Застосування частотного переналаштування для захисту безпілотних літальних апаратів

Application of the frequency-hoping for unmanned aerial vehicle protection

Роман Кутень
аспірант, асистент кафедри захисту інформації, e-mail: roman.b.kuten@lpnu.ua, ORCID: 0000-0002-5688-2976

Національний університет "Львівська політехніка", м. Львів, Україна

Roman Kuten
Ph.D student, Asistant of Data Protection Department, e-mail: roman.b.kuten@lpnu.ua, ORCID: 0000-0002-5688-2976

Lviv Polytechnic National University, Lviv, Ukraine

Received: April 10, 2024 | Revised: April 17, 2024 | Accepted: April 30, 2024

DOI: 10.33445/sds.2024.14.2.7

Мета роботи: дослідження можливостей імплементації методів та засобів захисту каналу зв'язку у малогабаритні і малопотужні безпілотні пристрої в контексті їхнього активного використання Збройними Силами України.

Метод: порівняльний аналіз та експеримент.

Результати дослідження: якісно визначено доцільність застосування методів частотного переналаштування та використання можливостей базових пристроїв, кількісно досліджено потенційні можливості для зміни частот і потужностей передавачів.

Теоретична цінність дослідження: дослідження було спрямовано на визначення оптимальних можливостей щодо застосування методів захисту каналу зв'язку враховуючи і застосовуючи базові засоби БПЛА.

Практична цінність дослідження: дана робота може виступати базою для подальших досліджень щодо покращення захисту каналу зв'язку безпілотних систем базового рівня, а безпосередньо отримані результати можуть бути вже використані для підвищення стійкості існуючих БПЛА.

Цінність дослідження: важливість цього дослідження і його результатів полягає у тому, що підвищення рівня живучості БПЛА на полі бою дає перевагу не тільки технічну (безпосередньо сам врятований БПЛА) а й дозволяє потенційно зберегти особовий склад, за рахунок наявності стабільного і стійкого засобу розвідки.

Тип статті: дослідницька.

Purpose: Investigation of the possibilities of implementing methods and means of communication channel protection in small-sized and low-power unmanned devices in the context of their active use by the Armed Forces of Ukraine.

Method: comparative analysis and experiment.

Findings: The expediency of applying frequency retuning methods and using the capabilities of basic devices has been qualitatively determined, the potential possibilities for changing frequencies and transmitter powers have been quantitatively investigated.

Theoretical implications: The research was aimed at determining the optimal possibilities for applying communication channel protection methods, taking into account and using the basic means of UAVs.

Practical implications: This work can serve as a basis for further research on improving the protection of the communication channel of basic level unmanned systems, and the results obtained can already be used to increase the resilience of existing UAVs.

Value: The importance of this research and its results lies in the fact that increasing the survivability of UAVs on the battlefield gives an advantage not only technical (directly the saved UAV itself) but also allows potentially saving personnel, due to the presence of a stable and resilient means of reconnaissance?

Paper type: research.

Ключові слова: дрон, захист зв'язку, частота, канал.

Key words: drone, communication protection, frequency, channel.

Вступ

У сучасному світі розвиток інформаційних технологій, та бездротових систем зокрема, вже набув такого рівня, що не можливо уявити щоденну діяльність людини будь-якої професії без застосування тої чи іншої бездротової технології. І це стосується не тільки професійної діяльності але й побутових речей. Найбільш поширеним на даний момент способом бездротового функціонування систем зв'язку, керування, чи будь-яких інших являється обмін даними за допомогою радіохвиль. Радіокерованими стають все більше речей, від гаражних воріт чи замків автомобіля, до домашньої кавоварки, яка керується смартфоном через WiFi.

Особливу нішу в людській діяльності зайняли радіокеровані пристрої і апарати, які можуть переміщуватися в просторі, та дозволяють без присутності людини в апараті проводити різноманітні маніпуляції чи спостереження, так звані безпілотні апарати (БПА). Особливої популярності серед них набули безпілотні літальні апарати (БПЛА), оскільки вони переміщуються повітрям і, відповідно, можуть долати наземні перешкоди, що складно проходяться наземною технікою, також вони можуть рухатися швидше і оглядати великі

території за відносно короткий час. Через це вони мають найбільш універсальне застосування: від завдань контролю території власником аж до військових розвідувальних, ударних операцій, чи цивільних пошуково-рятувальних операцій [1-4].

