

ЗАХИЩЕНА ВІД ВПЛИВУ НАВМИСНИХ ЗАВАД СИСТЕМА ЗВ'ЯЗКУ МАЛОГАБАРИТНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Кайденко М.М.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kkk610@ukr.net

PROTECTED FROM THE EFFECTS OF JAMMING COMMUNICATION SYSTEM OF SMALL-SIZED UAVs

This article describes the features of constructing a communication and control system of UAVs that is protected from the effects of deliberate interference. The structure of the UAV communication system and its features that provide protection against deliberate interference are presented.

На сьогоднішній день дослідженням в галузі створення систем зв'язку та управління безпілотних апаратів, захищених від впливу різноманітних завад, особливо навмисних, приділяється особлива увага вчених та інженерів в усьому світі. Навмисні завади можуть призводити до тимчасової втрати управління безпілотним апаратом, виведення його з ладу, перехоплення управління апаратом і, як наслідок, нецільового його використання. Найбільшу небезпеку несе нецільове використання безпілотного апарату зловмисниками, оскільки при цьому він може використовуватись як засіб для терористичних атак, наприклад на об'єкти підвищеної небезпеки.

В багатьох роботах відзначається, що безпека БПЛА є головною проблемою, особливо з точки зору кібератак і на даний час не існує типового способу його захисту від них. Зокрема роботи [1,2] присвячені дослідженню стійкості комерційних та недорогих моделей БПЛА спеціального призначення, які використовують технологію WiFi для зв'язку та управління. Визначено значну вразливість таких БПЛА до кібератак, що можуть призводити до перехоплення та нецільового використання.

Окремі роботи, зокрема російських дослідників [3], присвячені не методам захисту БПЛА від навмисних завад, а навпаки методам протидії безпілотним апаратам шляхом створення в тому числі і різних видів навмисних завад. При цьому основний акцент робиться не просто на кібератаку на БПЛА, а на подавлення каналу зв'язку, або перехоплення безпілотного апарату шляхом підміни інформації в каналі управління.

В роботах [4,5] було запропоновано архітектуру системи зв'язку безпілотного апарату для підвищення його живучості, яка досягається за рахунок застосування адаптації по діапазону частот з використанням додаткового каналу прийому для безперервного аналізу завадової обстановки, використанням двох та більше каналів передачі даних, складних алгоритмів оптимального вибору робочого діапазону, параметрів каналу передачі та адаптивних протоколів одночасної передачі даних по двом та більше каналам. Однак таке рішення не завжди може бути використано для захисту

малогабаритних БПЛА, оскільки основним обмеженням для застосування такої системи є обмеження на вагу корисного навантаження. Це обмеження призводить до того, що кількість бортової апаратури має бути мінімальною. При цьому використання двох каналів передачі потребує вдвічі більше енергетичних затрат, що призводить до необхідності збільшення ємності акумуляторної батареї.

Живучість безпілотного апарату з точки зору управління ним в першу чергу залежить від живучості системи зв'язку та управління, вихід з ладу якої призводить до повної втрати управління апаратом та, як наслідок до втрати самого апарату. За призначенням канал зв'язку від наземної станції до БПЛА є каналом управління, а канал зв'язку від БПЛА до наземної станції є каналом передачі телеметрії. В структурі системи зв'язку та управління безпілотного апарату, структура бортового обладнання якої показана на рис.1 використовується два канали прийому в двох фіксованих частотних діапазонах (як приклад для БПЛА цивільного використання 2,4 та 5,8 ГГц) та один канал передачі. Наземна станція зв'язку та управління БПЛА відповідно має два канали передачі та один канал прийому.

Використання частотного чи часового дуплексу відіграє також істотну роль в живучості каналу зв'язку. При частотному дуплексі канал передачі та прийому рознесені по частоті і тому визначення, на якій конкретній частоті працює канал управління БПЛА в точці перехоплення потребує істотно більшої чутливості приймача перехоплювача. При часовому дуплексі ж інформація про частоти роботи БПЛА легко може бути отримана перехоплювачем.

Використання одночасно двох каналів прийому з передачею повністю дубльованої інформації управління дозволяє істотно підвищити живучість каналу управління відносно енергетичної завади глушення каналу, оскільки для цього потребується або одночасна постановка енергетичної завади в двох діапазонах частот, або використання широкосмугової завади, для постановки якої використовуються станції постановки завад, вартість яких на порядки вища за вартість БПЛА, проти якого використовується така станція.

Для боротьби з завадами перехоплення та імітації каналу використовуються алгоритми виявлення імітаційних структурованих завад. Ці алгоритми базуються на синхронізації каналів, підтримці заданого рівня енергетики каналу та моніторингу енергетичних характеристик в каналах, маркуванні пакетів даних. Підтримка заданого рівня енергетики каналу, який повинен бути однаковим в обох каналах забезпечує додаткову скритність передачі інформації, знижуючи вірогідність перехоплення станцією, яка не знаходиться в зоні прямої видимості. Синхронізація каналів та підтримка заданого рівню енергетики реалізується шляхом використання технологій програмно-визначуваного радіо та систем на кристалі, описаних в [6]

Подавлення каналу телеметрії потребує більших енергетичних затрат від станції перехоплення, внаслідок того, що вона повинна розміщуватись набагато ближче до БПЛА, ніж до наземної станції управління. Тому нагальної необхідності в використанні двох каналів передачі немає. Не зважаючи на це, при використанні широкосмугового підсилювача потужності можна

комутувати виходи передавачів трансиверів з метою зміни діапазону частот каналу телеметрії.

