Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: «Захист каналу управління безпілотних літальних апаратів від несанкціонованого доступу»

Виконав(ла): студент(ка) VI курсу, групи СБм-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

		Фомін І.І.
	(підпис)	(прізвище та ініціали)
Керівник		Александер М.А.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Кареліна О.В.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Загородна Н.В.
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

Тернопіль 2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

(підпис) (прізвище та ініціали)

« » 2021 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Фоміна Івана Івановича
(прізвище, ім'я, по батькові)

1. Тема роботи «Захист каналу управління безпілотних літальних апаратів від несанкціонованого доступу»

Керівник роботи доктор технічних наук, професор кафедри КБ Александер Марек Богуслав
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*08*» *листопада* 2021_ року № *4/7-941*

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)
1 Структура сучасних безпілотних літальних апаратів.
2 Види організованої радіопротидії нормальному функціонуванню БпЛА.
3 Практичні рекомедації щодо захисту каналу управління БпЛА.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Презентація виконана на Microsoft PowerPointслайдах для подання за допомогою оверхедів (світлопроекторів) та комп'ютерних засобів.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г. М.		
Безпека в надзвичайних ситуаціях	Клепчик В.М. ст.викладач		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підбір наукової літератури	до 20.09.2021	**виконав**
2	Написання першого розділу роботи	до 24.09.2021	**виконав**
3	Написання другого розділу роботи	до 15.10.2021	**виконав**
4	Написання тез до публікації	до 30.10.2021	**виконав**
5	Написання третього розділу роботи	до 19.11.2021	**виконав**
6	Написання висновків по роботі	до 03.12.2021	**виконав**
7	Підготовка демонстраційних матеріалів	до 21.12.2021	**виконав**
8	Захист у ДЕК	23.12.2021	**виконав**

Студент _____ Фомін І. І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер М.Б.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Захист каналу управління безпілотних літальних апаратів від несанкціонованого доступу // Дипломна робота ОР «Магістр» // Фомін Іван Іванович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2021 // С. 66 , рис. – 6, додат. – 1, джер. – 33.

Ключові слова: БЕЗПІЛОТНИК, КІБЕРАТАКА, КІБЕРБЕЗПЕКА, ДПАС, ДППС, РАДІОЗВ'ЯЗОК, БПЛА, БЕЗПІЛОТНИКИ, ІНФОРМАЦІЯ, БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, РАДІОКАНАЛИ, РАДІОЕЛЕКТРОННИЙ ЗВ’ЯЗОК, ЗАХИЩЕННИЙ ЗВ’ЯЗОК, КАНАЛИ.

Дана магістерська кваліфікаційна робота присвячена дослідженню методів захисту каналу управління безпілотних літальних апаратів.

Для захисту каналу управління безпілотних літальних апаратів запропоновано використання криптографічного метода захисту.

У першій главі розглянуто загальну структуру сучасних безпілотників.

У другій главі проведено аналіз типічних способів взлому дронів. Описано декілька способів захисту БпЛА від несанкціонованого доступу.

У третій главі наведено опис криптографічного метода захисту канала управління.

У підрозділі "Охорона праці" розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин У підрозділі "Безпека життєдіяльності" описано окремі питання безпеки у виробничих приміщеннях.

ABSTRACT

Protection of unmanned aerial vehicles control channel against unauthorized access // Thesis of OR "Master" // Fomin Ivan Ivanovich // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity, SBm-61 group // Ternopil, 2021 // P. 66 , fig. - 6, added. – 1, sources - 33.

Keywords: DRONES, CYBER ATTACKS, CYBER SECURITY, DPAS, DPPS, Radio, UAVs, INFORMATION, SECURITY, INFORMATION SECURITY, ELECTRONIC COMMUNICATION, COMMUNICATION RESERVED, CHANNELS.

This master's thesis is devoted to the study of methods of protection of the control channel of unmanned aerial vehicles.

To protect the control channel of unmanned aerial vehicles, the use of cryptographic protection method is proposed.

The first chapter considers the general structure of modern drones.

In the second chapter the analysis of typical ways of breaking of drones is carried out. Several ways to protect UAVs from unauthorized access are described.

The third chapter describes the cryptographic method of protection of the control channel.

In the subsection "Occupational safety" the rules of occupational safety during operation of electronic computers are considered. In the subsection "Safety of life" separate questions of safety in industrial premises are described.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7
ВСТУП 8
1 СТРУКТУРА СУЧАСНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ 10
1.1 Класифікація безпілотних літальних апаратів 10
1.2 Система управління БпЛА 12
1.3 Особливості бортової системи БпЛА 13
1.3.1 Система навігації 14
1.3.2 Система зв'язку 15
1.4 Станція зовнішнього пілота 17
1.5 Канали управління та передавання даних БпЛА 19
1.6 Висновки з розділу 28
2 ВИДИ ОРГАНІЗОВАНОЇ РАДІОПРОТИДІЇ НОРМАЛЬНОМУ ФУНКЦІОНУВАННЮ БПЛА 29
2.1 Методи та засоби радіоелектронної боротьби в сучасних реаліях 29
2.2 Типові кібератаки на канали управління БпЛА 31
2.3 Взлом безпілотників та методи їх захисту 37
2.3.1 Способи взлому дронів 37
2.3.2 Методи захисту 38
2. 4 Висновки з розділу 39
3 ПРАКТИЧНІ РЕКОМЕДАЦІЇ ЩОДО ЗАХИСТУ КАНАЛУ УПРАВЛІННЯ БПЛА 40
3.1 Криптографічні методи захисту каналу управління 40
3.2 Висновки з розділу 54
4 ОХОРОНА ПРАЦІ 56
4.1 Аналіз впливу негативних чинників на оператора БпЛА 56
4.2 Безпека зорового аналізатора при роботі з екраном 58
4.3 Висновок 60
ВИСНОВОК 61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 62
ДОДАТОК А 65

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БпЛА	Безпілотній літальний апарат
БАК	Безпілотні авіаційні комплекси
ДПВС	Дистанційно пілотованих повітряних суден
ДПАС	Дистанційно пілотовані авіаційні системи
ЗС	Завадний сигнал
ІКС	Інформаційно комунікаційні системи
КП	Коефіцієнт придушення
ЛЗШ	лінії заданого шляху
НСК	Наземна станція контролю
ОС	Операційні системи
ПДК	Пульт дистанційного керування
ПДП	Пункти дистанційного пілотування
СЗП	Станція зовнішнього пілота
ЦАР	Цифрова антенна решітка
C&C	Command and Control - дані управління і контролю
GCS	Ground Control Station - наземна станція управління

ВСТУП

У сучасних умовах використання БПЛА і робототехніки стало звичайною нормою. З їх допомогою вирішуються завдання забезпечення військової безпеки, а також питання в дослідницькій, охоронної та інших областях. У боротьбі з тероризмом безпілотники та інші види робототехніки стають все більш ефективним і регулярно застосовуваним засобом. У той же час терористичні організації намагаються йти в ногу з прогресом і активніше задіють безпілотні апарати в своїй деструктивній діяльності. Саме тому розгляд питань про застосування БПЛА та протидію їм необхідно вести паралельно.

Поява великої кількості розробників і виробників БПЛА має ряд причин. Зазначені конструкції, як правило, набагато дешевше пілотованих літаків і вертольотів. Підготовка оператора безпілотної системи обходиться менш затратно, ніж льотчика. Крім того, відсутність пілота дозволяє зменшити масу і габарити БПЛА, збільшити діапазон допустимих перевантажень і інших факторів, що впливають. Велике значення має і фактор безпеки: втрата безпілотних апаратів не веде до загибелі пілотів.

Однак під час використання безпілотників виникає ціла низка проблем, адже доступ до каналів передачі інформації можуть отримати і злочинці, для задоволення власних потреб. Як і проводові мережі, безпілотні літальні апарати потрапляють під вплив різних атак.

В більшості випалків, вони вразливі до різних атак. Ці атаки призводять до суттєвих наслідків, включаючи комерційні та некомерційні втрати. В цьому контексті бракує належного розуміння того, як хакери виконують свої атаки та викрадають дрон, щоб його перехопити або навіть розбити. Насправді, безпілотники також можуть бути скомпрометовані в зловмисних цілях. Отже, існує потреба їх виявити та запобігти заподіянню шкоди. Точніше – бракує розуміння того, яким чином будується та може бути підвищенний захист радіоканалів управління безпілотними літальними апаратами.

Об’єкт дослідження – канал управління БПЛА.

Предметом дослідження є захисту каналу управління безпілотними літальними апаратами від несанкціонованого доступу.

Мета роботи – підвищити можливості захисту каналу управління при передачі даних від безпілотних літальних апаратів.

Методи дослідження. Для рішення поставлених задач у роботі використовуються криптографічні методи.

Для досягнення поставленої мети у роботі сформовані і вирішені наступні завдання:

– дослідження структури безпілотних літальних апаратів;

– аналіз видів організованої радіопротидії нормальному функціонуванню;

– розбір криптографічного метода захисту каналів управління безпілотними літальними апаратами.

У зв'язку з викладеним, тематика магістерської роботи є актуальною, а отримані в роботі результати мають важливе прикладне значення.

Апробація результатів. Основні положення і результати магістерської роботи доповідались і обговорювались у науковій-практичній конференції.

1 СТРУКТУРА СУЧАСНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

1.1 Класифікація безпілотних літальних апаратів

Безпілотний літальний апарат являє собою пристрій, управління якими здійснюється дистанційно без прямої участі пілота. БпЛА складається з таких компонентів як: повітряна платформа зі спеціальною системою посадки, силової установки, системи електроживлення всіх компонентів, бортового радіоелектронного обладнання. В свою чергу бортове обладнання складається з бортового комп'ютера або спеціальних процесорів, радіонавігаційної системи, альтиметра, гіровертикалі, бортової системи зв'язку та передачі даних, сервомашинкі. БпЛА можливо класифікувати за таким ознаками:

За способом використання безпілотно літальні апарати поділяють на: військові, антитерористичні, цивільні – же можна поділити на: державні, комерційні, транспортні.

За способом вирішення завдань такі безпілотники можливо в свою чергу розділити на: тактичні – дальність польоту такого дрона досягає до 80 км, оперативно-тактичні – до 300 км, оперативно-стратегічні – до 700 км.

За масою БпЛА діляться на: малорозмірні – вага таких апаратів досягає до 200 кілограм, середньорозмірні – від 200 кг до 2 тонн, великорозмірні – від 2т до 5т, важкі – понад 5т.

За тривалість польоту дрони ділять на: малої тривалості – час польту такого безпілотника триває до 6 год, середньої тривалості – до 12 год, великої тривалості – понад 12 год.

За максимальною висотою польоту БпЛА ділять: маловисотні – політ таких дронів сягає менше 1 км, середньовисокі – до 4 км, висотні – до 12 км, стратосферні – більше 12 км.

За типом літального апарата розподіляють на ті, що створенні за аеродинамічною схемою літака або гелікоптера і ті, що легші за повітря.

За місцем розміщення дрони ділять на: наземні – які пересуваються по земній поверхні, морські – орієнтовані на роботу у водному середовищі, космічні – орієнтовані на вихід у космос.

За типом системи управління літального апарата ділять на: Дистанційно пілотовані – управляється безпосередньо за участі оператора в межах його видимості; Дистанційно керовані – польоти здійснюються автономно, але можуть керуватися пілотом через підсистеми контролю; Автоматичні – дрон виконує попередньо запрограмовані дії. Дистанційно керовані авіаційні системи – керуються вбудованими системами.

За способом управління польту: візуальні – політ здійснюється світлий час доби в межах видимості пілота; приладовий – політ виконується в автоматичному режимі в будь-який час доби і не лише в межах видимої зони, але й в сліпих зонах; візуально приладовий – коли під час польоту використовуються візуальні та прилади.

За типом крил: фіксовані – ті, шо використовуються в літакх та гелікоптернах, плаваючі – вони використовуються в конвертопланах.

За видом паливної система, дана класифікація також залежить від кількості використання БпЛА: монозаправні – одноразова заправка, за звичай здійснюється виробником на заводі. Монозаправні дрони за звичай використовуються лише один раз для вирішення конкретної задачі; полізаправочні – багаторазова заправка, яка може здійснюватися наземно та бортова(морська). Це багаторазові дрони, для постійного використання.

За типом паливного баку: базові – літальні апарати, які мають основний паливний бак; базово-резервні – мають основний та резервний паливні баки.

За радіусом дії: ближнього радіусу дії – до 40 км; малого – до 70 км; середнього – до 300 км; дальнього – до 1500 км; великої тривалості польоту – не менше 1500 км.

За напрямком підйому та посадки поділяють. В основному їх поділять на горизонтальні, вертикальні та мульти (підйомі/спускові). Але внаслідок

специфіки посадки до цього типу можливо додати парашутні, мачтові, безпосадкові.

Також є дуже специфічна класифікація, як за типом підйома та посадки. За типом підйома діляться на: аеродромні, запускні, палубні, водні, ручні, нетипово підйомні, мультипідйомні. А за посадковим типом: аеродромні, точкові, палубні, водні, безпосадкові, нетипово посадкові, мультипосадкові.

1.2 Система управління БпЛА

Загальна структура системи управління представлена Рис. 1.1

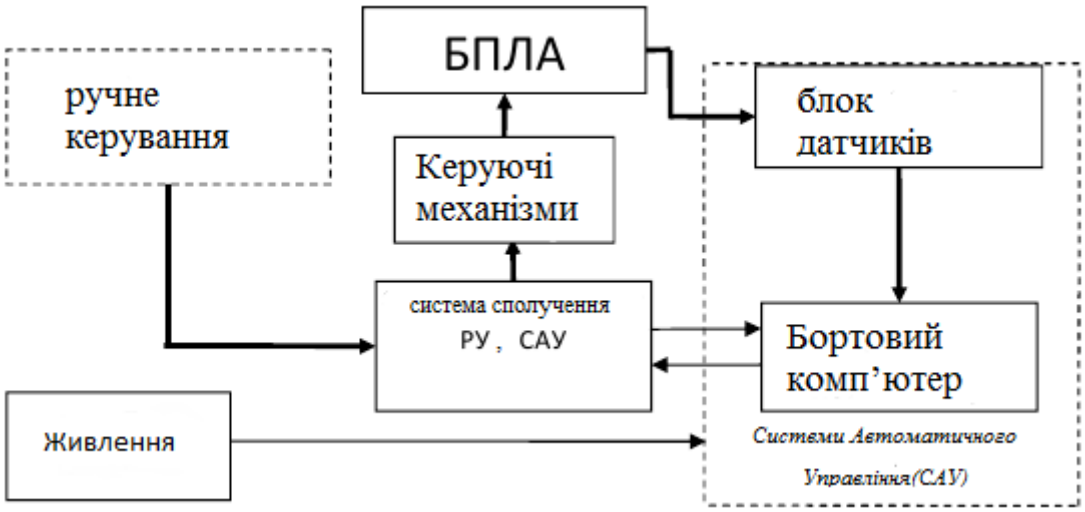

Рисунок 1.1 – Структура БпЛА із системою управління

Блок датчиків включає інерційний модуль, тривісний магнітометр, приймач супутникових навігаційних сигналів, приймачі статичного та динамічного тиску, ультразвуковий висотомір.