Разом із таким розвитком бездротових систем, росте і кількість викликів і завдань до забезпечення безпеки і якості радіозв'язку. Особливо актуальним питання захисту бездротових систем зв'язку і керування є саме зараз, коли під час повномасштабної війни, безпілотна авіація відіграє ключову роль у плануванні і проведенні операцій, вирішенні завдань розвідки сил противника або й нанесення йому вогневого ураження безпосередньо самими безпілотними засобами.

Теоретичні основи дослідження

Тема використання БПЛА в теперішній час є дуже актуальною, що зумовлює її постійне дослідження і обговорення, як у приватних розмовах так і у науковому товаристві. Так, зокрема, Станіслав Слободяник та співавтори у своєму дослідженні [5] дослідили зростання інтересу і попиту на безпілотні системи, особливо у військовій справі, де держава в особі Міністерства Оборони виступає основним замовником та користувачем цих технологій. Популярним напрямком у сфері забезпечення захисту і високої продуктивності та результативності застосування БПЛА є роботи по створенню систем навігації дрона на основі штучного інтелекту, системи організованого рою дронів, застосування моделі нечіткої логіки, тощо [3-6]. Ці системи певною мірою задовольняють вимоги, що ставляться до використання БПЛА, допомагають підвищувати їхню ефективність і зберігати працездатність у важких умовах та за непередбачуваних обставин. Разом з цим, такі системи не задовольняють задачі захисту системи телеметрії, системи керування, тощо. Телеметрія, передавання даних вимірів, фото- чи відеозйомки, керування переміщенням дроном з пульта керування – всі ці системи вимагають постійного і стабільного зв'язку із пультом оператора, що в принципі не передбачається при використанні моделей на основі ШІ, адже вони розраховуються більше на розумну автономну поведінку. Це може як і забезпечити перевагу, так і накладати суттєве обмеження на використання таких моделей функціонування і навігації у військовій сфері. Наприклад для ударного БПЛА система донаведення на ціль, побудована на основі комп'ютерного зору, буде великою перевагою, адже після захоплення цілі у нас вже не буде необхідності у зв'язку і керуванні дроном через це зменшується вплив засобів радіоелектронної боротьби (РЕБ) на результат операції. Але при завданні розвідки у невідомій місцевості, коли ми не знаємо наперед навіть приблизного розташування сил і засобів противника нам необхідний стабільний зв'язок як і для керування дроном вручну за виникнення потреби, так і стабільний зворотній зв'язок для отримання задовільної картинки на екрані. Автор Кізло Л. разом із колегами у своєму дослідженні [7] також особливо відмітили, що на даний час зарано говорити про автономне застосування дронів: все ж переважна більшість військових операцій із використанням БПЛА це дистанційно пілотовані польоти.

Для забезпечення якості і надійності пілотованих польотів доцільно зупинитися на сучасних дослідженнях і розробках у сфері захисту каналів бездротового зв'язку, яких також було проведено достатньо багато. За результатами розгляду і проведеного аналізу загально-оглядових робіт, навчальних посібників та статей аналітичного змісту [8,9,10] окреслимо основні класичні підходи до захисту каналів зв'язку та керування, які мають високу ефективність і постійно вдосконалюються, це: криптографічний захист, застосування антен різних параметрів під різні завдання, завадостійке кодування та методи на основі змін робочої несучої частоти.

У системах зв'язку БПЛА криптографія дозволяє вирішити завдання забезпечення конфіденційності та автентифікації оператора. У роботі [11] автором було представлено варіант криптографічного захисту за рахунок впровадження у БПЛА вбудованого пристрою на основі мікроконтролера, який працював як шифратор/дешифратор у якості проміжної ланки на лінії зв'язку радіоприймач-контролер польоту. Алгоритмом шифрування була звичайна сума за модулем 2 (операція XOR) між значенням повідомлення та закритим ключем. Ця система дозволяє забезпечити базовий захист від втручання у канал зв'язку, але має дуже низьку криптографічну стійкість, адже довжина ключа у системі лише 8 біт, що дозволяє швидко перебрати усі можливі комбінації.

