури за рахунок підвищення їхньої «живучості» в умовах роботи під впливом засобів радіо-електронної боротьби (РЕБ) та радіо-електронної розвідки (РЕР).

Виклад основного матеріалу дослідження

Питанням захисту каналів зв'язку присвячено чимало робіт і велика кількість науковців і інституцій провадить діяльність у такій галузі, для більш всебічного огляду, в роботі розглянемо вибірку актуальних наукових праць, які висвітлюють новітні підходи і розробки щодо захисту зв'язку загалом [8-14] і проаналізуємо можливості і механізми їхнього можливого використання у безпілотних системах згідно поставлених нами задач. Загалом, основними поширеними методами захисту інформації у радіоканалі є:

1. Шифрування даних при передачі дає змогу захистити інформацію від розкриття вмісту навіть при випадку її перехоплення зловмисником [9];

2. Використання спрямованих антен: при випромінюванні спрямовані антени дозволяють зосередити радіосигнал в певному напрямку, що збільшує дальність та якість зв'язку, а на приймальній стороні напрямлена антена також «відсікає» сторонні джерела сигналу [8, 10, 16];

3. Використання завадостійкого кодування: – цей метод полягає у впровадженні у інформаційне повідомлення кодових комбінацій із такою кодовою відстанню, яка дозволить нам виправити помилки передачі, що можуть виникати у реальних каналах зв'язку. Особливо корисна така його властивість під час користування БПЛА на дальній відстані, коли зв'язок із апаратом може не бути достатньо якісним для безпомилкового детектування сигналу.[13, 14]

4. Частотне переналаштування: Цей метод полягає у зміні частот передавання, що ускладнює процес пеленгації та моніторингу параметрів сигналу зловмисником [11, 12].

Оцінювальними критеріями для виявлення потенційної можливості застосування того чи іншого засобу у популярних БПЛА, згідно мети статті, було обрано: можливість застосування цього чи іншого методу в умовах бойових дій, потреба цих методів у обчислювальних потужностях, можливість їхньої реалізації як малогабаритного вбудованого пристрою.

Шифрування

В контексті захисту зв'язку із безпілотними апаратами криптографія дозволяє вирішити ряд завдань, серед яких – захист цілісності передаваної інформації та забезпечення виконання апаратом команд лише від легітимного передавача (тобто автентифікація оператора). Зокрема, у роботі [15] було запропоновано варіант так званого «навісного» захисту, застосування якого не передбачає значного втручання у системи і пристрої БПЛА, за рахунок впровадження шифратора/дешифратора, як проміжної ланки зв'язку (рис.1).

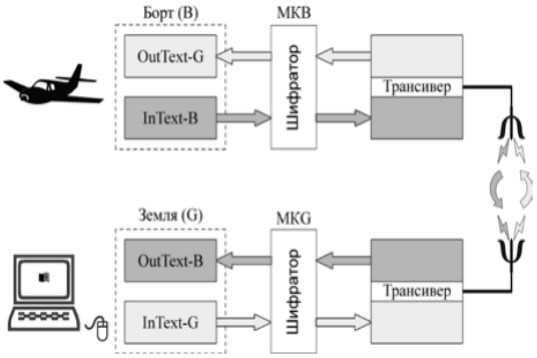


Рис.1 Схема включення шифратора у канал зв'язку БПЛА [15]

Ця система захисту, за дослідженнями та оцінками автора дозволяє забезпечити належний захист конфіденційності і цілісності інформації командного модулю та модулю телеметрії без суттєвого зменшення характеристик БПЛА загалом.

Можна дійти висновку, що шифрування є доцільним засобом захисту даних у системах зв'язку безпілотних пристроїв і надає нам можливість забезпечити конфіденційність і цілісність даних. Але криптографічні засоби мають обмеження в питаннях захисту доступності, відповідно оператор не захищений від повної втрати зв'язку, просторового зашумлення, чи випадкових спотворень сигналу.

