Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

Зав. кафедрою БІСТ

Сергій РАССОМАХІН

_____

« » 2022р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Дослідження захищеності каналів передачі даних і управління безпілотними літальними апаратами»

оцінка « » Керівник к. т. н., с. н. с. Сватовський І. І.

Голова ЕК Рецензент к.т.н., доцент Бакуменко Н.С.

Доценко С.І. _____ Виконавець : студент групи КБ-61

Конюшенко Р.В.

Харків – 2022

РЕФЕРАТ

В даній пояснювальній записці було використано 60 сторінок типу А4, 5 ілюстрацій, 9 таблиць, також були зроблені запозичення з 12 джерел за переліком посилань.

Об'єкт дослідження – захищеність каналів управління та передачі даних.

Предмет досліджень – методи формування і обробки сигналів, шифрування в каналах зв'язку та протидії засобам радіоелектронної боротьби.

Метою науково-дослідницької роботи є дослідження захищеності каналів передачі даних і управління БПЛА, визначення вразливих місць у методах шифрування даних та забезпечення захищеного зв'язку з літальними апаратами.

Написана робота являється результатом дослідження, опрацювання відповідних ресурсів, де було розглянуті відповідні технології та їхня реалізація, досягнувши мети, відповідно до мого дослідження, технологічного та програмного обладнання, які являються сучасними та використовуються повсякчас у різних силових структурах ключових відомств, що використовують безпілотні літальні апарати та сучасні методи і засоби протидії їм як знаряддя своєї праці.

В першому розділі було розглянуто безпілотний літальний апарат як сучасний пристрій, з конструкторської сторони, розглянуті основні життєзабезпечувальні для літального апарату засоби, а також засоби побудови каналів передачі даних від безпілотного літального апарату до пунктів управління ним. У другому розділі розглянуте практичне питання протидії каналам передачі даних, їхній вплив на кінцевий результат у передаваних сигналах та методи уникнення активного впливу на засоби протидії літальним апаратам.

Ключові слова: БПЛА, РЕП, РЛС, ПРОТИДІЯ, ЗАСОБИ ЗВ'ЯЗКУ, КАНАЛИ ПЕРЕДАЧІ ДАНИХ, РАДІОХВИЛІ, РАДІОТЕХНІЧНА РОЗВІДКА, ВІДСТЕЖЕННЯ, ВИЯВЛЕННЯ, СМУГА КАНАЛУ ПЕРЕДАЧІ ДАНИХ.

ABSTRACT

In this explanatory note, 60 A4 pages were used, 5 illustrations, 9 tables, and borrowings were made from 12 sources according to the list of references.

The object of research is the security of control and data transmission channels.

The subject of research is the methods of signal formation and processing, encryption in communication channels, and countermeasures against radio-electronic warfare.

The purpose of the research is to study the security of data transmission channels and the control of UAVs, identify vulnerabilities in data encryption methods, and ensure reliable and secure communication with the corresponding aircraft.

The writing of the paper is the result of research, the development of relevant resources where appropriate technologies were analyzed, and their implementation for my purposes, according to my research. According to my research, technological and software equipment, which are modern and are used all the time in various power structures of key agencies that use unmanned aerial vehicles and modern methods and means of countering them as tools of their work, are also modern.

In the first chapter, the unmanned aerial vehicle was considered a modern device. From the design point of view, the basic life-supporting means for the aerial vehicle were considered, as were the means of building data transmission channels from the unmanned aerial vehicle to its control points. The second chapter deals with the practical issue of countering data transmission channels, their impact on the final result of transmitted signals, and methods of avoiding active influence on anti-aircraft means.

Key words: UAV, REP, RADAR, COUNTERMEASURES, COMMUNICATIONS, DATA TRANSMISSION CHANNELS, RADIO WAVES, RADIO INTELLIGENCE, TRACKING, DETECTION, DATA TRANSMISSION CHANNEL BAND.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

STANAG	-	STANdardization AGreement – сімейство стандартів, прийнятих у збройних силах країн НАТО
БПЛА	-	безпілотний літальний апарат
ЕОМ	-	електронно-обчислювальна машина
ІТВ	-	інформаційно-технічний вплив
КРУ	-	командна радіолінія управління
МБД-БПП	-	маловисотний, великий дальності, великої продовжувальності польоту
ОСШ	-	відношення сигнал/шум
ОЕР	-	оптико-електронна розвідка
ОЕС	-	оптико-електронний засіб
ППРЧ	-	псевдовипадкова перебудова робочої частоти
РЕП	-	радіоелектронне протидія
РЕС	-	радіоелектронний засіб
РЛС	-	радіолокаційна станція
РРТР	-	радіо- та радіотехнічна розвідка
РСБН	-	радіотехнічна система ближньої навігації
РТР	-	радіотехнічна розвідка
СРНС	-	супутникова радіонавігаційна система
ССС	-	супутникова система зв'язку
ТТХ	-	тактико-технічні характеристики
УБКП	-	універсальний бойовий командний пункт
УВЧ	-	ультрависокі частоти, відповідають частотам від 300 МГц до 3 ГГц
УКХ	-	ультракороткі хвилі, відповідають довжинам хвиль від 10 м до 0,1 мм, що відповідає частотам від 30 МГц до 3000 ГГц

ФАР	-	фазована антенна решітка
ШПС	-	широкосмуговий сигнал

ВСТУП

БПЛА – безпілотний літальний апарат літакового чи гелікоптерного плану без екіпажу на борту, політ якого здійснюється за допомогою віддаленого керування і контролюється комп’ютером по завчасно змодельованим та запрограмованим діям або з абсолютно іншого місця: земля, інший літальний апарат, космос, по різним каналам зв’язку, і політ якого здійснюється абсолютно автономно.

З появою середніх та малих безпілотних літальних апаратів (БПЛА) завдання протидії їх застосуванню в особливо контрольованих зонах суттєво актуалізувалися. Починаючи з середини 2000-х років у засобах масової інформації стали регулярно з'являтися повідомлення про небезпечне використання малих БПЛА в районах аеропортів, а з середини 2010-х – про застосування малих БПЛА для ведення несанкціонованого спостереження важливих об'єктів, проведення терактів та диверсій, перенесення заборонених вантажів (зброї, наркотиків) та широкому використанні БПЛА у військовій справі. У зв'язку з цим у країнах розпочалася активна наукова розробка цього напрями досліджень, що можна судити за великою кількістю наукових робіт тих років. При цьому дана проблематика є відносно новою, оскільки найраніша з робіт з тематики протидії БПЛА відноситься до 2008 р., а початок активних наукових публікацій з цієї тематики відноситься до 2016-2017 років. У результаті до 2020 р. у Західному науковому друку було введено відносно усталені терміни, а також визначено основні напрямки досліджень у цій предметній галузі: «противодія БПЛА» – використовуються такі терміни як «C-UAV», «CUAV», "C-UAVs", "CUAVs" (Counter Unmanned Aerial Vehicles); "Системи протидії БПЛА" - використовуються такі терміни як "C-UAS", "CUAS" (Counter Unmanned Aircraft Systems), "C-UAV system", "CUAV-system", "AUDS" (Anti-UAV Defense System),

Counter-Drone Systems; "технології протидії БПЛА" - використовуються такі терміни як «Anti-Drone Technologies» та «Counter-UAVs Technologies».

При цьому, якщо на початковому етапі появи завдання протидії БПЛА (на початку 2000-х рр.), це завдання вирішувалося виключно засобами ураження (ракетами та снарядами) зенітно-ракетних комплексів (ЗРК) протиповітряної оборони (ППО), то в даний час наразі фахівці усвідомили, що пряме відображення масованого нальоту БПЛА засобами ЗРК ППО, по-перше, невиправдано економічно через використання дорогих ракет за великою кількістю відносно дешевих БПЛА, а по-друге, це веде до швидкого вичерпання бойового ресурсу ЗРК та подальшої їх нездатності відбити удар пілотованої авіації, а також крилатих ракет високоточної зброї (СОТ). У зв'язку з цим нині широко досліджуються нові способи протидії БПЛА, у тому числі такі як застосування засобів радіоелектронного протидії (РЕП), так і альтернативні види використання енергії. Способи протидії БПЛА на основі спільного використання комплексів РЕП і ЗРК вже активно використовуються в практиці локальних бойових дій. Аналіз публікацій у сфері протидії БПЛА показує, що серйозних робіт з даної тематики досить мало, а в переважній кількості досліджень у цій галузі переважають надмірно оптимістичні висновки щодо успішності поразки всіх видів БПЛА існуючими вітчизняними засобами ППО або ж глибоке переконання у надвисоку успішність засобів РЕП. Водночас проблема протидії БПЛА, і, особливо, малим БПЛА, є надзвичайно складною, багатогранною, і досі ефективно не вирішеною.

Основною причиною використання БПЛА є їхні малі розміри та концепція військових стратегій про те, що техніку зробити набагато легше, аніж добре навчити гарного солдата.

На сучасному етапі розвитку БПЛА призначені для вирішення широкого спектру задач, наприклад, спостереження (розвідка), нанесення ударів, транспортування вантажів, цілевказання, ретрансляція даних при їх дистанційним

управлінні оператором, чи шляхом автономних дій по завчасно закладеним програмам.

1 ПРИЗНАЧЕННЯ І КЛАСИФІКАЦІЯ БПЛА. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ БПЛА

1.1 Оцінка ефективності БПЛА

На сучасному етапі розвитку БПЛА призначені для вирішення широкого спектру задач, наприклад, спостереження (розвідка), нанесення ударів, транспортування вантажів, цілевказання, ретрансляція даних при їх дистанційним управлінні оператором, чи шляхом автономних дій по завчасно закладеним програмам.

Оцінка ефективності бойового використання БПЛА, ефективність/ціна:

Одним з основних критеріїв оцінки доцільності використання БПЛА являється показник ціна/ефективність, а саме власне ціна до виконаної бойової задачі, визначається за такою формулою[1]:

$$C_{цз} = \frac{C_{пц}}{P_{йз}},$$

де $C_{цз}$ – це приведена ціна виконання поставлених задач, $C_{пц}$ – повна ціна виконання виконання задачі, $P_{йз}$ - ймовірність виконання поставленої задачі.

Очевидно, що критерії $C_{пц}$ та $P_{йз}$ являються дещо статистичними, тож їхні формули приводяться нижче:

$$C_{пц} = N_{вт}C_{1БПЛА} + C_{1ч}T_{ч}(N_{БПЛА} - N_{вт}) + C_{сн} + C_{вик},$$

де $N_{вт}$ – кількість втрачених літальних апаратів, $C_{1БПЛА}$ – ціна одного БПЛА, $C_{1ч}$ – ціна однієї години польоту, $T_{ч}$ – час польоту при виконанні задач, $N_{БПЛА}$ – кількість апаратів доступних для виконання завдання, $C_{сн}$ – ціна спорядження, снарядів, та тому подібне, $C_{вик}$ – ціна забезпечення виконання задачі.

Ймовірність успішного виконання задачі, визначається лише якщо б хоча б один з БПЛА досяг цілі і виконав завдання:

$$P_{йз} = 1 - (1 - P_{вз})^{N_{БПЛА}},$$

де $P_{вз}$ – це ймовірність виконання окремих завдань з поставленої задачі.

Таким чином, випливає, що ймовірність це дещо відносна величина, яка залежить від маси факторів і визначається лише після хоча б одного успішного виконання. Але тенденції розвитку БПЛА у світових конструкторських бюро ведуть до того, що ціна одного примірника та його обслуговування зменшується, а бойова потужність збільшується, що само по собі покращує ймовірність і зменшує ціну всього завдання, а отже підвищує показник ефективність/ціна.

Таким чином, можна зробити висновок, що на сьогодні БПЛА становлять нову гілку розвитку літальних апаратів зі своєю концепцією використання та стратегією дій, яким досі не знайдено достатньо рівноцінного за ефективністю і ціною засобу протидії, але при достатньому спектрі в цій роботі розглянеться деякі з них.

Через усе це безпілотні літальні апарати стають достатньо прогресивною платформою для розвитку, які вже використовуються для успішних завдань, і в майбутньому вони лише будуть розвиватися і прогресувати у своїй конструкторських ідеях та являється однією з передових технологій без якої неможливо уявити майбутнє, в якому безпілотні літальні апарати стануть більш доступними для масового населення планети, через що почне розвиток поза законної діяльності подібних літальних апаратів, а тому їм має передувати подібні літальні апарати в силових структурах різних відомств різних країн, а також методи протидії їм без залучення вище згаданих організацій.

