МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
КРЕМЕНЧУЦЬКИЙ ЛЬОТНИЙ КОЛЕДЖ

Циклова комісія авіаційного і радіоелектронного обладнання

ТЕКСТ ЛЕКЦІЇ

навчальної дисципліни «Зв'язок»
обов'язкових компонент
освітньо-професійної програми першого (бакалаврського) рівня вищої освіти

272 Авіаційний транспорт
(Оператор безпілотних літальних апаратів)

за темою № 4 - Способи підвищення надійності та стійкості каналів телеметрії в умовах радіоперешкод та РЕБ

Кременчук 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від _30.08.23_№_7_

СХВАЛЕНО
Методичною радою
Кременчуцького льотного коледжу
Харківського національного
університету внутрішніх справ
Протокол від _28.08.23__№_1_

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічнихдисциплін
Протокол від _29.08.23_№_7_

Розглянуто на засіданні циклової комісії авіаційного і радіоелектронного обладнання, протокол від 28.08.2023 № 1

Розробник: *викладач циклової комісії авіаційного і радіоелектронного обладнання, спеціаліст вищої категорії, викладач-методист Стущанський Ю.В.*

Рецензенти:
1.К.т.н., спеціаліст вищої категорії, викладач-методист циклової комісії авіаційного і радіоелектронного обладнання Шмельов Ю.М.
2. Заступник директора з ОЛР, командир авіаційного загону ТОВ «ЕЙР ТАУРУС» Гетьман Ю.Ю.

План лекції:

1. Безпілотні літальні апарати, як об’єкт протидії супротивника
2. Вимоги до стійкості каналів телеметрії БПЛА.
3. Поняття радіоелектронної боротьби (РЕБ).
4. Класифікація завад
5. «Jamming» та «Spoofing» як основні завади для навігації БПЛА

Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна література:

1. Повітряний кодекс України
2. Наказ Державної авіаційної служби України, Міністерства оборони України 06.02.2017 № 66/73АВІАЦІЙНІ ПРАВИЛА УКРАЇНИ «Загальні правила польотів у повітряному просторі України»
3. Наказ Державноїавіаційної служби України 09 грудня 2021 року № 1920 АВІАЦІЙНІ ПРАВИЛА УКРАЇНИ «Організація повітряного руху»
4. Климаш М.М. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.
5. Логачова Л.М. Поширення земних радіохвиль та мобільний зв’язок / Л. М. Логачова, Т. І. Бугрова / Навчальний посібник. – Запоріжжя: ЗНТУ, 2019. – 236 с.
6. Пилінський В.В. Технічна електродінаміка та поширення радіохвиль/ навчальний посібник/ В.В. Пилінський – Національний технічний університет україни «КПІ», 2014. – 336с.

Допоміжна література:

1. Харченко В.П. Авіоніка. Навчальний посібник. К.: НАУ. 2013. – 272 с.;
2. Eurocontrol airspace strategy for the ECAC states. ASM.ET 1. ST 03.4000 – EAS – 01-00. - Luxembourg, Eurocontrol, 2001. – 74 p.;
3. Eurocontrol manual for airspace planning, common guidelines – Vol. 2. Luxembourg, Eurocontrol, - 2003. – 95 p.;
4. Guidelines document for the implementation of the concept of the flexible use of airspace. ASM.ET 1. ST 08.5000 – GUI – 02-00. - Luxembourg, Eurocontrol, 2003. – 43 p.;

Інформаційні ресурси в Інтернеті:

1. Юринець Ю. Л. Правовий статус безпілотних літальних апаратів [Електронний ресурс] / Ю. Л. Юринець, І. І. Романович // «АЕРО – 2017. Повітряне і космічне право» : матеріали Всеукраїнської конференції молодих і студентів. – Електрон. текст. дані. – Режим доступу : http://er.nau.edu.ua/handle/NAU/31654
.html
2. Сєдов А. Поради дроноводам-початківцям [Електронний ресурс] / Аркадій Сєдов // 50o NORTH. – Опубліковано 31.07.2017. – Електрон. текст. дані. – Режим доступу : http://www.50northspatial.org/ua/tips-getting-started-

with-drones/
3. Сєдов А. Огляд сфер використання БПЛА в повсякденному житті [Електронний ресурс] / Аркадій Сєдов // 50o NORTH. – Опубліковано 13.05.2016. – Електрон. текст. дані. – Режим доступу : http://www.50northspatial.org/ua/uavs-everyday-life/

Текст лекції.