Як бортовий обчислювач використано одноплатний комп'ютер. Хоча він і має дещо більші габарити та споживання живлення, ніж простіші

мікропроцесорні системи, проте гнучкість використання та запас обчислювальної потужності дозволяє значно прискорити дослідницький процес.

Стабілізація відносної висоти польоту виконується за даними з ультразвукового висотоміра та інформації про поточне вертикальне навантаження. Вибір ультразвукового висотоміра обумовлений його малими габаритами споживанням енергії, а також невеликою вартістю. Проблема невеликого діапазону вимірювання вирішується комплексуванням із сигналом супутникової навігаційної системи та барометричним висотоміром (при виході за діапазон вимірювання ультразвукового висотоміра літак виробляє плавне зниження доки висотомір не побачить землю).

Оскільки рельєф підстилаючої поверхні невідомий, з даних про вертикальне навантаження віднімається розрахункове значення навантаження, яке виникає при відпрацюванні нерівностей рельєфу. Це дозволить виділити перевантаження викликане зовнішніми обуреннями та парирувати їх. Також до сигналу навантаження додається оцінена зміна маси апарату (витрата палива та робочої речовини).

Для стабілізації бокового руху розраховується відхилення від лінії заданого шляху та задається відповідний кут крену для повернення на ЛЗШ. Оскільки акустичний висотомір має обмежену по куту зону стабільної роботи, якщо необхідний крен більше десяти градусів, то виконується плоский розворот через канал нишпорення.

1.3 Особливості бортової системи БпЛА

Для забезпечення відображення поверхні в реальному масштабі і часі підчас здійснення польоту та відеоспостереження будь-якої ділянки земної поверхні незалежно від важко жоступності, а також визначення координат його місце положення та зони дослідження, безпілотник повинний мати в своєму складі такі пристрої, як**:** Бортовий комп’ютер, пристрої отримання та виводу видової інформації, пристрій для збереження інформації, прилад зв’язку та

передачі даних та команд, систему навігації (GPS); пристрій командно-навігаційної радіолінії.

1.3.1 Система навігації

До складової системи навігації та керування безпілотника входять:

1. Інтегрована Навігаційна Система;
2. Приймач супутникової навігаційної системи;
3. Автопілот.

Автопілот подає керуючий широтно-імпульсний-модульований сигнал, що записані в його обчислювач.

Новітні пілотажно-навігаційні комплекси є вдосконаленою автоматичною системою вищого класу, бортового комп`ютера, в якому поєднано комплекс бортового навігаційного устаткування, системи зв'язку та передачі інформації і спостереження, та автопілота. Пілотажно-навігаційні комплекси забезпечують автоматичне і напівавтоматичне керування зльотом і посадкою в будь-яких погодних умовах. Комплекс здатний вирішувати не прості навігаційні задачі як: розрахунок і обробка навигаційно-пілотажної інформації; моделювання і корекція маршруту БпЛА, з можливістю посадки та зльоту дрону; визначення вектора навігаційних параметрів та індикація навігаційно важливої інформації.

Основним елементом управління пілотажно-навігаційного комплексу є системи автоматичного управління вони забезпечують стабільність польту, керованість параметрами польота.

До системи пілотажно-навігаційного комплексу входять: інерціальні навігаційні системи; інформаційні комплекси висотно-швидкісних параметрів; радіотехнічні системи; обчислювач інформаційної пілотажно-навігаційної системи; обчислювач траєкторного управління; автопілот і пульти управління; автомат тяги; стернові агрегати.

Внаслідок високих вимог до якості бортового навігаційного обладнання безпілотників створюються все нові і нові варіанти навігаційних систем дронів та літальних апаратів в цілому.

На даний час існує кілька видів традиційних навігаційних систем. Но нажаль жодна з цих систем не здатна окремо і не надає точну інформацію місця находження літального судна відносно пройденого шляху і часу роботи навігаційної системи. Ці проблеми легко вирішити за допомогою об’єднання різноманітного обладнання навігації в один комплекс, з використання новітніх методів обробки і фільтрації даних.

1.3.2 Система зв’язку

Більшість БпЛА використовують радіо для дистанційного керування і обміну відео і іншими даними. Ранні БпЛА мали тільки вузькосмуговий канал зв'язку. Спадні канали з'явилися пізніше. Ці двонаправлені вузькосмугові радіолінії передавали віддаленого оператору дані управління і контролю (C&C) і телеметричні дані про стан систем літака. Для польотів на дуже великі відстані військові БпЛА також використовують супутникові приймачі в складі супутникових навігаційних систем. У випадках, коли потрібна передача відео, БпЛА будуть реалізовувати окрему аналогову радиолинию для відеозв'язку.

У більшості сучасних додатків БпЛА потрібно передача відео. Таким чином, замість двох окремих каналів для C&C, телеметрії і відеотрафіка використовується широкосмуговий канал для передачі всіх типів даних по одному радіоканалу. Ці широкосмугові канали можуть використовувати методи якості обслуговування для оптимізації трафіку C&C для зменшення затримки. Зазвичай ці широкосмугові канали несуть трафік TCP / IP, який може бути маршрутизований через Інтернет.

Радіосигнал з боку оператора може надходити з:

1) Наземний контроль - людина, керуючий радіопередавачем / приймачем, смартфоном, планшетом, комп'ютером або вихідним значенням військової наземної станції управління (GCS). Нещодавно також було продемонстровано управління з носяться пристроїв, розпізнавання рухів людини, людські мозкові хвилі.

2) Дистанційна мережева система, така як супутникові дуплексні канали передачі даних для деяких військових держав. Цифрове відео в низхідному напрямку по мобільних мереж також вийшло на споживчі ринки, в той час як пряме управління висхідною лінією зв'язку з БпЛА через стільникову мережу і LTE було продемонстровано і проходить випробування.

3) Інший літак, що виконує роль ретранслятора або мобільної станції управління, - військовий пілотований безпілотний комплекс (МУМ-Т).

4) Протокол MAVLink стає все більш популярним для передачі даних управління і контролю між наземним пультом управління і автомобілем.

На даний час можливо здійснювати управління літальним апаратом без зв’язку з наземною станцією управління, завдяки автопілоту. Хоч і автопілот надає можливість виключити з безпілотника командно-телеметрична радіолінія зв'язку, але внаслідок високої вартості літального апарата та потрібної час від часу корекції параметрів польоту БпЛА. Не надає змогу вилучити цю радіолінію з експлуатації.

На даний час є актуальним завдання передачі корисної інформації безпілотника на наземний комплекс. В такому випадку потрібно забезпечити велику кількість передачі даних за умов що вказуються смузі пропускання, з можливістю появи бітової похибки.

При розробці малих і надмалих дронів слід враховувати розміри приладу прийому-передачі інформації та антено-фідерного обладнання.

З великою кількістю вимого по стресостійкості, які вимагаються до БпЛА, котрий виконую навігацію і пілотування, що потребує ручного управління посадки, до сервоприводу та системи автоматичного порятунку. Вище сказане обладнання входить до І групи класифікації і гарантує якість приладів безпілотника. Пошкодження будь-якого частини обладнання, що входить до складу І групи спричиняє негайне викидання парашуту і якщо є можливість то повернення до бази дрона.

Решта обладнання БпЛА до ІІ групи класифікації. При пошкодженні такого же, обладнання рішення про подальший політ дрону приймає голова

зміни яка здійснює керування комплексом. Взаємодія I групи та II групи виконую через інтерфейс програмного управління.

Підчас роботи системи зв’язку є можливість появи бітової помилки, для зменшення ймовірності появи такої похибки використовують розподіл телеметричного потоку даних між декількаами каналами. Розподіл каналів допомагає підвищити якість передачі даних, і в одно час його вважають зайвим, з погляду ефективності застосування радіочастотного спектру. Для підвищення ефективності системи зв’язку можливо вважати один адаптивний метод роботи системи. Цей метод дозволяє передати по командно-телеметричному каналу невелику кількість даних корисного навантаження, кількість таких даних змінюється від умов передачі радіосигналу.

Зазвичай відстань між дроном і пультом управління на даний момент дорівнює понад 100 км. Для такої великої відстані використовують супутниковий зв’язку, через використання такого зв’язку зменшується кількість інформації про стан безпілотника, інтервал даного типу передачі даних складає від 30 сек. до 5 хв.

В даний час у системи зв’язку з дронами є популярний напрямок розвитку з використанням частот вище 5 ГГц. Це надає змогу збільшити обсяг корисної інформації в режимі реального часу. Одними з негативних факторів даного напрямку є обмеження радіусу дії радіосистеми та висока залежність від умов поширення електромагнітних сигналів від метеорологічних умов.

1.4 Станція зовнішнього пілота

Станція зовнішнього пілота СЗП – робоче місце, з якого зовнішній пілот керує польотом безпілотного повітряного судна. Член зовнішнього екіпажу – член екіпажу, на якого покладено обов'язки управлінням дистанційно пілотованих повітряних суден протягом всього польоту.

Згідно з визначенням, СЗП є елементом дистанційно пілотованої авіаційної системи, що включає обладнання, яке використовується для пілотування дистанційно пілотованого повітряного судна". В цілому функції

СЗП аналогічні функціям кабіни повітряного судна з пілотом на борту, тому зовнішньому пілотові повинні бути надані еквівалентні можливості для управління польотом і його організації.

Незважаючи на те що основні функції аналогічні функціям кабіни повітряного судна з пілотом на борту, специфічна форма, розмір, склад обладнання і компонування будь-якого ПДП будуть відрізнятися, що обумовлено такими аспектами, як:

a) вид виконуваних польотів (VLOS або BVLOS);

b) складність ДПАС;

c) тип використовуваного керуючого інтерфейсу;

d) кількість зовнішніх пілотів, необхідне для управління ДПВС;

e) місце розташування СЗП (стаціонарне положення на землі або на іншому транспортному засобі / платформі (наприклад, на морському судні або повітряному судні)).

СЗП забезпечує можливість здійснення зовнішніх пілотом ДПАС моніторингу та управління ДПВС на землі і в повітрі. Однак інтерфейс між зовнішнім пілотом / СЗП і ДПВС забезпечується через лінію С2. Конструкція ДПАС повинна надавати зовнішньому пілотові необхідні можливості для ефективного управління польотом. У зв'язку з цим органи управління, засоби індикації та сигналізації можуть відрізнятися від тих, які використовуються на повітряних судах з пілотом на борту, що вплине на процедури, підготовку і видачу свідоцтв членам зовнішнього льотного екіпажу, а також на вимоги льотної придатності елементів системи.

Незважаючи на ці потенційні відмінності, основні вимоги до забезпечення інтерфейсу між зовнішнім пілотом / ПДП як і раніше аналогічні вимогам, що пред'являються до повітряних суден з пілотом на борту, і коротко їх можна викласти наступним чином:

a) конструкція органів і систем управління повинна бути такою, щоб зводилася до мінімуму можливість заклинювання, мимовільного спрацювання і ненавмисного включення стопорних пристроїв поверхонь управління;

b) конструкція ПДП повинна бути такою, щоб зводилася до мінімуму можливість неправильного або скрутного використання зовнішніх льотним екіпажем органів управління внаслідок втоми, плутанини або втручання. При цьому увага повинна приділятися, як мінімум, наступного:

1) розташуванню і чіткому позначенню органів управління і приладів;

2) забезпечення швидкого виявлення аварійних ситуацій;

3) напрямку відхилення важелів управління;

4) вентиляції, опалення і рівню шуму;

c) повинні забезпечуватися засоби, які або автоматично запобігають, або дозволяють зовнішньому пілотові усувати аварійні ситуації, пов'язані з передбачуваними відмовами обладнання і систем, вихід з ладу яких буде загрожувати безпеці повітряного судна;

d) маркування та написи на приладах, обладнанні, органах управління і т. д. включають, принаймні, такі обмеження або відомості, які вимагають безпосередньої уваги зовнішнього пілота в польоті, крім того, для ПДП, що забезпечують виконання польотів BVLOS:

e) повинна надаватися адекватна інформація щодо умов, в яких виконують польоти ДПВС, що забезпечує можливість формування у зовнішнього пілота ситуаційної обізнаності, що дозволяє безпечно виконувати політ ДПВС.

1.5 Канали управління та передавання даних БпЛА

Перше покоління радіолінійного зв’язку з безпілотниками, яке використали країни НАТО вже на той час, одну із створених комунікаційних інфраструктур «JTIDS/Link 16». Таку ж ідею використали розробники автоматизованої системи протидії терористичним загрозам «LEXXWAR». Але нажаль пропускна здатність «Link 16» не перевищує 50 Кбіт/с, що не дає змоги реалізувати весь потенціал безпілотників. На теперішній час ринок розробки радіоприладів зв’язку з дронами, майорить різноманіттям методів їх створення.

Но най популярнішим продуктом ринку зв'язку БпЛА, займають традиційні методи, ті які провірені часом модуляції сигналів. Наприклад, як аналоговий канал передачі відеоданих з борту німецького БПЛА.

Ще одним з старших стандарту «STANAG 4609» є метод постійного сигналу зв'язку з звичайною частотою модуляції сигналів «GMSK», що були розробленя організацією «Enerdyne», для програмованих модемів тактичних систем літальних апаратів EnerLinksIII, які зображенні на (Рис.1.2) та Рис.1.3). В режимі прямої видимості модем надсилає відео данні у NTSC. Швидкість такої передачі даних досягає 11 Мбіт/с на відстані 138,9 км або 75 морських миль та 5 Мбіт/с на відстані до 185 км. У звичайному обладнанні використовують параболічну антену з постійним супроводом дрона в межах прямої видимості.