1.2 Призначення, переваги та недоліки БПЛА

Сьогоднішній етап розвитку людства надає майже необмежений доступ виробників БПЛА до технологій світу, що не обмежує можливості передових компаній у розбудові їх літальних апаратів. Але основним покупцем, в подальшому користувачем стають збройні формування, які власне і диктують вимоги до виробників.

В основній своїй масі БПЛА вирішують такі основні задачі:

- Ведення спостереження і розвідки, в тому числі і в реальному часі;

- Нанесення ударів по всім доступним цілям, самостійно чи носимими засобами ураження;
- Постановка радіоелектронних завад;
- Цілевказання для інших видів ураження, а також корегування їх використання;
- Транспортування і доставка вантажів і засобів в заданий район;
- Ретрансляція даних між віддаленими абонентами зв’язку;
- Відволікання уваги чи використання їх в якості псевдо цілей.

Основними перевагами БПЛА, що ускладнюють задачу їх виявлення і протидії, є:

- Можливість віддаленого виконання задач при безпечному віддалення оператора і повного його інформування в задачі, виконуваній цим апаратом, в реальному часі;
- Використання широкого спектру малогабаритних цільових навантажень на сучасні радіолокаційні прилади і тому подібне;
- Можливість тривалої присутності над зоною завдань, а також можливість самостійного подавлення та ураження засобів протидії БПЛА;
- Низька помітність БПЛА в радіолокаційному та оптичному діапазоні за рахунок менших малогабаритних характеристик відносно інших літальних апаратів, а також через використання великої кількості різних композитних матеріалів таких як: пластик, келар, карбонові суміші і таке подібне;
- Можливість звершувати маневри з високими перевантаженнями, а також використання таких режимів польоту, що призводять до суттєвого зниження ефективності сучасних і перспективних засобів противодії БПЛА, наприклад, мала висота, мала швидкість, малий розмір, що у зв’язці з активним рельєфом та інших предметів, сприйматиметься не як подібний літальний апарат, і тому подібне;

- Мала геометрична форма, що знижує ймовірність ураження засобами зенітної артилерії, а також різних типів снарядів сучасних засобів протиповітряної оборони;
- Зниження виявлення БПЛА через відносно меншу шумність та використання режимів радіомовчання до підльоту до місця завдання.

Специфіка льотно-технічних характеристик БПЛА, що визначає ряд важливих переваг для їх побудови, конструювання і використання:

- Використання класичної аеродинамічної схеми, що забезпечує стійкість та простоту управління, зменшує затрати на обрахунок самостійного польоту тими засобами і попередньо встановленими програмами без втручання оператору БПЛА;
- Можливість використання електричних двигунів, що несе низку переваг таких як: відносно двигунів внутрішнього згорання дає безшумність, простоту використання і подальшої експлуатації і тому подібне;
- Можливість використання альтернативних джерел енергії, наприклад, сонячних систем, що в рази збільшить автономність руху без повернення на місце постійної дислокації;
- Значне зниження проблем і затрат з перебазуванням, базуванням, технічним обслуговуванням та іншим, у зв’язку з малим габаритами усіх компонентів систем використання, керування і власне самих БПЛА;
- Низька вартість розробки і експлуатації відносно інших літальних апаратів, що виконують низку аналогічних завдань, що дає змогу зберегти найцінніший навчений персонал.

Недоліками БПЛА є:

- Для деяких категорій БПЛА обмеження використання у зв’язку з погодними умовами, такі як: неможливість використання майже всіх БПЛА при сильному вітрів більше 10 м/с, проблематика підйому і

посадки за сильних поривах вітру, при використанні малих БПЛА важливу роль відіграє вологість повітря і тому подібне;

- Через недостатній розвиток БПЛА в сучасних передових країнах, використовуються мало інтелектуальні системи управління в автономному режимі;
- Низька секретність і скритність каналів зв’язку і передачі даних;
- Низька живучість конструкцій, через використання легких композитних матеріалів, що призводить до малого протидії сильним зовнішнім силам, що можуть дезорієнтувати системи керування БПЛА та його оператора, наприклад, сильні пориві вітру призводять до так званого перекидання чи некерованих петель, які неможливі на тих чи інших літальних апаратах цього типу, також слабка протидія зовнішнім механічним подразникам: уламкам, птахам, теплим масивам повітря (горіння);
- Низька завадостійкість;
- Відносно мала дальність дії дистанційного управління БПЛА без використання додаткових систем зв’язку або ретрансляції;
- Сильне обмеження по масі та складу корисного навантаження.

1.3 Класифікація БПЛА

При розгляді протидії БПЛА, треба мати певну класифікацію цих літальних апаратів, і визначення пріоритетних цілей. Таким чином різними військовими керівництвами різних військових апаратів світу виділено такі як американська, європейська і країн ближнього сходу, представлені на таблицях 1.1-1.3 [2], що в свою чергу надасть нам змогу зробити певну уніфікацію з доступних матеріалів і в подальшому в роботі спиратися саме на неї як на найрентабельнішу систему класифікацій подібних безпілотних літальних апаратів.

Таблиця 1.1 – Американська класифікація

Класифікаційний тип	Маса, кг	Висота польоту, км	Швидкість, км/год	Приклади
I	0-9	до 0,365	до 185	RQ-11 Raven, RQ-20 Puma, Wasp III, RQ-16 T-Hawk
II	9,5-25	до 1,07	до 460	ScanEagle
III	більше 600	до 5,5	-	RQ-2 Pioneer, RQ-5 Hunter, RQ-7 Shadow, RQ-21 Blackjack
IV	більше 600	до 5,5	-	RQ-1/MQ-1 Predator, MQ-1C GreyEagle, X-47, YMQ-18 Hummingbird, MQ-8 Fire Scout
V	більше 600	вище 5,5	-	RQ-4 Global Hawk, MQ-9 Reaper

З вищезгаданих класифікацій виділяють більше стандартизовану і гармонізовану систему класифікацій, таблиця 1.4.

Також, через основну загрозу БПЛА у вигляді будь яких систем протиповітряної оборони, зазвичай, їх розділяють за швидкістю, адже після можливості виявлення виділяють саме можливість протидії, де активну роль грають зенітно-ракетні комплекси, які обмеженні в часі на протидію.

Класифікація по швидкісній ознаці:

- Малошвидкісні – зі швидкістю польоту до 200 км/год, і номінальною до 250 км/год;
- Середньошвидкісні – зі швидкістю до 400 км/год і номінальною до 450 км/год;
- Швидкісні – зі швидкістю від 350 км/год, при середній швидкості в цьому класі у більшості виробників в 900 – 950 км/год.

Таблиця 1.2 – Західноєвропейська класифікація

Класифікаційний тип	Висота польоту, км	Середній радіус дії, км	Середній час польоту, год	Приклади
Micro-UAV (мікро-БПЛА)	0,6	2	до 1	EMTAIadin (Німеччина)
Mini-UAV или Close-Range UAV(міні-БПЛА чи БПЛА ближнього радіуса дії)	до 2	до 10	до 2	Bird Eye 400 (Ізраїль)
Short-range UAV (БПЛА малого радіуса)	до 3	50-150	до 6	Speiwer (Франція)
Medium-range UAV (БПЛА середнього радіусу)	до 6	100-300	до 12	Hermes 450 (Ізраїль)
MALE (Medium-altitude,long-endurance) (середньовисотний БПЛАтривалого польоту)	5-15	200-500	до 24	Patroller (Франція)
HALE (High-altitude,long-endurance) (висотний БПЛА тривалого польоту)	вище 9,1	глобальний	більше 24	Global Hawk (США)

В цій роботі треба зробити акцент на такі категорії БПЛА:

За призначенням:

- Багаторазові (майже всі види безпілотних апаратів);
- Одноразові (БПЛА - псевдо цілі, камікадзе і тому подібне).

Таблиця 1.3 – Східноєвропейська класифікація

Класифікаційний тип	Підйомна вага, кг	Дальність дії, км
Нано - БПЛА ближнього радіусу дії	до 0,25	до 2
Мікро - і міні - БПЛА ближнього радіусу	до 5	25-40
Легкі БПЛА малого радіуса дії	5-50	10-70
Легкі БПЛА середнього радіуса дії	50-100	70-150 (до 250)
Середні БПЛА	100-300	150-1000
Середні – важкі БПЛА	300-500	70-300
Важків БПЛА середнього радіусу дії	500	70-300
Важкий БПЛА великого часу польоту	1500	1500
Безпілотні бойові літаки (ББС)	500	1500

За рівнем військового управління в інтересах якого БПЛА вирішують завдання:

- Стратегічні;
- Оперативно-тактичні;
- Тактичні.

Деяку зрозумілість такого вибору можуть встановити стратегічна цінність БПЛА та їх властивості зв’язку, так наприклад, БПЛА одноразового типу використання визначають використання ними будь яких каналів зв’язку, здебільшого такі літальні апарати не керуються оператором взагалі, і лише використовують попередньо задані маршрути та передають лише інформацію як звичайний апарат аєрозвідки, якщо визначати за рівнем військового управління, то велику увагу вже треба приділити тим чи іншим БПЛА, які використовуються тими чи іншими військовими установами, їхньої важливості, їх оснащенням, їх

засобами зв’язку, їх небезпечність для опонента, власне відносно саме цих характеристик вибудовується тип зв’язку в БПЛА.

Таблиця 1.4 – Узагальнена класифікація

Клас БПЛА	Категорія	Міжнародне позначення	Позначення	Назва	Підйомна вага, кг	Радіус дії, км	Максимальна висота, км	Час польоту, год
Малі	I	η	η	Нано	<0,25	до 1	0,1	<1
		μ	μ	Мікро	<5	до 10	3	1
		Mini	Міні	Міні	<25	10-40	3	<4
Легкі	II	CR	БлД	Ближньої дії,клас 1	25-50	25-70	3	2-4
				Ближньої дії,клас 2	50-150	50-100	3	<6
Середні	III	SR	МД	Малої дальності	<200	до 150	4	6-8
		MR	СД	Середньої дальності	<500	200	5	10-12
	IV	MRE		Середньої дальності з тривалим часом польоту (СД-ТЧП)	500	500	8	10-18
		LADP	БД	Маловисотні великої дальності (МВД)	<250	більше 250	до 4	1,5-2
Важкі	V	LALE		Маловисотні великої дальності і часу польоту	<250	більше 500	4	18
	V-VI	MALE		Средневисотні великої дальності і часу польоту	<1000	більше 1000	8	24
	VII	HALE		Висотний великої дальності і часу польоту	<2500	більше 4000	20	24<
Бойові	VIII	UCAV	Б	Беспілотний ударний	1000<	більше 500	12	1,5-2
		DEC		Беспілотний імітаційна ціль	150-500	0-500	0,05-5	<4
		TGT		Беспілотна мішень	10-10000	5-200	0,05-10	0,5<
Змішані	IX	OPA	ОП	Пілотований за вибором ЛА	<200			
		CMA	ПП	Переобладнаний пілотований ЛА				

1.4 Система управління і будова

За способами управління БПЛА поділяються на:

- автономні;
- напівавтономні;
- керовані.

В залежності від складності і специфіки виконання завдань, що ставляться перед БПЛА, обирається один з способів управління. Зазвичай, великі БПЛА типу «літак» в загальних принципах і ієрархіях літальних апаратів відповідає таким як пілотовані, на відміну від малих, які в свою чергу мають трьохрівневе ієрархічне компонування систем управління:

1) Нижній – рівень, що відповідає за окремі пристроїв, механізмів, датчиків, сканерів і тому подібне.
2) Середній – рівень, що відповідає власне за сам процес польоту спираючись на бортові контролери та модулів, які відповідають за їхню комунікацію, ввід та вивід сигналів управління.
3) Верхній – рівень інтерфейсу та управління безпосередньо оператором БПЛА, де зв’язок будується між ним та програмою польоту через інтерфейс, що зв’язує ще й середній рівень через його контролери.

Нижній рівень управління утворюється за допомогою установки, що приводить всю конструкцію у рух, датчиків навігаційних систем, додаткове обладнання, перспективне для виконання певних цілей і завдань, таке як радіолокаційні станції, обладнання спостереження і тому подібне.

Середній рівень, зазвичай, відповідає бортовим механізмам та засобам управління. Бортова система управління малих БПЛА розміщується на бортових обчислювальних машинах, які в свою чергу управляються відкритими або спеціалізованими операційними системами, останні в свою чергу все більше і більше виборюють нішу операційних систем для БПЛА та вже створюються лише для цього.

Можна класифікувати обладнання БПЛА так:

- Планер і силова конструкція;
- Рушійна силова конструкція;
- Системи енергозабезпечення;
- Системи управління;
- Навігаційні системи;
- Системи телеметрії;
- Системи зв’язку (рис.1.1).