1. Безпілотні літальні апарати, як об'єкт протидії супротивника

В умовах ведення бойових дій, що відбуваються зараз в Україні, все більше уваги приділяється такому озброєнню, як безпілотні літальні апарати (БПЛА). Ці засоби набули широкий спектр їх застосування: розвідувальні, коригувальні, ударні. Використання БПЛА в умовах бою стикається з потужною протидією зі сторони ворога. Це обумовлено, як фізичним знищенням безпілотних літальних апаратів засобами вогневого ураження, так і впливом на них засобами радіоелектронної боротьби (РЕБ). Метою дії засобів РЕБ на БПЛА є придушення каналів радіонавігації та телеметрії безпілотника.

Безпілотний авіаційний комплекс здатен проводити цифрове картографічне фотографування місцевості; фото-, відеореєстрацію з невеликих висот подій та об'єктів на місцевості; виявляти наявність й характер інженерного обладнання місцевості, райони руйнувань. Основна перевага БПЛА – вони можуть застосовуватися в надзвичайних ситуаціях без ризику для життя та здоров'я пілотів, що дуже важливо. Попри численні переваги аерознімання із застосуванням БПЛА, особливості отриманих даних, є деякі проблемні питання: низька якість зображень за поганих погодних умов; невелика точність даних GPS; похибки, пов'язані з нестабільністю польоту. Все це вимагає додаткового оброблення, що дасть змогу зменшити вплив цих недоліків та отримувати якісний вихідний результат.

Необхідність опрацювання великих масивів інформації призводить до її можливого старіння або навіть втрати частини важливої інформації.

Досвід ведення озброєної боротьби дає можливість не тільки зробити висновки про результати випробувань нового виду озброєння, але і намітити подальші шляхи їх модернізації і розвитку, підвищення ефективності способів їх застосування. Перемога у збройній боротьбі в сучасних умовах можлива тільки за умови високого рівня розуміння намірів і дій супротивника, її можна досягти тільки у разі оснащення військ високо-ефективними засобами розвідки, їх умілого і комплексного застосування. Підвищити оперативність виявлення об'єктів можливо за рахунок застосування програмно-апаратного комплексу автоматичного розпізнавання зображень у режимі реального часу.

Для вирішення розвідувальних завдань у режимі реального часу ефективно використовувати програмно-апаратні засоби автоматичного розпізнавання зображень об’єктів, встановлені на борту БПЛА .

2. Вимоги до стійкості каналів телеметрії БПЛА

Цифрове оброблення зображень, отриманих з БПЛА, набуває особливого поширення. Різноманітність методів і алгоритмів пов’язана з широким колом проблем, які виникають під час оброблення та передавання цифрових даних в апаратурі БПЛА, а особливо з проблемою оброблення у реальному масштабі часу.

Аналіз тенденцій розвитку використання алгоритмів цифрового оброблення для отримання інформації з БПЛА та напрямів їх подальшого розвитку дає підстави зробити висновок, що сьогодні актуальним завданням є аналізування та встановлення особливостей функціонування і застосування алгоритмів цифрового оброблення апаратурою БПЛА.

Для якісного виконанні завдання БПЛА та його збереження від втрати необхідний надійний зв’язок оператора зі своїм літальним апаратом. Канали телеметрії з БПЛА використовуються для корекції траєкторії польоту, зміни завдання в залежності від умов протидії та радіозавад, зйому параметрів та інформації з систем безпілотника в режимі on-line. Якщо при втраті каналу супутникової навігації політ може продовжуватися завдяки автономним навігаційним системам, то при втраті каналу телеметрії може бути втрачена не тільки зібрана інформація, а і сам БПЛА.

