МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ЕЛЕКТРОНІКИ, РОБОТОТЕХНІКИ І ТЕХНОЛОГІЙ
МОНІТОРИНГУ ТА ІНТЕРНЕТУ РЕЧЕЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Шутко В.М.
«____»_____ 2020 р.

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА
ЗІ СПЕЦІАЛЬНОСТІ 171 «ЕЛЕКТРОНІКА»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ЕЛЕКТРОННІ ПРИЛАДИ ТА ПРИСТРОЇ»

Тема: «Забезпечення кіберзахисту лінії управління дистанційно пілотованої авіаційної системи (ДПАС)**»**

Виконавець
студент групи ЕС-208М _Штинь Тарас Анатолійович_____

Керівник
д.т.н., професор _____Іванов Володимир Олександрович_____

Консультант розділу
«Охорона праці» _____ Козлітін О.О.

Консультант розділу
«Охорона навколишнього середовища» _____ Маджд С.М.

Нормоконтролер _____ Сініцин Р.Б.

КИЇВ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Інститут (факультет) __факультет аеронавігації, електроніки та телекомунікації____

Кафедра __кафедра електроніки, робототехніки і технологій моніторингу та інтернетнету речей_____

Напрям (спеціальність) _____171 «Електроніка»_____

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____
«_____» _____ 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи (проекту)
_____Штиня Тараса Анатолійовича_____
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): Забезпечення кіберзахисту лінії управління дистанційно пілотованої авіаційної системи (ДПАС)

затверджена наказом ректора від 02 жовтня 2020 р. № 1900 / ст

2. Термін виконання роботи (проекту): з 05.10.2020 р. по 27.12.2020 р.

3. Вихідні дані до роботи (проекту):

Дистанційно пілотовані авіаційні системи.

Безпілотний літальний апарат.

Кібербезпека.

Кіберзахист.

4. Зміст пояснювальної записки:

Дистанційно пілотуємі повітряні судна.

Архітектура дистанційно пілотованої авіаційної системи (ДПАС).

Види організованої радіопротидії нормальному функціонуванню ДПАС.

Методи захисту ДПАС від кібератак.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:

Структура БПЛА з системою управління, узагальнена схема навігації БПЛА, формування пасивних завад, індивідуальний захист об’єкту, груповий захист об’єктів

6. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Дистанційно пілотовані повітряні судна	05.10 – 16.10	
2.	Архітектура ДПАС	16.10 – 23.10	
3.	Види організованої протидії нормальному функціонуванню ДПАС	23.10 – 06.11	
4.	Методи захисту ДПАС від кібератак	06.11 – 13.11	
5.	Охорона праці	13.11 – 27.11	
6.	Охорона навколишнього середовища	27.11 – 04.12	
7.	Оформлення пояснювальної записки	04.12 – 27.12	

7. Консультанти з окремих розділів

Назва розділу	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
5 Охорона праці	Старший викладач Козлітін Олексій Олександрович		
6 Охорона навколишнього середовища	професор, д.т.н., професор Маджд Світлана Михайлівна		

8. Дата видачі завдання: "_05_" __жовтня__ 2020 р.

Керівник дипломної роботи (проекту) _____ _Іванов В.О.___
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ _Штинь Т.А.___
(підпис здобувача) (П.І.Б.)

Реферат

Пояснювальна записка до дипломної роботи «Забезпечення кіберзахисту лінії управління дистанційно пілотованої авіаційної системи (ДПАС)»: 119 сторінок, 15 рисунків, 3 таблиць, 33 літературних джерела.

Об’єкт дослідження: забезпечення кіберзахищеності безпілотно пілотованих повітряних суден.

Мета роботи: визначити уразливі місця лінії управління дистанційно пілотованої авіаційної системи та способи забезпечення їх кіберзахищеності.

Методи дослідження: визначення уразливих місць, порівняльний аналіз, обробка літературних джерел.

Результати магістерської роботи рекомендується використовувати під час проведення наукових досліджень та в практичній діяльності.

БЕЗПІЛОТНИК, КІБЕРАТАКА, КІБЕРБЕЗПЕКА, ДПАС, ДППС, РАДІОЗВ'ЯЗОК.