Використання спрямованих антен

Спрямовані антени – це антени, які мають властивість зосереджувати випромінювання та/або прийом радіохвилі в певному напрямку, зменшуючи за рахунок цього втрати його потужності і відповідно збільшуючи дистанцію передавання сигналу [16]. За рахунок використання у системах зв'язку спрямованих антен можна досягти:

- зниження ймовірності перехоплення сигналу сторонніми;
- зниження ймовірності придушення сигналу;
- зниження ймовірності виявлення сигналу;
- зниження ймовірності локації сигналу (пеленгація);
- зниження ймовірності ідентифікації сигналу.

Відмінності між спрямованими антенами і всенаправленими полягають у геометрії елементів антени, її розмірах, тощо (рис. 2).

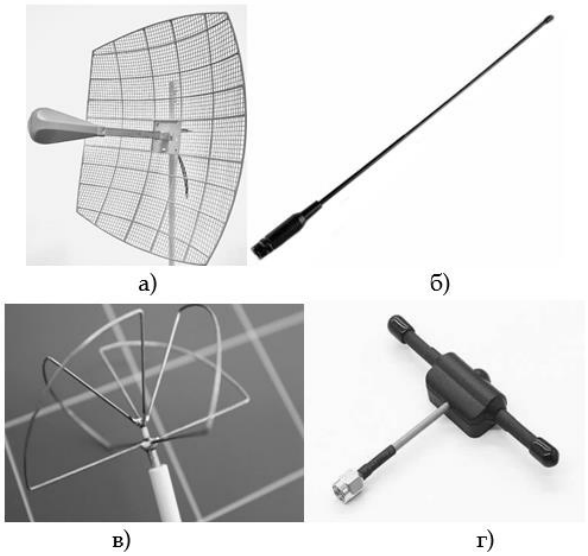


Рис.2 Загальний вигляд декотрих видів антен: а – параболічна (вузькоспрямована), б – штирова (має всенаправлену дію), в – чотирипелюсткова «lollipop» (має всенаправлену дію), г – дипольна (має всенаправлену дію).

Вузькоспрямовані антени порівняно із всенаправленими мають вищий коефіцієнт підсилення антени, що дозволяє збільшити дистанцію прийому-передачі в рази. Також, коли вузькоспрямована антена працює на прийом сигналу – це дозволяє фізично «відсікати» сигнали зашумлення та сторонні радіозавади при умові їхнього розташування не за напрямком прийому. Але, не зважаючи на такі переваги, використання вузькоспрямованих антен має ряд дуже суттєвих обмежень, які за певних умов унеможливлюють повноцінне їх використання. Основне обмеження – такі антени вимагають точного налаштування та орієнтування на іншого абонента зв'язку, в іншому випадку належного прийому сигналу не буде. Це загалом досить складне завдання в умовах зони бойових дій і надзвичайно складне завдання, якщо говорити про приймальну антену,

встановлену безпосередньо на засобах БПЛА, які під час роботи можуть здійснювати довільні переміщення, оберти за напрямками сторін світу і що найскладніше – при маневруванні апарати змінюють кути нахилу корпусу відносно лінії горизонту: кут тангажу (вперед-назад) та кут крену (вправо-вліво), які при різких маневрах можуть сягати значень понад 45º. При таких положеннях вузькоспрямована антена буде орієнтована в небо чи землю і не забезпечить прийом сигналу. Також ці антени більше вразливі до зміни умов розповсюдження радіохвиль, таких як рефракція, дифракція, відбиття, розсіювання та інтерференція, тощо [16].

Як висновок, можна зазначити, що хоча застосування вузькоспрямованих антен дозволяє збільшити ефективність, дальність та захищеність зв'язку, зокрема, не допускає перехоплення даних зловмисником за рахунок зосередження енергії хвилі у напрямку передачі, використання цієї технології у системах керування БПЛА має значні обмеження. Для покращення характеристик передачі даних у каналі керування безпілотними апаратами доцільно скористатися такою комбінацією: на стороні апарату використовується всенаправлена антена для забезпечення стабільного зв'язку в незалежності від положення апарату; на стороні пульта керування оператора, у свою чергу, використовується вузькоспрямована антена, орієнтована в напрямку роботи апарата. Такі заходи дадуть змогу збільшити дальність зв'язку при однаковій потужності передавача і при цьому уникнути втрати зв'язку із апаратом при виконанні ним тих чи інших маневрів.