До відкритих стандартів НАТО, що регламентують передавання даних з безпілотних авіаційних платформ, належить і стандарт STANAG 4607 / AEDP-7. У ньому визначено зміст і формат даних, одержуваних з радарів виявлення рухомих цілей на земній поверхні (GMTI-Ground Moving Target Indicator).

Залежно від пропускної здатності каналів зв’язку, описаний у стандарті формат GMTI дає змогу передати тільки інформацію про рухомі цілі або ще й супутні радіолокаційні зображення з високою роздільною здатністю.

Надалі доцільно обґрунтувати вимоги до процесу оброблення цифрових відеозображень, отриманих з безпілотного літального апарата, оскільки в статтях їх не подають.

Враховуючи теперішній конфлікт на сході держави, українським військовим необхідно переймати досвід у закордонних партнерів, в яких галузь безпілотної авіації розвинена на дуже високому рівні. На нашу думку, варто перейняти досвід у США, оскільки останнім часом українські військові плідно обмінюються досвідом із заокеанськими колегами.

Останніми роками в США замість терміна “безпілотні літальні апарати” фактично використовують термін “безпілотні авіаційні системи” (БПАС). Усі польоти в системі повітряного простору США регулює або в разі військового використання координує Федеральне управління цивільної

авіації США (FAA) згідно з чинним законодавством. Федеральне управління цивільної авіації США регулює політ, використовуючи норми публічного права США згідно з Кодексом федеральних правил (розділ 14 – аеронавтика та дослідження космічного простору). Головним документом, який оприлюднює політику FAA щодо регулювання застосування БПЛА, є AFS-400 UAS Policy 05-01 (Основні принципи експлуатації безпілотних авіаційних комплексів 05-01).

Документ є зведенням тимчасово чинних директив, за якими надається дозвіл на застосування БПАС та виконання польотів у повітряному просторі США. У зв'язку зі швидким розвитком технологій.

3. Поняття радіоелектронної боротьби (РЕБ)

Керівні документи Армії США визначають радіоелектронну війну (РЕВ) як дії військ (сил) з використання електромагнітної енергії і засобів спрямованої енергії з метою здійснення управління (контролю) випромінюваннями електромагнітного спектру частот (у тому числі й використання самого спектру частот) або дії (атаки) на особовий склад, радіоелектронні системи і засоби, об'єкти, озброєння та військову техніку противника.

Радіоелектронна війна включає три основних взаємозв'язаних і взаємодоповнюючих один одного елементи: радіоелектронну атаку, радіоелектронний захист і забезпечення ведення РЕВ. Радіоелектронний захист як один з елементів РЕВ одним із напрямків передбачає підсилення захисних якостей об'єктів (цілей), зокрема, створення спеціальних схем, екранів, сховищ, технічних засобів захисту (у першу чергу мова йде про фізичні та технічні засоби захисту від дії електромагнітних випромінювань радіоелектронних засобів (РЕЗ) своїх військ або військ противника). Для забезпечення ведення РЕВ визначені склад сил і засобів – органи управління, розвідки, тилового та технічного забезпечення, – а також напрямки оперативної та бойової підготовки. Підкреслюється, що РЕВ є одним з елементів інформаційних операцій.

У Збройних силах України під терміном радіоелектронна боротьба (РЕБ) розуміють сукупність узгоджених за метою, завданнями, місцем і часом одночасних і послідовних дій з радіоелектронного подавлення систем управління військами та зброєю противника і заходів щодо радіоелектронного захисту РЕЗ своїх систем управління, які спрямовані на забезпечення переваги у використанні електромагнітного спектру. Радіоелектронне подавлення (РЕП) розглядають як сукупність узгоджених за метою, завданнями, місцем і часом радіоелектронних впливів на радіоелектронні системи і засоби управління військами та зброєю, які здійснюються силами та засобами РЕБ за єдиним замислом і планом відповідно з радіоелектронною обстановкою, що склалася. У свою чергу,

радіоелектронний захист (РЕЗах) – це комплекс організаційно-технічних заходів і дій, спрямованих на забезпечення стійкої роботи своїх систем управління військами і зброєю з метою забезпечення переваги у використанні електромагнітного спектру.