Для роботи на незначній дальності, де кутова швидкість БпЛА може перевищити можливості карданної підвіски наземної антени, використовується всеспрямована антена. Антени перемикаються автоматично. Крім аналогового режиму роботи, розробники рекламують можливість перепрограмування EnerLinksIII для цифрових методів модуляції, що свідчить про перспективність цифрових технологій передачі даних. Зокрема, саме цифрові версії EnerLinks використовуються фірмою DRS Technologies під час модернізації її БПЛА Sentry та Neptune. Нещодавно фірма Insitu оголосила про плани застосування EnerLinks у її БпЛА Integrator та Scan Eagle.

Розробники рекламують можливість перепрограмування EnerLinksIII для цифрових методів модуляції, що свідчить про перспективність цифрових технологій передачі даних. Зокрема, саме цифрові версії EnerLinks використовуються фірмою DRS Technologies під час модернізації її БпЛА Sentry та Neptune. Нещодавно фірма Insitu оголосила про плани застосування EnerLinks у її БПЛА Integrator та Scan Eagle.

Розробники рекламують можливість перепрограмування EnerLinksIII для цифрових методів модуляції, що свідчить про перспективність цифрових технологій передачі даних. Зокрема, саме цифрові версії EnerLinks

використовуються фірмою DRS Technologies під час модернізації її БПЛА Sentry та Neptune. Нещодавно фірма Insitu оголосила про плани застосування EnerLinks у її БпЛА Integrator та Scan Eagle. Ширина смуги пропускання радіоканалу системи EnerLinksIII пов'язана зі швидкістю передачі даних і, наприклад, для 10 Мбіт/с становить менше 12 МГц за рівнем -20 дБс (тобто щодо максимальної амплітуди сигналу на центральній частоті смуги), а за рівнем -50 дБс – близько 24 МГц. При компресії зображення відповідно до стандарту H.264 забезпечується передача даних двох каналів у режимі NTSC з максимальною роздільною здатністю 560×480 пікселів або 550×576 – в режимі PAL. При цьому максимальна швидкість передачі від такого джерела відеосигналів становить 3,5 Мбіт/с.

Нова система передачі даних Starlink ізраїльської компанії Elisra призначена для забезпечення зв'язку з БпЛА на відстані до 100 км у С-діапазоні частот. Система використовує тимчасове дуплексування (TDD), ширина кожного частотного каналу – 4 МГц. Радіолінія може функціонувати в одночастотному режимі або в режимі стрибкоподібної зміни частоти. Інша розробка цієї фірми – система ADLS-2, призначена для роботи одночасно з п'ятьма малорозмірними БпЛА . Вона здатна обслуговувати 24 IP-джерела відео- та аудіоданих, у тому числі аналогових, бортові РЛС із синтезованою апертурою, GPS-датчики тощо.

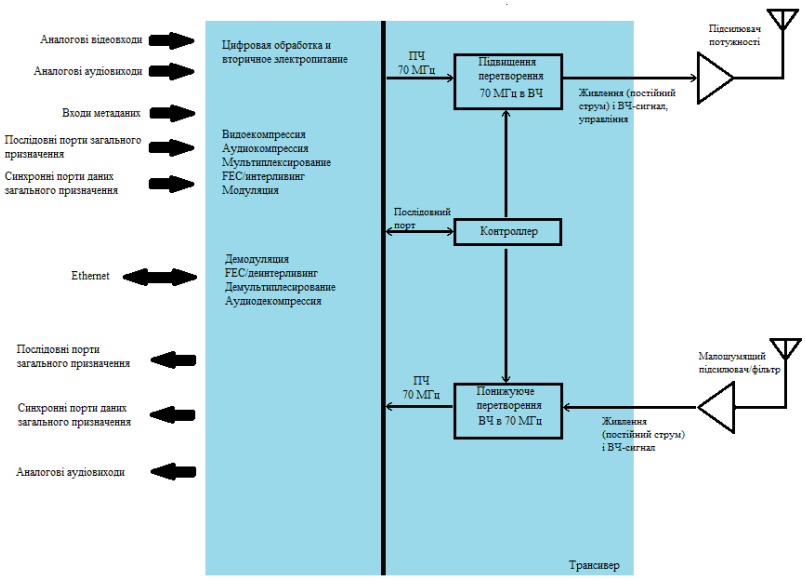

Рис.1.2. Бортовий модем EnerLinksIII

Згідно вимог до пропускної здатності розробники системи зв’язку з дроном змушені створювати нові підходи задля збільшення швидкості передачі інформації від широк спеціалізованих бортових платформ. Один із найбільш ефективних підходів – застосування модуляції OFDM та C-OFDM. Один з перших проектів, було досліджено спосіб OFDM-модуляції у системі зв’язку БпЛА. Даний проекту дісталася назва MinuteMan реалізований проект був 2004 році Каліфорнійського університету в Лос-Анджелесі.

Метою проекту була розробка системи радіозв'язку та обміну даними сил флоту з безпілотними повітряними, надводними та наземними апаратами (Рис.1.3). Серед основних напрямів проекту виділимо розробку фундаментальних засад організації рухомої бездротової інтелектуальної мережі зв'язку – "інтернет у небі"; надання динамічних послуг для мережевих обчислень; організацію відмовостійкого зв'язку та самореконфігурацію для розподілу інформації в реальному масштабі часу, управління завданнями, ситуативна поведінка; передачу голосу, відео, зображень, даних у реальному масштабі часу з адаптивним забезпеченням якості послуг (QoS – Quality of Service) та управління ресурсами. управління завданнями, ситуативна поведінка; передачу голосу, відео, зображень, даних у реальному масштабі часу з адаптивним забезпеченням якості послуг (QoS – Quality of Service) та управління ресурсами. управління завданнями, ситуативна поведінка; передачу голосу, відео, зображень, даних у реальному масштабі часу з адаптивним забезпеченням якості послуг (QoS – Quality of Service) та управління ресурсами.

В Україні же OFDM-сигнали використали в проекті Інституту електроніки та зв'язку Української академії. В проекті досліджується створення системи передачі даних з використанням висотного безпілотник. В наземній системі управління використали стандарт DVB-S з модуляцією OFDM-256. А для маловисоких дронів вони пропонують використати метод множинного доступа з тимчасовим частотним поділом, смуга одного такого радіоканалі за частотою -30 дБс 40 ≈ МГц. При граничній зоні обслуговування однієї

центральної станції при умові що потужність передавача сигналу дрона буде дорівнювати 50 мВт та щільністю опадів 40 мм/год, за умови прямої видимості, тоді радіус становитиме до 60 км. Щоб збільшити зону покриття, потрібно збільшити потужність бортового передавача, тоді радіус такої зони досягатиме до 250 км.

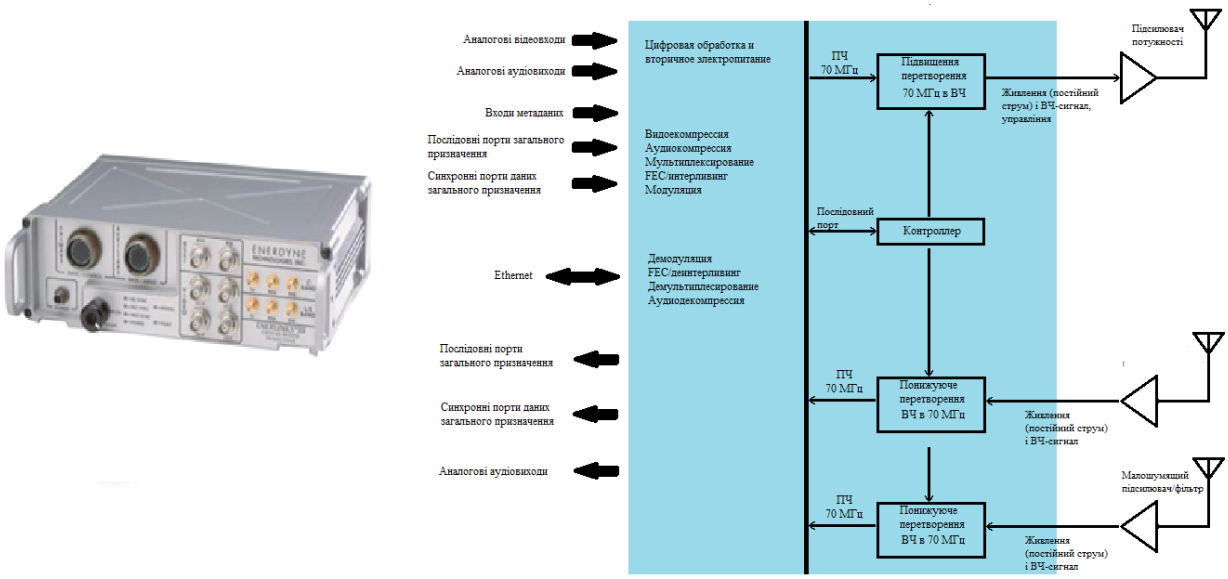

Рис.1.2. Наземний модем EnerLinksIII

Використовувати OFDM-модуляцію у поєднанні з розміщенням плоских цифрових антенних решіток (ЦАР) на борту БпЛА передбачено у проекті Корейського космічного університету з розробки системи передачі відео з безпілотних платформ на основі технології WiBro (Wireless Broadband, IEEE 802.16). Адаптивне цифрове формування променя з компенсацією просторових еволюцій планера БпЛА у разі прямої видимості дозволяє орієнтувати максимум діаграми спрямованості бортової ЦАР на наземний приймальний пункт і цим підвищити енергетику каналу зв'язку на 15 дБ і більше. Це дозволить збільшити висоту польоту БпЛА під час передачі даних без внесення змін до наземної інфраструктури.
Постійно розширюється і військовий напрямок застосування OFDM-модуляції. У сухопутних військах НАТО з'явилися системи зв'язку, що використовують військову версію стандарту IEEE 802.11g, їхнє виробництво освоїла нідерландська фірма MobiComm.

Компані Nova Engineering розробила серійний систему зв'язку за принципом OFDM.

Внаслідок глобального поширення технології OFDM, призвів до того, що дані технології модуляції сигналів були обрані в якості фізичної основи розробки тактичних широкосмугових мереж в рамках програми Joint Tactical Radio System. В перспективі тактичні широкосмуговані мережі будуть використовувати, як радіоліній зв’язку у частотному діапазоні 225-400 МГц. При цьому швидкість передачі буде досягати до 10 Мбіт/с. При зміні смуги системи зв’язку передачі частоти матимуть можливість збільшити швидкість обміну даними. Наприклад модем SDR-4000 компанії L-3 Communications Nova Engineering, при ширині смуги 10 МГц видає швидкість передачі до 20 Мбіт/с.

Для найпростішого з’єднання декількох дронів використовують кодові OFDM-сигнали. Компанія GMS Products використала в свої системі зв’язку, в основі даної система лежать сигналів DVB-T з модуляцією C-OFDM.

Для одночасного зв'язку з декількома БпЛА у найпростішому випадку використовуються кодовані OFDM-сигнали. Наприклад, фірма Cobham Surveillance (GMS Products) просуває систему зв'язку на основі сигналів DVB-T з модуляцією C-OFDM і шестигранної антеної решітки.

Їхня система функціонує діапазонах частоти від 1,7 до 2,5 ГГц, завдяки вбудованій в прилад шестигранії антенії решіткі, дозволяє забезпечити зв'язок із мобільними джерелами сигналів. Так, при 2048 номінальних піднесучих та модуляції піднесучих методом 16-QAM допустимо доплерівський зсув частот до 570 Гц, що відповідає максимальній швидкості взаємного руху передавача та приймача сигналів 280 км/год при центральній несучій 2,2 ГГц. Кожна з шести панелей антени (Рис.1.4) працює із сигналами вертикальної поляризації, коефіцієнт посилення – 12 дБ, діаграма спрямованості – 53° по азимуту та 20° по куту місця (на рівні -3 дБ).

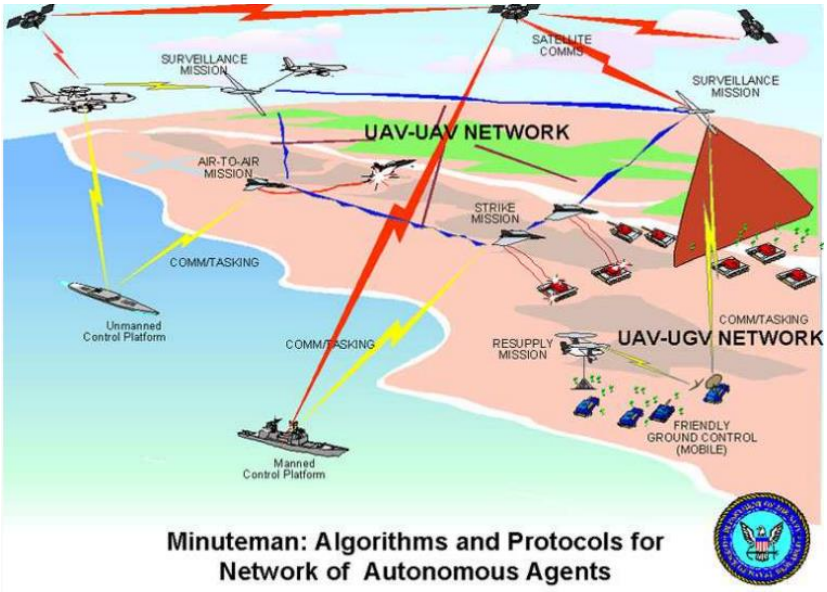

Рис.1.3. Сутність проекту MinuteMan

Американська компанія Aeronix пропонує готові модемні рішення для двостороннього зв'язку з БпЛА у стандарті IEEE 802.16-2004 (режим WirelessMAN_OFDM). При цьому на відстані до 75 морських миль забезпечується швидкість передачі даних від 12 до 65 Мбіт/с. Об'єм модему 802.16 EDL Digital Data Link – 24 куб. дюйма, маса – близько 360 р. Випускається міні-версія модему (802.16 EDL Mini Digital Data Link) для спорядження малих БПЛА . Її об'єм 10 куб. дюймів, маса – близько 150 р. Модеми працюють у діапазонах 5,725–5,825 і 4,5–4,8 ГГц, у яких вибирається одне із чотирьох чи дев'яти (в діапазоні 4,5–4,8 ГГц) каналів шириною 17 МГц з кроком 20 МГц. При обробці сигналів застосовуються дві проміжні частоти – 20 та 570 МГц.