Використання різних типів антен, що описане у роботах [9,10] дозволяє покращувати якість, стабільність та/або дальність зв'язку за допомогою методів антенного проектування або звичайним підбором необхідної за характеристиками антени вже існуючої конструкції. Наприклад описані у роботі [10] антени із вузькою діаграмою спрямованості дозволяють значно покращити дальність передачі, «відсікти» області де потенційно може знаходитися зловмисник таким чином, що прийом нашого сигналу для нього буде фізично не можливим. А антени із круговою діаграмою спрямування мають меншу дистанцію передачі, здатні ловити завади зі сторонніх напрямків, але дозволяють нам стабільно і без перебоїв приймати сигнали у будь якому просторовому положенні пристрою. Остання властивість якраз і зумовлює використання у сучасних моделях БПЛА, поширених серед військових, дипольних або чотирипелюсткових антен. Адже, не зважаючи на переваги використання спрямованих антен, ставити їх на БПЛА не доцільно із кількох причин: зазвичай такі антени мають складну геометрію і значно більші розміри, а також вони вимагають чіткого налаштування і скерування в напрямку іншого абонента зв'язку, що не можливо в умовах польоту і постійного маневрування пристрою.

Методи на основі зміни робочої частоти є одними із найбільш потужних засобів захисту зв'язку і такими, які зараз найбільше досліджуються і стрімко розвиваються. Так, у роботі [12] описано сучасну систему зв'язку із псевдовипадковим переналаштуванням робочої частоти, що забезпечує високий рівень стійкості такої системи до засобів електромагнітного придушення, засобів РЕБ та РЕР. Інший дослідник, Дзяйло В. В. у своїй роботі [13] провів аналіз основних характеристик каналів зв'язку зі схожим принципом захисту – частотним мультиплексуванням, а також описав способи та засоби покращення характеристик захищеності та стабільності роботи таких каналів зв'язку. Основною перевагою такого підходу до захисту каналу зв'язку в першу чергу є сам факт можливості передачі інформації на різних частотах, це дозволить навіть у випадку електромагнітного зашумлення каналу, перейти на іншу незайняту робочу частоту для подальшої роботи. Завдяки цьому значно підвищується стійкість системи зв'язку в умовах активного протиборства. Другим важливим аспектом захисту шляхом частотних змін також є те, що при регулярній зміні частоти, значно ускладняється задача не тільки перехоплення чи придушення сигналу зловмисником а й самого його виявлення. Так, автори Бігун Наталія та Грозовський Роман у своїй роботі [14] дослідили захищеність каналів зв'язку зі зміною частоти до засобів радіоелектронної розвідки та радіопеленгації і виявили, що захищеність каналу зв'язку до виявлення постійно зростає зі збільшенням швидкості переналаштування. А із наближенням швидкості переналаштування частоти засобу зв'язку до швидкості сканування частотного діапазону засобом радіопеленгації, або її перевищенням ймовірність виявлення прямує до нуля, тобто сигнал на певній частоті з'являється і зникає швидше, ніж сканер може його проглянути.

Повною мірою такі заходи захисту реалізовані у великих, промислових зразках БПЛА, по типу "Валькірія", "Лелека", ТВ-2 "Bayraktar", а моделі військового призначення типу американського MQ-9 "Reaper" взагалі мають багаторівневий захист та систему зв'язку через орбітальний супутник. Проте зовсім по-іншому ситуація виглядає із малими дронами, зокрема

розвідувальними і ударними FPV, які зараз дуже активно використовуються нашими Збройними Силами. Ці засоби зараз складають основу безпілотної авіації на полі бою, а реалізовуються на основі схемних рішень, які розроблялися для завдань хобі-польотів, комерційного цивільного використання, тощо. Тому перед розробниками і дослідниками зараз дуже гостро постають такі питання: як можна захистити систему зв'язку або керування малогабаритних БПЛА? Чи в принципі це можливо, використовуючи все ті ж польотні засоби? Які зміни та модернізації для цього треба зробити?