Використання завадостійкого кодування

Завадостійке кодування є важливим інструментом в сучасних системах радіозв'язку. Він дозволяє виявити та виправити помилки, що виникають під час передачі даних [13]. Завадостійке кодування високого порядку використовується для забезпечення високої надійності передачі даних. Однак, використання такого типу кодування вимагає значно більше ресурсів при обробці даних і може знижувати швидкість передачі даних, це зумовлено необхідністю передачі додаткових бітів інформації (контрольних бітів). Для вирішення такої проблеми і «балансування» між завадостійкістю і надлишковістю кодів на оптимальному рівні у дослідженні [14] автором було представлено метод кодування інформації в системах передачі інформації, який базується на адаптації різноманітних кодових структур. Особливість цього методу полягає в застосуванні різних за структурою завадостійких кодів за різної ситуації у приймально-передавальному тракті.

Можна підсумувати, що завадостійке кодування високого порядку із виправленням помилок є важливим компонентом радіокомунікаційної системи, який допомагає забезпечити надійну і стабільну передачу даних, особливо на дистанціях передачі, близьких до максимальної. Однак, зміна алгоритмів кодування в окреслених нами умовах, а саме при використанні вже наявних безпілотних засобів, вимагає щонайменше заміни модулів передавачів, оскільки у типових застосунках (зокрема популярних передавачах сімейства «TBS Crossfire») вже застосовуються власні кодові конструкції, «зашиті» у програму заводом виробником. Для застосування інших методів необхідна прошивка мікропрограми передавачів, або навіть розроблення принципово іншого модуля-передавача під той чи інший алгоритм. При цьому, за недостатності кодової відстані і незадовільної надійності алгоритму відновлення помилок базових пристроїв оптимальний вихід із такої ситуації є – можна застосувати підхід, аналогічний зображеному на рис.1, де замість шифратора буде знаходитися пристрій кодування, який в сучасних реаліях може являти собою логічний пристрій на базі мікроконтролера і реалізувати безліч інших додаткових функцій.

Частотне переплутування

Частотне переплутування – метод захисту каналу зв'язку, який ґрунтується на регулярній заміні несучої частоти передачі сигналу, що дозволяє завадити його перехопленню, придушенню, чи іншому перешкоджанню процесу передачі. Методи частотного переплутування дозволяють змінювати частоту передачі сигналу відповідно до певного алгоритму або правила [11, 12]. Ці методи можна реалізувати такими способами, як:

- псевдовипадкове перелаштування робочої частоти;
- частотне стрибання;
- частотне розподілення;
- частотне кодування.

Можливість зміни робочої частоти є незамінним інструментом системи зв'язку орієнтованої на роботу з максимальною доступністю, оскільки у такому випадку у нас є можливість переключитися на іншу частоту, якщо противник виявить і придушить канал зв'язку на основній робочій частоті.

У роботі [17] також розглянуто питання захисту, який забезпечує нам регулярна зміна частот, незалежно від стану приймально-передавального тракту. Зокрема, використання підходу із постійним програмним перелаштуванням робочої частоти та використанням широкосмугових сигналів може значно ускладнити завдання радіоелектронної розвідки противника і дозволяє зменшити ймовірність виявлення та пеленгації сигналів, а також збільшити складність визначення структури системи зв'язку. При цьому при збільшенні швидкості зміни робочої частоти ймовірність контакту із засобом розвідки зловмисника зменшується, а при досягненні технічної швидкості пеленгації (швидкості перегляду діапазону частот засобом розвідки) зводиться практично до 0. Таким чином, при достатньо швидкому перелаштуванні частоти можна досягнути неможливості виявлення каналу зв'язку зловмисником. [17] Такий підхід дозволить зберегти значну перевагу в інформаційному просторі та забезпечити ефективне управління військовими операціями.