Залежно від дальності зв'язку, швидкості руху БпЛА та завадової обстановки можуть застосовуватись різні рівні амплітудно-фазової модуляції піднесучих, з відповідною зміною швидкості: 6 Мбіт/с (BPSK); 15 Мбіт/с (QPSK); 22,5 Мбіт/с (8-PSK1); 30 Мбіт/с (16-QAM або 16-PSK1); 65,5 Мбіт/с (64-QAM). Істотно, що надійний зв'язок забезпечується при максимальному зсуві доплерівському частоти, що відповідає взаємній швидкості пунктів прийому і передачі даних 2500 миль/ч.

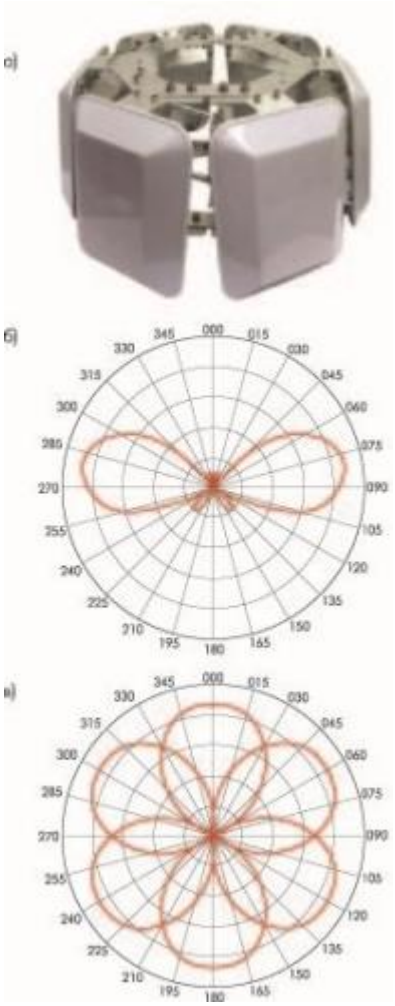

Рис.1.4. Антенна система фірми Global Micriwave System (а), перерізу її діаграм спрямованості у вертикальній (б) та горизонтальній (в) площинах при куті місця 10°

При багатопроменевому поширенні радіохвиль на пересіченій місцевості та множинних перевідображення сигналів актуальна технологія багатоантенних систем MIMO, що базуються на застосуванні цифрових решіток (ЦАР). Один із перших прикладів використання технології MIMO для зв'язку з літальними апаратами – двоантена передача телеметричних даних з борту літального апарату на наземну станцію телеметрії .

У роботі була продемонстрована ефективність застосування найпростішої схеми просторово-часового кодування за алгоритмом Аламоуті для варіанта "2 бортові антени – один наземний приймач" (схема MISO, багато входів – один вихід) (Рис.1.5). Наявність двох антен на корпусі БпЛА дозволило вирішити проблему підтримки надійного зв'язку за різних орієнтацій

корпусу БпЛА щодо направлення на наземну станцію. Надалі була експериментально доведена стаціонарність коефіцієнтів передачі MISO-каналу протягом декількох секунд без маневру літального апарату. Це створило передумови розробки більш просунутих MIMO-решений, використовують багатоелементні антенні решітки.

Принцип MIMO використовується, наприклад, для прийому даних від бортових сенсорів вертолітного міні-БпЛА , розробленого Фраунгоферським інститутом хімічних технологій (Німеччина). Відповідна 4-елементна антенна система приймально-передавальної станції зв'язку з БпЛА у діапазоні частот 2,4 ГГц була представлена на виставці TechDemo'08.

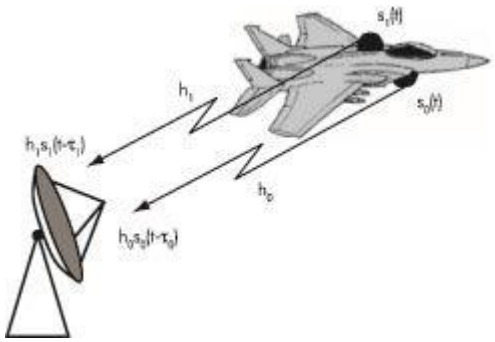

Рис. 1.5. Типова система MIMO за схемою "2×1" під час вирішення завдань бортової телеметрії

Основна умова успішного застосування MIMO-систем – стаціонарність коефіцієнтів передачі радіоканалу з їх оцінювання до завершення трансляції масиву даних. Зрозуміло, що для низькошвидкісних БпЛА ці умови дотримуватись набагато простіше, ніж для високошвидкісних. Однак при прийомі сигналів поза прямою видимістю коефіцієнти передачі каналу можна вважати псевдостаціонарними і для БпЛА , що рухаються з великою швидкістю. Дійсно, кути падіння електромагнітних хвиль на поверхню розсіювання в районі наземної приймальні станції мало змінюються при великому видаленні джерела сигналів. Наприклад, кут приходу хвилі зміниться на 1° при зміщенні БпЛА на 17,6 м на відстані 1 км або на 1746 м при видаленні в 100 км.

Таким чином, при формуванні вимог до перспективних радіоліній зв'язку з БПЛА необхідно орієнтуватися на краще застосування сигналів з модуляцією C-OFDM у поєднанні з технологіями цифрового діаграмоутворення, MIMO і мультиMIMO (MultiUser MIMO). При OFDM-модуляції важливим є метод попереджувальної компенсації ефекту Доплера за отриманими за допомогою пілот-сигналів оцінками доплерівських зміщень частоти. Все це дозволяє забезпечити максимальну спектральну ефективність каналів зв'язку та їхню стійкість до впливу перешкод.

1.6 Висновки з розділу

Спираючись на вище сказане, можливо дійти до висновку, що в залежності від типу призначення безпілотника: військові, антитерористичні та цивільні. В дронах використовують різні види систем зв’язку, через яку здійснюється керування. В свою чергу керування оператором БпЛА може здійснюватися з:

1) З наземний точки контролю – тобто оператор, здійснює управління радіопередавачем / приймачем, смартфоном, планшетом, комп'ютером або військовою наземною станцією управління.

2) Дистанційно використовуючи мережеву систему, такі як супутникові дуплексні канали передачі даних та через пряме управління висхідною лінією зв'язку з БПЛА через стільникову мережу і LTE було продемонстровано і проходить випробування.

3) Іншого літака, що виконує роль ретранслятора або мобільної станції управління, наприклад військовий пілотований безпілотний комплекс (МУМ-Т).

2 ВИДИ ОРГАНІЗОВАНОЇ РАДІОПРОТИДІЇ НОРМАЛЬНОМУ ФУНКЦІОНУВАННЮ БПЛА

2.1 Методи та засоби радіоелектронної боротьби в сучасних реаліях

Радіолокаційні завади розділять на: активні — для створення таких завад використовують станції прийому-передачі радіосигналів або спеціальні передавачі завад, а для створення пасивних завад використовують відбивачі радіохвиль. Обидва види завад націлені маскування або дезінформацію сигналів.

Маскувальні завади виконуються постійним потоком хаотично-шумових сигналів, в наслідок цього радіолокаційний ефір забивається, що не дає змогу відразу виявити потрібний сигнал. Дезінформуючі сигнали вони являться тотожними до оригінального сигналу, але містять хибні данні. Маскуючі активні завади зазвичай мають вигляд радічастотних коливань, які подібні до власних шумів радіолокаційного приймача.

Також, за шириною частотного спектра завади ділять на прицільні та загороджувальні. Ширина спектра прицільних завад є тотожною з пропускною здатність радіо-приймача. Такі завади є налаштованими на фіксовану частоту та мають вузький спектр дії. Метою прицільних завад являється пригнічення окремих радіо завад. Для їх створення потрібні точні параметри локатора, котрий потрібно дестабілізувати. Такий тип завад дозволяє створити перевищення рівня завади над відбитим радіолокаційним сигналом для станцій з невеликим радіусом дії. Загороджувальні же завади перекривають частину радіочастотного діапазонна.

Активні завади можуть одночасно буди маскуючими та дезінформуючими, при умові що радіолокаційний сигнали буде зондуючого типу, які модульовані по амплітуді та інших характеристик сигналу.

В залежності від типу сигналу, що пригнічується та класу радіоелектронного прилада, обираються різні інформаційні критерії.

Оцінку маскуючим завади прийнято давати за допомогою ентропії завадового сигналу. Маскуючі завади зобов’язані перешкоджати можливій передачі корисного сигналу, з ймовірністю появи деякими обмежуючими умовами. Одною з таких умов є передбачення корисного сигналу. Рівень відомих даних може коливатися, але апріорна відомість про корисні сигнали, за правилами розподілу сигналів, які підвладні даному класу, повинні бути відомими. В інакшому випадку працездатність системи може бути під питанням.

За масковані завади створюють певні умови, що після отримання корисного сигналу під дією такої завади, залишає в системі інформаційного забезпечення, невпевненість в достовірності даних. Така невизначеність забезпечую масковані сигнали від потенційного усунення.

За наявності повної відсутності завад, і в результаті аналізу апріорного сигналу невизначеності була б знята, в результаті апостеріорна невизначеність буде рівна нулю.

Під час створення завад засобами радіозв'язку, після прийому сигналу та його аналізу невизначеність не зазнає змін. Під час першого наближення ентропії рівна апостеріорній невизначеності, яка в свою чергу рівна ентропії впливу шумового завадового сигналу. Щоб зменшити кількість отриманих даних, потрібно збільшити ентропію сигнала.

Щоб оцінити потенційні без конкретних методів їх аналізу в придушуючих пристроях, використовую ентропію в якості маскуючої характеристики завадового сигналу.

У розробників завадових пристроїв завжди є необхідні інформація критерії, які допоможуть створити кращій варіант ЗС.

Для оцінювання якості завадового сигналу без прив'язки до подавляючих пристроїв і принципів прийняття рішення противником в умовах завад, використовують інформаційні критерії. Для їх використання при оцінці якості імітаційних сигналу та знати апостеріорні статистичні характеристики хибних цілей.

Найважливішою енергетичною характеристикою завадового сигналу є мінімальне відношення енергії сигналу до енергії корисного сигналу на вході приймального радіоелектронного пристрою, який глушиться в смузі його лінійної частини, при якому з’являється інформаційний збиток. Інформаційний збиток утворюється внаслідок впливу завад, він проявляється в затримці передачі даних, імітації та маскуванні. Характер шкоди, який буде нанесений інформації залежить від видів завадового сигналу та пристрої радіочастотних пригнічення.

Коефіцієнт придушення визначається за формулою (2.1). КП зазвичай виражають через співвідношення потужностей завадового і корисного сигнала на вході пристроя.

$$К_П = \left(\frac{P_з}{P_c}\right) \qquad (2.1)$$

,де Рз — потужність завадового сигналу; Рс — імпульсна потужність корисного сигналу.

Числові значення КП можуть бути знайденими тільки для заданих завадового сигнала і подавляючого пристрою. Внаслідок цього енергетичний критерій на відміну від інформаційного потребує точноих параметрів придушуючих систем.

Якщо на відомі параметри відомі, то можливо знизити енергетичні затрати. Використовуючи відповідні сигнали, не обов'язково тотожних до інформаційних параметрів.

2.2 Типові кібератаки на канали управління БпЛА

Кіберпростір — це концепція, що описує широко поширену взаємопов'язану цифрову технологію. Термін увійшов у популярну культуру з наукової фантастики і мистецтва, але в даний час використовується технологічними стратегами, фахівцями з безпеки, урядовими, військовими, лідерами промисловості та підприємцями для опису області глобальній технологічного середовища, зазвичай визначається як позначення глобальної мережі взаємозалежною інфраструктури інформаційних технологій,

телекомунікаційних мереж і систем комп'ютерної обробки. Інші вважають кіберпростір всього лише умовним середовищем, в якій спілкування відбувається через комп'ютерні мережі. Це слово стало популярним у 1990-х роках, коли використання Інтернету, мереж і цифрових комунікацій різко зросло, і термін кіберпростір зміг позначити безліч нових ідей і явищ.

Як соціальна сфера. Використовуючи цю глобальну мережу, люди можуть взаємодіяти, обмінюватися ідеями, інформацією, надавати соціальну підтримку, вести бізнес, керувати діями, створювати художні медіа, грати в ігри, брати участь в політичних дискусіях і т.д. іноді їх називають кібернавтами. Термін кіберпростір став загальноприйнятим засобом опису всього, що пов'язано з Інтернетом і різноманітною інтернет-культурою. Уряд Сполучених Штатів визнає взаємопов'язані Інформаційні технології та взаємозалежну мережу інфраструктур інформаційних технологій, що діють у цьому середовищі, як частина національної критично важливої інфраструктури. Серед людей в кіберпросторі вважається, що існує кодекс загальних правил і етичних норм, які є взаємовигідними для всіх і називаються кіберетикою. Багато хто вважає право на недоторканність приватного життя найбільш важливим для функціонального кодексу кіберетики. Така моральна відповідальність йде рука об руку при онлайн-роботі з глобальними мережами, зокрема, коли думки пов'язані з соціальним досвідом в Інтернеті.

За словами чіпа Морнінгстара та Ф. Рендалла Фармера, кіберпростір визначається соціальними взаємодіями, а не його технічною реалізацією. На їхню думку, обчислювальне середовище в кіберпросторі є розширенням каналу зв'язку між реальними людьми. Основною характеристикою кіберпростору є те, що воно пропонує середовище, що складається з безлічі учасників, здатних впливати і впливати один на одного. Вони виводять цю концепцію з спостереження, що люди шукають багатство, складність і глибину у віртуальному світі.

За сучасних реалій кіберпростору, поява нових загроз кібератаки національній та міжнародній безпеці виникають майже кожного року. На

сьогодні кібератаки через кіберпростір, хакерськими угрупованнями направленні на: пошкодження ІКС та системи зв'язку за допомогою вірусного спаму; несанкціонований доступ до конфединційних даних з метою їх оприлюднення або спотворення; блокування офіційних та державо потребних веб-ресурсів за допомогою DDOS-атак.

Як прикладом кібератаки є Спуфінг – це кібератака, яка відбувається, коли шахрай маскується під надійне джерело для отримання доступу до важливих даних або інформації.

Як приклад завданням спуфінга є утримання конфеденційної інформаці, яка може призвести до втрати грошей, метод розповсюдження по мережі спотворених посилань чи сайтів, які є шкідливими для пз.

Визначення супуфінг появилося близько одного століття назад, початково термін носив значення будь-якої форми обману. Але в реаліях сучасності визначення набуло характерний вид злочинності, як кіберзлочинність.