ЗМІСТ

ВСТУП	8
1ДИСТАНЦІЙНО ПІЛОТОВАНІ ПОВІТРЯНІ СУДНА	10
1.1 Класифікація дистанційно пілотованих повітряних суден (ДППС)	10
1.2 Процедури впровадження ДППС у загальний повітряний простір	17
1.3 Специфіка аеродромів для ДППС	20
1.4 Вимоги до забезпечення безпеки польотів ДППС у загальному повітряному просторі	26
1.5 Висновки з розділу	30
2 АРХІТЕКТУРА ДИСТАНЦІЙНО ПІЛОТОВАНОЇ АВІАЦІЙНОЇ СИСТЕМИ (ДПАС)	32
2.1 Функціональна електромагнітна павутина	32
2.2 Бортові системи навігації, зв’язку, спостереження і управління ДППС та їх особливості	33
2.2.1 Системи навігації	33
2.2.2 Системи зв’язку	37
2.2.3 Системи спостереження	39
2.2.4 Електронні системи обробки інформації та управління ДППС	40
2.3 Станція зовнішнього пілота	42
2.4 Лінії зв’язку та передавання даних ДПАС	43
2.4.1 Лінія С2	47
2.4. 2 Лінія С3	50
2.5 Висновки з розділу	51
3 ВИДИ ОРГАНІЗОВАНОЇ РАДІОПРОТИДІЇ НОРМАЛЬНОМУ ФУНКЦІОНУВАННЮ ДПАС	54

3.1 Шляхи проникнення сторонніх електромагнітних збурень в радіоканали та структурні елементи ДПАС 54
3.1.1 Види організованих радіозавад 54
3.1.1.1 Неперервні шумові завади 60
3.1.1.2 Завади модуляційного типу 61
3.1.1.3 Імпульсні завади 61
3..2 Загальні аспекти кібербезпеки 63
3.2.1 Кіберпростір 63
3.2.3 Види спуфінгу 64
3.2.4 Алгоритмізація процедури виявлення кібератаки 66
3. 3 Висновки з розділу 69
4 МЕТОДИ ЗАХИСТУ ДПАС ВІД КІБЕРАТАК 71
4.1 Організаційні методи протидії кібератакам 71
4.2 Криптографічні методи захисту 74
4.3 Алгоритмічні методи захисту 79
4.4 Програмні методи захисту 82
4.5 Висновки з розділу 86
5 Охорона праці 88
5.1 Вступ 88
5.2 Аналіз умов праці на робочому місці 89
5.3 Аналіз шкідливих та небезпечних виробничих факторів 92
5.3 Розробка заходів з охорони праці 97
5.4 Пожежна безпека виробничого приміщення 98
5.6 Висновки з розділу 100
6 ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА 101
6.1 Вступ 101
6.2 Аналіз основних джерел впливу та їх наслідків на людину та її оточення 102

6.3 Рекомендації щодо зниження негативних чинників електромагнітного поля 109
6.4 Висновки з розділу 113
ВИСНОВКИ 114
ПЕРЕЛІК ВИКОРИСТАНИ Х ДЖЕРЕЛ 117

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.

Діапазон існуючих і розроблюваних апаратів дуже широкий, від мікро- і міні-дронів до важких багатотонних апаратів, а також БПЛА, здатних виконувати наддалекі і сверхвисотні польоти.

Призначення сучасних безпілотників не обмежується тільки військовою сферою. Стрімко розширюється і сфера їх цивільного застосування в таких галузях, як нафтогазова промисловість, транспорт, будівництво, сільське господарство, зв'язок та ін., що надає додатковий імпульс розвитку безпілотної авіаційної техніки.

На жаль, необхідно констатувати той факт, що на сьогоднішній день розширюється залучення БПЛА і в злочинних цілях. Перекидання наркотиків, комерційне шпигунство, контрабанда - ось далеко не повний список незаконного застосування дронів. Активно використовують безпілотники і терористичні організації.