Пропонований концепт захисту БПЛА

Врахувавши параметри технологічних рішень, що використовуються у сучасних системах безпілотної аеророзвідки (такі продукти як "SpeedyBee", "TBS", "Happymodel", "TBS CrossFire", "Arduino Arduflight", тощо) та дані аналітичного огляду матеріалу, можна запропонувати метод перелаштування

частоти як найбільш вдалий і оптимальний для застосування його у БПЛА. Це зумовлено тим, що для більшості популярних моделей приймачів (наприклад сімейства "TBS CrossFire") є можливість задання значень частоти передачі сигналу на рівні користувацьких налаштувань, що не вимагає натискання кнопок, чи зміни фізичних параметрів якихось елементів мікросхеми, при цьому, для приймача типової цивільної робочої частоти 868 МГц, цю зміну можна провести в досить широкому діапазоні: від 860 МГц аж до 928 МГц і для приймача 5.8 ГГц: від 5705 МГц до 5945 МГц (рис. 3, 4).

Frequency Setting	Frequency	Max. power level	Settings locked	Operating frequency
868	868MHz	No limitations	no	860 - 885MHz
915	915MHz	No limitations	no	902 - 928MHz
868CE	868MHz, LBT technique	No limitations	no	860 - 885MHz
915C-Tic	915MHz	No limitations	no	915 - 928MHz
915FCC	915MHz	No limitations	no	902 - 927MHz
868 Race	868MHz	No limitations	no	860 - 885MHz
915 Race	915MHz	No limitations	no	902 - 928MHz

Рис. 3 Частотні характеристики приймачів сімейства «TBS CrossFire» 868 МГц [18]

Channel	1	2	3	4	5	6	7	8	
Band A	5865	5845	5825	5805	5785	5765	5745	5725	MHz
Band B	5733	5752	5771	5790	5809	5828	5847	5866	MHz
Band E	5705	5685	5665	5645	5885	5905	5925	5945	MHz
Airwave	5740	5760	5780	5800	5820	5840	5860	5880	MHz
Race Band	5658	5695	5732	5769	5806	5843	5880	5917	MHz

Рис.4 Частотні характеристики приймачів сімейства «TBS CrossFire» 5.8 ГГц [18]

Також в асортименті популярних засобів зв'язку для безпілотних систем наявні моделі, які здатні працювати у кількох частотних діапазонах, наприклад, 868 МГц та 2.4 ГГц, що дозволяє переналаштувати робочу частоту у значно ширшому діапазоні і тим самим збільшити надійність такої системи передачі, оскільки невеликі польові засоби РЕБ досить часто мають технічну можливість придушення лише певного набору використовуваних каналів та/або того чи іншого діапазону частот. В такому випадку навіть при виявленні і придушенні каналу зв'язку на одній робочій частоті у нас залишається резервний набір каналів на інших частотах.

Для цього у пристроїв такої конфігурації також передбачено кілька антенних портів, що дає можливість використання декількох антен для кожного частотного діапазону (рис. 5).

Керування і налаштування таких модулів зв'язку здійснюється через логічний інтерфейс, як правило це послідовний порт UART. Для локального зв'язку між модулями безпілотного апарату також застосовуються послідовні порти: UART чи SPI. Це означає, що за умови використання мікроконтролера із достатньою кількістю портів, можна використати його як своєрідний «бортовий комп'ютер» який буде відповідати за забезпечення безпеки та стабільності зв'язку без серйозних змін у апаратурі, а у випадку, якщо на борту існуючого безпілотного пристрою вже є передавач із підтримкою кількох діапазонів і кількох антен – ми можемо навіть модернізувати таким покращенням вже працюючий апарат.