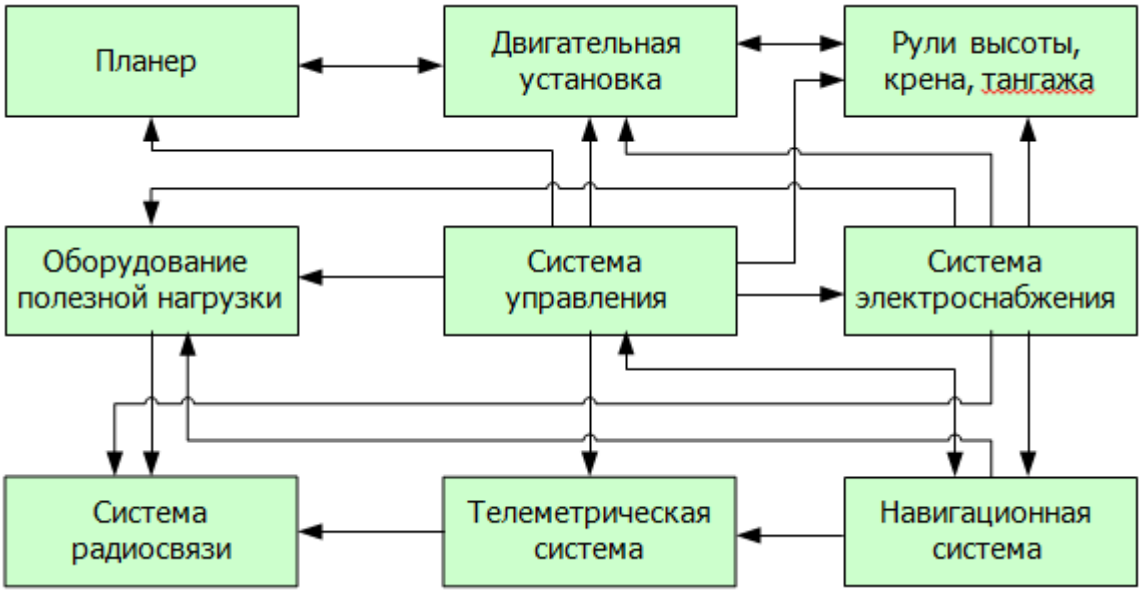

Рисунок 1.1 – Взаємозв’язок між системами БПЛА

Оскільки, БПЛА не перші підкорюють небо, то майже всі з вище згаданих систем мають вже готове рішення для подібного класу техніки військового чи подвійного призначення, але у зв’язку з малими розмірами даних літальних апаратів виникають додаткові проблеми, для прикладу одна звичайна станція зв’язку на літаку займає в середньому від двадцяти до п’ятдесяти літрів вільного простору між силовою установкою, при чому статистичний літак несе від двох до трьох засобів резервного зв’язку, через що у побудові БПЛА, треба враховувати всі можливі ризики відмови від резервних систем зв’язку. Деякі виробники йдуть по стандартному шляху, відмовляючись від малих розмірів задля побудови безпілотного літака, який буде водночас і вразливіший, але й нести більше корисне навантаження та розвідувальну потужність. Також історії відомо

використання БПЛА створених в «домашніх» умовах, які були і є найнебезпечнішими, через відсутність іншої дії, окрім як руйнівної, та через дешевизну і масовість використання в одному масовому запуску. Тому найскладнішою задачею перед виробниками є саме не порушити баланс простоти і технологічності на одному літальному апараті, через що, певні завдання великих систем перекладають на потужні сучасні процесори.

На сьогодні існує багато рішень, де на одній платі розміщується і сама обчислювальна техніка і контролери (висоти, температури, вологості і тому подібне). В свою чергу ця плата розміщується у відповідний відсік, корпус або ж то навіть в найпримітивніших моделях взагалі ніяк не захищається від зовнішніх подразників і інших непереборних сил. Найпопулярнішим і найдешевшим з таких на ринку є системні плати на платформі Rasbery, де на заводі виготовлювачі буде повішено обладнання відповідне від побажань замовника, мається на увазі процесор, що відповідає потребам відповідної операційної системи та її обчислювальним завданням, яка гратиме лише роль інтерфейсу між приймачем радіозв’язку та іншими платами, які замовник додає відповідно окремо, які в свою чергу створюються вже під усіма грифами секретності відповідного виготовлювача та виконують запрограмоване для них завдання (рис.1.2).

Зазвичай всі ці системи працюють окремо відповідно до свого рівня, лише поєднуються системною платою найвищого рівня і далі на радіопередавач. Через що дуже спрощується побудова будь якого БПЛА, адже кожен рівень відповідає лише за свої завдання, тому при грамотному розбитті систем можна отримати ідеальну модульність літального апарату. Тому, зазвичай, на заводах виготовлювачах покупцям пропонують лише готовий комплект з каркасу системи управління та системи зв’язку з наземною станцією, і окремо системи, які відповідають за інші завдання БПЛА.

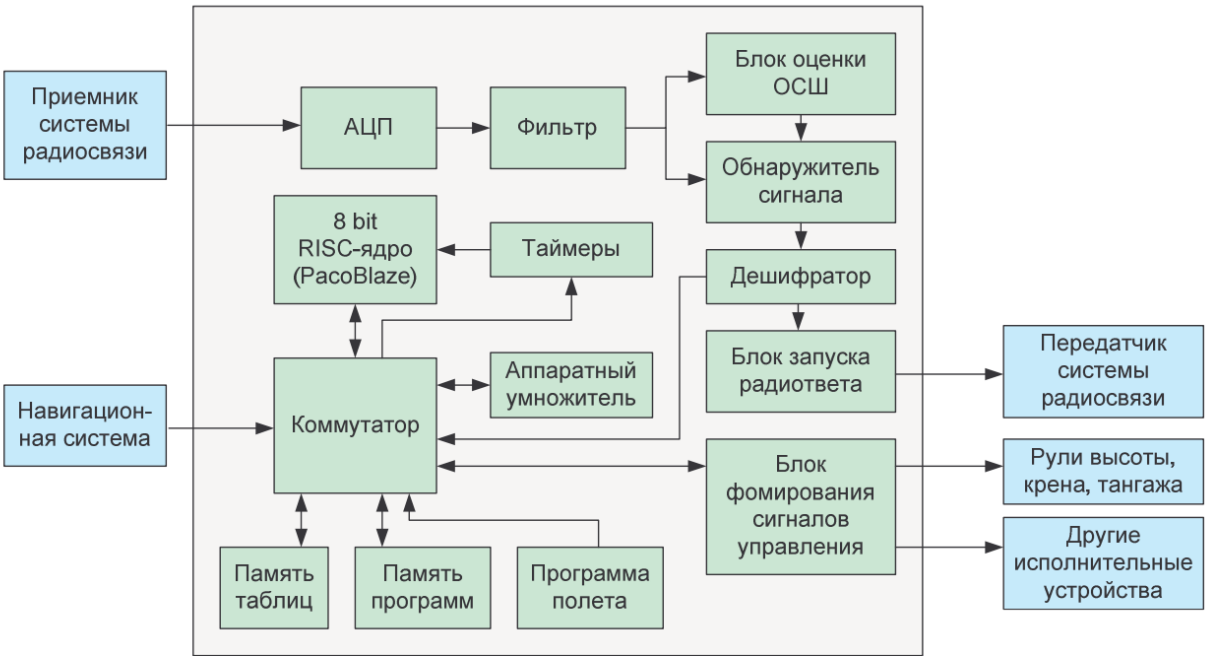

Рисунок 1.2 – Приклад побудови системи всіх механізмів використовуваних на БПЛА

Тому, зараз на ринку можна зустріти готові типові рішення від найбільших виробників тих чи інших обчислювальних процесорів так плат до них, такі як: Qualcomm, Intel та Nvidia. В ці набори входять типові ідеально збалансовані між собою рішення такі як:

- Власне центральний процесор управління;
- Бортова операційно електрона система;
- Графічний процесор, що обробляє всі можливі отримані від інших систем дані;
- Систему зв’язку, в основному на технологіях Wi-Fi (табл.1.5).

Таблиця 1.5 - Порівняльна таблиця найпоширеніших варіантів на ринку

Виробник	Qualcomm Snapdragon Flight	Intel Edison for Arduino	Nvidia Jetson TX1	Leadcore LC1860
CPU	4×Qualcomm Krait 400	22 нм dual-core Intel Atom	64-bit ARM A57 core	6-core Cortex A7
Частота CPU	2,5 ГГц	500 МГц	2 ГГц	2 ГГц

Продовження таблиці 1.5 «Порівняльна таблиця найпоширеніших варіантів на ринку»

GPU	Qualcomm Adreno 330	Intel HD Graphic	Maxwell architecture, 256 CUDA cores	Dual-core Mali T628
Потужність GPU	167 GFLOPs	невідомо	1 TeraFLOPs	невідомо
Використання енергії	невідомо	35 мВт	менше 10 Вт	невідомо
Wi-Fi и Bluetooth	Так	Так	Так	Так
Бінокулярний стерео датчик	Так	Зовнішні датчики	Так	Так
Роздільна здатність камери	4096×2160	Не менше 1280×720	4096×2160	2048×1080
Розмір	58 мм × 40 мм	127 мм × 72 мм	87 мм × 50 мм	41 мм × 61,5 мм
Переваги	Збалансоване рішення за критерієм «ціна/потужність»	Контакт з зовнішніми датчиками; Висока точність точність і широкий діапазон використання	Висока потужність в багато поточних задачах	Низька ціна
Недоліки	Відносно вузька спеціалізація використання	Низька енергоефективність і висока ціна	Низька енергоефективність і висока ціна	Відносно низька потужність

Продовження таблиці 1.5 «Порівняльна таблиця найпоширеніших варіантів на ринку»

Переваги для використання на БПЛА	Енергоефективне рішення для управління БПЛА; підтримується версія для керування групою БПЛА	Висока потужність	Рішеня для управління БПЛА з використанням технологій машинного зору та ШІ	Збалансоване рішення за критерієм «ефективність /ціна»

Верхній рівень управління відповідає архітектурі «безпілотник – пункт управління», що утворюється телеметричним обладнанням, системою збору даних про стан апарату, системою зв’язку та власне сам пункт управління та його обладнання, де обробляються телеметрія, визначається стан та місцезнаходження, модулюються або змінюється програма польоту і відповідно від попередніх даних система повертає команди назад на борт БПЛА.

Найбільш критичним показником для вирішення задач протидії БПЛА є технічні характеристики найслабшої ланки літального апарату, і такою є система зв’язку.

Також потрібно відмітити, що переважна кількість БПЛА не мають можливості взагалі на будь яке прийняття рішень щодо ризиків, загроз, різких змін рельєфу, погоди і тому подібне. Зазвичай вони мають просто якийсь надісланий з пункту управління маршрут він може бути не обов’язково прямим, але дуже часто не враховуються жодні непереборні сили, такі як рельєф, флора та фауна тих територій на яких відбувається політ, а також антропогенних об’єктів: лінії електропередачі, будинки так їхні надбудови, інші літальні апарати.

Тому найпрогресивнішим зараз завданням перед передовими виробниками являється збалансованість між можливістю управління БПЛА, за допомогою штучного інтелекту, швидкодії реагування на загрози, та дешевизною

використання в апаратах, які достатньо ймовірно так чи інакше буде втрачений під час виконання завдань.

З вище сказаного випливає, що на сьогодні не існує абсолютно не вразливого з точки зору управління БПЛА, тож механізм протидії це вплив на його систему управління та системою радіозв'язку, адже коли одна з цих систем виходить з ладу, ми маємо літальний апарат зі статичним маршрутом польоту, а отже при виведенні з ладу системи управління (взагалі не працює, виникнення команд управління, які створюють технічно не поєднуванні команди і порушення правил польоту, що призводить до аварійних падінь, відсутність команд управління від пункту управління противника, перехоплення команд управління), або ж втрата керування пунктом управління противника, після чого літальний апарат виконує план завчасно запрограмованого маршруту або падіння через відсутність команд управління або ж статичне вирівняння і прямування по прямій.

1.5 Система радіозв'язку

Система радіозв'язку БПЛА представляє собою сукупність різних ліній, які в свою чергу використовуються для передачі великих за об'ємом даних телеметричного обладнання або простих, але важливих даних управління.

Тому інформацію для передачі через лінію зв'язку поділяють за об'ємом даних, рівень важливості, рівня крипто захисту.