На зорі своєї появи БПЛА застосовувалися терористами не стільки для розвідки, скільки для зйомки красивих агітаційних відеороликів з висоти пташиного польоту для пропаганди своїх ідей. Пізніше терористи стали задіяти квадрокоптера і інші безпілотники для розвідки і управління на полі бою, як, наприклад, в Іраку і особливо в Сирії.

Поза зон збройних конфліктів особливо небезпечно застосування терористами дронів-камікадзе. Вони несуть, як правило, невелика кількість дрібних вражаючих елементів, які призводять в основному до легким пораненням і контузія. Цим досягається одна з фундаментальних цілей терористів - не тільки викликати людські жертви, а й посіяти страх і паніку серед населення.

1 ДИСТАНЦІЙНО ПІЛОТОВАНІ ПОВІТРЯНІ СУДНА

1.1 Класифікація дистанційно пілотованих повітряних суден (ДППС).

За сучасним визначенням, «безпілотником» є тільки той апарат, який знаходиться під постійним дистанційним контролем пілота або пілотів і призначений для повернення на аеродром і для подальшого повторного використання. Тобто крилата ракета до категорії «безпілотників» не належить .

Раніше радіокеровані та повністю автоматизовані апарати об'єднували поняттям безпілотна авіація — літаки, керування (пілотування) якими здійснюється без пілота, за допомогою приладів різних систем, що засобами радіо (радіолокації, телебачення) подають команди на автопілот. Елементи системи керування містяться поза літаком і можуть бути на землі, на воді і в повітрі, на місці старту, на маршруті польоту і в районі цілі. Для передачі на пункт управління даних, отриманих з бортових сенсорів, у складі БПЛА є радіопередавач, що забезпечує зв'язок з наземним обладнанням. Залежно від формату зображень та їхнього стискання, регламентованих, наприклад, в STANAG 4609, швидкість передавання цифрових радіоканалів зв'язку з БПЛА, може становити одиниці-сотні Мбіт/с. Перед передаванням з борту БПЛА отриманих зображень високої чіткості, їх піддають сегментації.

Залежно від принципів керування, розрізняють такі різновиди безпілотних літальних систем:

- безпілотні некеровані;
- безпілотні автоматичні;
- безпілотні дистанційно-пілотовані літальні апарати (ДПЛА).

У авіації після 2000 року йде стрімке розширення саме останнього типу апаратів, й про них йдеться, коли вживають термін «безпілотник», «дрон» (англ. drone), або абревіатуру UAV. Тобто, під терміном «безпілотник», «БПЛА», «UAV» мається на увазі саме повітряне судно, яким через канали зв'язку керує один або декілька пілотів. Екіпаж БПЛА може також включати командира, оператора сенсорів, оператора

вогневих засобів. Екіпажі БПЛА під час довготермінових місій змінюються — як на приклад, кожні 4 години.

Безпілотні (англ. unmanned — без людини на борту) літальні апарати, відповідно до стандартів НАТО, так само, як і літаки із пілотом на борту (англ. manned aircraft), керуючись значенням повної злітної маси розділено на 3 класи:

I — повна злітна маса до 150 кг.;

II — повна злітна маса до 600 кг.;

III — повна злітна маса більше 600 кг.;

Клас I підрозділяється на категорії: «мікро» — до 2 кг, «міні» — до 15 кг, «малі» — від 15 кг..

Від наведеної вище класифікації НАТО дещо відрізняється класифікація безпілотних авіаційних систем (UAS), що її застосовано у документі Департаменту оборони США (DOD-USRM-2013 2013, p. 6). Згідно цього документу, виділяють п'ять груп UAS:

Група 1 (мікро-, міні тактичні) — від 0 до 9 кг, до 300 метрів над ґрунтом, основний представник — «RQ-11 Raven».