В супуфінгу використовують системи зв’язку та спеціалізовані пристрої. Щоб успішність атаки 100% шахраї використовують соціальну інженерію, за допомогою неї зловмисники використовують людських емоціях.

У спуфінга є чотири основних види, які можуть використовуватися в мережі Інтернет: MAC-spoofing, ARP-spoofing, IP-spoofing, DNS-spoofing, GPS-spoofing. Крім них, має місце бути ще й телефонний спуфинг, але це вже не кіберзлочинів, а шахрайство іншого роду.

IP-spoofing - атака полягає в підміні адрес відправників в IP-пакетах, що йдуть на атакується комп'ютер. У підмінений пакеті вказується адреса хостингу, який користується довірою жертва. Хоча насправді пакети йдуть з комп'ютера хакера. Мета даного виду спуфинга в тому, щоб атакується комп'ютер прийняв і пропустив через себе пакети з даними необхідними зловмисникові.

Даний вид спуфинга легко здійснимо в UDP-, а в деяких випадках можливий і в TCP-судинних.

Захист від IP-спуфінга здійснюється шляхом тонкої настройки фільтрів на мережевому рівні. Вони повинні бути налаштовані таким чином, щоб не пропускати ті пакети, які не могли прийти з зазначених в них мережевих інтерфейсів. А гарантовано від даного виду спуфинга захищає настройка фільтрів таким чином, щоб вони зіставляли MAC-адресу і IP-адреса відправника.

На сьогоднішній день сервіси використовують для аутентифікації ім'я користувача і логін, а крім того, передають дані в зашифрованому вигляді. Через це нюанс НСК , використання IP-спуфинга в злочинних цілях відпала. Однак даний вид спуфинга використовується не тільки для того, щоб нашкодити. Наприклад при тестуванні продуктивності використовуються сотні, а іноді і тисячі віртуальних користувачів у яких вказані неіснуючі IP-адреси. Технічно, це є IP-Спуфінга, але аж ніяк не карається, оскільки робиться з санкції власника web-ресурсу.

DNS-spoofing - при використанні даного виду спуфинга принцип ідентичний IPСпуфінга, але використовуються DNS-протоколи.

ARP-spoofing - вид спуфинга в мережах використовують ARP-протоколи, що дозволяє перехоплювати трафік завдяки уязвимостям даного виду протоколів.

Основний недолік ARP-протоколів в тому, що вони абсолютно не захищені і не володіють навіть мінімальними способами перевірки справжності запитів або відповідей. За рахунок цього недоліку APR-протоколи дозволяють перенаправляти трафік таким чином, щоб він проходив не безпосередньо від комп'ютера-жертви до адресата, а робив гак через комп'ютер зловмисника. Дозволяючи останньому отримувати дані йдуть з трафіком (такі як паролі, логіни і дані кредитних карт).

Варто також відзначити, що APR-Спуфінга схильні комп'ютери працюють як під операційною системою Windows, так і під операційною системою Linux, а програми для проведення даного виду атак, поширюються абсолютно безкоштовно.

MAC-spoofing - вид спуфинга при якому змінюється MAC-адресу мережного пристрою, що дозволяє обійти списки контролю маршрутизаторів, серверів або приховати комп'ютер в мережі. Використовується для тестування мереж і передачі шкідливих програм, збору конфіденційної інформації і паролів. Найбільш часто даний вид спуфинга використовується в громадських wi-fi мережах.

GPS-spoofing - застосовується для того, щоб обдурити GPS-приймач, шляхом передачі трохи більше потужного сигналу, ніж той, який надходить від GPS-супутників. Оскільки GPS системи працюють вимірюючи час, за який сигнал проходить від супутника до приймача, то зловмиснику необхідно не тільки точно знати де знаходиться жертва, а й сам підроблений сигнал повинен нагадувати безліч нормальних GPSсигналів. Спочатку спуфер передає вірні координати, проте поступово відхиляє сигнал в сторону. Робити це неспішно необхідно для того, щоб GPS-приймач не заблокований всі сигнали з-за різкої зміни місця розташування. Наприклад, є припущення, що захоплення американських безпілотних апаратів на північному сході Ірану в 2011 році був результатом подібної кваліфікованої атаки.

Щоб найти слід подібних кібератак потрібно пам’ятати такі фактори і дотримуватися таких правил: 1) слідкувати за цілісністю програмних файлів та інших інформаційних ресурсів, котрі потребують захисту; 2) контроль трафіку мережі та дій користувачів під час користування програмним забезпеченням; 3) захист від фізичного впливу на елементи інформаційної системи, наприклад демонтаж або пошкодження носіїв пам’яті; 4) ретельне спостереження за діями адміністратора та дослідження минулих інцидентів кібератак.

Дослідницько-консалтингова компанії Gartner дослідила ринок інформаційних технологій безпеки та авторитетно заявила, що на сьогодні найбільш затребуваними є: аналіз мережного трафіка(Network Traffic Analyzer) — ця технологія здійснює аналіз інформаційної безпеки таких, як журнали, мережевий трафік, котрі є джерелом інформації про загрози і порушення політики безпеки; виявлення і реагування на загрози на робочому місці

(Endpoint Detection and Response) — дана технологія допомагає засобам попередити про винекнення загроз на вузлах, функціями виявлення, реагування і розслідування; аналіз поведінки користувачів (User behavior analytics) — ця технологія допомагає перескочити від статичних правил в системах захисту до динамічного дослідження поведінки порушників інформаційної безпеки користувачів; хмарні брокери/посередники безпеки (Cloud Access Security Broker) — дана технологія опосередковує дані між внутрішніми IT-архітектурами та хмарними середовищами постачальників.

Майже всі кібератаки можливо виявити шляхом аналізу журналів реєстрації спеціальними засобами або вручну. Недоліками ж, таких методів аналізу являється те, що час роботи таких процесів збільшується та не дозволяє своєчасно виявити кібератаку і перешкодити її. Томе рекомендовано застосовувати спеціальні автоматизовані інформаційні системи, які спрямовані на виявлення порушень цілісності інформаційні безпеці.

Щоб підвищити ефективність системи виявлення кібератаки, використовують новітні методи аналізу даних: статистичного підходу; експертних систем; нейронних мереж. Дані методи зазвичай не використовують окремо один від одного, так як вони в сукупності перекривають свої недоліки.

Системи виявлення кібератак розділяють на такі види: за способом реагування; за способом виявлення; за способом збору інформації про кібератаку.

В свою чергу за способом реагування поділяють на пасивні та активні. Пасивні системи виявлення кібератаки фіксують сам момент атаки та записують у регістер і повідомляють факт здійснення атаки. Активні же, чинять супротив атаці, наприклад, змінюють параметри міжмережного екрану.

За способом виявлення атаки системи ділять на два вида: виявлення аномальної поведінки (anomalybased); виявлення зловживань (misuse detection або signature-based). Та найбільш поширеною класифікацією є за способом збору інформації про кібератаку: виявлення атак на рівні мережі

(networkbased); виявлення атак на рівні хоста (host-based); виявлення кібератак на рівні додатка (applicationbased).

2.3 Взлом безпілотників та методи їх захисту

2.3.1 Способи взлому дронів

Є декілька способів взламати дрон. Технічно це не так вже й складно, тим більше що багато власників не дуже дбають про захист. Виявивши безпілотник, кіберзлочинець може взяти його під свій контроль або перехопити відео та зображення, які дрон передає на базову станцію.

Зловмисник може, наприклад, замінити сигнал GPS. Отримавши інші координати, дрон скасує початковий маршрут і полетить туди, куди накаже новий господар. Злочинець може змусити його розбитися (просто заради розваги) або врізатися в лобове скло машини, людини або навіть в інший дрон. Також він може посадити дрон і викрасти його, а разом з ним бортову камеру та всі файли на карті пам'яті.

Дрон можна зламати, навіть перебуваючи за кілометр від нього. Радіосигнал рідко шифрується, тому його легко розкодувати за допомогою спеціальної програми – аналізатора трафіку (сніфера). Для цього не потрібні особливі технічні навички чи обладнання. Перехоплюючи сигнал від оператора, зломщик отримує повний контроль над дроном та його системами. А ще сигнал можна просто заглушити, змусивши дрон забути прохання справжнього власника.

Дослідник Семі Камкар (Samy Kamkar) провів експеримент під назвою Skyjack: він викрав дрон з Raspberry Pi і за його допомогою підпорядкував собі інші безпілотники, таким чином заволодівши цілим роєм дронів. Захоплення одного безпілотника за допомогою іншого значно розширює потенціал загрози. Так само ботнети - армії приватних пристроїв, захоплених зловмисниками, - роблять DDOS-атаки.

Зловмисники можуть перехоплювати дані, які дрон передає на базову станцію, наприклад відеозапис, що транслюється на контролер системою First

Person View (FPV). Часто виробники звичайних дронів, що продаються в магазинах, не захищають їх шифруванням, а незашифровані дані – легкий видобуток для зловмисників. Це якраз і довів експеримент.

2.3.2 Методи захисту

Проаналізувавши вище сказане можливо виділити декілька методів захисту цивільних квадрокоптерів:

• Регулярно оновлюйте прошивку дрона. Основні виробники дронів випускають виправлення з появою нових загроз - регулярне оновлення допоможе вам уникнути їх. Наприклад, компанія DJI випустила виправлення після того, як зловмисники зламали сайт виробника, отримавши доступ до бортових журналів, відео, фотографій та карт користувачів у режимі реального часу. Проте деякі клієнти не встановили виправлення, там залишивши свої дані вразливими для атаки.

• Встановіть надійний пароль для базової станції. Придумайте складну комбінацію з літер, цифр та спеціальних символів – більшість зловмисників здадуться після кількох невдалих спроб злому та шукатимуть легший видобуток. До того ж, найімовірніше, надійний пароль захистить дрон від перехоплення сигналу.

• Якщо ви керуєте дроном через смартфон або ноутбук, захищайте їх від шкідливого програмного забезпечення. У 2012 році кілька дронів, що належать армії США, були інфіковані після того, як оператор скачав і встановив гру зі шкідливим ПЗ на комп'ютер, що управляв. Використовуйте антивірус і не завантажуйте сумнівні програми та програми.

• Підключіть віртуальну приватну мережу (VPN), щоб захистити дані, що надсилаються онлайн. VPN створить між вашим пристроєм та сервером захищене з'єднання – так зловмисники не зможуть перехопити ваші дані.

• Переконайтеся, що до базової станції підключено лише один пристрій. Так хакери не зможуть перехопити сигнал для керування дроном через інші пристрої.

• Переконайтеся, що у дрона увімкнено функцію повернення додому (Return to Home, RTH). Вкажіть місцезнаходження бази. Так дрон зможе повернутися до вас у разі втрати або глушіння сигналу та при низькому заряді батареї. Ця функція допоможе вам врятувати дрон від угону. Однак, оскільки функція RTH працює тільки при увімкненому GPS, дрон буде вразливим для заміни GPS-координат.

2. 4 Висновки з розділу

Аналізуючи вище сказане, радіосигнали завдяки, яким здійснюється передача керуючих команд. Піддаються впливу маскуючим і дезінформуючим завадам, активного та пасивного впливу.

Маскувальні завади виконуються постійним потоком хаотично-шумових сигналів, в наслідок цього радіолокаційний ефір забивається, що не дає змогу відразу виявити потрібний сигнал. Дезінформуючі сигнали вони являться тотожними до оригінального сигналу, але містять хибні данні.

А також, внаслідок використання в деяких дронах, дистанційного управління через простори кіберпростору. Збільшується можливість кібератак на них, шляхом супуфінгу та DDOS атак. І щоб уникнути таких проблем, потрібно дотримуватися простих на перший погляд правил: слідкувати за можливими підключеннями до дрона; завжди мати включену програму «повернення додому»; користуватися ліцензійним програмним забезпеченням управління БпЛА.

3 ПРАКТИЧНІ РЕКОМЕДАЦІЇ ЩОДО ЗАХИСТУ КАНАЛУ УПРАВЛІННЯ БПЛА

3.1 Криптографічні методи захисту каналу управління

Безпілотні авіаційні комплекси (БАК), як правило, об’єднує в собі наземну станцію керування, безпілотний літальний апарат і канали зв'язку між ними. Залежно від характеристик та завдань БпЛА, управління ним може здійснюватися як автоматично, так і вручну за допомогою команд, що передаються оператором на безпілотнник через пульт дистанційного керування (ПДК), що є окремим видом наземної станції управління.

Захист каналів зв'язку між НСК та дроном від зовнішніх програмно-апаратних впливів нині є однією з найактуальніших проблем. Атаки на літальний апарат можуть бути спрямовані на перехоплення управління, виведення БпЛА з ладу, отримання або спотворення інформації, що передається корисним навантаженням безпілотник, або для подальшої атаки на НСК та системи, що взаємодіють з нею.

В даний час існує безліч засобів захисту цілісності та конфіденційності інформації, що передається різними каналами зв'язку та бездротово. Однак існує певна специфіка захисту авіаційних комплексів , яка визначається сукупністю способів несанкціонованого або випадкового доступу до систем БАК, внаслідок якого можливе порушення конфіденційності, цілісності та доступності інформації. Зокрема, при розробці засобів захисту для для таких комплексів необхідно враховувати такі особливості:

1) БпЛА, як і інші роботизовані комплекси, зазвичай функціонують під управлінням операційних систем (ОС), спеціально призначених для управління роботизованими комплексами та системами, серед яких – спеціалізовані операційні системи реального часу (Real-Time Operation System – RTOS). Як одну з основних вимог до таких ОС висувається вимога забезпечення передбачуваності або детермінованості поведінки системи в найгірших зовнішніх умовах, що різко відрізняється від вимог до ОС загального

призначення, які, в основному, належать до їхньої продуктивності та можливості застосування на різних апаратних платформах.

2) Безпілотник являє собою складну інтегровану автоматизовану систему - апаратура та агрегати на борту БпЛА структурно об'єднані у системи, призначені для вирішення окремих завдань. Окремі системи можуть об'єднуватися у більші структурні елементи - комплекси. Комплекс бортового обладнання – сукупність функціонально-пов'язаних систем, приладів, датчиків, обчислювальних пристроїв. Система керування дронів забезпечує управління та взаємодію між усіма комплексами або системами БпЛА.

3) Безпілотні літальні апарати можливо подати як телекомунікаційну систему, що складається з пристроїв, між якими здійснюється обмін інформацією за спеціальними протоколами.