Найпоширенішим рішенням для управління і обміну інформації з БПЛА є створення так званих напрямків важливості цієї інформації:

- Напрямок вгору визначається від пункту управління до БПЛА і включає в себе передачу команд управління польотом, та командами управління спец апаратурою і засобами корисного навантаження, що розміщуються на БПЛА
- Напрямок вниз визначається власне БПЛА до пункту управління і включає в себе телеметричну інформацію підсистем БПЛА та ці ж

дані, що характеризують спецапаратуру, наприклад: кут нахилу польоту, температуру систем, завантаженість обчислювальної техніки, підтвердження виконання команд і тому подібне. А також високошвидкісна лінія передачі даних від спецапаратури і технічних засобів і контролерів корисного навантаження

Вищезгадані лінії можуть відрізнятися і методами побудови, наприклад, кожан лінія може організовуватися в своєму окрему частотному діапазоні, або ж навіть використовувати різні режими з ретрансляцією або ж її відсутністю, зазвичай, так чи інакше це залежатиме від типу і важливості цих даних.

Різними службами різних країн і різних відповідно пропрацьованих сценаріїв використання БПЛА з різними методами зв'язку, тож спираючись на малу культуру використання БПЛА країн агресорів зазначених в доктрині про безпеку України будемо спиратися на найпростіші методи.

Використання всієї ширини радіочастот при прямій видимості від пункту управління до БПЛА, використання інших літальних апаратів як ретрансляторів між БПЛА та пунктом управління, а також використання систем супутникового зв'язку.

Через використання країною агресором своїх БПЛА на не підвладній території та високій ймовірності втрати малих БПЛА пропустимо використання технологій зв'язку доступних цивільним особам, наприклад: мережі мобільних операторів, мережі Bluetooth та Wi-Fi і тому подібне.

При неотриманні команд управління польотом від пункту управління, як вже згадувалося раніше, в основній своїй масі БПЛА переходять в автономний режим, де можуть бути реалізовані як найпростіші алгоритми, такі як повернення додому, прямолінійний політ, баражування, політ на малих висотах з імітації польоту великих птахів, так і більш складних (в залежності від наявності в пам'яті електронних карт місцевості або інших навігаційних систем на БПЛА).

1.6 Система навігації

Навігаційна система БПЛА в різних конструкторських програмах реалізовується дуже по-різному, може мати різну складність, і власне базуватися на різних фізичних факторах.

Так в залежності від розмірів і складності завдань можуть використовуватися такі види навігаційні системи:

- Навігаційна система, що базується лише на апаратних можливостях лише БПЛА, такі як в найпростіших безпілотниках навігаційна система супутникового зв'язку, що використовується в смартфонах.
- Проста інтегрована навігаційна система, основана на суміщенні різних показників механічних інерційних навігаційних систем, таких як обрахунок кожної дії систем управління польотом (поворот закрилок при зльоті, показники висотоміра, швидкість польоту при певному спротиві вітру з різних сторін відносно літального апарату)
- Інтегрована навігаційна система на основі високої кількості високоточних датчиків (лазерне або радіо визначення висоти, відстані від пункту управління, кут відхилення від декількох пунктів управління).
- Інтегрована навігаційна система на основі комплексності даних декількох навігаційних систем та пристроїв, таких як: авіаційні системи навігації, супутникові дані місцезнаходження, висотомірів, радіосистеми найближчої точки навігації, систем автоматичного спостереження за літальним апаратом. Зазвичай, повністю повторює систему навігації пілотованого літального апарату і характерна для великих і тяжких БПЛА.

Системи навігації на БПЛА другого і третього типу, використовується на здебільшого середніх і малих безпілотниках, але через збалансованість ціни та дрейфу гіроскопічних датчиків, швидкодії обчислювальної техніки не може гарантувати точного визначення місцезнаходження без поправок від пункту управління, в середньому без корегування похідних даних за хвилину польоту

може бути до 3 метрів в будь якій площині систем x, y, z, а на кожній наступній хвилині польоту без коригування буде лише рости в геометричній прогресії.

В переважній кількості на середніх та важких БПЛА використовується надточна навігаційна система четвертого типу, але за похибку менше одного процента відбувається плата вагою, так середня вага подібної навігаційної системи складає вісім кілограмів, що інколи може погано вплинути на взлітні характеристики середніх БПЛА.

Також, через достатньо новий ринок для всіх виробників БПЛА, навігаційні системи дуже стрімко розвиваються. До таких вдосконалень можна віднести:

- Використання навігації багато станційних локальних РСБН чи систем імітаторів сигналів. Через локальність цих станцій можуть розміщуватися мобільно на будь якому транспорті.
- Використання електронних карт місцевості, політ по яким відбувається по даним висотомірів та РЛС чи ОЕС видимого діапазону.
- Використання для навігації різних автономних систем технічного зору, такі як за акустично чи радіосигналом побудова карт місцевості в реальному часі та звірка їх з пройденим шляхом.
- Автономний політ БПЛА в напрямку до цілі, що підсвічується певними джерелом випромінювання, зазвичай використовується в системах управління ракетами.

1.7 Висновки за перший розділ

Безпілотний літальний апарат, станція керування та зв’язку – це дуже складний і технологічний комплекс засобів і пристроїв, які в своїй сукупності мають ефективне використання дуже простих на перший погляд літальних апаратів.

Але для максимальної технологічності виробники змушені відмовлятися від малих габаритів, що покращують можливість не виявлення, і навпаки чим

більш невидимим стає літальний апарат, тим менше він несе корисного навантаження.

БПЛА залежне від зовнішніх джерел інформації, чи то дані управління польотом чи то дані навігаційної системи, тому як найслабшу ланку було визначено радіозв’язок та навігаційна система, тому в наступних розділах буде розглянуто пряму систему боротьби з БПЛА як боротьбу з відповідними системами літального апарату.

З вищезгаданих розділів, також можна виділити першочергові критичні місця, які можуть так чи інакше піддатися впливу зовнішніх втручань, що призведе до того, що буде втрачено контроль над групою літальних апаратів, або ж піддатися несанкціонованому контролю над керівними станціями, що призведе до виведення даного комплексу до поки не можливо буде забезпечити безпечність роботи БПЛА.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ПРОТИДІЇ БПЛА

2.1 РЕП переваги і недоліки

Одним з найперспективніших методів протидії БПЛА вважається засоби РЕП, ресурс при наявності зовнішнього живлення вважається майже безмежним. Одні з найпоширеніших сценаріїв використання засобів РЕП та їх комбінації:

- Придушення чи нав’язування помилкових режимів роботи пункту управління та безпосередньо каналам передачі даних БПЛА
- Придушення чи нав’язування псевдо режимів роботи каналу навігації БПЛА, що базується на прийомі та обробці сигналів від пунктів управління.

Застосування засобів РЕП проти БПЛА в порівнянні з засобами вогневого ураження мають певні переваги:

- засоби РЕП не витрачають будь-яких матеріальних засобів ураження, а лише відновлюваний ресурс електромагнітної енергії;
- сучасні засоби РЕП можуть формувати широкий спектр радіоелектронних перешкод (рис. 2.1[1]), обираючи ті з них, які максимально ефективні щодо суб’єктів протидії;
- засоби РЕП мають «купольний ефект», що дозволяє одночасно вражати велику кількість БПЛА, які використовують однакові або подібні що мають подібне радіо електронне обладнання, єдину командну радіолінію управління, принципи навігації, засновані на використанні сигналів тих самих СРНС;
- за умови успішного придушення конкретних цілей, як окремих ІРІ, можна створити засобами РЕП, так звану безпілотну зону для БПЛА, що керуються ІРІ з певними параметрами, наприклад, пункт управління БПЛА, що формує КРУ з певною структурою сигналів, або сигнали певної СРНС;

- в окремих випадках, за умови успішного виявлення, протидії та власне класифікування методів зв’язку БПЛА, наприклад, структура сигналів і формат повідомлень, що передаються в КРУ і в каналі навігації, то засоби РЕП можуть повністю перехоплювати управління або ж займатися нав’язуванням своїх сигналів на рівні з базовою станцією керування.

Рисунок 2.1 – Номенклатура можливих радіоелектронних перешкод

Також, одночасно з вищезгаданими перевагами, засобам РЕП властиві такі недоліки:

- засоби РЕП можуть впливати, лише за електромагнітної доступності БПЛА;
- придушення каналу управління та навігації БПЛА можливе тільки за умови активного дистанційного керування БПЛА, з використанням навігації за сигналами СРНС. Політ БПЛА в режимі «радіомовчання» за заздалегідь закладеною програмою, як правило, не дозволяє розкрити факт польоту такого БПЛА засобами РРТР та, відповідно, сформувати цілевказівку засобам РЕП на протидію таким БПЛА;
- застосування засобів РЕП проти БПЛА в умовах мирного часу обмежено певною потужністю, внаслідок необхідності виконання вимог щодо електромагнітної сумісності з іншими РЕМ. Ці РЕМ можуть перебувати як на об'єкті, що захищається від БПЛА, так і можуть бути іншими засобами протидії БПЛА, які, поряд з засобами РЕП, інтегровані в комплекс протидії, наприклад, РЛС або засоби РТРР виявлення БПЛА;
- енергетична ефективність засобів РЕП зменшується пропорційно квадрату відстані, внаслідок цього засоби РЕП формально тільки для ближньої дії, причому їх ефективність зростає при наближенні БПЛА до місця розташування засобів РЕП, так званий контрольованому рубіж;
- загороджувальні перешкоди, що володіють «купольним ефектом» і орієнтовані на придушення кількох каналів керування та навігації мають низьку енергетичну ефективність, особливо, в умовах використання для керування та навігації БПЛА широкосмугових сигналів (ШПС)) та сигналів з псевдо випадковою перебудовою робочої частоти (ППРЧ);

- перешкоди, які діють прицільно за частотою та структурою сигналів КРУ та СРНС, які є найбільш ефективними для порушення управління БПЛА, зокрема, шляхом нав'язування хибних режимів польоту, даний тип перешкод для свого формування вимагає оперативного розкриття засобами РРТР структури сигналів і формату переданих повідомлень у КРУ і в каналі навігації, або завчасного формування баз даних (БД) відповідних сигналів, що використовуються в конкретному БПЛА. У результаті такі високоефективні перешкоди ефективно можуть бути використані тільки проти обмеженого числа окремих моделей БПЛА, і більш придатні для демонстрації можливостей засобів РЕП, ніж для реальної протидії групи БПЛА;
- ефективність засобів РЕП істотно залежить від сценарію застосування БПЛА, профілю їх польоту, рівня автономності тощо. Але зазвичай, стандартною процедурою є вибір профілю польоту на низькій висоті, з урахуванням складок місцевості, завчасне формування для навігаційної системи профілю польоту по електронній карті місцевості, дотримання режиму «радіомовчання», а також застосування інших способів радіоелектронного захисту БПЛА істотно знижує можливості засобів РЕП.

2.2 Радіоелектронне придушення навігаційної системи БПЛА

При розгляді питань придушення каналу навігації БПЛА необхідно враховувати, що навігаційна система БПЛА може мати різний рівень складності та враховувати для визначення розташування БПЛА кілька сигналів, що надходять від датчиків різної фізичної природи:

1) навігаційна система, заснована лише на апаратурі споживачів (АП) найбільш поширених СРНС – така система характерна для найпростіших малих БПЛА-квадрокоптерів;

2) проста інтегрована навігаційна система, на основі комплексування даних мікромеханічних інерційних навігаційних систем (ІНС) та АП СРНС – така навігаційна система характерна для широкого класу малих БПЛА-квадрокоптерів для професійного використання з різною метою;

3) інтегрована навігаційна система, на основі комплексування даних кількох навігаційних пристроїв: мікромеханічних ІНС, АП СРНС, барометричного висотоміра, радіо або лазерного висотоміра – така навігаційна система характерна для професійних малих БПЛА, а також для БПЛА середнього класу;

4) інтегрована навігаційна система, на основі комплексування даних кількох навігаційних пристроїв: авіаційних ІНС, АП СРНС, висотомірів (барометричного та радіо), РСБН VOR/DME (Very high frequency Omni directional radio Range/Distance Measuring Equipment) така навігаційна система фактично повністю повторює навігаційну систему пілотованого ЛА та характерна для БПЛА важкого класу.