Група 2 (малі тактичні) — від 9.5 до 25 кг; до 1000 метрів над ґрунтом, представник — «Scan Eagle»

Група 3 (тактичні) — менш, ніж 600 кг, представник — «RQ-7 Shadow»

Група 4 (персистентні) — більш, ніж 600 кг; представник — «MQ-1B Predator»

Група 5 (пенетрувальні) — більш, ніж 600 кг; представник — «MQ-9 Reaper»

Рис. 1.1. Наземний пункт керування безпілотним літальним апаратом. Екіпаж виконує бойовий (спостережний) політ над територією. Ліворуч — пілот, праворуч — оператор сенсорів

БПЛА повсюдно застосовуються у військовій справі, в першу чергу для ведення повітряної розвідки — як тактичної, так і стратегічної. Безпілотники під-класів «міні-» та «мікро-» все ширше застосовуються під час бойових дій на рівні взводу та відділення для термінового отримання інформації типу «що за тим пагорбом», тобто для вирішення завдань військової розвідки. Далекосяжним напрямком їх застосування є вирішення завдань у складі рою. Також використовуються БПЛА для коригування вогневих ударів по наземних цілях та як ударні.

Крім того, невійськові дрони застосовуються для розв'язання широкого кола завдань, виконання яких пілотованими літальними апаратами з різних причин недоцільно. Такими завданнями є:

- моніторинг повітряного простору, земної й водної поверхонь,
- екологічний контроль,
- керування повітряним рухом,

- контроль морського судноплавства,

- розвиток систем зв'язку,

- польова логістика (трансфер запчастин, акумуляторних батарей, боєприпасів, медикаментів тощо),

- художня фотографія.

За своїм загальним призначенням літальні апарати в БАС поділяться на види, надані на рис. 1.2.

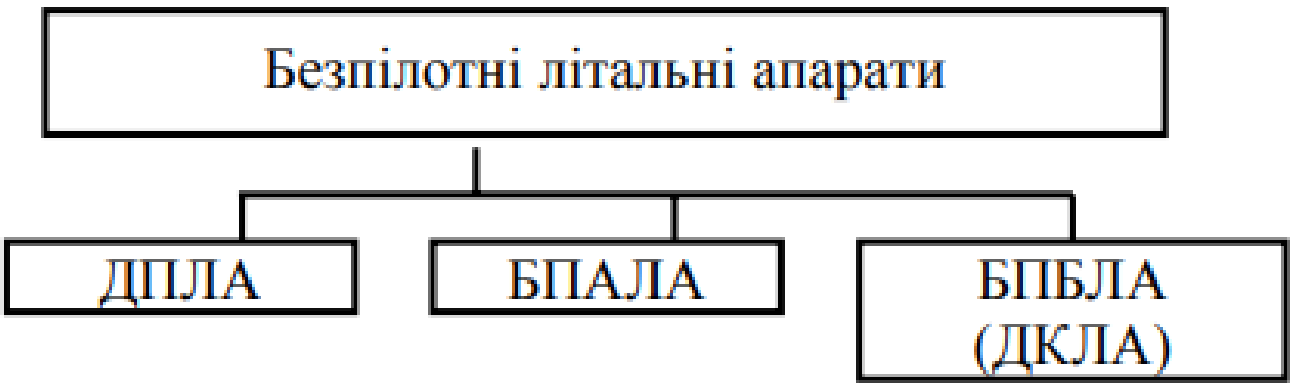


Рис. 1.2 Класифікації БПЛА за призначенням

Безпілотний літальний аппарат – багаторазово реалізовує своє функціональне призначення без безпосереднього розміщення людини на борту з метою управління. Загальноприйняте поняття має досить широкий сенс і не завжди точно відображає специфіку літального апарата. Таким чином, у даний клас не включаються безпілотні модифікації серійних літаків, використовувані як повітряні мішені, а також всі види балістичних і крилатих ракет.

Дистанційно пілотований літальний апарат (ДПЛА) – безпілотний літальний апарат з безперервним управлінням, яке здійснюється тим або іншим способом з нерухомого або рухомого пункту управління.

Безпілотний автоматичний літальний апарат (БПАЛА) – безпілотний літальний апарат, що реалізовує своє функціональне призначення в автоматичному режимі відповідно до закладених у нього алгоритмів і програм функціонування (крилаті ракети, літаки-розвідники і т.д.).

Останнім часом у провідних авіаційних державах ведуться інтенсивні роботи над створенням БАС, призначених для заміни бойових пілотованих літальних апаратів. За кордоном їх називають безпілотними бойовими літальними апаратами (БПБЛА).