Крім того, найважливішими експлуатаційними характеристиками БпЛА є такі взаємопов'язані властивості, як максимальна вага корисного навантаження дроону та максимальна тривалість і дальність польоту. Оскільки живлення бортового обладнання дронів здійснюється від власного джерела живлення, що має обмежений ресурс, тому всі системи безпілотників повинні відрізнятися економічністю, тобто мінімальним енергоспоживанням.

Тому засоби захисту інформації від зовнішніх програмно-апаратних впливів, тому бортова частина авіаційного комплекса повинна мати малогабаритну характеристики і низьку ресурсомісткість. Шифрування сигналів БпЛА не повинний ускладнювати процес обміну даними у реальному масштабі часу, це може порушити оперативність передачі команд та інформаційних потоків. Отже, системи захисту каналів зв'язку безпілотників повинні бути малогабаритними та мати змогу надати мінімальну можливість до обчислювальних ресурсів з метою мінімізувати негативний вплив на перелічені вище основні експлуатаційні характеристики БпЛА.

Вище сказані загрози атак на безпілотник може виникнути внаслідок утворення каналу реалізації загрози між джерелом загрози та дроном. Оскільки БпЛА використовують бездротові канали з наземною станцією керування,

реалізація загрози може здійснюватися шляхом атаки канал бездротового зв'язку з літальни апаратом.

В ідеалі захисту повинні підлягати усі бездротові канали БпЛА та НСК. Однак внаслідок вимог до мінімізації ресурсоємності системи захисту дронів, виконується захист тільки критичних каналів зв’язку, до яких відносяться:

- канал управління, оскільки основні загрози БпЛА (такі як перехоплення управління або виведення з ладу) найбільш просто здійснити у разі успішної експлуатації атакуючим каналу керування дрону;

- канал телеметрії, оскільки успішна підміна атакуючим телеметричної інформації , може призвести до реалізації перелічених вище загроз БпЛА.

Слід зазначити, що у даний час існує досить велика кількість методів захисту інформації для стандартних протоколів бездротового зв'язку та його реалізацій. Однак їх безпосереднє використання для захисту каналів зв'язку між дроном та станцією неможливе або являється недоцільне з таких причин:

1. Методи, протоколи та реалізації криптографічних алгоритмів залежать від організації самого радіоканалу і структури бездротової мережі. Пряме копіювання будь-якого набору методів та протоколів інформаційної безпеки для використання в каналах зв'язку БпЛА неможливе через розбіжність принципів організації радіоканалів, кількості об'єктів зв'язку та структури їх зв'язності.

2. Багато методів, наприклад, організація довіреного центру автентифікації об'єктів, центру генерації та розподілу ключів, мають значну надмірність у застосуванні до безпілотно авіаційного комплекса.

3. Застосування багатьох методів безпеки призводить до значного підвищення навантаження на канали зв'язку і знижує пропускну здатність каналів. У системі управління БпЛА будь-яке зайве навантаження на канали зв'язку може призвести до зниження швидкості передачі інформації і вплинути на керованість і динаміку польоту самого літального апарату.

4. Одними з основних принципів стандартів масового зв'язку є зручність, простота та прозорість налаштувань для звичайного користувача. Даний

принцип поширюється і на методи забезпечення безпеки, що призводить до того, що виробники змушені користуватися стандартними налаштуваннями, які дозволяють підключатися до систем зв'язку, але знижують показники безпеки передачі даних.

5. Некоректна реалізація криптографічних алгоритмів і особливо систем управління криптографічними ключами, а також їх розробка без урахування особливостей подальшого застосування призводять до вразливості в таких реалізаціях.

Зазначимо, що специфіка застосування БпЛА вимагає застосування спеціально адаптованих для дронів схем генерації, розподілу та використання ключової інформації, яка значно відрізняються від звичайних в протоколах захисту бездротового зв'язку.

Існують багато патентних способів захисту системи зв’язку БпЛА, створених по криптографічним алгоритмам і які легко адаптуються для використанні в подібних системах анологічних приладах.

Наприклад, в патенті США US 8219799 від 10.07.2012 р. компанія Lockheed Martin пропонується захищену систему зв'язку, що включає в себе процесор обробки даних, конвертер Інтернет-протоколу, який перетворює дані, шифратор/дешифратор для забезпечення додаткової безпеки, криптографічний модуль, що оцінює рівень безпеки даних і перевіряє криптографічні ключі. Процесор зв'язку забезпечує керування в реальному часі і може змінювати джерело або одержувач даних, ключ шифрування, рівень безпеки, протокол зв'язку у відповідь на дані датчиків, отримані від комунікаційного об'єкта або від командних сигналів підключеної або дистанційної системи управління.

У патенті США US 9531689 від 27.12.2016 р. запропонований спосіб і система шифрування і дешифрування даних в пристрої пам'яті і в пакетах даних, що передаються по мережі зв'язку. Система складається з двох пристроїв мережевої обробки, одне з яких призначене для прийому і зберігання переданих даних, а друге - для їх передачі. При передачі проводиться інкапсулювання інформації в кадр пакетів даних. Пакети можуть бути стиснуті до шифрування.

Запатентована система може бути використана для захисту каналів зв'язку в БпЛА.

У патенті Китаю CN 105491564 від 13.04.2016 р. запропоновано спосіб для встановлення захищеного зв'язку в середовищі з декількома БАК з використанням надійного протоколу взаємодії, що дозволяє уникнути помилкових запитів і відповідей. Дані шифруються за допомогою закритого ключа, що забезпечує конфіденційність повідомлень.

Значна частина патентів присвячена ідентифікації, аутентифікації та авторизації об'єктів і суб'єктів доступу в системах, що застосовують БпЛА.

Наприклад, китайською фірмою SZ DJI Technology володіє групою патентів захисту системи аутентифікації та методів формування правил польотів безпілотників, що містять центр аутентифікації і систему управління польотами, створенні для управління доступом до дрона на основі аутентифікації БпЛА та відповідного користувача літальнго апарата за допомогою їх ідентифікаторів.

Американською фірмою Microsoft Technology Licensing було запатентована система авторизації для БпЛА, яка здійснює контроль доступу до управління безпілотника. Дана система містить контролер БАК, який зв'язаний по інтерфейсу з блоком авторизації управління, що містить процесор, інтерфейс зв'язку і пам'ять. Отримуючи ідентифікаційний код від контролера БпЛА, який вводиться оператором, засіб авторизації проводить перевірку його відповідності, яка зберігається підписаному цифровому сертифікату. Аналогічна процедура аутентифікації проводиться для будь-якої прийнятої керуючої команди. Якщо цифровий сертифікат недійсний, засіб авторизації не дозволяє оператору ініціювати Керуючі інструкції і не передає інструкцію управління БпЛА.

Крім рішень щодо забезпечення захисту каналів дрона за допомогою криптографічних алгоритмів, варто звернути увагу, на ряд патентів, що забезпечують захист переданої інформації без застосування криптографії.

Наприклад, в міжнародному патенті WO 2005020445 від 10.11.2005 р. для керування безпілотником пропонуються спеціальні мікрохвильові антени для безпечної передачі даних, що забезпечують надійний зв'язок «точка-точка» в мережах бездротової передачі даних на короткі відстані, і транспондер з високою спрямованістю сигналу і додатковим сигналом глушіння того ж спектру, що запобігають перехопленню переданих повідомлень.

Також цікаверішення запропонувала компанія Northrop Grumman Systems, вони представили спосіб захисту повідомлень між дронами і спутником на частоті в діапазоні 50-70 ГГц за патентом США US 8594662 від 26.11.2013 р, який включає в себе вибір частоти сигналу на основі висоти польоту літака і кута положення між космічним апаратом і літаком.

Крім того, досить велика кількість патентів присвячено методам і засобам розподілу ключової інформації, які можуть бути використані в БпЛА або дистанційно керованих апаратах.

Наприклад, у патенті США US 5841864 від 24.11.1998 р. компанією Motorola запропоновала метод, що забезпечує односторонню аутентифікацію пристрою та обмін сесійними ключами на основі попередньо розподіленого секрету для подальшого захисту повідомлень, що передаються по каналу зв'язку.

Найбільш близькими до пропонованих способу і систем криптографічного захисту каналів зв'язку безпілотника є спосіб і система захищеного керування і моніторингу дистанційно керованих пристроїв, запропонований фірмою The Charles Stark Draper Laboratory (США) і описаний в патенті США US 9871772 від 16.01.2018 р.

Система і методи, що розглядаються в якості прототипу, забезпечують досить високий рівень безпеки передачі даних для невеликих апаратів з обмеженими обчислювальними ресурсами, які управляються по бездротовому каналу зв'язку. Окремим випадком таких апаратів є БпЛА.

Основними компонентами, що описані в патенті США US 9871772 системи є наступні:

- дистаційно керований апарат (RCD-Remotely Controlled Device), аналогом якого є безпілотний апарат;

- основний керуючий елемент (PCE-Primary Control Element), аналогом якого є наземна система керування;

- опціональний керуючий елемент-додаткова станція керування, що знаходиться перша за передбачуваним курсом руху керованого апарату Forward Observer.

Вказаному вище патенті метод полягає у виконанні наступної послідовності дій з боку основного керуючого елемента:

1. PCE запитує і отримує від безпілотника його параметри.

2. На основі отриманих параметрів PCE вибирає відкритий ключ, асоційований з конкретним екземпляром RCD.

3. PCE генерує основний (перший) ключовий набір, що діє протягом майбутньої місії RCD і включає Майстер-ключ даного екземпляра RCD.

4. PCE зашифровує згенерований ключовий набір з використанням відкритого ключа RCD.

5. Зашифрований ключовий набір передається на RCD по інтерфейсу завантаження ключів.

6. PCE зашифровує першу команду, призначену для RCD, на першому ключі шифрування, породженому з майстер-ключа даного екземпляра RCD.

7. Перша команда і інформація, необхідна для аутентифікації PCE з боку RCD (мітка аутентифікації), відправляється на RCD по бездротовому каналу зв'язку.

Передбачається, що інтерфейс завантаження ключів в RCD використовується одноразово (в рамках підготовки до виконання конкретної місії) і за визначенням є довіреним, тобто являє собою, наприклад, провідний інтерфейс, який задіюється тільки в довіреному оточенні, тоді як подальша відправка команд здійснюється по бездротовому інтерфейсу, що не є довіреним.

У свою чергу, RCD виконує наступну послідовність дій, що відповідають на дії, ініційовані з боку PCE і описані вище:

1. RCD отримує зашифрований ключовий набір від PCE.

2. RCD розшифровує ключовий набір для отримання з нього свого майстер-ключа.

3. RCD отримує першу зашифровану команду від PCE по бездротовому каналу зв'язку.

4. RCD аутентифікує PCE на основі отриманої мітки аутентифікації з використанням попередньо завантаженого ключа хешування.

5. RCD розшифровує першу отриману команду на першому ключі шифрування, породженому з майстер-ключа.

Надалі команди, що передаються на RCD з боку PCE, зашифровуються на поточному використовуваному ключі шифрування, який синхронно змінюється на RCD і PCE через певну кількість команд (в т. ч. можливий варіант зміни ключа після кожної команди) або через зумовлені інтервали часу.

Параметри RCD можуть включати в себе як який-небудь ідентифікатор, однозначно визначає конкретний екземпляр RCD, так і безпосередньо відкритий ключ RCD. Параметри можуть бути нанесені на зовнішню поверхню RCD (наприклад, у вигляді штрих-коду) і зчитуватися оптичним способом або можуть перебувати в пам'яті радіочастотної мітки ближнього поля (NFC - Near-Field Interface) і зчитуватися за допомогою відповідного рідера.

При наявності однієї або більше додаткових станцій управління (FO) відправляються керуючі команди на RCD з боку FO зашифровуються за допомогою додаткового (другого) ключового набору, що містить додатковий Майстер-ключ, призначений для захисту обміну даними по бездротовому каналу зв'язку між FO і конкретним екземпляром RCD. Механізми породження поточних ключів шифрування з даного майстер-ключа і їх зміни аналогічні таким при взаємодії PCE і RCD.

PCE і FO можуть одночасно керувати кількома екземплярами RCD, при цьому описані вище принципи взаємодії компонентів системи не змінюються.

Патент США US 9871772 описує також один з можливих варіантів реалізації апаратного модуля, що забезпечує захист каналів зв'язку відповідно до запропонованого способу (криптографічного модуля). В описі патенту наголошується, що криптографічний модуль повинен бути реалізований у вигляді виділеного пристрою, причому конкретна реалізація алгоритмів, що лежать в основі запатентованого способу, може бути виконана апаратно (у вигляді спеціалізованих мікросхем) або програмно (у вигляді програмованих логічних інтегральних схем або у вигляді програмного забезпечення, що виконується на мікропроцесорах (мікроконтролерах) загального призначення). Відзначимо також, що алгоритми роботи криптографічного модуля дещо різняться в залежності від його конкретного застосування (на RCD, PCE або FO); проте, всі ці компоненти системи можуть бути оснащені однотипними криптографічними модулями з можливістю їх параметризації для забезпечення різних варіантів застосування. Описаний в патенті США US 9871772 криптографічний модуль є прототипом заявляється пристрою.

Крім описаних вище основного (першого) і додаткового (другого) ключових наборів, спосіб допускає використання третього ключового набору для захисту даних, що передаються по бездротовому каналу зв'язку з боку RCD на PCE, і четвертого ключового набору для захисту даних, що передаються по бездротовому каналу зв'язку з боку RCD на FO.

Відзначимо, що патент США US 9871772 описує ряд варіацій способу захищеного управління і моніторингу віддалено керованих пристроїв, відмінності між якими полягають в наступному:

- які конкретно використовуються параметри для ідентифікації RCD, яким чином вони зберігаються і зчитуються;

- за яким принципом здійснюється зміна поточних ключів шифрування;

- яким чином здійснюється зберігання ключів шифрування на RCD;

- чи використовуються методи електронного підпису для захисту цілісності завантажуваних на RCD ключових наборів;

- чи використовуються однотипні криптографічні модулі на всіх компонентах системи;

- чи використовується процедура безпечного встановлення з'єднання між РСЕ і FO;

- яким чином здійснюється управління ключовими наборами та їх використання при наявності декількох FO в системі;

- чи допускається одночасне управління декількома RCD з боку РСЕ і FO;

- чи використовуються третій і четвертий ключові Набори для захисту даних, що передаються з боку RDC по бездротовому каналу зв'язку, відповідно, на РСЕ і FO.