Постановка проблеми

Основною проблемою, взятою до розгляду у цій статті, є недостатня захищеність найбільш застосовуваних зараз засобів безпілотної авіації, таких як FPV-дрони, та інші БПЛА що використовуються захисниками але мають перш за все цивільне призначення і характеристики.

Також, деякі готові рішення, які є широко використовувані, мають функціонал, який опосередковано описаний в документації і допускає виконання додаткових функцій, які прямо не задекларовані виробником.

Методологія дослідження

Для побудови і конструювання безпілотних пристроїв зазвичай використовуються засоби і рішення від таких популярних виробників як SpeedyBee, HappyModel, FlashHobby, TBS, Eachine, JHEMCU, та ін. Вони мають свої особливості, відрізняються тими чи іншими параметрами і конфігурацією портів, але в загальному принцип їхньої дії і функціонування протоколів у них схожі.

Для дослідження буде розглядатися схема одного із вказаних виробників. Оскільки декотрі розглянуті у роботі протоколи здобули популярності і є імплементовані у схемах різних виробників із збереженням конструкцій, логіки команд, тощо, то дане дослідження буде релевантне також і для багатьох пристроїв із переліку.

Результати

Якщо розглядати військове використання БПЛА, то основними проблемами є заглушення системи дистанційного керування або передавання відео засобами РЕБ або перехоплення відео-сигналу і його відтворення противником, що дає йому цінні відомості. Так, якщо рівня сигналу від відеопередавача буде достатньо для його задовільного детектування у точці знаходження противника при злеті або посадці апарату, це дасть змогу противнику змалювати обстановку та орієнтири довкола позиції запуску і таким чином виявити позицію для своїх подальших дій.

Серед розглянутих нами методів, для протидії таким загрозам мною було обрано метод переналаштування несучої частоти, оскільки передавачі мають кілька наборів каналів із частотним розділенням, відповідно для зв'язку ми можемо використовувати ті чи інші канали. Наприклад, для передавачів сімейства TBS розрахованих на роботу на частоті 5.8 ГГц доступне таке частотне розподілення каналів.

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

Рисунок 1 – Частоти наборів каналів доступних для передавачів.

Джерело: TBS CROSSFIRE R/C System: Adaptive Long-Range Remote-Control System User Manual. (2022) [15]

Така чітка визначеність каналів зумовлена тим, що передавачі, як було сказано раніше, перш за все розраховані для цивільного їхнього використання, а допустимі діапазони частот для вільного займання цивільними користувачами каналу в тих чи інших регіонах або країнах є строго регламентованими і законодавчо врегульованими. Це і є враховано виробниками пристроїв, щоб убезпечити операторів від ненавмисного порушення законодавства. Така визначеність має дуже негативний наслідок – ворог про неї також знає, адже це відкрита інформація. У випадку якщо ми і реалізуємо частотне переналаштування між каналами і забезпечимо перемикання каналів оператором на пульті керування БПЛА, смуга частот стандартного набору каналів є відносно не великою і складає від 5705 МГц до 5945 МГц. Також ці набори каналів, як бачимо з рисунку 1, мають фіксовані значення. Це дало змогу розробити відносно компактні засоби РЕБ для локального використання, які працюють на визначеному частотному діапазоні із переліку вище. Зазвичай ці засоби здійснюють електромагнітне зашумлення визначеного неперервного діапазону так званим "білим" шумом і можуть звести нанівець користь і переваги перемикання каналів, адже може виявитися так, що засіб РЕБ заглушив усі доступні для вибору канали.

Але таке неперервне зашумлення використовується як правило в найбільш простих варіантах реалізації пристроїв електромагнітного придушення, оскільки воно має суттєвий недолік – при роботі такого пристрою можна вивести з ладу зв'язок і своїх безпілотних пристроїв, які потраплять у зону дії РЕБ. Тому все частіше у пристрої для придушення БПЛА впроваджується механізм фільтрації, який може працювати за двома принципами: перший дозволяє залишати робочими необхідні нам канали і всі інші заглушити, а другий дозволяє залишити всі канали робочими а глушити конкретний.