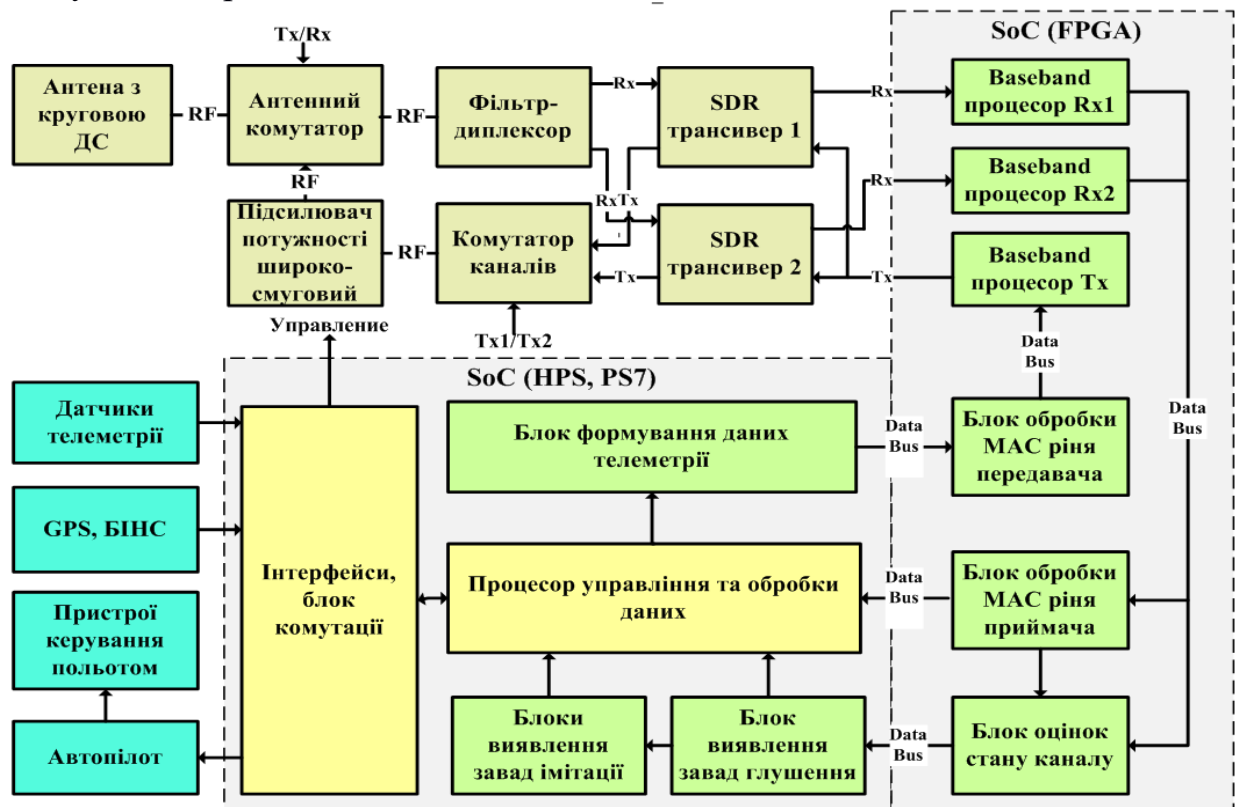


Рис.1. Структура бортового обладнання системи зв'язку та управління безпілотного апарату в режимі TDD.

Література

1. Carlos Augusto Tovar Bonilla, Octavio José Salcedo Parra, Jhon Hernán Díaz Forero. Common Security Attacks on Drones. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 4982-4988 [<http://www.ripublication.com> 4982].
2. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A., Watkins, L., Robinson, W., Alexis, W.: Securing commercial WiFi-based UAVs from common security attacks. In: MILCOM 2016—2016 IEEE Military Communications Conference (2016), [DOI: 10.1109/MILCOM.2016. 7795496].
3. Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, No1 (2017), [<http://naukovedenie.ru/PDF/13TVN117.pdf>].
4. M. Kaidenko and S. Kravchuk, "Creation of communication system for unmanned aerial vehicles using SDR and SOC technologies," 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2019, pp. 1-4, [doi: 10.1109/UkrMiCo47782.2019.9165422].
5. Kaidenko M., Kravchuk S. (2021) Autonomous Unmanned Aerial Vehicles Communications on the Base of Software-Defined Radio. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. [https://doi.org/10.1007/978-3-030-58359-0_16].
6. Kaidenko M.M., Roskoshnyi D.V. (2019) Software Defined Radio in Communications. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham DOI, [https://doi.org/10.1007/978-3-030-16770-7_11 Print ISBN 978-3-030-16769-1].