Говорячи про придушення каналу навігації БПЛА, необхідно чітко розуміти, що сам факт радіоелектронного впливу (придушення або нав'язування неправдивих режимів роботи) стосується тільки сигналів, що приймаються АП від одного або кількох СРНС, що відповідають лише одному каналу з безлічі каналів. надходження даних до навігаційної системи БПЛА. Таким чином, з використанням РЕП можливо забезпечити значне порушення роботи тільки найпростіших навігаційних систем БПЛА. Для БПЛА з повноцінною інтегрованою навігаційною системою, заснованої на використанні кількох каналів отримання навігаційних даних, порушення супутникового каналу (у тому числі і надходження по ньому хибних навігаційних даних, що суперечать даним іншим каналів), у більшості випадків буде виявлено, після чого навігаційна система перестане використовувати супутниковий канал для визначення розташування БПЛА. Зазначимо, що в середніх і важких БПЛА, в переважній кількості випадків, як основний канал формування навігаційних даних використовується інформація

саме від авіаційних ІНС на основі лазерних або волоконно-оптичних гіроскопів. Детально ТТХ таких ІНС розглянуто у роботі. Дані ІНС у середньому забезпечують помилку обчислення колії близько 1,85 км за 1 год польоту. При цьому інформація іншими каналами (дані від АП СРНС, дані висотомірів, сигнали РСБН та АЗН-В) є вторинною і після верифікації та комплексування вона використовується тільки для корекції показань ІНС. Додатково зазначимо, що середні та великі БПЛА, які використовуються для вирішення спеціальних та військових завдань, при цьому в них АП СРСН використовує не «відкриті», а «закритий» сигнали СРНС, що мають більший запобіжний захист і криптозахист. При цьому обладнання навігаційних супутників може формувати окремі зони взагалі без перешкод. Внаслідок цього завдання порушення коректного функціонування навігаційних систем таких БПЛА стає ще більш скрутним, фактично неможливим.

Швидкий розвиток БПЛА призводить до вдосконалення їхнього навігаційного забезпечення, у тому числі, для застосування в умовах поганого прийому сигналів СРНС.

До таких напрямів розвитку належать такі:

1) використання підвищення точності навігації з великою кількістю локальних станцій РСБН чи систем – імітаторів сигналів СРНС, при цьому станції цих систем можуть бути мобільними, знаходячись на автомобілях, і заздалегідь розгортатися у зоні можливого застосування БПЛА. Зокрема, використання подібних систем дозволяє підвищити відношення сигнал/шум на 35-50 дБ у зоні поганого прийому сигналів СРНС та забезпечити прийом навігаційних сигналів при потужностях активних шумових та доплерівських перешкод у зоні дії РСБН;

2) використання для навігації електронних карт місцевості, політ якими здійснюється відповідно до даних радіо або лазерного висотоміра, РЛС або ОЕС видимого діапазону;

3) використання для навігації різних автономних систем технічного будови карт місцевості, контролю поточного розташування БПЛА та пройденого шляху;

4) автономний прямолінійний політ БПЛА у напрямку мети, що підсвічується зовнішнім джерелом випромінювання.

Таким чином, узагальнюючи вище сказане, можна зробити висновок, що застосування засобів РЕП, у тому числі й шляхом формування «інтелектуальних» перешкод, прицільних за частотою та структурою сигналів СРНС, з метою нав'язування хибного визначення та траєкторії польоту, орієнтовано малі навіть проти малих БПЛА із найпростішими навігаційними системами. При цьому високий темп розвитку БПЛА, а також можливість розробки в найближчому майбутньому навігаційних систем на основі електронних карт місцевості або систем технічного зору зробить придушення каналів СРСН марним навіть проти малих БПЛА.

2.3 Особливості радіоелектронного придушення навігаційної системи БПЛА, що ґрунтується на прийомі сигналів СРНС

Системи навігації на переважній кількості малих БПЛА становить АП, що приймає сигнали однієї або кількох СРНС. До найпоширеніших СРНС належать системи: ГЛОНАСС (Росія), GPS/NAVSTAR (США), Beidou (Китай), Galileo (ЄС). Сигнали СРНС формуються на літерних частотах у діапазоні 1,1-1,6 ГГц. Як правило, прості навігаційні системи, що встановлюються на малі БПЛА, використовують інтегрований режим обробки сигналів від кількох СРНС, що забезпечує точність навігації 1-2,5 м як у горизонтальній площині, так і у висотній.

Серед перешкод, що використовуються для придушення каналів СРНС найбільш широко застосовуються:

- шумова перешкода – білий шум високої потужності на частотах каналів СРНС;
- гармонійна перешкода – одночастотне або модульоване гармонійне коливання на частотах корисного сигналу;

- прицільна перешкода, що імітує – перешкода імітує структуру сигналів СРНС з частотною і тимчасовою неузгодженістю, а також з фіксованим значенням фази обгинаючої маніпулюючої функції;
- перешкода стеження – перешкода імітує структуру сигналів СРНС, але із змінною початковою фазою маніпулюючої функції, закон зміни якої відповідає зміні відстані від приймача до станції РЕП;
- загороджувальна перешкода, що імітує набір сигналів супутників СРНС з однаковим частотним неузгодженістю для всіх компонентів і різним тимчасовим неузгодженістю для кожного компонента.

Для організації перешкод, що імітують, потрібна розвідка не тільки несучої частоти і фази, але й амплітуди сигналів СРНС, а також маніпулюючих функцій, що являють собою кодову послідовність для поділу сигналів і навігаційних даних. При цьому для формування прицільної перешкоди та перешкоди стеження, що імітують, необхідна розвідка частотних, фазових та часових параметрів корисних сигналів СРНС. Простішою в реалізації є загороджувальна перешкода, що імітує, оскільки вона не вимагає для формування точних часових параметрів сигналу.

Найбільш ефективними перешкодами для порушення нормального функціонування АП СРНС є перешкоди, що імітують або відтворюють структуру реального сигналу СРНС з частотними, фазовими та тимчасовими параметрами, що дозволяють нав'язати АП СРНС помилковий режим роботи і як наслідок – хибне місцевизначення БПЛА. Модифікація параметрів даних перешкод дозволяє керувати траєкторією польоту БПЛА. При цьому параметри перешкоди повинні бути якомога ближчими до відповідних параметрів реальних сигналів СРНС.

Постановка імітаційних перешкод проводиться у два етапи:

1) постановка шумової перешкоди, загороджувальної каналами СРНС – викликає «відв'язування» АП від поточних сигналів СРНС, переривання режиму стеження та перехід у режим виявлення та пошуку сигналів;

2) формування імітаційної перешкоди з високим енергетичним потенціалом – викликає «прив'язку» АП СРНС до хибних сигналів, з подальшим переходом у хибний режим роботи.

З наведених у таблиці 2.1[1] результатів випливає, що з усіх перешкод, що розглядаються, найменший енергетичний потенціал станції РЕП потрібно при постановці загороджувальної імітаційної перешкоди. При дії загороджувальної імітаційної перешкоди на канал виявлення та канал стеження за затримкою ймовірність придушення АП СРСН становитиме близько 0,9. При поставленні шумової або гармонійної перешкод з енергетичним потенціалом станції РЕП, що дорівнює 8,5 дБВт, ймовірність придушення АП СРНС становитиме близько 0,5. З метою збільшення ймовірності придушення АП РЕП необхідно при постановці шумових перешкод мати енергетичний потенціал станції РЕП порядку 20 дБВт, а при постановці гармонійних перешкод – 25 дБВт.

Результати досліджень придушення каналів АП СРНС при використанні різних типів перешкод показують, що перешкодостійкість стандартних АП СРНС становить 34-36 дБ для АП, що рухаються динамічно, і 38-40 дБ для слабко динамічних АП. [3]

У роботі наведено оцінки рівня потужності навмисних перешкод, які можуть бути створені типовими засобами РЕП на вході приймача АП СРНС авіаційного базування:

- при висоті польоту льотно-підйомного засобу з АП СРНС 100 м:
  - наземні засоби РЕП: -78 ... -166 дБВт;
  - авіаційні засоби РЕП: -82 ... -103 дБВт;
  - тактичне БПЛА із засобами РЕП: -94 ... - 96 дБВт;
  - від малогабаритного закидається передавача перешкод: -81 ... -83 дБВт;
- при висоті польоту льотно-підйомного засобу з АП СРНС 5 км:
  - від авіаційних засобів РЕП: -82 ... -103 дБВт;

- від тактичного БПЛА із засобами РЕП: -97 ... - 99 дБВт;
- від малогабаритного ЗПП: -101 ... -103 дБВт;
- від наземних засобів РЕП: -81 ... -102 дБВт.

Таблиця 2.1 - Результати досліджень придушення каналів АП СРНС при використанні різних типів перешкод

Канал АПСРНС	Тип завад	Ймовірність успішного подавлення каналу АП	Потрібний енергетичний потенціал Станції РЭП, $P_{ПП}G_{ПП}$, дБВт
Канал виявлення	Шумова	0,5	8,5
	Гармонічна	0,5	8,5
	Загороджувальна імітаційна	0,67	–3,6…–9,5
Канал відстеження за частотою	Шумова	0,32	19,5
	Гармонічна	0,32	24,4
Канал відстеження за затримкою сигналу	Шумова	0,5	10,4
	Гармонічна	0,5	54
	Загороджувальна імітаційна	0,67	–3,6…–9,5
Квадратичний детектор	Шумова	0,1	18,7
	Гармонічна	0,1	18,7

Результати експериментальних досліджень, щодо здатності виконання АП СРСН навігаційних задач у режимах виявлення та стеження за сигналами СРСН в умовах шумових та гармонійних перешкод[1-3], представлені в таблиці 2.2.

Таблиця 2.2 - Значення ОСШ на вході АП СРНС, при яких відсутні рішення навігаційних задач [1-3]

Види завад	Режим роботи АП СРСН	Значення ОСШ, дБ
Гармонічна	виявлення	–36…–46
	відстеження	–57…–60
Шумова широкополосна	виявлення	–41…–48
	відстеження	–44…–49

Для підвищення перешкодозахищеності АП СРНС у БПЛА можуть бути використані такі способи та засоби [145, 151, 152]:

- використання далекомірних кодів підвищеної точності, що надходять «закритими» каналами СРНС;
- одночасний прийом та обробка в АП сигналів від різних СРНС (ГЛОНАСС, GPS, Galileo тощо);
- просторова селекція сигналів СРНС;
- комплексування АП з ІНС;
- передкореляційна обробка суміші сигналів та перешкод;
- алгоритмічна посткореляційна обробка сигналів;
- поляризаційна селекція сигналів.

З зазначених способів, найбільшого поширення набув спосіб просторової селекції сигналів СРНС за рахунок установки на БПЛА фазованої антеної решітки (ФАР). Наявність на БПЛА всього лише 6 елементів ФАР дозволяє досить ефективно формувати «нулі» діаграми спрямованості антени (ДНА) у напрямку на наземні джерела перешкод та «максимуми» ДНА ФАР – у напрямку на космічні апарати СРНС, тим самим забезпечуючи просторову режекцію перешкод. [1]

2.4. Радіоелектронне придушення радіоліній управління та передачі БПЛА

Потрібно зазначити, що в порівнянні з завданням радіоелектронного придушення навігаційної системи БПЛА, завдання придушення радіоліній «ПУ –

БПЛА» та «БПЛА – ПУ» не є принципово новим і фактично зводиться до відомого завдання формування на вході засобу зв'язку такого придатного значення ОСШ, яке не дозволяє забезпечити прийом даних з необхідною достовірністю. Дана задача є класичною в теорії РЕП, а особливістю її вирішення, стосовно БПЛА, є облік типів сигнально-кодових конструкцій, що використовуються в радіолініях, типів переданих даних, які і визначають достовірність, а також сигнальних, енергетичних, просторових та інших параметрів радіоліній.

Під час розгляду питань придушення КРУ і каналів передачі БПЛА необхідно враховувати, що підсистема управління і радіозв'язку БПЛА є сукупністю різних ліній, в якій надаються дані принципово різного типу, рівня важливості, обсягу, рівня криптозахисту тощо.

Для управління та обміну даними з БПЛА організовуються такі напрями зв'язку:

- напрям «вгору» – організовується від ПУ до БПЛА і включає:
  - направлення «вгору» КРУ для передачі команд управління БПЛА, а також команд управління спеціальною апаратурою та технічними засобами корисного навантаження, розміщеними на БПЛА;
- напрямок «вниз» – організовується від БПЛА до ПУ і включає:
  - напрям «вниз» КРУ для передачі телеметричної інформації (ТМІ) про стан підсистем БПЛА, спеціальної апаратури та технічних засобів корисного навантаження, а також квитанцій про виконання команд управління;
  - високошвидкісна лінія передачі даних від спеціальної апаратури та технічних засобів корисного навантаження, розміщених на БПЛА.

Вищевказані лінії зв'язку можуть організовуватися в різних частотних діапазонах, використовувати різні режими з ретрансляцією і без неї,

використовувати різні сигнально-кодові конструкції, спеціально адаптовані під тип і важливість даних, що передаються.