Пропонований заявниками спосіб криптографічного захисту каналів зв'язку БАК має ряд переваг в порівнянні зі способом, описаному в прототипі, які зводяться до наступних:

1. Спрощений в порівнянні з прототипом протокол розподілу ключової інформації, що не погіршує якості захисту. Крім того, запропонований протокол розподілу ключової інформації забезпечує захист від атак класу «людина посередині» (man-in-the middle, MITM), тоді як в описі прототипу явним чином сказано, що використовувані схеми розподілу ключів не забезпечують захист від атак даного класу.

2. Виконання у всіх випадках тільки взаємної аутентифікації БпЛА і НСК , тоді як в прототипі не передбачена аутентифікація FO з боку RCD, що може привести до потенційного перехоплення управління RCD шляхом впровадження в систему помилкових FO.

3. Крім криптографічного захисту, в заявляється способі передбачений також додатковий фактор захисту, заснований на псевдовипадкової перенастроювання параметрів радіозв'язку між БпЛА і НСК .

4. Заявляється спосіб передбачає, крім каналів керування та телеметрії, шифрування також інформації корисної навантаження БпЛА, переданої на НСК , тоді як в прототипі шифрування каналу управління є обов'язковим, шифрування каналу телеметрії - опціональним, а з усього спектру варіантів

інформації корисної навантаження БпЛА допускається тільки шифрування відеосигналу, причому тільки в тому випадку, якщо він використовується для віддаленого управління RCD з боку РВЄ або FO і тільки в необхідних для такого управління обсягах.

5. Заявляється спосіб передбачає можливість реалізації передбачених ним алгоритмів і протоколів криптографічного захисту каналів зв'язку БАК не тільки у виділеному апаратному криптографічному модулі, але і у вигляді програмних модулів, що виконуються безпосередньо на польотному контролері БПЛА або на обчислювальних ресурсах існуючого обладнання НСК . Відсутність необхідності установки апаратного криптографічного модуля на БПЛА, з одного боку, не вимагає внесення конструктивних змін в БпЛА і, з іншого боку, в значно меншій мірі (тільки за рахунок додаткового енергоспоживання) погіршує основні експлуатаційні характеристики БпЛА, тобто максимальна вага корисного навантаження БпЛА і/або максимальну тривалість/дальність польоту.

6. Заявляється спосіб підвищує якість захисту каналів зв'язку БАК в порівнянні з прототипом, оскільки він має на увазі шифрування повідомлень цілком, тоді як в описаній структурі повідомлень прототипу існують нешифруемие службові поля (поля «bypass»), через які теоретично можливий витік інформації.

7. Заявляється спосіб також передбачає, що апаратна або програмна реалізація криптографічних перетворень оснащена додатковими модулями, що забезпечують контроль працездатності модулів, що виконують криптографічні перетворення, а також їх самотестування - при старті і періодичне в процесі роботи.

Пропонована заявниками система криптографічного захисту каналів зв'язку БАК реалізує пропонований спосіб і, крім описаних вище переваг способу криптографічного захисту каналів зв'язку БАК, володіє також наступними перевагами в порівнянні з системою, описаною в прототипі:

1. На відміну від прототипу, в якому жорстко зафіксована структура повідомлень між компонентами системи і система команд, заявляється система не накладає обмежень на використовувану систему команд. Це робить заявлену систему значно більш гнучкою і універсальною, оскільки система може бути побудована на значно ширшому спектрі обладнання, що застосовується в БпЛА і НСК , тоді як система, описана в прототипі, може бути реалізована тільки на обладнанні, що реалізує описані структуру повідомлень і систему команд, тобто. на обладнанні, спочатку розробленому з метою використання в такій системі.

2. Можливість реалізації криптографічного модуля у вигляді програмних модулів, що виконуються безпосередньо на польотному контролері БпЛА, дозволяє, з одного боку, здешевити систему в цілому в порівнянні з прототипом і, з іншого боку, реалізувати систему з використанням більш широкого спектру існуючого обладнання як БпЛА, так і НСК , оскільки не вимагає внесення конструктивних змін в апаратну частину існуючих БпЛА/НСК для забезпечення підключення апаратного криптографічного модуля, передбаченого прототипом.

Заявляється пристрій являє собою один з варіантів реалізації заявляється способу криптографічного захисту каналів зв'язку БАК.

Технічний результат досягається наступним чином:

1. Спосіб криптографічного захисту каналів зв'язку між НСК і БпЛА полягає у виконанні наступної послідовності дій:

Крок 1) за допомогою ключового носія НСК , оснащеного обчислювальними ресурсами і енергонезалежною пам'яттю, а також криптографічними функціями, генерується пара асиметричних ключів НСК : секретний і відкритий Ключі НСК .

Крок 2) за допомогою ключового носія БпЛА, оснащеного обчислювальними ресурсами і енергонезалежною пам'яттю, а також криптографічними функціями, генерується пара асиметричних ключів БпЛА: секретний і відкритий Ключі БПЛА.

Крок 3) здійснюється копіювання відкритих ключів НСК і БпЛА на, Відповідно, ключовий носій БпЛА і ключовий носій НСК , після якого ключовий носій НСК містить секретний і відкритий Ключі НСК і відкритий ключ БпЛА, а ключовий носій БпЛА містить секретний і відкритий Ключі БпЛА і відкритий ключ НСК .

Крок 4) криптографічний модуль БпЛА, оснащений програмною або апаратною реалізацією криптографічних алгоритмів, можливістю ініціювання передачі повідомлень на НСК і опціональною можливістю блокування порту підключення польотного контролера БпЛА до каналів зв'язку, ініціює генерацію ключовим носієм БпЛА загального секретного пре-майстер-ключа (призначеного для подальшої генерації на його основі майстер-ключа) на основі секретного ключа БпЛА і відкритого ключа НСК .

Крок 5) криптографічний модуль БпЛА зчитує з ключового носія БпЛА відкритий ключ БпЛА, відкритий ключ НСК і загальний секретний пре-Майстер-ключ.

Крок 6) криптографічний модуль НСК , оснащений програмною або апаратною реалізацією криптографічних алгоритмів, можливістю ініціювання передачі повідомлень на БпЛА і опціональною можливістю блокування інтерфейсу обміну з програмним забезпеченням, що здійснює управління БПЛА, ініціює генерацію ключовим носієм НСК загального секретного пре-майстер-ключа на основі секретного ключа НСК і відкритого ключа БпЛА.

Крок 7) криптографічний модуль НСК зчитує з ключового носія НСК відкритий ключ НСК , відкритий ключ БпЛА і загальний секретний пре-Майстер-ключ.

Крок 8) криптографічний модуль БпЛА перевіряє стан своєї готовності до роботи.

Крок 9) криптографічний модуль БпЛА ініціює відправку повідомлення криптографічному модулю НСК , що містить відкритий ключ БпЛА і випадкове число БпЛА.

Крок 10) криптографічний модуль НСК , що знаходиться в режимі очікування повідомлень з каналу зв'язку, отримує дане повідомлення від БпЛА і перевіряє, чи є у нього отриманий відкритий ключ БпЛА. Якщо такого відкритого ключа у криптографічного модуля НСК немає, то криптографічний модуль НСК ігнорує отримане повідомлення і повертається в режим очікування повідомлень.

Крок 11) криптографічний модуль НСК ініціює відправку відповідного повідомлення криптографічному модулю БпЛА, що містить відкритий ключ НСК і випадкове число НСК .

Крок 12) криптографічний модуль БпЛА отримує відповідне повідомлення від криптографічного модуля НСК і перевіряє, чи є у нього отриманий відкритий ключ НСК . Якщо такого відкритого ключа у криптографічного модуля НСК немає, то криптографічний модуль БПЛА ігнорує дане повідомлення і повертається до кроку 9.

Крок 13) криптографічний модуль БпЛА виробляє Майстер-ключ (призначений для подальшої генерації на його основі сеансових криптографічних ключів) на основі пре-майстер-ключа, випадкового числа БПЛА і випадкового числа НСК .

Крок 14) криптографічний модуль НСК виробляє Майстер-ключ на основі пре-майстер-ключа, випадкового числа БпЛА і випадкового числа НСК .

Крок 15) криптографічний модуль БпЛА на основі майстер-ключа виробляє сеансовий ключ шифрування і сеансовий ключ обчислення.

Крок 16) криптографічний модуль НСК на основі майстер-ключа виробляє сеансовий ключ шифрування і сеансовий ключ обчислення.

Крок 17) криптографічний модуль БпЛА формує тестове повідомлення, зашифроване на виробленому сеансовому ключі шифрування, і ініціює його відправку криптографічному модулю НСК .

Крок 18) криптографічний модуль НСК отримує і розшифровує тестове повідомлення від криптографічного модуля БпЛА і перевіряє його відповідність очікуваному тестовому повідомленню. Якщо тестове

повідомлення не відповідає очікуваному, то криптографічний модуль НСК вважає, що сталася помилка встановлення сеансових криптографічних ключів, і повертається в режим очікування повідомлень.

Крок 19) криптографічний модуль НСК формує у відповідь тестове повідомлення, зашифроване на виробленому сеансовому ключі шифрування, і ініціює його відправку криптографічному модулю БпЛА.

Крок 20) криптографічний модуль БпЛА отримує і розшифровує тестове повідомлення від криптографічного модуля НСК і перевіряє його відповідність очікуваному тестовому повідомленню. Якщо тестове повідомлення не відповідає очікуваному, то криптографічний модуль БпЛА вважає, що сталася помилка встановлення сеансових криптографічних ключів, і повертається до кроку 9.

Крок 21) криптографічний модуль БпЛА виставляє прапор готовності до роботи.

Крок 22) криптографічний модуль НСК виставляє прапор готовності до роботи.

Крок 23) криптографічний модуль БпЛА відкриває порт підключення польотного контролера.

Крок 24) криптографічний модуль НСК відкриває інтерфейс обміну з програмним забезпеченням, що здійснює управління БпЛА.

Крок 25) подальший обмін інформацією по каналах управління і телеметрії між НСК і БпЛА ведеться в захищеному режимі з використанням шифрування на основі виробленого сеансового ключа шифрування і з контролем цілісності на основі виробленого сеансового ключа обчислення імітo-вставки.

3.2 Висновки з розділу

Конкретизуючи все вище сказане, щоб захисти систему управління безпілотників. Слід зазначити, що у даний час існує досить велика кількість

методів захисту інформації для стандартних протоколів бездротового зв'язку та його реалізацій. Однак їх безпосереднє використання для захисту каналів зв'язку між дроном та станцією неможливе або являється недоцільне з таких причин:

1. Методи, протоколи та реалізації криптографічних алгоритмів залежать від організації самого радіоканалу і структури бездротової мережі. Пряме копіювання будь-якого набору методів та протоколів інформаційної безпеки для використання в каналах зв'язку БпЛА неможливе через розбіжність принципів організації радіоканалів, кількості об'єктів зв'язку та структури їх зв'язності.

2. Багато методів, наприклад, організація довіреного центру автентифікації об'єктів, центру генерації та розподілу ключів, мають значну надмірність у застосуванні до безпілотно авіаційного комплекса.

3. Застосування багатьох методів безпеки призводить до значного підвищення навантаження на канали зв'язку і знижує пропускну здатність каналів. У системі управління БпЛА будь-яке зайве навантаження на канали зв'язку може призвести до зниження швидкості передачі інформації і вплинути на керованість і динаміку польоту самого літального апарату.

4. Одними з основних принципів стандартів масового зв'язку є зручність, простота та прозорість налаштувань для звичайного користувача. Даний принцип поширюється і на методи забезпечення безпеки, що призводить до того, що виробники змушені користуватися стандартними налаштуваннями, які дозволяють підключатися до систем зв'язку, але знижують показники безпеки передачі даних.

5. Некоректна реалізація криптографічних алгоритмів і особливо систем управління криптографічними ключами, а також їх розробка без урахування особливостей подальшого застосування призводять до вразливості в таких реалізаціях.

4 ОХОРОНА ПРАЦІ

4.1 Аналіз впливу негативних чинників на оператора БпЛА

Згідно з Законом України «Про охорону праці» № 2694-XII від 14 жовтня 1992 року, охорона праці – це система правових та соціально-економічних, організаційно технічних та санітарно-гігієнічних, лікувально-профілактичних заходів та засобів, які спрямовані на збереження здоров’я й працездатності працюючої людини.

Відповідно до ст. 4 Закону України "Про охорону праці": державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована саме на створення належних, безпечних та здорових умов для праці, також попередження нещасних випадків і професійних захворювань.

За порушення законів й інших нормативних правових актів з охорони праці, і створення перешкод у діяльності, а саме, посадових осіб органів державного нагляду за охороною праці, а ще представників професійних спілок, усіх їх організацій та об'єднань винні у цьому особи підлягають дисциплінарній, адміністративній, матеріальній та кримінальній відповідальності відповідно до Закону (ст. 44 Закону "Про охорону праці").

Впровадження комп'ютерних технологій докорінно змінило характер роботи різних категорій фахівців, вимоги до організації робочого процесу та охорони праці, включаючи операторів дистанційного керування БПЛА. Оператори в ході праці використовують комп'ютерні технології (екран монітору), випробуючи їх величезний потенціал.

Робота на комп'ютері є високоризиковою роботою, згідно з переліком високоризикових робіт, затвердженим наказом Державного комітету України, відповідно, з нагляду у сфері охорони праці № 123 від 30 листопада 1993 року.

Інструкція є розробленою відповідно до «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними

пристроями», які затверджені Наказом Міністерства соціальної політики України від 14.02.2018 року № 207.

Недотримання вимог безпеки призводить до того, що через деякий час після роботи за комп'ютером співробітник починає відчувати певний дискомфорт, а саме: з'являються головні болі і біль в очах, стомлюваність і дратівливість. У деяких людей порушується сон, погіршується зір, починають боліти м'язи рук, шиї, поперек і т. д.

До найбільш поширених помилок, пов'язаних із забезпеченням умов праці операторів, які працюють на комп'ютерах, відносяться:

• недостатня площа і обсяг виробничого приміщення;

• недотримання вимог до температури і вологості робочих приміщень;

• низький рівень освітленості в приміщеннях і на робочих поверхнях обладнання;

• підвищений рівень низькочастотних магнітних полів від моніторів;

• довільне розміщення обладнання, порушення вимог організації робочого місця;

• недотримання вимог до режиму (відпочинок, праця);

• надмірне виробниче навантаження працівників;

• відсутність навичок зниження впливу психоемоційного стресу.