Окремо розглядають радіоподавлення як дії щодо порушення роботи радіо-, радіорелейних, тропосферних і супутникових ліній зв'язку, засобів радіолокації і радіонавігації противника шляхом впливу на них електромагнітними випромінюваннями, застосуванням оманних радіолокаційних цілей і пасток, передачі повідомлень, що дезінформують, у радіомережах противника або своїх військ, демонстрації (помилкової) роботи своїх радіоелектронних засобів або імітація роботи РЕЗ противника, а також зміни умов розповсюдження радіохвиль. Для ведення РЕБ залучають спеціальні сили та засоби – батальйони, вузли РЕБ, індивідуальні і групові засоби РЕБ, у тому числі літальних апаратів, пристрої (прилади) радіоелектронного захисту засобів військ. Аналогічний підхід до тлумачення понять і дій РЕБ прослідкується і в інших джерелах.

Широке застосування в житті суспільства знайшли пристрої Hi-Tech: засоби зв'язку, обробки інформації, навігації, Wi-Fi камери, тепловізори, безпілотні літальні апарати (БПЛА) невеликих розмірів і т.д. Ці пристрої є засобами подвійного призначення і породжують масу проблем збройним силам (ЗС) і силам охорони правопорядку (СОП), до яких відноситься Національна гвардія України (НГУ). Пристрої Hi-Tech використовують терористичні угруповання і незаконні збройні формування (НЗФ) для зв'язку і протидії підрозділам сил охорони правопорядку і ЗС.

Основними доступними засобами зв'язку Hi-Tech у вільному продажу є: аналогові і цифрові портативні і автомобільні радіостанції діапазонів VHF (146-174 МГц), UHF (400-480 МГц), мобільні телефони GSM і CDMA, супутникові телефони, Wi-Fi, скануючі приймачі, вбудовані пристрої GPS-навігації, зв'язок з віддаленим доступом (Internet Radio). До засобів Hi-Tech в останні роки додалися радіокеровані моделі БПЛА, зокрема квадрокоптери, з відеокамерами високої роздільної здатності та професіональними функціями. Їх технології удосконалюються, поліпшуються надійність, безпека, керованість та інші характеристики. У цих "іграшок" з'явились такі функції, як "повернення додому", системи FPV з відстеженням "положення голови" (спосіб управління БПЛА за допомогою відеокамери на борту – відео реального часу дозволяє оператору управляти апаратом, який знаходитися поза зором оператора), 3D FPV окуляри, режим огинання перешкод, функція "слідуй за мною" та інші. Навіть при невеликому часі польоту (15-30 хвилин) "іграшка" в руках терориста перетворюється на ефективний засіб розвідки і протидії підрозділам СОП, особливо в міських умовах.

4. Класифікація завад

Вплив радіозавад може призвести до таких наслідків, як перевантаження приймального пристрою, маскування чи спотворення радіосигналу або його імітації.

На кінцевий результат дії навмисних радіозавад впливають такі фактори:

– співвідношення сигнал/шум на вході радіоприймача, що піддається впливу завади;

– співвідношення ширини спектру корисного радіосигналу до сигнала радіозавади;

– особливості побудови засобу радіозв'язку, параметри його роботи (модуляція, частота роботи, потужність передавача та чутливість приймача) та структури корисного сигналу (використання кодування, методи розширення спектру);

– параметри самих радіозавад.

Класифікація навмисних радіозавад доволі широка, може ділитись по багатьом параметрам. Стисла класифікація наведена на Рис. 1