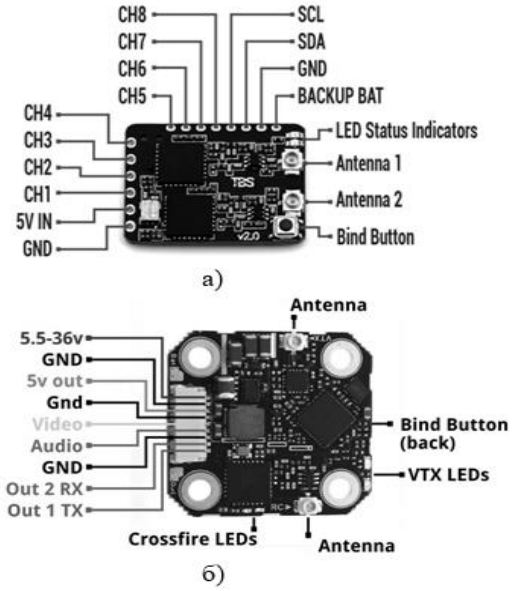


Рис.5 Схема і виводи кількадіапазонних передавачів (а – NanoDiversity, б – Sixty9) [18]

Підключивши такий мікроконтролер через послідовний порт до входу налаштування модуля зв'язку, можна з його допомогою автоматизувати переналаштування передавача згідно потрібного нам алгоритму. Підключивши його іншими незайнятими портами як проміжну ланку між контролером пристрою і модулем передавання (за прикладом способу підключення шифратора на рис.1), ми також відкриємо для себе можливість кодування та/або шифрування даних, до їх подання в передавач, що дозволить уникнути необхідності його заміни, чи прошивки і вирішить проблеми, описані під час огляду кодування.

Висновки. У даній статті було проведено детальний огляд та аналіз методів, засобів та інструментів, що спрямовані на захист бездротових комунікаційних каналів та забезпечення їх надійності. Серед розглянутих засобів були такі як криптографічне шифрування, частотне переналаштування, використання направлених антенних систем та кодування з можливістю виявлення і виправлення помилок.

В результаті аналітичної роботи було оцінено можливості застосування сучасних методів і засобів в області захисту каналів радіозв'язку у поширених зараз безпілотних пристроях невеликих розмірів, побудованих на базі рішень для цивільного або подвійного призначення та виявлено спосіб і механізм оптимального їхнього застосування у популярних зараз малогабаритних БПЛА, що дає нам змогу підвищити ефективність використання БПЛА та зменшити втрати апаратури за рахунок підвищення їхньої «живучості» в умовах роботи під впливом засобів радіо-електронної боротьби (РЕБ) та радіоелектронної розвідки (РЕР), а також дає підґрунтя для подальшої роботи в напрямку розв'язання проблеми недостатньої захищеності каналів зв'язку малогабаритних безпілотних пристроїв за умов їхнього нестандартного використання, та використання в умовах активного інформаційного протиборства.

Для найбільш оптимального використання ресурсів і одночасного забезпечення покращення ха-

рактеристик БПЛА запропоновано застосування методу частотного переналаштування, та надано практичну рекомендацію щодо його реалізації: на базі мікроконтролера із декількома послідовними портами вводу/виводу (UART, SPI, I2C), що дозволить з його допомогою адаптивно змінювати характеристики пристрою під час його роботи.

Запропонований підхід надасть нам такі переваги, як: відносно не висока вартості його реалізації, також, за певних умов, є можливості його впровадження у вже існуючі і працюючі системи без значних конструктивних змін, а також залишається потенційна можливість застосувати невикористані ресурси мікроконтролера для вирішення інших потрібних задач. А також це відкриває можливості для подальшої праці у цьому напрямку досліджень і розширення за рахунок таких вбудованих пристроїв функціоналу безпілотних систем у майбутньому.

Список літератури

[1]. Юн Х. М., Мединський Д. В. Використання безпілотних літальних апаратів в сільському господарстві. Високотехнологічні технології. 2017. № 4(36). С. 335-341. DOI: 10.18372/2310-5461.36.12232.