Залежно від умов праці, в яких використовуються ПК, та характеру виконуваної роботи, працівники можуть також піддаватися впливу інших небезпечних і шкідливих виробничих факторів.

Відповідно до ст. 14 Закону «Про охорону праці» роботодавець зобов'язаний забезпечити:

• безпеку працівників при експлуатації обладнання;

• використання засобів індивідуального захисту;

• відповідні вимоги охорони праці, умови праці на кожному робочому місці;

• дотримання режиму праці й відпочинку;

- навчання безпечнішим методам, прийомам виконання робіт;
- інструкцію (з охорони праці);
- організацію контролю встановлених умов праці на робочих місцях;
- атестацію робочих місць;
- інформування працівників про умови праці та охорону праці на робочому місці, існуючий ризик заподіяння шкоди здоров'ю, а ще про компенсацію та засоби індивідуального захисту, на які у них є право.

4.2 Безпека зорового аналізатора при роботі з екраном

Місця розміщення оператора та персонального комп’ютера повинні відповідати: вимогам НПАОП 0.00-7.15-18 "Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями", які затверджені наказом Міністерства соціальної політики України від 14.02.2018 № 207, «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно – обчислювальних машин», затверджених постановою Головного державного санітарного лікаря України від 10.12.1998 року № 7 (ДСанПіН 3.3.2-007-98).

При розташування робочих станцій з комп'ютерами відстань, між робочими столами з екранами моніторів, має бути мінімум 2,0 м, а відстань між бічними поверхнями екранів моніторів – більше 1,2 м.

Робоча зона з комп'ютером в приміщеннях, де імовірне існування шкідливих виробничих факторів розташовують в окремих кабінах, обов'язково, з якісним повітрообміном.

Екран монітора повинен бути розташовуваним від очей працівника на відстані 600 – 700 мм, але далі 500 мм, якщо брати на рахунок розмір буквено-цифрових знаків й позначень.

Висота столу, за нормами, повинна складати близько 680 – 800 мм, але якщо це неможливо, то висота робочої поверхні повинна бути 725 мм. Модульні розміри робочої поверхні столу користувача ПК, за якими

розраховуються розрахункові розміри, це: ширина – 800, 1000, 1200 та 1400 мм, глибина – 800 або 1000 мм при невстановленій висоті 725 мм.

Працівник повинен мати вільний простір для ніг висотою, обов’язково, близько 600 мм, шириною більше 500 мм, глибиною не менше 450 мм на рівні коліна та 650 мм при витягнутих ногах.

Конструкція крісла робочого місця повинна цілком забезпечувати підтримку встановленої пози для роботи за ПК, не обмежувати положення що б зменшувати статичну напругу м'язів шиї і спини, запобігати розвитку стомлення.

Робоче місце користувача ПК, обов’язково, повинно бути обладнане підставкою для ніг шириною більше ніж 300 мм, глибиною – 400 мм, регулюванням висоти до 150 мм та кутом нахилу опори стійкі до 20 градусів. Матеріал поверхні підставки повинен бути рифленим та висотою 10 мм уздовж передньої кромки.

Клавіатура (або інші контролери, в випадку управління БПЛА – ручка управління) повинна розміщуватись на поверхні робочого столу на відстані від 100 до 300 мм від краю, який знаходиться біля користувача, або на спеціальній регульованій підставці по висоті робочої поверхні, яка відокремлена від основної стільниці робочого місця.

Існує три види робіт, що виконуються на ПК:

• група А – робота по зчитуванню інформації з екрану;

• група Б – робота по введенню інформації;

• група В – творча робота в діалоговому режимі з ПК.

При виконанні певних робіт, пов'язаних з різними видами робіт на протязі робочої зміни, основною роботою з ПК слід вважати ту, яка займає більше 50% часу робочої зміни або робочого дня.

Для видів робіт виділяють три категорії тяжкості та інтенсивності роботи з ПК, які визначаються:

• для групи А зчитується загальна кількість символів за зміну, але не більше 60 тисяч символів за зміну;

• для групи В за загальною кількістю символів, прочитаних або реалізованих за робочу зміну, але не більше 40 тисяч символів за зміну

• для групи В за загальним часом безпосередньої роботи з ПК за робочу зміну, але максимум 6 годин за зміну.

4.3 Висновки з розділу

Таким чином, враховуючи основні функції зорового аналізатора, умови зорової роботи можна оцінити за трьома основними показниками: кутовими розмірами, які розрізняють об'єкти, освітленість робочого місця і контрастності об'єкта розпізнавання з фоном. Ці показники є основою гігієнічної регламентації освітлення на робочому місці, викладеної у відповідних офіційних документах (ДБН В.2.5- 28:2018 і галузеві стандарти на природне і штучне освітлення).

Тривалість безперервної роботи з екранами без регламентованої перерви не повинна перевищувати однієї години. Загальний час регламентованих перерв залежить від тривалості роботи, виду і категорії трудової діяльності з використанням ПК.

Під час регульованих перерв доцільно виконувати спеціально розроблені комплекси вправ з метою зниження нервово-емоційної напруги, стомлення зорового аналізатора, усунення впливу гіподинамії і гіпокінезії, попередження розвитку статичного стомлення.

Відповідальність за недотримання вимог законодавства до умов праці несе роботодавець, який покладає ці функції на службу охорони праці організації або на фахівця з охорони праці, що залучається на договірній основі.

ВИСНОВОКИ

В магістерській кваліфікаційній роботі було:

досліджено структуру безпілотника, класифікацію БПЛА та бортове обладнання дрону. Також було розглянуто системи управління безпілотників;

зазначено неохідність виокремлення безпеки основних програм БПЛА та розглянуто основні проблеми конфіденційності, безпеки, які можуть бути порушені порушенням безпеки;

представлено основні вразливі пункти безпеки та загрози, які можна використати, щоб поставити під загрозу безпеку безпілотників.

проаналізовано існуючі рішення безпеки для захисту безпілотних систем, включаючи криптографічні та некриптографічні рішення. Криптографічні рішення по суті спрямовані на захист зв'язку безпілотників та переданих даних, тоді як некриптографічні рішення (IDS) спрямовані на виявлення та відновлення від можливих атак безпеки;

досліджено можливі заходи безпеки безпілотника/БПЛА та протидію/БПЛА, на додаток до методів запобігання, та рішення, пов’язані з безпекою зв’язку та мереж безпілотників/БПЛА, які є важливими для збройних сил та рятувальні роботи;

розроблено рекомендації щодо підвищення безпеки безпілотників/БПЛА з урахуванням обговорення основних загроз безпеці та конфіденційності, атак та відповідних технічних рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Глотов В., Церклевич А. Аналіз і перспективи аерознімання з безпілотного літального апарата // Вісник Національного університету "Львівська політехніка". – Сер.: Сучасні досягнен- ня геодезичної науки та виробництва. – Львів : Вид-во НУ "Львівська політехніка". – 2014. – Вип. I (27). – С. 131-136.

2. Дементьєв Д.О. Бойові Літальні комплекси в складі єдиної інформаційно-розвідувально-навігаційно-ударної системи / Дементьєв Д.О. // Зб. наук. пр. Військового інституту Київського національного університету ім. Тараса Шевченка. – К. : ВІКНУ, 2015. – №27. – С. 74-77.

3. Зинченко, О. Н. Беспилотный летательный апарат: применение в целях эрофотосъемки для картографирования [Електронний ресурс] / О. Н. Зинченко. – Режим доступу: http://www.racurs.ru/?page=681.

4. Кутовий, О.П. Тенденції розвитку безпілотних літальних апаратів / О.П. Кутовий // Наука і озброєння – 2014. – № 4. – С. 39 – 47.

5. Луцький М.Г. Розвиток міжнародного регулювання та нормативної бази використання безпілотних літальних апаратів / М.Г. Луцький, В.П. Харченко, Д.О. Бугайко // Вісник НАУ. – 2015. – № 4. – С. 5-14.

6. Моисеев, В. С. Прикладная теория управления беспилотными летательными аппаратами: монография / В. С. Моисеев. – Казань: ГБУ «Республиканский центр мониторинга качества образования» (Серия «Современная прикладная математика и информатика»), 2013. – С. 768.

7. Ростопчин В.В. Безпілотні авіаційні системи: основні поняття / В.В. Ростопчин, І.Е. Бурдун / ЕЛЕКТРОНІКА: Наука, Технологія, Бізнес. – 2016. – №7. – С. 82-88.

8. Сальник Ю.П. Аналіз технічних характеристик і можливостей безпілотних авіаційних комплексів оперативно-тактичного та тактичного радіуса дії армій розвинених країн / Ю.П. Сальник, І.В. Матала // Військовотехнічний зб. – 2013. – № 7 – С. 70-74.

9. Стратегія розвитку вітчизняної авіаційної промисловості на період до 2020 року: [затверджена розпорядженням Кабінету Міністрів України від 27 грудня 2008р. N 1656-р] [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/1656-2008-%D1%80.

10. Харченко О.В. Класифікація та тенденції створення безпілотних літальних апаратів військового призначення / О.В. Харченко, В.В. Кулєшин, Ю.В. Коцуренко // Наука і оборона. – 2015. – № 6 – С. 47-54

11. В. Фурашев. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки // “Інформація і право”. – № 1(4)/2012.

12. Вопросы техники безопасности, пожарной и взрывной безопасности. Методические указания по дипломному проектированию / Сост.:А. Г. Ревук, Г. М. Франчук. – К.: КИИ ГА, 1997.

13. Гонін С.М. та ін. Безпілотні літаючі апарати / Гонін С.М., Карпенко А.В., Мезов Г.Ф., Ковпачеров В.В. - СПб .: Пітер, 1999.

14. ДЕРЖАВНА АВІАЦІЙНА СЛУЖБА УКРАЇНИ. Тимчасовий порядок використання повітряного простору України. 2018.

15. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011.

16. Інтернет ресурс. https://ru.qaz.wiki/ Безпілотний літальний апарат - Unmanned aerial vehicle Безпілотний літальний апарат.

17. Інтернет ресурс. Nau.edu.ua. БПС М-7 "Небесний патруль".

18. Кописов О.Е. Інерціальні навігаційні системи: лекція. [Електронний ресурс], 2013.

19. Купервассер О.Ю., Рубінштейн А.А. Система навігації безпілотних літальних апаратів за допомогою відео. [Електронний ресурс] // Методолог, 2012. 8 грудня.

20. Лорін А. Безпілотна повітряна розвідка. - М .: Воениздат, 1997.

21. Міжнародна організація громацької авіації. Doc 10019 AN/507. Керівництво по дистанційно пілотованих авіаційним системам (ДПАС). 2015.

22. Монаков А.А. Теоретичні основи радіонавігації: Учеб. посібник / СПбГУАП. СПб., 2002.

23. Мосальов В. Підрозділи безпілотних літаючих апаратів. - М .: Вища. шк., 2000.

24. Національний стандарт України. Охорона праці. Терміни та визначення основних понять. ДСТУ 2293:2014. 2015.

25. О.І. Тимочко, Д.Ю. Голубничий, В.Ф. Третяк, І.В. Рубан. Харківський університет Повітряних Сил ім. Івана Кожедуба, Харків. Класифікація літальних апаратів. 2007.

26. Петров В.Ф., Барунін А.А., Терентьєв А.І. Модель системи автоматичного управління безпілотним літальним апаратом. Известия Тульського державного університету. Технічні науки, 2014. № 12-2.

27. Полинкін А.В. Дослідження характеристик радіоканалу зв'язку з безпілотними літальними апаратами. 2013.

28. Правил охорони праці під час експлуатації електронно-обчислювальних машин (НПАОП 0.00-1.31-99). 1999.

29. Семенова Л.Л. Сучасні методи навігації безпілотних літальних апаратів. 2015. 30. Скляр Б. Цифрова зв'язок. Теоретичні основи і практичне застосування, Изд. 2-е, испр .: Пер. з англ. / Б. Скляр. - М .: Видавничий дім «Вільямс», 2003.

31. СНиП II-4-79 «Естественное и искусственное освещение. Нормы проектирования", ДБН В.2.5-28-2006 «Природне і штучне освітлення».

32. Технічний регламент засобів індивідуального захисту. Затверджено постановою Кабінету Міністрів України від 27 серпня 2008 р. № 761.

33. Фурашев В.М. Ключові аспекти проекту Закону України "Про безпеку інформації" // "Віче". – 2012. – № 6/2012(315).

ДОДАТОК А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

ІХ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.056.53
І.І. Фомін
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИСТ КАНАЛУ УПРАВЛІННЯ БПЛА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

UDC 004.056.53
I.I. Fomin

PROTECTION OF UAV CONTROL CHANNEL FROM UNAUTHORIZED ACCESS

Як правило, основний обов'язок, який покладено на комплекси БПЛА(Безпілотний літальний апарат), – проведення розвідки важкодоступних районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене або ж є небезпечним для здоров'я та навіть життя людей. Крім військового використання застосування комплексів БПЛА відкриває можливість оперативного і недорогого способу обстеження важкодоступних ділянок місцевості, періодичного спостереження заданих районів, цифрового фотографування для використання в геодезичних роботах і у випадках надзвичайних ситуацій. Отримана бортовими засобами моніторингу інформація повинна в режимі реального часу передаватися на пункт управління для обробки і прийняття адекватних рішень.

В наш час найбільшого поширення набули тактичні комплекси мікро і міні-БПЛА. У зв'язку з більшою злітною масою міні-БПЛА за своїм функціональним складом найбільш повно представляє склад бортового обладнання, що відповідає сучасним вимогам до багато-функціонального розвідувального БПЛА.

Спостерігається різке збільшення застосування різних безпілотних авіаційних комплексів у всіх сферах життєдіяльності людини - від торгівлі до військової справи. Безпілотні авіаційні комплекси, як правило, включають в себе оператора (пілот-оператор, пункт управління), безпілотний літальний апарат та канали зв'язку, проте їх захисту від зовнішніх програмно-апаратних впливів, не дивлячись на зростання кількості інцидентів, не приділяється достатньої уваги.

Атаки можуть бути спрямовані на перехоплення управління, виведення з ладу БПЛА, отримання розвідувальної інформації або для подальшої атаки на пілота-оператора і взаємодіючі з ним системи.

Література.

1. Barnard J. Small UAV command-control and communication issues// IEEE on communicating with UAV's. 2007.
2. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. – Режим доступу : //www.official-document/cm76/7642/7642.pdf.