Така варіативність вже потенційно відкриває нам вікно можливостей для того, щоб "прощупати" вільний канал і переключитися на нього, але тут виникають інші супутні проблеми: для перемикання каналів оператором використовуються програмовані кнопки або тумблери пульта (так звані AUX перемикачі) кількість яких обмежена, що означає по-перше, невеликий вибір каналів для перемикання, а по-друге, для перемикання каналу, необхідно щоб сигнал пульта все ж у певний момент дістався апарату і той за командою змінив частоту, що може не статися при достатньо серйозному впливі.

Для вирішення цієї проблеми у даній статті розглянемо і дослідимо можливості протоколів, які були відносно нещодавно впроваджені у нові моделі популярних передавачів для дронів. Це протоколи TBS SmartAudio та IRC Tramp, вони є досить слабо документовані і не достатньою мірою досліджені, але згідно загального опису вони мають досить цікаві можливості із точки захисту каналу зв'язку, особливо в контексті використання частотних переналаштувань.

Наявність таких протоколів у пристроях як правило декларується виробником у інструкції, а також його можна побачити по конфігурації виводів контролера (приклад на рис.2).

Рисунок 2 – Виводи радіопередавача TBS Eachine TX5258,
бачимо вивід протоколу SmartAudio

Основна ідея цих протоколів – реалізувати зовнішній інтерфейс керування і налаштування передавача за допомогою команд, передаваних із зовнішніх пристроїв через фізичне підключення дротом. Тобто ми отримуємо змогу керувати передавачем програмно, через порт вводу-виводу зовнішнім, наприклад, мікроконтролером. Це значно розширює можливості імплементації заходів частотного захисту, адже у мікроконтролер ми можемо запрограмувати довільний необхідний нам функціонал.

Реалізовані ці протоколи на основі послідовного порту вводу/виводу UART, з одною особливістю – це напівдуплексний UART із одним проводом передачі даних. Працює це таким чином контролер (MCU) та радіопередавач (RFX) працюють у режимі Slave і очікують передавання інформації. Коли необхідно виконати якусь дію MCU переходить в режим Master і відправляє запит до RFX, після чого переходить в режим Slave і очікує відповіді. RFX, у свою чергу, отримавши запит, опрацьовує його і переходить із режиму Slave у режим Master і відправляє відповідь на запит, після чого знову перемикається у режим Slave.

Згідно документації [16], працює цей протокол в режимі UART 8N2, що означає сеанс передачі із 8 біт даних, одного стартового біту і 2 стоп-бітів на фіксованій швидкості 4800бод. Важливо враховувати, що при роботі передавач може нагріватися (особливо на великих потужностях) через що можливе відхилення від швидкості передачі +/- 5%.

Для здійснення налаштувань, та отримання даних стану у цьому протоколі передбачені такі команди (включно з їх шістнадцятковими кодами):

- Get_settings 0x01
- Set_power 0x02
- Set_channel 0x03
- Set_frequency 0x04
- Set_operation_mode 0x05

Структура запиту до передавача виглядає наступним чином:

<Start_code><Command><Frame_len><Payload><CRC>

Старт код – це стандартна послідовність для синхронізації (0xAA 0x55), команда – це код команди зі списку, наведеного вище, довжина фрейму – позначає скільки параметрів ми передаємо (включно із контрольною сумою), а CRC – значення контрольної суми переданої послідовності утвореної циклічним кодом із твірним поліномом 0xD5. Важливо зазначити, що для надсилання команди передавачу, код команди у запиті має бути логічно зсунутий вліво із встановленням наймолодшого значущого біта. Наприклад для команди вибору каналу (0x03) у запиті в полі <Command> повинно бути значення 0x07. А у відповіді на запит, код команди буде 0x03. У протоколі SmartAudio кожен запит, в тому числі на встановлення якогось значення, супроводжується відповіддю у якій містяться дані про стан передавача після виконання команди, що дає змогу оперативно контролювати результат виконання тої чи іншої команди.

У даній роботі для випробувань був використаний передавач TBS Eachine TX5258 а в якості керуючого пристрою мікроконтролер Cypress CY8CKIT-059 (вибір схем зумовлений тим, що вони були вже наявні в руках на час дослідження).

