

ХАРАКТЕРИСТИКИ НАВМИСНИХ ЗАВАД, ЩО ДІЮТЬ НА КАНАЛ ЗВ'ЯЗКУ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

Гетьман О.В., Кайденко М.М.

Навчально-науковий інститут телекомунікаційних систем

КПІ ім. Ігоря Сікорського, Україна

E-mail: kkk610@ukr.net

CHARACTERISTICS OF INTENTIONAL JAMMING ACTING ON THE COMMUNICATION CHANNEL OF AN UNMANNED AERIAL VEHICLE

This article presents the structure of the organization of electronic countermeasures to the UAV communication channel, gives a characteristic of intentional interference that can affect the UAV communication channel, and presents the results of testing the effect of such interference.

Вплив на канал зв'язку БПЛА навмисних завад незалежно від його призначення (військовий чи цивільний) є своєрідним засобом радіоелектронної боротьби. Відносно каналів зв'язку БПЛА можна виділити три складові радіоелектронної боротьби: пасивне радіоелектронне забезпечення (Electronic Support Measures - ESM); активне радіоелектронне подавлення (Electronic CounterMeasures - ECM); протидія радіоелектронному подавленню - радіоелектронний захист (Electronic Counter-CounterMeasures — ECCM). Пасивне радіоелектронне забезпечення стосовно БПЛА полягає переважно у радіорозвідці, яка забезпечує перехоплення сигналів, визначення напрямку їхнього приходу та їх аналіз. Особливістю останніх двох складових частин є те, що розробка використовуваного для їх реалізації устаткування супроводжується постійним змаганням однієї з другою.

Типовий сценарій радіоелектронної боротьби – це протистояння між силами та засобами всіх трьох складових: радіоелектронного забезпечення, радіоелектронного подавлення та радіоелектронного захисту. При цьому важливим аспектом є те, щоб програмне забезпечення системи радіоелектронного захисту було модифікованим, тобто мало б відкриту архітектуру [1]. Для забезпечення ефективного радіоелектронного захисту важливо знати, які типи навмисних завад можуть діяти на канал зв'язку БПЛА, особливості їх застосування та характеристики. Для протидії БПЛА використовуються станції радіоелектронної боротьби, що поєднують у собі функції радіорозвідки і радіоподавлення, що працюють у широкому діапазоні частот наприклад [2], а також малогабаритні малопотужні антидрон рушніці з обмеженим діапазоном частот та функціональністю, наприклад [3]. Станція радіоелектронної боротьби завжди розташовується ближче до об'єктів виконання місії БПЛА, або в безпосередній близькості до них. Внаслідок цього просторові та енергетичні характеристики каналу зв'язку БПЛА та каналу подавлення істотно відрізняються за протяжністю та напрямком випромінювання.

На рисунку 1 показана структурна схема організації радіоелектронної протидії безпілотному літальному апарату, в якій показані канал передачі даних від наземної станції управління БПЛА, організація каналу постановки завади та структура сигналу на вході приймача з усіма викривленнями та завадами.

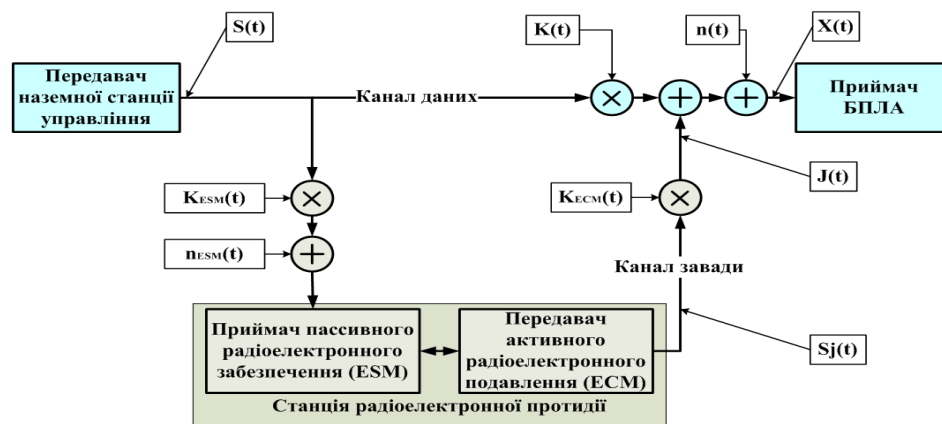


Рис.1. Структурна схема організації радіоелектронної протидії БПЛА.