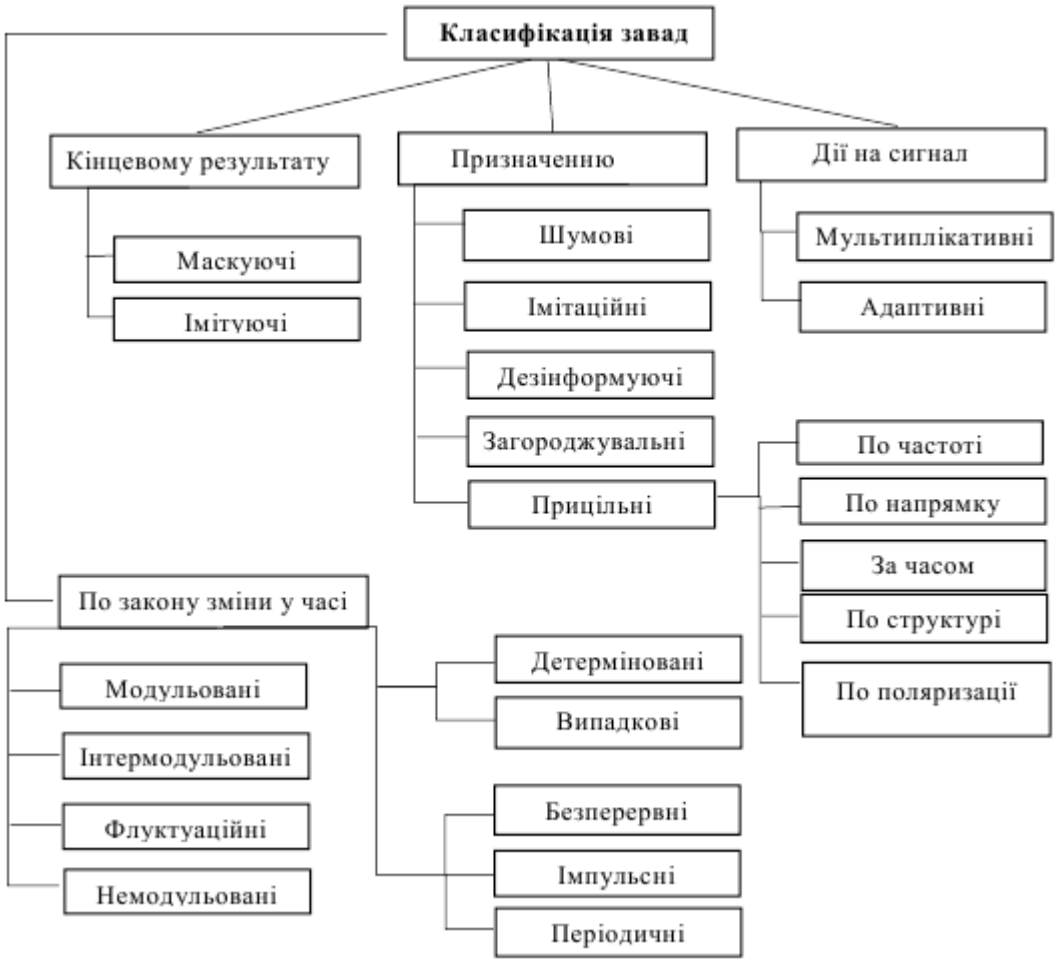

Рисунок 1 – Класифікація завад

За параметрами більш детально радіозавади класифікуються за:
– джерелом походження. Розрізняють завади які з'явилися у наслідку природних явищ та штучні – утворені пристроями, що випромінюють енергію електромагнітних хвиль;
– виду випромінюваної енергії. Існують електромагнітні, оптичні та акустичні завади;
– співвідношенню спектрів. Завади, чий спектр значно перевищує спектр корисного сигналу називають загороджувальними. Прицільними називають такі завади, чий спектр порівняний с спектром корисного сигналу, а частота змінюється у діапазоні роботи ЗРЗ;
– структурою випромінювання. Розрізняють імпульсні завади, що являють собою серії модульованих або не модульованих радіоімпульсів, та безперервні, які можуть бути промодульовані по частоті, фазі чи амплітуді;
– характером впливу на ЗРЗ. Розрізняють маскуючи, що ускладнюють виявлення та розпізнавання параметрів прийнятого корисного радіосигналу. Іншим видом є імітуючи радіозавади, мета яких створити помилкові (не вірні) радіосигнали на вході приймача;
– потужності. Слабкі радіозавади, чий рівень не перевищує рівень корисного сигналу та викликає втрату не більше ніж 25% корисної інформації.

Середні радіозавади по рівню потужності можна порівняти з рівнем корисного сигналу, вони можуть викликати втрату не менше 50% корисної інформації. Сильні радіозавади по рівню потужності значно перевищують корисний сигнал, можуть привести до повної втрати корисної інформації. В окремих випадках можуть перевищувати динамічний діапазон радіоприймального пристрою.