Проте, виходячи із способу інформаційної взаємодії літального апарата з оператором управління, їх доцільно називати дистанційно керованими літальними апаратами (ДКЛА). ДКЛА – безпілотні літальні апарати, що реалізовують своє функціональне призначення в основному автономно, при епізодичному втручанні оператора управління для перенацілювання або перепрограмування системи управління літальним апаратом.

Наявність розвиненого штучного інтелекту у ДКЛА, яке забезпечує не тільки політ, але і процес ухвалення самостійного рішення на застосування бортової зброї, переводить їх не в наступне покоління БАС, а в окрему групу дистанційно керованих авіаційних систем.

Дистанційно керована авіаційна система – перспективний дистанційно керований літальний апарат, властивості і можливості якого з найбільшим наближенням відповідають пілотованому літального апарату аналогічного призначення. Такий літальний апарат управляється з пункту управління (наземного або повітряного, стаціонарного або мобільного) у дискретно-імпульсному режимі і виконує задану бойову задачу відповідно до власних алгоритмів функціонування, інформаційних та силових дій навколишнього середовища і команда зовнішнього управління (від пункту управління).

Сучасні функціональні методи класифікації, використовувані зарубіжними військовими аналітиками, грунтуються на первинній різниці між бойовими безпілотними літальними апаратами і БЛА забезпечення (рис. 3).

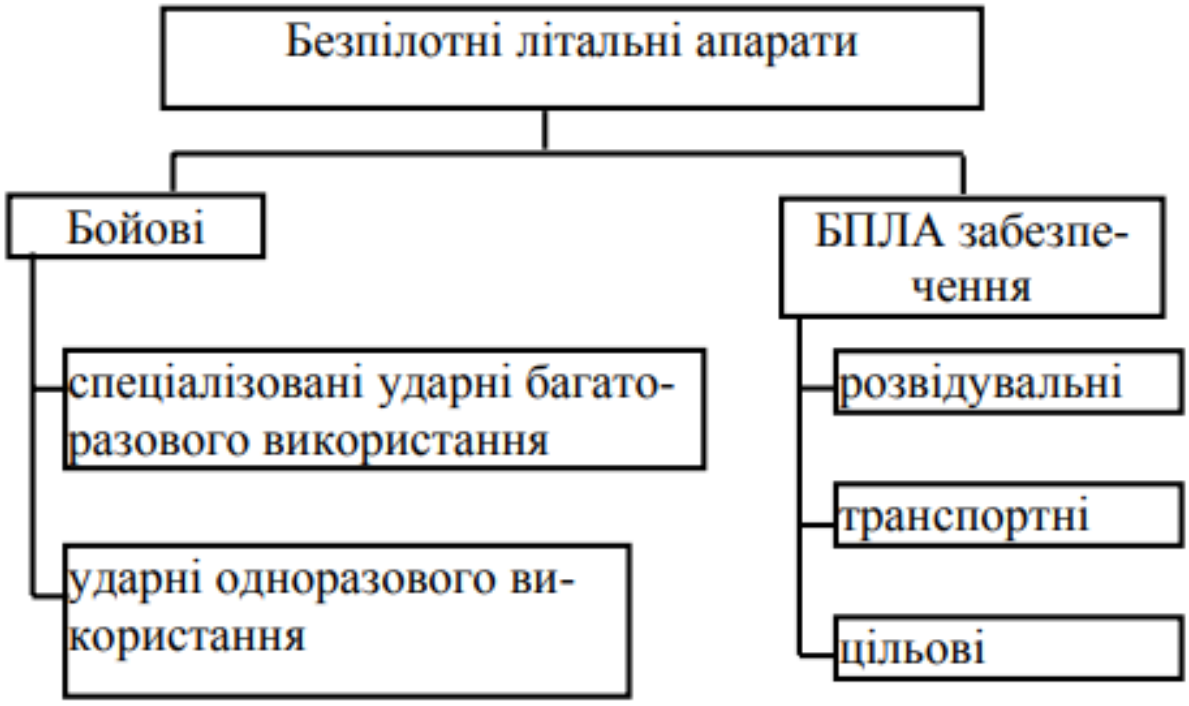


Рис. 1.3. Функціональна класифікація БПЛА

Бойові БПЛА включають спеціалізовані ударні БПЛА багаторазового застосування й ударні апарати одноразового застосування.