[2]. Лещенко Г. А., Мандрик Я. С., Стратонов В. М., Давидов С. А. Методи використання безпілотних літальних апаратів під час авіаційного пошуку та рятування. Високотехнологічні технології. 2021. № 3 (51). С. 271-280. DOI: 10.18372/2310-5461.51.15998.

[3]. Глотов В., Гуніна А. Аналіз можливостей використання безпілотних літальних апаратів для аерофотозйомки. Сучасні досягнення геодезичної науки та виробництва. 2014. № 2. С. 65-70.

[4]. Є.А. Дружинін, М.І. Ковалевський, О.К. Погудіна, В.О. Чарановський. Методи та інформаційні технології впровадження безпілотних літальних апаратів в повітряний простір України. Збройні системи та військова техніка. 2021. № 4(68). С. 84-90. DOI: 10.30748/soivt.2021.68.12.

[5]. Слободяник С., Петренко С., Цибізов А., Бондаренко Ю. Можливі шляхи розвитку перспективних українських систем БПЛА, з урахуванням сучасних світових тенденцій. Журнал наукових статей "Соціальний розвиток та безпека", Том. 13, № 3, 2023. С. 135-145. DOI: 10.33445/sds.2023.13.3.9.

[6]. Д. В. Стасенко, В. С. Яковіна. Аналіз існуючих методів та засобів поліпшення навігації БПЛА за допомогою штучного інтелекту. Науковий вісник НЛТУ України. 2023. Том. 33, № 4. С. 78-83. DOI: 10. 36930/40330411.

[7]. Кізло Л., Троценко О., Жук. О. Тенденції розвитку безпілотних літальних апаратів в Україні. Українські військові сторінки. 2021. Доступно за адресою: https: //www.ukrmilitary.com/2021/05/uav. html (Дата звернення: 17 лютого 2024).

[8]. І.В. Бурляй. Системи радіозв'язку та їх застосування оперативно-рятувальною службою / І.В. Бурляй, Б.Б. Орел, О.М. Джулай: Посібник. Чернігів: РВК "Деснянська правда", 2007. 288 с. ISBN 978-966-502-351-7. Доступно за адресою: https:// www. academia.edu/10574082/Системи_радіозв_язку_та_їх_застосування_оперативно_рятувальною_службою (Дата звернення: 25 лютого 2024).

[9]. О.М. Ляшук. MHED. Високоефективний метод захисту даних на основі багатошарового гібридного шифрування. Вісник Національного технічного університету України "КПІ". 14. Випуск 56. С. 144-151. DOI: 10.20535/RADAP.2014.56.144-151.

[10]. Д.А. Гриб. Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін / Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, Т.В. Кулешова // Наука і техніка Повітряних Сил Збройних Сил України. 2019. Том 1, № 43. С. 12-22. DOI: 10.30748/ nitps.2019.34.02.

[11]. Дзяйло В.В. Покращення характеристик каналів радіозв'язку з частотним мультиплексуванням: автореф. магістра: 8.05090103 - радіоелектронні пристрої, системи та комплекси "/ В.В.Дзяйло; Тернопільський національний технічний університет імені Івана Пулюя. Тернопіль: ТНТУ, 2017. 7 с. Доступно за адресою: https: // elartu.tntu.edu.ua / bitstream/123456789/19322/1/aref_dziailo.pdf (Дата звернення: 27 лютого 2024).

[12]. Василенко, С.В. Системи радіозв'язку з псевдовипадковим переналаштуванням робочої частоти / С.В. Василенко // Електронне наукове фахове видання-журнал Проблеми телекомунікацій. 2016. № 1 (18). С. 91-100. Доступно за адресою: https://pt. nure.ua/wp-content/uploads/2020/01/161_vasilenko_ pprch.pdf (Дата звернення: 4 березня 2024).

[13]. В.Л. Банкет, П.В. Іващенко, М.О. Іщенко. Завадостійке кодування в телекомунікаційних системах: навчальний посібник. Модуль 4. 2011. 254 с. Доступно за адресою: https://duikt.edu.ua/uploads/ l_265_53269880.pdf (Дата звернення: 10 березня 2024).