Використовуючи команду Set_Channel ми з мікроконтролера можемо встановити канал зв'язку (будь-який із вказаної на рис. 1 таблиці). Після відправки із контролера запиту:

0xAA 0x55 0x07 0x01 0x0A 0xF2

Відповідь прийшла наступна:

0xAA 0x55 0x03 0x03 0x0A 0x01 0x3A

Ми бачимо, що після команди вибору каналу 0x0A (10-й канал у десятковій формі) у відповіді робочий канал став також 0x0A, перевірити його значення конкретне у МГц можна командою Get_settings – надсилаємо запит:

0xAA 0x55 0x03 0x00 0x9F

отримуємо відповідь: 0xAA 0x55 0x09 0x06 0x0A 0x00 0x1A 0x16 0x78 0xDA, тут доцільно проінтерпретувати її по байтах: 0xAA 0x55 (стартові байти) 0x09 (версія протоколу SA) 0x06 (довжина даних) 0x0A (канал) 0x00 (рівень потужності) 0x1A (режим роботи) 0x16 0x78 (поточна частота) 0xDF (контрольна сума) якщо перевести отримане значення робочої частоти 0x1678 у десяткову форму, отримаємо значення 5752, що правильно відповідає частоті у відповідному полі таблиці.

Але набагато цікавішою і кориснішою виявилася команда задання частоти не номером каналу, а безпосереднім значенням частоти: Set_frequency. Після експериментального запиту на зміну частоти на ту, яка не входить до набору частот із таблиці, такого вигляду:

0xAA 0x55 0x09 0x02 0x13 0xFB 0x3C, де:

0xAA 0x55 0x09(команда) 0x02(кількість значень) 0x16 0xE9(частота 5115) 0x3C(CRC8)

Відповідь модуля була

0xAA 0x55 0x04 0x04 0x13 0xFB 0x01 0xCF, де:

0xAA 0x55 0x04(команда) 0x04(кількість значень) 0x16 0xE9(частота 5115) 0x01 (зарезервоване значення) 0xCF(CRC8)

Із цього ми бачимо, що через використання протоколу SmartAudio у нас є можливість виходу за межі стандартних частот, які доступні для налаштування через стандартні застосунки із графічним інтерфейсом. В ході подальших експериментів було виявлено, що зміна частоти працює коректно на всьому діапазоні значень від 5000 МГц до 6000 МГц і змінює частоту сигналу на задану. При виході за ці межі, задання нової частоти ігнорується і у відповіді на запити я спостерігав, що значення поточної частоти залишалося незмінним.

Також протоколом SmartAudio можна програмно змінювати рівень потужності передавача командою Set_power. Для версій протоколів 1.0 та 2.0 це здійснюється у вигляді фіксованих значень згідно таблиці у документації, а пристрої із підтримкою протоколу версії 2.1 допускають встановлення рівня сигналу у дБм.

Висновки

У даній роботі було розглянуто питання захищеності безпілотних авіаційних систем у контексті їхнього використання у сучасних бойових діях. Основна увага була зосереджена на тому, що переважна більшість комплексів є малогабаритними БПЛА цивільного проектування і це викликає певні обмеження у їх використанні, які зумовлені обмеженістю їхніх характеристик. В ході дослідження були особливо виділені методи на основі частотних переналаштувань, як такі, що є найбільш перспективні і теоретично придатні до відносно не трудомісткої реалізації у пристроях не високого класу.

Під час експерименту із протоколами низького рівня, зокрема TBS SmartAudio у їх реалізації для передавача TBS Eachine TX5258 було досліджено можливість зміни усіх базових параметрів передавачів таких як потужність передачі сигналу, канал передачі, та робоча несуча частота сигналу. Основним позитивним моментом дослідження було те, що в ході експерименту виявлено, що за допомогою низькорівневого керування через порт S-Audio у

нас є можливість використовувати не стандартні частоти, які виходять досить далеко за межі стандартизованих таблиць.