Найбільша увага при розробці бойових ударних БПЛА приділяється спеціалізованим ударним апаратам багаторазового застосування, які за своїми тактико-технічними характеристиками наближаються до сучасних тактичних винищувачів. У початковому періоді будь-якого регіонального конфлікту, коли система ППО супротивника ще боєздатна, ефективну роль у її придушенні (особливо в знищенні радіолокаційних станцій і пунктів управління) можуть зіграти ударні БПЛА UCAV (Unmanned Combat Vehicle). Такі апарати входитимуть до складу першого ешелону повітряного удару і застосовуватимуться перед крилатими ракетами (КР) та бойовими літаками.

Рис. 1.4. М-7 Небесный патруль

Проблема підвищення надійності польотів БПЛА впритул торкається основи його компонування. Потрібно нагадати, що два двигуни з цієї точки зору, завжди краще, ніж один. У зв'язку з цим, у 2005 році керівництву НАУ був запропонований проект "Небесний патруль", який мав на меті отримання двомоторного маршрутного БПЛА зі стартовою масою близько 100 кг. Серед компонувальних схем розглядалися найрізноманітніші, в тому числі і "тандемна", як у "Хантера". Однак вибір був зроблений на користь несподіваною - тандемной, асиметричною.

На думку розробників, вона повинна була дозволити отримати низький рівень впливу передньої силової установки на цільове навантаження, розміщується, як правило, в гондолі. Літальний апарат отримав назву М-7 "Небесний патруль" (пат. України No. 33977). Його створенням в НАУ займалися протягом 2006-2007 рр. Компенсація шкідливих моментів від розміщення двигунів виконується відповідним "викошування" останніх. БПЛА неодноразово демонструвався на авіасалонах в 2008-2010 рр. На ньому були відпрацьовані технологія отримання композитних вклейок, деякі способи і прийоми отримання технологічних роз'ємів і багато іншого. Перший зліт прототипу здійснений в 2008 році.

В основі проекту лежить завдання поліпшення умов роботи бортового наглядової обладнання БПЛА з метою збільшення меж огляду передньої півсфери і зменшення вібрацій на зазначене обладнання.

М-7Д Небесний патруль є двомоторний безпілотним ВС нормальної схеми з високо розташованим крилом. БПЛА виготовлений переважно з композитних матеріалів з частковим застосуванням деревини та металу. Для доступу в відсік корисного навантаження передня верхня і задня частини гондоли виконані у вигляді знімних обтекателей. Стандартне цільове навантаження - гіростабілізований денна CCD - камера.

В основі проекту лежить завдання збільшення маси корисного (цільової) навантаження двомоторного БПЛА і отримання високих злітно-посадочних характеристик.

М-7В5 Небесний патруль є літальним апаратом нормальної схеми з високо розташованим крилом, яке закріплене на одному пілоні. Планер виготовлений з композитних матеріалів. Крило з середньою / високим ступенем механізації у вигляді висувних однощілинні закрилків і однощілинні флаперонов.

Безпілотна авіаційна система (БАС) складається з 1 (одного) БПЛА М-7В5 Небесний патруль, яке знаходиться на причепі-контейнері в транспортному положенні. Умови базування БАС: на всіх видах ВПС, включно з необладнаних. Транспортується причіп за допомогою тягача (а / м "УАЗ", "Газель").

БПЛА розрахований на польоти з перевантаженнями до 4 одиниць в маршрутну відстань близько 1500 км. В залежності від варіанту цільової навантаження (20-70 кг) зазначено відстань може змінюватися в межах 1200-2700 км при тривалості польоту 7-15 год.

1.2 Процедури впровадження ДППС у загальний повітряний простір

Польоти безпілотних ПС організовуються та здійснюються згідно з вимогами нормативно-правових актів України у галузі цивільної та державної авіації відповідно з дотриманням правил польотів у повітряному просторі України та цього Тимчасового

порядку. Відповідальність за організацію таких польотів несуть користувачі повітряного простору (керівники авіапідприємств, організацій або власники ПС тощо), що планують або проваджують зазначену діяльність.