Пасивні радіоелектронні завади створюються завдяки відбиттю (розсіюванню) електромагнітного випромінювання, що надходить від інших радіоелектронних пристроїв. Це випромінювання може надходити завдяки відбиттю від штучних об'єктів, таких як дипольні та кутові відбивачі, лінзи Люнеберка, аерозолі, тощо. Зазвичай, результуючий сигнал утворений відбиттям є сумою елементарних сигналів з випадковими параметрами амплітуди, частоти і фази.

Активні радіоелектронні завади створюються з використанням спеціальних пристроїв – генераторів завад чи станцій постановки завад. Параметри сигналу завади визначаються призначенням, структурою цих генераторів перешкод.

Далі проведено опис основних видів активних радіоперешкод. Найбільш універсальною за сферами використання є загороджувальна шумова завада, що являє собою білий гаусівський шум з певною спектральною щільністю потужності у обмеженій полосі частот. Як виходить з назви, полоса частот

завади перекриває діапазон роботи засобу радіозв'язку. Спектральну щільність потужності можна визначити за формулою (1.1):

$$G_z = \frac{P_Z}{\Delta f_c} \qquad 1.1$$

Де Pz – потужність завади
fc – ширина спектру завади

Найбільш ефективно загороджувальна радіозавада діє у випадках, коли рівень потужності радіозасобу, що подавлюється нижче або дорівнює рівню самої завади, але такі випадки рідкі. Рис. 1 демонструє ситуацію, де спектр корисного сигналу перекритий завадою, але його рівень потужності значно вищій ніж рівень завади. Світло–сірим показана завада, чорно–сірим корисний сигнал.

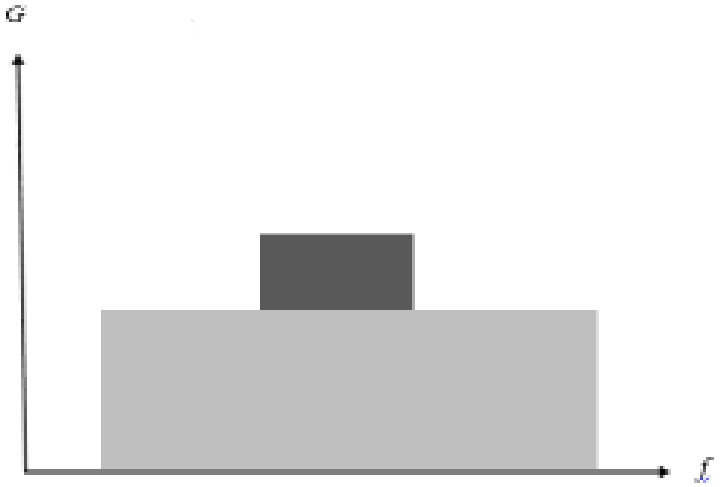

Рисунок 2 – Ефективний вплив загороджувальної завади

Маскуючи радіозавади мають на меті ускладнення виявлення корисного сигналу (збільшення ймовірності помилкової тривоги) шляхом створення завадового фону на приймальній частині засобу зв'язку. На рівень завданого ускладнення впливають співвідношення частотних, часових та структурних параметрів корисного сигналу та радіозавади.

У якості активних маскуючи радіозавад зазвичай використовуються безперервні шумові завади. Прицільні радіоперешкоди характеризуються тим, що їх спектр співвідносний чи повністю збігається зі спектром корисного сигналу ЗРЗ що подавлюється. Імітуючи радіозавади мають на меті внести хибну інформацію на приймальній стороні ЗРЗ що подавлюється. Параметри такої завади зазвичай близькі до значень параметрів корисного сигналу, що імітується.

В деяких випадках у якості сигналу, що імітує, може бути використана частина корисного сигналу, яка починає ретранслюватися станцією завад.