Отримані результати відкривають широкі можливості для подальшого дослідження і впровадження на практиці у існуючі безпілотні пристрої засобів та методів захисту каналу зв'язку не тільки на основі частотних переналаштувань а й менеджменту потужності передавача. Шляхом впровадження у БПЛА керуючого мікроконтролера ми отримуємо можливість реалізації широкого спектру алгоритмів забезпечення відмовостійкості зв'язку, наприклад: постійне частотне переналаштування із вибором наступної робочої частоти за певним правилом дозволить збільшити прихованість каналу зв'язку для засобів пеленгації, застосування не стандартних частот каналів для 5.8 ГГц передавачів дозволить нам уникнути просторового електромагнітного зашумлення, оскільки портативні засоби РЕБ можуть мати не такий широкий діапазон частот, як той, що доступний для налаштування через мікроконтролер.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Юн Х. М., Мединський Д. В. (2017). Використання безпілотних літальних апаратів в сільському господарстві. Високотехнологічні технології. № 4(36). С. 335-341. https://doi.org/10.18372/2310-5461.36.12232.
2. Лещенко Г. А., Мандрик Я. С., Стратонов В. М., Давидов С. А. (2021). Методи використання безпілотних літальних апаратів під час авіаційного пошуку та рятування. Високотехнологічні технології. № 3(51). С. 271-280. https://doi.org/10.18372/2310-5461.51.15998.
3. Глотов В., Гуніна А. (2014). Аналіз можливостей використання безпілотних літальних апаратів для аерофотозйомки. Сучасні досягнення геодезичної науки та виробництва. № 2. С. 65-70.
4. Дружинін Є.А., Ковалевський М.І., Погудіна О.К., Черановський В.О. (2021). Методи та інформаційні технології впровадження безпілотних літальних апаратів в повітряний простір України. Збройні системи та військова техніка. № 4(68). С. 84-90. https://doi.org/10.30748/soivt.2021.68.12.
5. Слободяник С., Петренко С., Цибізов А., Бондаренко Ю. (2023). Можливі шляхи розвитку перспективних українських систем БПЛА, з урахуванням сучасних світових тенденцій. Соціальний розвиток та безпека, Том. 13, № 3. С. 135-145. https://doi.org/10.33445/sds.2023.13.3.9.
6. Стасенко Д. В., Яковина В. С. (2023). Аналіз існуючих методів та засобів поліпшення навігації БПЛА за допомогою штучного інтелекту. Науковий вісник НЛТУ України. Том. 33, № 4. С. 78-83. https://doi.org/10.36930/40330411.
7. Кізло Л., Троценко О., Жук. О. (2021) Тенденції розвитку безпілотних літальних апаратів в Україні. Українські військові сторінки. URL : https://www.ukrmilitary.com/2021/05/uav.html.
8. Бурляй І.В. (2007). Системи радіозв'язку та їх застосування оперативно-рятувальною службою: Посібник. Чернігів: РВК "Деснянська правда". 288 С.

9. Гриб Д.А., Демідов Б.О., Кучеренко Ю.Ф., Ткачов А.М., Кулешова Т.В. (2019). Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін. Наука і техніка Повітряних Сил Збройних Сил України. Том 1, № 43. С 12-22. https://doi.org/10.30748/nitps.2019.34.02.
10. Ільїнов М.Д., Гурський Т.Г., Борисов І.В., Гриценок К.М. (2018). Лінії радіозв'язку та антенні пристрої: навчальний посібник. Київ: Військовий інститут телекомунікацій та інформатизації, 249 с.
11. Навроцький Д. (2014). Криптографічна система захисту радіоканалів БПЛА від несанкціонованого втручання / Український науковий журнал Інформаційна безпека, том. 20, випуск 3, с. 248-252.
12. Василенко С.В. (2016). Системи радіозв'язку з псевдовипадковим переналаштуванням робочої частоти / Електронне наукове фахове видання-журнал Проблеми телекомунікацій. № 1 (18). С. 91-100.
13. Дзяйло В.В. (2017) Покращення характеристик каналів радіозв'язку з частотним мультиплексуванням: автореф. магістра: Тернопільський національний технічний університет імені Івана Пулюя. Тернопіль: ТНТУ, 7 С.
14. Бігун Н., Грозовський Р. (2019). Оцінка розвідзахищеності системи зв'язку, побудованої на сучасних засобах радіозв'язку: Сучасні інформаційні технології в галузі безпеки та оборони, № 1(34), С. 53-58. https://doi.org/10.33099/2311-7249/2019-34-1-53-58.
15. TBS CROSSFIRE R/C System: Adaptive Long Range Remote Control System User Manual. (2022). 88 C. URL : https://www.team-blacksheep.com/media/files/tbs-crossfire-manual.pdf.
16. TBS Unify Pro/SmartAudio. User Manual. (2018). 10 C. URL : https://www.team-blacksheep.com/media/files/tbs_smartaudio_rev09.pdf.