Найбільш критичним елементом для функціонування БПЛА є КРУ. Саме придушення КРУ у напрямку «вгору» здатне забезпечити максимальний ефект з точки зору порушення нормального функціонування БПЛА. Разом з тим при вирішенні цього завдання зустрічається низка труднощів:

- розголошення параметрів лінії КРУ «вгору» вимагає спостереження за ПУ, при цьому ПУ може перебувати на суттєвому віддаленні від засобів РЕП та використовувати для організації зв'язку антенну систему з гостронаправленою ДНА і з придушенням бокових пелюсток, що різко знижує можливості засобів РРТР у складі комплексу РЕП щодо розголошення параметрів КРУ БПЛА, важливих для її подальшого придушення;
- варіанти організації КРУ на тих самих частотах в дуплексному режимі зустрічаються виключно на простих малих БПЛА. Варіантом організації КРУ для БПЛА спеціального призначення, що досить часто зустрічається, є формування напрямків "вгору" і "вниз" не тільки на різних частотах, але навіть у різних частотних діапазонах (L, C, S, Ku діапазони), і з різними частотно-часовими параметрами. У результаті успішний розголос параметрів КРУ «вниз», при підльоті БПЛА до контрольованого рубежу, не дозволяє сформувати цілевказання засобам РЕП для тиску КРУ у напрямку «вгору»;
- у КРУ, як у найбільш важливому елементі системи управління БПЛА, широко використовуються різні способи підвищення завадостійкості: ШПС, автоматична перебудова частоти на найменш уражені перешкодами канали, використання режиму ППРЧ, резервування каналів, багаторазове дублювання команд управління та переданих ТМІ, використання антен з спрямованими ДНА, високий рівень криптозахисту даних і т.д.

Проте першочерговими проблемами є те, що навіть при успіху придушення КРУ, відсутні гарантії, що БПЛА припинить свій політ у бік контрольованої зони. Як правило, за відсутності зовнішнього управління, БПЛА переходить в автономний режим, при цьому його дії в цьому режимі повністю визначаються попередньо закладеною програмою автономного польоту. При цьому суттю програми може бути не «повернення до ПУ», а продовження подальшого польоту до контрольованого об'єкта та виконання цільового завдання з використанням усіх доступних способів навігації. Для БПЛА, які використовуються в незаконних чи військових цілях, саме ця програма реалізується найчастіше. Таким чином, придушення КРУ може знизити ймовірність успішного виконання БПЛА цільового завдання, але не гарантує жодних однозначних дій щодо припинення польоту БПЛА у напрямку контрольованого рубежу, активації «програми повернення» або «програми посадки» тощо. Саме відсутність однозначної реакції БПЛА на успішне придушення КРУ є суттєвим недоліком комплексів протидії БПЛА, заснованим виключно на РЕП.

Наступною за важливістю радіолінією БПЛА, яка є я вразливою для засобів РЕП є лінія «вниз» у напрямку «БПЛА – ПУ», призначена для передачі даних від спеціальної апаратури та технічних засобів корисного навантаження, розміщених на БПЛА. Справа в тому, що досить поширеним способом управління БПЛА залишається режим ручного керування ним з боку оператора за візуальними даними від ОЕС видимого діапазону. Особливістю цієї лінії є те, що відеодані, що передаються від ОЕС на ПУ, мають великий обсяг, вимагають широкої смуги частот для передачі, і у зв'язку з їх високими швидкостями і необхідністю передачі в режимі реального часу, можуть не піддаватися криптозахисту навіть на БПЛА спеціального та військового призначення. При цьому складність організації на БПЛА з гостроспрямованих антенних систем великого розміру веде до того, що найчастіше ці дані передаються через кругобічну антену, або через антену з широкою головною пелюсткою ДНА

(порядку 60-90°). Це дозволяє відносно легко не тільки розкривати сигнально-частотні параметри даної лінії зв'язку, але й отримувати доступ до відео, що передаються. Придушення такої лінії потенційно дозволило б позбавити оператора візуального зворотного зв'язку, і змусити його керувати БПЛА, так би мовити, «по приладах» тобто. тільки за даними ТМІ, що надходять по КРУ «вниз», що різко знизило б ефективність та ергономічність управління. Водночас високоефективне пригнічення цієї лінії зв'язку вимагає знання розташування ПУ або проміжного вузла-ретранслятора, які використовуються для управління БПЛА. При цьому висота польоту БПЛА, а також можливість розміщення ПУ або вузлів-ретрансляторів на льотно-підйомних засобах потенційно забезпечують більший радіогоризонт і, як наслідок, більш високу дальність організації зв'язку прямої видимості, ніж дальність дії наземних засобів РЕП . В результаті вельми ймовірна ситуація, коли за наявності повної інформації про сигнально-частотні параметри лінії «вниз» буде неможливо придушити ПУ і вузли-ретранслятори через їх просторову недоступність для наземних засобів РЕП.

Вищезазначене відноситься до переважної кількості БПЛА і є фундаментальними обмеженнями, що накладаються на ефективність існуючих комплексів РЕП, орієнтованих на протидію БПЛА.

2.5 Особливості радіоелектронного придушення радіоліній управління та передачі БПЛА

Ефективність придушення радіоліній управління та передачі БПЛА визначається такими факторами:

- умовами поширення радіохвиль на шляху радіоліній БПЛА – ПУ, а також на шляху радіопридушення;
- енергетичною, тимчасовою та просторовою доступністю приймачів засобів зв'язку на БПЛА та ПУ для засобів РЕП, а також їхньою чутливістю;

- потужністю передавачів засобів зв'язку БПЛА та ПУ, а також засобів РЕП;
- типом антенних систем, взаємною орієнтацією ДНА засобів зв'язку БПЛА та ПУ, а також засобів РЕП;
- використовуваними для передачі шириною смуги частот, типом сигналу, типом перешкодостійкого кодування, швидкістю коду.

Для придушення радіоліній управління та передачі даних БПЛА використовуються такі типи перешкод:

1) Перешкоди, що перекривають робочий діапазон частот, що ймовірно використовується для організації зв'язку з БПЛА. Даний тип перешкод використовується при відображенні масованого нальоту БПЛА, коли неможливо розкрити параметри приватних КРУ окремих БПЛА і потрібно перекрити весь діапазон частот, що використовується, або при неможливості засобами РРТР розкрити частотні параметри ліній зв'язку.

До таких перешкод належать:

- загороджувальна шумова перешкода (білий шум високої потужності) у всьому діапазоні частот;
- вузькосмугова шумова або гармонійна перешкода, що ковзає по діапазону частот.

2) Перешкоди, прицільні за частотою ліній управління та зв'язку БПЛА. Цей тип перешкод використовується при придушенні одиночних БПЛА або групи БПЛА, керованих по одній КРУ, коли засобами РРТР достовірно розкрито частотні параметри ліній зв'язку. До таких перешкод належать:

- шумова перешкода, прицільна за частотою лінії зв'язку;
- гармонійна перешкода, прицільна за частотою лінії зв'язку;
- вузькосмугова шумова або гармонійна перешкода, що ковзає по діапазону частот, що використовується (при використанні ліній зв'язку з ШПС або ППРЧ);

- імітаційна перешкода, прицільна за частотою лінії зв'язку та структурою переданих сигналів (імітує структуру сигналів лінії зв'язку);
- імітаційна перешкода, прицільна за частотою і структурою сигналу, а також за структурою і форматом даних, що передаються (імітує помилкові дані, що передаються по лінії зв'язку), з метою нав'язування помилкових режимів роботи.

Ефективність придушення може бути підвищена, якщо засобами моніторингу розкривається очікувана траєкторія польоту БПЛА та засоби РЕП можуть формувати вищезазначені перешкоди прицільно у напрямку БПЛА або його ПУ за рахунок зміни орієнтації ДНА антенних систем.

В даний час широкого поширення набули шумові перешкоди, прицільні за частотами ліній зв'язку БПЛА - ПУ. При цьому з огляду на більш високу ефективність перспективним є використання імітаційних перешкод, прицільних за структурою сигналу. Однак цей режим придушення більш складний у реалізації, але перспективний для майбутніх генерацій.

При організації придушення ліній управління та передачі даних БПЛА засоби РЕП, як правило, дотримуються наступної логіки функціонування.

1) При виявленні факту нальоту БПЛА засоби РРТР намагаються розкрити частотні параметри ліній радіозв'язку «вгору» та «вниз». Якщо розкриття частотних параметрів даних ліній неможливе, то засіб РЕП переходить у режим випромінювання загороджувальних або ковзних перешкод по всьому діапазону частот, що потенційно використовується для організації зв'язку з БПЛА по лініях «вгору» / «вниз». У цей же режим засіб РЕП переходить у разі якщо кількість розкритих ліній зв'язку перевищує можливості засобів РЕП щодо встановлення перешкод, прицільних за частотою та за напрямом.

2) Якщо здійснено успішне розкриття частотних параметрів ліній «вгору» / «вниз», то засоби РРТР намагаються визначити сигнально-структурні та просторові параметри цих ліній. Якщо розголошення таких параметрів

неможливий, то за раніше визначеними частотними параметрами формуються шумові або гармонійні перешкоди, прицільні за частотою. Цей же тип перешкод формується, якщо успішне розкриття сигнальних і структурних параметрів радіолінії показує, що дані радіолінії мають стійкий криптографічний захист.

3) Якщо функціонал засобу РЕП дозволяє керувати ДНА, то надавати перешкод лінії «вгору» здійснюється з урахуванням орієнтації ДНА на БПЛА та його траєкторного супроводу. Якщо за результатами розкриття просторових параметрів радіоліній визначено напрямок на ПУ, то постановка перешкод лінії «вниз» здійснюється з урахуванням орієнтованості ДНА засобів РЕП на ПУ БПЛА.

4) Якщо за результатами розголосу сигнально-структурних параметрів радіоліній визначені тип і структура сигналів і ширина сигналу дозволяє зробити його запис та відтворення [1], то імітаційні структурно-прицільні перешкоди формуються шляхом циклічного відтворення на частоті лінії раніше записаного сигналу. Якщо певний тип і структура сигналів, але ширина сигналу не дозволяє зробити його запис, наприклад, внаслідок того, що використовується сигнали ШПС або ППРЧ, то використовується або широкосмугова шумова перешкода в смузі частот радіолінії, або вузькосмугова шумова або гармонійна перешкода, що ковзає по смузі частот радіолінії.

5) Якщо за результатами розкриття сигнально-структурних параметрів радіоліній визначені не тільки тип і структура сигналів, але також розкрито формат і структура даних, що передаються, тип використовуваного протоколу або кодеку зв'язку, то з'являється можливість заміни керуючих команд БПЛА або передачі хибних даних шляхом формування імітаційної перешкоди, прицільної за частотою і структурою сигналу, а також за структурою і форматом даних, що передаються. Цей тип перешкод може бути сформований, якщо в лінії використовується вразливий або має низьку криптографічну захищеність протокол шифрування. Найбільш поширеним прикладом такого придушення є розголос формату переданих сигнальних даних у каналі «вниз», із записом та

наступним циклічним відтворенням раніше переданого сигналу, що фактично блокує зворотний зв'язок для оператора.

Приблизна оцінка ефективності придушення ліній управління та передачі може бути оцінена шляхом використання двох основних підходів:

- розрахунок завадостійкості (за показником BER (Bit Error Rite) – ймовірності помилкового прийому біта Pb) використовуваної в радіолінії комбінації сигналу і завадостійкого коду при значенні ОСШ на вході приймача, з подальшим порівнянням її з граничними $P_{b\,тр}$ для використовуваного протоколу зв'язку;
- розрахунок енергетичного бюджету радіолінії, з подальшим порівнянням отриманого значення із граничними значеннями чутливості приймача.

При використанні цих підходів передбачається, що перешкода являє собою адитивний білий гаусівський шум (АБГШ) у смузі частот сигналу[1].

Знання значення ОСШ на вході ПРМ і типу сигналу дозволяє визначити значення ймовірності помилкового прийому біта Pb. Порівняння значення Pb з необхідними значеннями $P_{b\ тр}$ для КРУ та каналу передачі даних (таблиця 2.3) дозволяє зробити висновок про потенційну ефективність придушення.

Для корекції та експериментальної перевірки аналітичних виразів оцінки завадостійкості Pb(q), для найбільш поширених сигналів, типів кодування, а також умов застосування БПЛА розглядалися нижче вказані моделі багатохвильового поширення [9,10]:

1) Модель гаусівської лінії – відповідає радіолінії з АБГШ, у якому багатохвильовість повністю відсутня, тобто розглядається єдиний прямий промінь між ПРД та ПЗМ. Таким чином, дана модель описує ідеальні умови розповсюдження на трасі «ПУ – БПЛА», які, як правило, не зустрічаються на практиці, але найчастіше відповідає верхньому кордону оцінки перешкодозахищеності Pb, отриманої розрахунково-теоретичним шляхом [3-8].