Модель сигналу, що передається від наземної станції управління до БПЛА у разі відсутності радіопротидії в загальному випадку описується як:

$$X(t) = K(t) * S(t) + n(t) \quad (1)$$

За наявності радіопротидії модель каналу може бути описана як:

$$X(t) = K(t) * S(t) + n(t) + J(t) \quad (2)$$

При цьому канал радіопротидії, аналогічно каналу зв'язку з БПЛА, може бути підданий впливу багатопроменевості і на вхід приймача надходить адитивна перешкода, що описується як:

$$J(t) = K_{ECM}(t) * S_j(t) + n(t) \quad (3)$$

Слід зазначити, що адитивна завада $n(t)$ у виразах 2 і 3 це та сама завада, обмежена по смузі частот вхідним трактом і фільтрами основної селекції приймача БПЛА.

На вхід приймача станції радіорозвідки надходить сигнал, який можна описати аналогічно (1). В ідеальному варіанті станція радіорозвідки розпізнає наявність сигналу управління БПЛА, класифікує його, визначає параметри (частота несучої, вид модуляції, швидкість передачі). Оскільки вимоги за часом реакції станції радіорозвідки та включення системи радіоподавлення не є «жорсткими» в порівнянні з тими, що пред'являються до радіолокаційних систем радіоелектронної боротьби, обробка сигналу в реальному масштабі часу не потрібна і може виконуватись із записаним фрагментом сигналу. Після цього станція радіоелектронної боротьби формує сигнал навмисної перешкоди. В якості такого сигналу можуть бути використані такі завади:

- Енергетична шумова завада (широкосмугова, або вузькосмугова). У першому наближенні вона може розглядатися як рівномірний «білий шум», що випромінюється в діапазоні робочих частот станції управління БПЛА (широкосмугова завада) або в смузі робочих частот каналу управління (вузькосмугова завада). Використання широкосмугової завади вимагає від станції великої потужності для досягнення N_0 достатнього для забезпечення

$SNR < SNR_{min}$, при якому ймовірність помилкового прийому приймачем БПЛА BER гарантовано перевищить заданий рівень (менше 10^{-3});

- Енергетична структурована завада, яка випромінюється на робочій частоті каналу управління БПЛА і повторює його параметри (вид модуляції, смуга частот). Вплив такої завади на канал зв'язку призводить до зриву синхронізації (частотної, фазової, часової) та повного руйнування інформаційного повідомлення. Результати випробувань впливу такої завади на канал зв'язку з модуляцією QPSK показали, що частковий зрив синхронізації в каналі зв'язку відбувається вже при $P_s/P_j = 10 \text{ dB}$, а повне руйнування каналу при $P_s/P_j = 6 \text{ dB}$. Ці випробування проводилися з використанням SDR трансиверів *Arradio* [4] в якості основного і *Pluto SDR* [5] в якості джерела перешкоди, при цьому відстань від передавачів до приймача була однаковою. Для порівняння, в результаті аналогічних випробувань впливу на канал з обмеженою фільтрами приймача смугою частот адитивного білого шуму частковий зрив синхронізації відбувався при $P_s/P_j = -3 \text{ dB}$, повне руйнування каналу при $P_s/P_j = -6 \text{ dB}$;

- Імітаційна завада типу атак повторення (replay attack), при якій в якості сигналу завади використовується запис реального сигналу в каналі зв'язку (наприклад з прямолінійним рухом БПЛА), яка повторює всю структуру сигналу, включаючи елементи криптозахисту каналу. Для ефективного впливу такої завади на канал зв'язку на вході приймача має виконуватись умова $P_j/P_s > P_{jmin}$. Результати випробувань у каналі зв'язку з QPSK модуляцією без завадового кодування показали, що P_{jmin} склало 10 dB при ймовірності помилки $BER < 10^{-3}$;

- Імітаційна завада повного чи часткового заміщення інформаційного повідомлення у вигляді введення помилкових даних (false data injection attack). Такий вид завад є найбільш шкідливим з точки зору «живучості» БПЛА, оскільки він дозволяє повністю перехопити керування безпілотним апаратом. Для реалізації такого виду завади станція радіорозвідки повинна повністю детектувати інформаційне повідомлення, включаючи криптозахист і після цього сформувати нове змінене повідомлення. Для ефективного впливу такої завади на канал зв'язку також має виконуватися умова $P_j/P_s > P_{jmin}$.

Література

1. 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
2. "Groza-S" counter-UAV electronic warfare station: <https://www.bvpservice.by/en/catalog/radio-intelligence-and-electronic-warfare-equipment/groza-s-counter-uav-electronic-warfare>
3. REX-2: <https://zala-aero.com/production/means-of-ew/rex-2/>
4. HSMC ARRADIO Daughter Card: <https://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&No=946>
5. ADALM-PLUTO. Software-Defined Radio Active Learning Module: <https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html#eb-overview>