Таблиця 1 – Загальна аналітика станцій РЕБ, що використовуються

Приймачі розвідки радіозв'язку	**Радіостанції зв'язку**	**Антени***	**Радіоукриття***
Радіостанції з функцією сканунування	Передавачі перешкод*	Пеленгаційні	На основі куткової антени
Скануючі приймачі*	Передавачі перешкод з віддаленим доступом	Спрямовані для подавлення	Екрануючий шатер з металізованої тканини
Скануючі приймачі з віддаленим доступом	Передавачі подавлення БПЛА**	З керованою діаграмою	Площинний екран розмірами n λmax·m λmax

*VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

** Передавачі перешкод видимого та IR діапазонів

Зазвичай, станції радіоелектронної боротьби працюють в парі, або мають обладнання засобів радіоелектронної розвідки. Для вдалої роботи, станція повинна геренувати завади тих частот, які використовує ворог, та направити цю завати в сектор де він знаходиться. Найбільш ефективні станції РЕБ, які проінформовані частотами на яких працює ворог, тоді для визначення цих частот самостійно не потрібнь витрачати час, а зразу починати працювати для встановлення завади.

Таблиця 2 – Загальна характеристика антен станцій РЕБ

Завдання	**Діаграма**	**Поляризація**	**Діапазон**
Радіомаскування активне	Секторна*	Вертикальна, горизонтальна	VHF,UHF,3G, Wi-Fi
Радіорозвідка (пеленгація)	Двопелюсткова	Вертикальна	VHF,UHF,3G, Wi-Fi
Подавлення радіостанцій зв'язку	Секторна, однопелюсткова	Вертикальна	VHF,UHF,3G, Wi-Fi
Подавлення каналів управління рухомих командних пунктів	Кругова, секторна*	Вертикальна, кругов	VHF,UHF,3G, Wi-Fi
Подавлення каналів управління і передавання інформації БПЛА	Секторна, однопелюсткова, косекансна	Вертикальна, горизонтальна	VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

* Передавачі перешкод видимого та IR діапазонів

Існують ряд частот, які використовуються для навігації та управління БПЛА:

Таблиця 3 – Діапазони та смуги частот БПЛА

Діапазон	Смуга	Призначення
WiFi 5.8 ГГц	5.7-5.9 ГГц	Передавання відео
WiFi 2,4 ГГц	2400-2480 МГц	Управління
GPS L1	1575.42 МГц	Навігація
GPS L2	1227.60 МГц	Навігація
433 МГц		Пульт управління
800/900 М, 850-965МГц		Пульт управління

5. «Jamming» та «Spoofing» як основні завади для навігації БПЛА

5.1 Jumming

Jamming - це акт навмисного спрямування електромагнітної енергії на систему зв'язку (і навігації), щоб порушити або запобігти передачі сигналу.

Таким чином, пристрої перешкод GNSS транслюють свій сигнал перешкод у діапазоні частот, який використовується для супутника навігація. Атаку з перешкодами можна класифікувати як відмову в обслуговуванні – GNSS все ще доступна, але потужніть перешкод повністю перекриває сигнали від супутників.

Треба розрізняти військові та цивільні перешкоди.

У кризових і не тільки ситуаціях глушіння можуть впроваджувати військові для локальних операцій, чи захисту певних об'єктів. Але, як показує практика, jummer це найбільший ворог насамперед для своїх. Практика показує, під час війні в Україні наші РЕБ станції робили більше лиха ніж ворожі. Джамери зазвичай покривають зону куполом, тому використання нашими бійцями БПЛА навіть далеко на свої території викликало певні питання про силу російського РЕБ, але це все свій РЕБ що стоїть поряд, про існування якого ніхто не знає. Цю проблему вирішує тільки чітка скоординованість груп що виконують завдання в одній зоні.

Джамери активно використовуються також в цивільній сфері, насамперед поблизу критичних інфраструктур, такиз як аеропорти , атомні електростанції, квартали влади чи різних консульств. Протягом останніх кількох років комерційні перешкоди – так звані пристрої захисту конфіденційності Privacy Protection Devices (PPD) – стають дедалі популярнішими, але також привернули увагу громадськості через кілька випадків зловживання. Ці пристрої PPD можна придбати, напр. через Інтернет, починаючи від 30 євро за звичайний автомобільний із живленням від прикурювача до дуже складних GPS-автодіапазонів (включно з GSM, WiFi) із зовнішніми антенними роз'ємами та настроюваними режимами роботи за кілька сотень євро.