2) Модель райсівської лінії - відповідає радіолінії з перешкодами (АБГШ, імпульсні та гармонійні перешкоди), моделює наявність прямого променя та кількох відбитих променів з різними потужністю та затримками приходу в точку прийому, статистичні властивості яких описуються розподілом ймовірностей Райса. Ця модель відповідає умовам польоту БПЛА у прямій радіовидимості ПУ, з урахуванням перетворення електромагнітних хвиль від поверхні Землі та інших об'єктів.

3) Модель релеївської лінії – відрізняється від райсівської відсутністю прямого променя, причому статистичні властивості відбитих променів описуються розподілом ймовірностей Релея. Відповідає умовам польоту БПЛА без прямої радіовидимості ПУ на відносно низькій висоті в пересіченій місцевості або у висотній міській забудові.

Таблиця 2.3 - Необхідні значення достовірності передачі даних для КРУ та каналу передачі даних

Параметри	КРУ «вгору»	КРУ «вниз»	Лінія передачі даних «вниз»
Інформація передавань	Команди управління	ТМИ	Дані від бортових засобів ОЭС, РЛС и т.д.
Протоколи передачі	IP/TCP, X.25, MAVlink, SLT.DSM, XBee, пропріетарні протоколи		DVB, MPEG-TS,MPEG-2/4, H.264
Вимоги до достовірності , Pb тр	10^{-6}		10^{-3}

Дослідження лінії радіозв'язку ПУ – БПЛА проводились для QPSK, 16QAM, 64QAM сигналів. Як перешкодостійкий код використовувалося кодування Вітербі зі швидкостями R = 1/2, 2/3, 3/4, 5/6, 7/8. Як перешкода

розглядалася шумова перешкода – АБГШ. При врахуванні багатопроменевого поширення радіохвиль використовувалися стандартні моделі каналів RC20 та RL20 [9]. Вплив доплерівського зсуву частот не враховувалося. Результати експериментальної оцінки перешкодозахищеності КРУ з QPSK, 16QAM, 64QAM сигналами, при типовій швидкості кодування R=3/4, представлені у вигляді середнього значення ймовірності помилки на біт Pb, який відповідає ймовірності помилкового прийому біта після різних етапів декодування– на вході декодера Вітербі (Pb in Vit) та на виході цього декодера (Pb out Vit). (рис. 2.2).

З рисунку виходить, що значення показників Pe out Vit на виході декодера Вітербі в райсівській лінії (політ БПЛА у прямій радіовидимості ПУ) відповідає погіршенню їх на 1,5-5 дБ щодо гаусової лінії, що відповідає значенню втрат за рахунок прийому перевідбитих сигналів. У міру зростання ОСШ q збільшується відхилення показників Pb out Vit, що відповідає зміні структури помилок (спостерігається групування помилково прийнятих біт) у радіолінії та на виході декодера Вітербі.

Аналогічний ефект характерний і для релеївської моделі радіолінії рис.2.2 (справа). Спостерігається зрушення значень Pb out Vit на виході декодера Вітербі на 10-20 дБ праворуч, у релеївській лінії щодо гауссівської, а також серії помилкових бітів (до 10 біт), розділених інтервалами безпомилкового прийому до кількох десятків секунд. Дане дослідження якісно та кількісно відповідає результатам, отриманим у роботі [8].

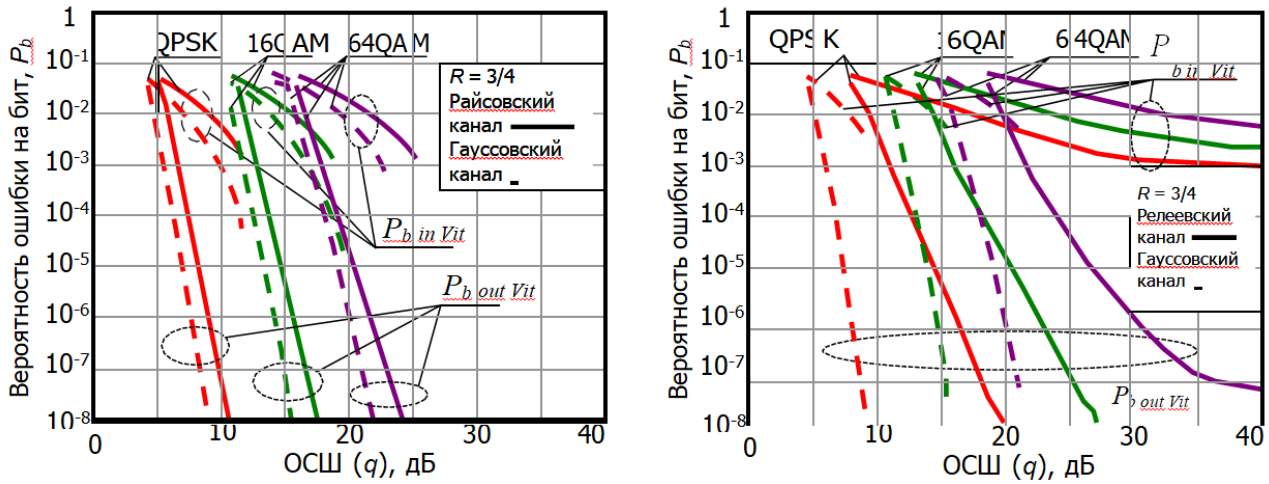

Рисунок 2.2 - Залежність Pb(q) на вході (Pb in Vit) та виході кодера Вітербі (Pb out Vit) для гаусівської та релеївської радіоліній (зліва) та залежність Pb(q) на вході (Pb in Vit) та виході кодеру Вітербі (Pb out Vit) для гаусівської та релеївської радіоліній (справа)[10, 11]

Оцінка вкладу завадостійкого кодування у підвищення завадостійкості радіоліній зв'язку з БПЛА проводилося шляхом оцінки значення ймовірності помилки на біт на вході (Pb in Vit) та на виході декодера Вітербі (Pb out Vit). Дані значення для райсівської та релеївської радіоліній для кодових швидкостей R = 1/2, 2/3, 3/4, 5/6, 7/8 для сигналу 64QAM.

За результатами аналізу можна сформовано приблизні граничні значення ОСШ q (таблиця 2.4), при яких досягається необхідний рівень достовірності прийому для типових схем сигнально-кодових конструкцій, що використовуються в КРУ та лінії передачі даних. При орієнтуванні на ці дані слід мати на увазі, що, як правило, розробниками КРУ закладається додатковий запас на стійкість до перешкод 10 дБ. Зазначені в таблиці 2.4 дані є дуже приблизною та грубою оцінкою, кінцева оцінка необхідних енергетичних витрат, необхідних для порушення функціонування КРУ та лінії передачі даних засобами РЕП, проводиться після розкриття сигнально-кодових конструкцій, що використовуються в радіолініях "ПУ - БПЛА".

Значення ОШП у таблиці 2.4 не враховують можливості використання таких способів підвищення перешкоди, як розширення бази сигналу або використання режиму ППРЧ. Питання впливу перешкод на такі складні типи сигналів як ШПС та ППРЧ розглянуто у роботах [10] та [11] відповідно.

Таблиця 2.4 - Приблизні значення ОСШ, при яких досягається необхідний рівень достовірності прийому в радіолініях зв'язку «ПУ – БПЛА» для типових схем сигнально-кодових конструкцій

Умови польоту	Тип радіолінії, тип даних, що передаються	Требуемая достовер-ность приема, $P_{b\,тр}$	Значение ОСШ при котором достигается требу-емая достоверность приема, дБ									
			BPSK, 1/2	BPSK, 3/4	QPSK, 1/2	QPSK, 3/4	16QAM, 1/2	16QAM, 3/4	64QAM, 1/2	64QAM, 3/4	64QAM, 5/6	64QAM, 7/8
Політ БПЛА в прямій радіовидимості ПУ	КРУ «вгору», команди управління БПЛА	10^{-6}	6	7	8	9	14	16	17	22	24	25
	КРУ «вниз», ТМИ для ПУ, квитанції про виконання команд											
	Радиолиния передачи данных «вниз», видео-данные от ОЭС*	10^{-3}	4	5	6	7	11	13	14	18	19	21
Політ БПЛА у відсутності радіовидимості ПУ, на пересічній місцевості чи в мімі мім забудові	КРУ «вверх», команды управления БПЛА	10^{-6}	11	13	16	17	21	23	20	30	46	н/д
	КРУ «вниз», ТМИ дляПУ, квитанции о вы- полнении команд											
	Радиолиния передачи данных «вниз», видео-данные от ОЭС*	10^{-3}	7	8	10	11	14	16	16	22	25	28

2.6 Особливості інформаційно-технічного впливу з метою втручання у процес функціонування систем БПЛА чи перехоплення управління

Якщо за результатами аналізу КРУ засобами РРТР вдається визначити не тільки тип і структуру сигналів, але також розкрити формат і структуру даних, що передаються, тип використовуваного протоколу управління або кодеку зв'язку, то з'являється можливість заміни керуючих команд БПЛА або передачі неправдивих даних шляхом формування імітаційної перешкоди, прицільної за частотою і структурою сигналу, а також структурою і форматом переданих даних. Фактично завдання розголосу формату і протоколу даних, що передаються в КРУ, відноситься вже не до завдань, які вирішуються засобами РРТР, а до завдань засобів форматної, потокової та мережевої комп'ютерної розвідки (КР). При цьому формування вищезгаданого типу перешкод відповідає вже не «чистому» РЕП, а більшою мірою імітонав'язуванню помилкового управління [1] або інформаційно-технічному впливу (ІТВ) на БПЛА, що реалізується через його КРУ [2]. Однією з основних переваг впливу ІТВ на БПЛА є її скритність. Відсутність явних ознак деструктивних впливів на БПЛА суттєво ускладнює своєчасне та адекватне вжиття заходів протидії з боку ПУ та операторів системи.

Доступ засобів КР до форматів даних КРУ можливий якщо в ній використовується протокол шифрування з низькою криптостійкістю, або протокол шифрування не використовується взагалі. Для БПЛА, в яких КРУ реалізується на основі комерційних технологій Wi-Fi, WiMAX Mobile та LTE, засобами КР можуть експлуатуватися такі вразливості:

- підміна даних авторизації при встановленні або підтримці з'єднання в КРУ;
- використання у Wi-Fi для шифрування переданих даних протоколів WEP (Wired Equivalent Privacy) та WPA (Wi-Fi Protected Access), які мають низьку криптографічну стійкість, при цьому відомі способи, що дозволяють розкрити ключову інформацію за лічені хвилини. [1];

- використання WiMAX Mobile для шифрування алгоритму DES (Data Encryption Standard) з ключами TEK (Traffic Encryption Key), які мають обмежений термін дії, а також використання помилкових сертифікатів ідентифікації абонентських станцій X.509 [1];
- вразливості процедур «attach», «detach» та «paging» для мереж LTE [1] і т.д.

Після доступу засобів КР до форматів даних, що передаються в КРУ, аналізу їх структури та особливостей, з'являється можливість зробити висновок про наступні аспекти управління БПЛА:

- використовувані протоколи та формати передачі даних у КРУ на канальному, мережевому та транспортному рівнях моделі OSI (Open System Interconnect);
- протокол управління БПЛА, що використовується;
- поточне завдання БПЛА, поточна послідовність виконуваних команд;
- дані про стан підсистем БПЛА (у складі TMI), дані від бортових засобів корисного навантаження (насамперед ОЕС);
- місцезнаходження БПЛА за даними від бортової навігаційної системи;
- структура адресації, маршрутизації, а також пріоритетності при передачі команд управління та даних корисного навантаження в мережі управління групою БПЛА;
- типи використовуваних на БПЛА та ПУ керуючої операційної системи (ОС), програмного забезпечення (ПЗ), мікроконтролерів (МК) управління радіомережею, окремими бортовими підсистемами та засобами корисного навантаження БПЛА.

Вищезазначені ознаки формують вихідні дані для аналізу вразливостей одиночного або групи БПЛА як стандартної віддаленої інформаційної системи (ІС) або, як нині їх ще часто називають, кіберфізичної системи, каналом доступу

до якої є КРУ. Загальна класифікація стандартних ІТВ, які можуть бути реалізовані щодо ІС, представлена на рис. 2.3.