Польоти ДППС масою до 2 кг включно виконуються без подання заявок на ВПП, без отримання дозволів на ВПП, без інформування органів управління Повітряних Сил ЗС України та органів ОЦВС, органів Державної прикордонної служби України, органів ОПР та відомчих органів УПР, за умови дотримання наступних вимог:

1) польоти виконуються тільки вдень;

2) польоти виконуються без перетину державного кордону;

3) польоти виконуються поза межами встановлених заборон та обмежень ЗПС, крім випадків, установлених Положенням про ЗПС;

4) польоти виконуються не ближче 5 км від зовнішніх меж злітно-посадкових смуг та руліжних доріжок аеродромів/вертодромів, або не ближче 3 км від зовнішніх меж злітно-посадкової смуги ЗПМ, крім випадків узгодження з експлуатантом ЗПМ;

5) польоти виконуються не ближче 500 м від ПС, які знаходяться в повітрі;

6) польоти не виконуються над:

- дорогами державного значення (міжнародні, національні, регіональні, територіальні);

- центральними вулицями міст, селищ міського типу та сіл;

- залізними дорогами державного та регіонального значення;

- над та вздовж ліній електропередачі, продуктопроводів, крім випадків виконання польотів за узгодженням з власником об'єкту;

- промисловими зонами, електростанціями, залізничними станціями, морськими портами, сховищами пального, нафти, газу, інших небезпечних речовин та рідин тощо, крім випадків виконання польотів за узгодженням з власником об'єкту;

- місцями (районами) аварій та катастроф (крім задіяних в ліквідації їх наслідків та пошуково-рятувальних роботах);

- установами виконання покарань та слідчими ізоляторами, крім випадків виконання польотів в інтересах адміністрацій зазначених установ та ізоляторів;

- іншими важливими державними та потенційно небезпечними об'єктами, крім випадків виконання польотів за дозволом повноважних органів;

- об'єктами, які визначені Міністерством оборони України, Міністерством внутрішніх справ України, Державною прикордонною службою України, Службою безпеки України, Національною поліцією України, Національною гвардією України, Управлінням державної охорони, іншими військовими формуваннями та правоохоронними структурами, утвореними відповідно до законів України, та відносно яких здійснюється охорона, крім випадків виконання польотів за дозволом зазначених вище органів;

7) польоти не виконуються у:

- зонах поліцейських/антитерористичних/спеціальних операцій (крім задіяних в цих операціях);

- зонах, визначених для забезпечення безпеки осіб, відносно яких здійснюється державна охорона;

8) польоти виконуються в межах прямої видимості (VLOS), але не далі ніж 500 м від зовнішнього пілота;

9) максимальна висота польоту не вище 50 м над рівнем земної (водної) поверхні та тільки за умов візуальної видимості ДППС зовнішнім пілотом;

10) швидкість польоту ДППС складає не більше 160 км/год;

11) зовнішній пілот не здійснює керування ДППС з ПС або з іншого транспортного засобу, які рухаються;

12) зовнішній пілот керує польотом тільки одного ДППС;

13) польоти виконуються:

- не ближче 30 м від іншої особи, яка не пов'язана із виконанням цих польотів;

не ближче 50 м від груп людей до 12 осіб, які знаходяться поза межами приміщень, тварин, транспортних засобів, кораблів, човнів, об'єктів приватної власності;

- не ближче 150 м від груп людей кількістю більше 12 осіб, які знаходяться поза межами приміщень, та від районів забудов багатоповерховими житловими будинками, а також над зазначеними групами та районами.

В інших випадках польоти ДППС масою до 2 кг включно та усі без винятку польоти ДППС масою більше 2 кг виконуються у межах заборон/обмежень ВПП з дотриманням вимог щодо подання заявок на ВПП, отримання дозволів та умов ВПП, інформування органів управління Повітряних Сил ЗС України, органів Державної прикордонної служби України, органів ОЦВС, органів ОПР/УПР.