References

1. Yun H. M., Medinskyi D. V. (2017). Use of unmanned aerial vehicles in agriculture. High-tech technologies. No. 4(36). P. 335-341. https://doi.org/10.18372/2310-5461.36.12232.
2. Leshchenko H. A., Mandryk Ya. S., Stratonov V. M., Davidov S. A. (2021). Methods of using unmanned aerial vehicles during aviation search and rescue. High-tech technologies. No. 3(51). P. 271-280. https://doi.org/10.18372/2310-5461.51.15998.
3. Glotov V., Gunina A. (2014). Analysis of the possibilities of using unmanned aerial vehicles for aerial photography. *Modern achievements of geodetic science and production*. No. 2. P. 65-70.
4. Ye.A. Druzhinin, M.I. Kovalevskyi, O.K. Pohudina, V.O. Cheranovskyi. (2021). Methods and information technologies for implementing unmanned aerial vehicles in the airspace of Ukraine. Armed systems and military equipment. No. 4(68). P. 84-90. https://doi.org/10.30748/soivt.2021.68.12.
5. Slobodyanik S., Petrenko S., Tsybizov A., Bondarenko Yu. (2023). Possible ways of development of promising Ukrainian UAV systems, taking into account modern world trends. *Social development and security*, Vol. 13, No. 3. P. 135-145. https://doi.org/10.33445/sds.2023.13.3.9.
6. Stasenko, D. V., Yakovyna, V. S. (2023). Analysis of existing methods and means of improving UAV navigation using artificial intelligence. *Scientific Bulletin of NLTU of Ukraine*. Vol. 33, No. 4. P. 78-83. https://doi.org/10.36930/40330411.
7. Kizlo L., Trotsenko O., Zhuk. O. (2021). Trends in the development of unmanned aerial vehicles in Ukraine. Ukrainian military pages. Retrieved from: https://www.ukrmilitary.com/2021/05/uav.html.

8. Burlyai, I.V. (2007). Communication systems and their use by the operational rescue service: Manual. Chernihiv: RVK "Desnyanska pravda". 288 P.
9. Hryb, D.A., Demidov, B.O., Kucherenko, Yu.F., Tkachov, A.M., Kuleshova, T.V. (2019). Principles, methods and technologies of conducting armed struggle, managing forces and means in conditions of active information confrontation of conflicting parties. *Science and technology of the Air Forces of the Armed Forces of Ukraine*. Vol 1, No. 43. P 12-22. https://doi.org/10.30748/nitps.2019.34.02.
10. Ilyinov, M.D., Gursky, T.G., Borisov, I.V., Grytsenok, K.M. (2018). Communication lines and antenna devices: a textbook. Kyiv: *Military Institute of Telecommunications and Informatization*, 249 p.
11. Navrotskyi D. (2014). Cryptographic system for protecting UAV radio channels from unauthorized interference. *Information security*, vol. 20, issue 3, p. 248-252.
12. Vasilenko, S.V. (2016). Communication systems with pseudorandom retuning of the operating frequency. *Problems of telecommunications*. No. 1 (18). P. 91-100.
13. Dzyaylo V.V. (2017). Improvement of communication channel characteristics with frequency multiplexing: author's ref. master: Ternopil National Technical University named after Ivan Puluj. Ternopil: TNTU, 7 P.
14. Bigun N., Grozovsky R. (2019). Assessment of the reconnaissance protection of the communication system built on modern means of communication: Modern information technologies in the field of security and defense, No. 1(34), P. 53-58. https://doi.org/10.33099/2311-7249/2019-34-1-53-58.
15. TBS crossfire R/C System: Adaptive Long Range Remote Control System User Manual. (2022). 88 P. Retrieved from: https://www.team-blacksheep.com/media/files/tbs-crossfire-manual.pdf.
16. TBS Unify Pro/SmartAudio. User Manual. (2018). 10 P. Retrieved from: https://www.team-blacksheep.com/media/files/tbs_smartaudio_rev09.pdf