Існує багато різних причин для використання PPD, більшість із яких межує з незаконністю, як-от вимикання протиугінної системи в автомобілі, яка передає дані GPS положення транспортного засобу до центрального блоку, або в обхід читання систем збору проїзду та страхування оплати за те, що ви ведете, або виходу з системи керування автопарком; або вимкнення системи автоматичної ідентифікації суден; або для захисту конфіденційності агентів з доставки посилок від їхніх роботодавців. Незважаючи на те, що деякі з мотивів можуть бути розумними, вплив використання PPD часто незрозумілий для користувачів.

Вони не усвідомлюють, що такий крихітний PPD може порушити або спотворити цілісність GNSS на відстані кількох кілометрів.

5.2 Spoofing

Spoofing — це навмисна передача фальшивих сигналів GNSS з наміром обдурити приймач GNSS, щоб він надав неправдиву інформацію про місцезнаходження, швидкість і час. Мета підробки полягає в тому, щоб таємно змусити приймач GNSS відстежувати підроблений сигнал (або оманливі сигнали) з метою надання або принаймні спонукання до визначення неправильного визначення місцезнаходження. Використання підробки секретних сигналів захист криптографічного сигналу, як військовий GPS P(Y) або Galileo PRS, практично неможливий. Однак навіть секретні сигнали не є такими захист від атак meaconing: Meaconing означає запис і ретрансляцію автентичних сигналів GNSS. Якщо приймач відстежує сигнали, створені апаратним забезпеченням без вимірювання, помітивши це, приймач отримає не своє правильне положення, а замість нього положення вимірювального обладнання або його дещо змінену версію.

Незалежно від джерела спуфінгові атаки можна класифікувати таким чином:

– без перекриття;
– перекриваючі;
– за їх відносною потужністю.

Без перекриття - у цьому випадку код і фаза підмінного сигналу не синхронізується зі справжнім сигналами. Піки кореляції підмінного і робочого сигналів не перекриваються. Якщо під час холодного запуску потужність спуфінгового сигналу вище, ніж у справжньому, вхідному тракті пошуку та ідентифікації сигналів навігаційних супутникових приймачів може бути обмануто.

Коли ж супутникові сигнали вже відстежуються приймачем (виповнена ініціалізація), приймач ігнорує всі несинхронізовані сигнали. Отже, спуфінговий сигнал більш високої потужності не пов'язаний з відображенням подовжених супутникових сигналів, якщо затримкі або додаткові частоти не вирівняні.

Перекриваючі - більш складний тип спуфінгової атаки, джерело підмінного сигналу, може синхронізувати свою фазу, код і доплерівську частоту з фазою, кодом і доплеровской частотою справжнього сигналу. Перекриваючі типи спуфінгової атаки, піки кореляції спуфінгових і подовжених сигналів об'єднуються, щоб конструктивно або деструктивно змінити форму піка кореляції.

Цей тип спуфінгової атаки може бути сформований генератором спуфінга на основі приймача, де спуфер знає поточний час, спостережувані супутники, місце розташування та параметри роботи атакуючого приймача. Правильне виявлення спуфінгової атаки з перекриттям є складною задачею, оскільки виявлені, викликані спуфінговими сигналами, схожі на помилки, викликані багатолучевістю.

За відносною потужністю - потужність сигналу атаки спуфінга є важливою складовою при обмані GNSS приймача. Відносний рівень потужності сигналів спуфінгу в порівнянні з рівнем справжніх сигналів може сильно вплинути на ефективність і можливість перешкоди спуфінгу. Виявлення спуфінгової атаки на основі їх відносної потужності більш складно, оскільки для цього потрібна інформація про канал поширення спуфінгу, діаграму посилення антени та її орієнтацію.

Висновок: у разі відсутності будь-якого захисту приймача, БПЛА буде реагувати на кожну підміну в результаті чого автопілот намагатиметься компенсувати зміни підмінного положення. Таким чином це може призвести до того, що апарат вилетить із контрольованої зони.