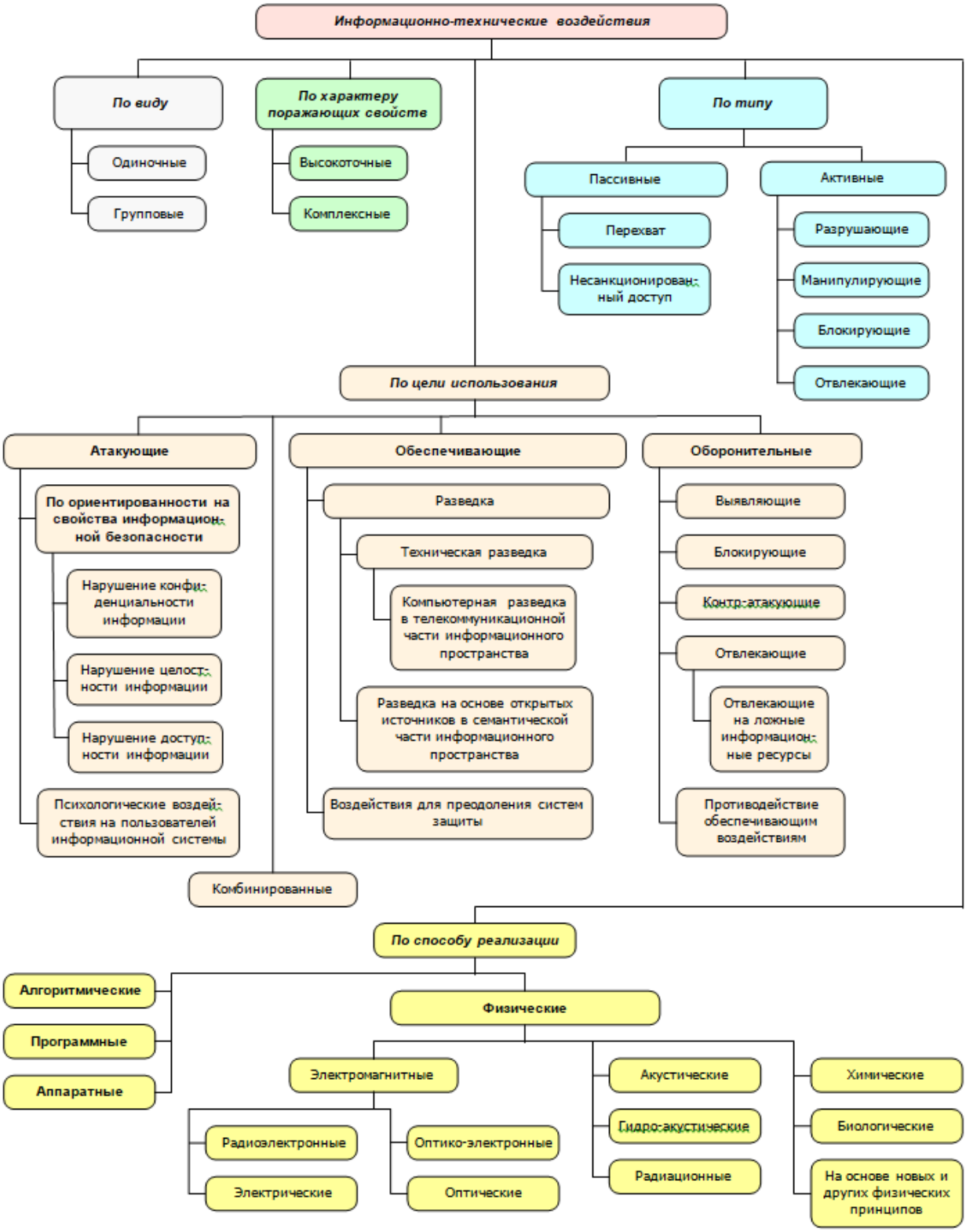

Рисунок 2.3 – Класифікація ІТВ

На основі аналізу уразливостей системи «ПУ – БПЛА» як стандартної ІС можна припустити, що щодо цієї системи можуть бути успішно реалізовані такі ІТТ:

- ІТВ, засновані на порушенні доступності БПЛА або ПУ:
- ІТВ, спрямовані на порушення синхронізації та правил входження у зв'язок;
  - ІТВ, спрямовані на зниження ефективності протоколів канального або мережевого рівнів радіомережі [1];
  - ІТВ типу DOS або DDOS-атаки на вхідні порти ІВ, з метою переповнення вхідного буфера [1];
  - ІТВ порушення нормального функціонування ПО МК, управляючих засобів зв’язку;
  - ІТВ, засновані на порушенні конфіденційності та цілісності зв'язку між БПЛА або ПУ:
  - впровадження в КРУ помилкового ПУ з метою перехоплення управління БПЛА та нав'язування йому нових режимів польоту;
  - відправлення на БПЛА некоректних або різноспрямованих команд, які переводять його в аеродинамічно-нестійкий режим польоту;
  - відправка на БПЛА команд «зниження» або «відключення живлення двигунів», а також інших команд, які однозначно ведуть до негайного припинення польоту БПЛА;
  - відправлення на БПЛА команд відключення бортової апаратури корисного навантаження;
  - впровадження в КРУ хибного «віртуального» БПЛА, що надає ПУ таку хибну ТМІ, яка змушує ПУ формувати свідомо некоректні команди управління БПЛА, які переводять останній в аеродинамічно-нестійкий режим польоту;

- ІТТ засновані на порушенні цілісності та доступності ОС або ПЗ на БПЛА або ПУ:
    - використання стандартних уразливостей керуючих ОС або ПЗ для формування ІТВ на них з метою блокування нормального режиму їх функціонування;
    - приховане переведення апаратних засобів БПЛА в режим підвищеної витрати енергії або в аеродинамічно-нестійкий режим польоту;
    - впровадження у управляючі ОС чи ПО комп'ютерних вірусів, які створюють умови порушення функціонування ОС і ПО чи перехоплення управління БПЛА;
    - впровадження в БПЛА програмних або апаратних закладок, що реалізують несанкціоновані режими роботи або під'єднання до іншого «несанкціонованого ПУ» та виконання його команд з вищим пріоритетом.

В цілому при формуванні ІТВ на БПЛА, останній розглядається як стандартна ІС. У цьому сенсі таргетована атака на ОС та ПО БПЛА фактично не відрізняється атакою будь-якої іншої віддаленої ІВ. При цьому, особливістю ІТВ на БПЛА є те, що формовані ІТВ повинні призводити до максимально швидкого припинення польоту БПЛА до контрольованого рубежу з мінімальними збитками.

Розглядаючи питання організації ІТВ на БПЛА, слід зазначити, що незважаючи на поширення в популярних ЗМІ великої кількості повідомлень про успішний «злам» БПЛА та перехоплення управління ними, створення такої системи є досить нетривіальним науково-технічним завданням. Організація ІТВ на БПЛА вимагає інтеграції засобів РРТР і КР у єдиний комплекс розвідки сигнальних, форматних, потокових та мережевих параметрів КРУ, що забезпечують автоматичне розтин та отримання даних про ОС та ПЗ, що використовуються на БПЛА та на ПУ, у стислі терміни (у кращому випадку – близько кількох десятків секунд, поки БПЛА рухається до контрольованого

рубежу), ґрунтуючись на дуже обмеженій кількості перехоплених пакетів із відносно низькошвидкісної лінії КРУ.

Формування ІТВ потребуватиме інтегрування в єдиний комплекс засобів РЕП та ІТВ, які б на основі даних про сигнальні, форматні, потокові та мережеві параметри КРУ, БПЛА та ПУ автоматично вибирали сценарії найбільш оптимальних ІТВ і потім у режимі реального часу формували таргетовані атаки на елементи системи « БПЛА – ПУ», з метою якнайшвидшого припинення польоту БПЛА.

Разом з тим, в окремих проектах систем РЕП для протидії БПЛА зустрічаються технічні рішення, спрямовані на визначення факту використання одного з найпоширеніших протоколів управління комерційними малими БПЛА (MAVlink, SLT.DSM, XBee та ін.) та формування в рамках цього конкретного протоколу хибних команд управління БПЛА: "посадки", "зниження" і т.д.

Більш реалізованим, при вирішенні задачі протидії малим комерційним БПЛА, виглядає спосіб розробки спеціальних програмних закладок, що впроваджуються в керуючу ОС або ПЗ БПЛА при їх сертифікації, наприклад, для продажу та застосування на території Росії. При цьому дана програмна закладка повинна передбачати прийом за стандартними радіоканалами (наприклад, Wi-Fi) та обробку з найвищим пріоритетом спеціалізованих команд заборони польоту, які можуть транслюватися «віртуальними ПУ», що розміщуються на кордонах контрольованих зон. Такий захід дозволить на 90% однозначно закрити проблему протидії комерційним малим БПЛА в зонах, де їхній політ заборонено, причому без розробки дорогих засобів РЕП з потенційно сумнівною ефективністю.

2.7 Висновки за другим розділом

Сучасні засоби навігації і зв’язку в однобічному користуванні не мають такого успіху як, коли вони використовуються в комплексі.

Підсумовуючи оцінку можливостей придушення ліній КРУ та передачі даних, необхідно ще раз акцентувати увагу на тому, що незважаючи на достатні

можливості існуючих засобів РЕП щодо ефективного придушення цих ліній, таке придушення не гарантує будь-якої певної реакції БПЛА у вигляді припинення польоту БПЛА у напрямку контрольованого рубежу, активації «програми повернення» або «програми посадки» тощо. Саме відсутність однозначної реакції БПЛА на успішне придушення радіоліній є суттєвим недоліком комплексів протидії БПЛА, заснованим виключно на РЕП.

ВИСНОВКИ

Оскільки в майбутньому розвиток, а отже і успіх безпілотних літальних апаратів неминучий, то вже в теперішніх системах управління і передачі даних потрібно пророблювати такі можливості, які б надали змогу оминути вплив застосування засобів радіоелектронної протидії, або ж побудова абсолютно нового за концепцією «щита» проти безпілотних літальних апаратів, щоб дало б змогу на вдосконалення як засобів протидії так і самих літальних апаратів

На сучасному етапі розвитку технологій і їх щільне використання в конструюванні і подальшій розбудові безпілотних літальних апаратів корисними будуть такі рекомендаційні дії:

- використання каналів зв’язку на основі технологій розширення спектру;
- використання вузьконаправлених антен для побудови каналу зв’язку між безпілотним літальним апаратом і його станцією керування;
- зниження використання кругових або ж широко направлених антен для побудови каналів зв’язку між безпілотним літальним апаратом та його пунктом управління;
- зниження використання широко направлених антен для навігаційних систем для подальшого цілевказання місцезнаходження;
- побудова широкосмугових каналів зв’язку;
- використання для обміну інформацією між безпілотним літальним апаратом та його станцією керування засобів криптографічного шифрування, серед яких треба віддати перевагу симетричним через їхню простоту та швидкість реалізацій, прикладом таких може бути будь яка конфігурація алгоритмів Advanced Encryption Standard;
- використання трансмітерних надвисотних безпілотних літальних апаратів для зменшення можливості використовувати «купольний

ефект» для придушення сигналів управління, а також зменшення можливості фіксації місця перебування пункту управління, а в подальшому і придушення його сигналів.

-

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Харкевич А. А. Борьба с помехами. 5-е изд. – М.: Либроком, 2018. 280 р.
2. Палий А. И. Радиоэлектронная борьба. – М.: Военное издательство, 1989. 350 р.
3. Комашинский В. И. Максимов А. В. Системы подвижной радиосвязи с пакетной передачей информации: основы моделирования. – М.: Горячая линия – Телеком, 2007. 176 р.
4. Борисов В. А., та ін. Радиотехнические системы передачи информации: Учебное пособие для вузов / под ред. В.В. Калмыкова. – М.: Радио и связь, 1990. 304 р.
5. Маслов П. В. Сравнительный анализ методов цифровой модуляции // Молодежный научно-технический вестник. 2013. № 2. Р. 46.
6. Песков С. Н., Ищенко А. Е. Расчет вероятности ошибки в цифровых каналах связи // Телеспутник. 2010. № 11. Р. 70-75.
7. Иванов Ю. А., Невструев И. А. Структура и помехоустойчивость систем беспроводного доступа с OFDM // Электротехнические и информационные комплексы и системы. 2009. Т. 5. № 3. Р. 25-29.
8. Пантенков Д. Г. Методический подход к интегральной оценке эффективности применения авиационных комплексов с БПЛА. Часть 1. методики оценки эффективности решения задач радиосвязи и дистанционного мониторинга // Труды учебных заведений связи. 2020. Т. 6. № 2. Р. 60-78.
9. Красносельский И.Н., Канев С.А. Исследование помехоустойчивости системы DVB-T на модели канала с многолучевым распространением // Электросвязь. 2010. № 7. Р. 28-30.
10. European Standard (Telecommunications series) ETSI EN 300 744 V1.6.1. – Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for

digital terrestrial television. 2009. – URL: http://www.etsi.org (дата доступа 01.09.2022).

11. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. 384 р.
12. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: – Свое издательство, 2013. 166 р.