[14]. Б.В. Горлинський. Методи забезпечення достовірності інформації в безпроводових засобах передачі даних за рахунок адаптивного кодування: автореф. дис. кандидата технічних наук: 05.03.06. Київ, 2019. 20 с. Доступно за адресою: https://itgip. org/wp-content/uploads/2020/01 / aref1487.pdf (Дата звернення: 12 березня 2024).

[15]. Навроцький Д. Криптографічна система захисту радіоканалів БПЛА від несанкціонованого втручання // Український науковий журнал Інформаційна безпека, 2014, том. 20, випуск 3, С. 248-252.

[16]. М.Д. Ільїнов, Т.Г. Гурський, І.В. Борисов, К.М. Гриценок. Лінії радіозв'язку та антенні пристрої: навчальний посібник. Київ: Військовий інститут телекомунікацій та інформатизації, 2018. 249 с. ISBN 978-966. Доступно за адресою: https: // sprotyvg7.com.ua/wp-content/uploads/2023/05/антеніілінії.pdf (Дата звернення: 13 березня 2024).

[17]. Бігун Н., Грозовський Р. Оцінка розвідзахищеності системи зв'язку, побудованої на сучасних засобах радіозв'язку: Сучасні інформаційні технології в галузі безпеки та оборони, 2019, № 1(34), С. 53-58. DOI: 10.33099/2311-7249/2019-34-1-53-58.

[18]. TBS CROSSFIRE R/C System: Adaptive Long-Range Remote-Control System User Manual. 2022. p. 88. Доступно за адресою: https://www.team-blacksheep. com/media/files/tbs-crossfire-manual.pdf (Дата звернення: 17 березня 2024).

УДК 004.8; 004.75

Kuten R., Akhmedova A. Enhancing the level of protection and viability of unmanned aviation devices

Abstract. *With the modern development of information technology, remote control devices are becoming increasingly widespread. Their proliferation is primarily due to their main advantage - the ability to conduct observations or perform certain operations in places that are dangerous or completely unsuitable for human presence. One such application is the use of unmanned devices during military operations, which allows the operator to be in relative safety. Such use of unmanned systems, in turn, encourages the creation and development of methods to counter these systems, disabling communication and control channels, or detecting and locating the operator's location. For this, there is a wide range of electronic intelligence tools, electronic warfare, direction finding stations, etc. The object of this study is the task of increasing the level of protection of unmanned devices and complexes against enemy electronic warfare means and the task of restoring communication and functionality of the device in case of failures in its operation due to accidental obstacles or actions of the attacker. The article contains a brief overview of modern methods and means used to ensure the protection of radio transmissions and analyzes the possibility of their application in small unmanned aviation systems, which are now most used by the military at the current stage of confrontation with the enemy. Based on this, a method of implementing communication protection measures to restore the functionality of the unmanned device was proposed, the principle of its operation is described. The main relevant problem underlying the study is the insufficient protection of communication and navigation systems in civilian solutions and electronic devices that are now actively used to build unmanned vehicles used in military and reconnaissance operations. The obtained results will allow to increase the protection of unmanned systems by applying frequency retuning means to improve the stability and reliability of communication in UAV control systems.*

Keywords: *unmanned device, protection of information in communication channels, frequency confusion, direction finding, electronic warfare, 'drone'.*

Кутень Роман Богданович, аспірант, асистент кафедри захисту інформації Національного університету «Львівська політехніка».

Roman Kuten, postgraduate student, assistant of the Department of Information Protection of the Lviv Polytechnic National University.

Ахмедова Аліна Самедівна, студентка, кафедра захисту інформації Національного університету «Львівська політехніка».

Alina Akhmedova, student, Department of Information Protection of the Lviv Polytechnic National University.

Отримано *21 лютого 2023 року,* затверджено редколегією *1 квітня 2024 року*