1.3 Специфіка аеродромів для ДППС

12 квітня 2005 року під час першого засідання 169-ї сесії Комісія з повітряного навігації попросила Генерального секретаря проконсультуватися з вибраними державами та міжнародними організаціями щодо: наявної та передбаченої діяльності міжнародних цивільних безпілотних літальних апаратів (БПЛА) у цивільному повітряному просторі; процедури усунення небезпеки для цивільних літальних апаратів, що створюються БПЛА, що експлуатуються як державні літальні апарати; та процедури, які можуть існувати для видачі спеціальних дозволів на експлуатацію для міжнародних цивільних операцій БПЛА.

Перша неформальна зустріч ІКАО з питань БПЛА.

Після вищезазначеного, перша дослідницька нарада ІКАО щодо БПЛА відбулася в Монреалі 23 і 24 травня 2006 р. Її метою було визначити потенційну роль ІКАО у роботі з розробки нормативів БЛА. Зустріч домовилася, що, хоча з часом буде широкий спектр технічних та технічних характеристик та стандартів, лише частина з них повинна стати САРП ІКАО. Також було визначено, що ІКАО не є найбільш підходящим органом для керівництва зусиллями з розробки таких специфікацій. Однак було домовлено, що в цьому є потреба гармонізація термінів, стратегій та принципів щодо нормативної бази та що ІКАО має виступати в ролі координатора.

Друга неформальна нарада ІКАО щодо БПЛА.

У другій неофіційній нараді ІКАО (Палм-Кост, штат Флорида, січень 2007 р.) Було зроблено висновок про те, що робота над технічними характеристиками операцій безпілотника ведеться як в межах RTCA, так і в EUROCAE і адекватно координується через спільний комітет їх двох робочих груп. Отже, головне питання ІКАО було пов'язане з необхідністю забезпечення безпеки та однаковості в міжнародних операціях цивільної авіації. У цьому контексті було вирішено, що на цьому ранній стадії немає особливої потреби в нових SARPS ІКАО. Однак виникла необхідність узгодження понять, понять та термінів. Учасники зустрічі домовились, що ІКАО має координувати розробку стратегічного керівного документа, який би керував еволюцією регуляторних органів. Навіть незважаючи на обов'язковість, керівний документ буде використаний як основа для розроблення нормативно-правових актів різними державами та організаціями. Оскільки нормативні матеріали, розроблені державами та організаціями, набули зрілості, такий матеріал може бути запропонований для включення до керівного документа ІКАО. Потім цей документ послужить основою для досягнення консенсусу при подальшій розробці SARP.

На засіданні було вирішено відчути, що можливий розвиток SARP повинен здійснюватися добре узгоджено. Оскільки це нова технологія, що з'явилася, було відчутно, що існує унікальна можливість забезпечити гармонізацію та однаковість на ранній стадії, і що всі зусилля ІКАО повинні базуватися на стратегічному підході та підтримувати роботу інших регуляторних органів. Нарада також запропонувала з цього моменту цю тему називати безпілотними літаковими системами (UAS), відповідно до RTCA та EUROCAE угод.

Нарешті, було зроблено висновок, що ІКАО має слугувати центром глобальної взаємодії та гармонізації, розробляти регуляторну концепцію, координувати розробку SARP UAS, сприяти розробці технічних специфікацій іншими органами та визначати зв'язок вимоги до діяльності UAS.

Стаття 8 Конвенції про міжнародну цивільну авіацію, підписаної в Чикаго 7 грудня 1944 року та доповнена Асамблеєю ІКАО (Doc 7300) (далі - Чиказька конвенція), передбачає, що:

Жодне повітряне судно, яке може пролетіти без пілота, не може проходити без пілота над територією Договірної Держави без спеціального дозволу цієї Держави та відповідно до умов такого дозволу.

Глобальна оперативна концепція управління повітряним рухом (Doc 9854) зазначає, що "Безпілотний літальний апарат - це безпілотний літак, у значенні статті 8 Конвенції про міжнародну цивільну авіацію, який пролітає без бортового пілота. або управляється дистанційно і повністю з іншого місця (наземного, іншого літального апарату, космосу), або запрограмований і повністю автономний ". Це розуміння БПЛА було схвалено на 35-й сесії Асамблеї ІКАО.

Нормативно-правова база, яка розробляється ІКАО, формується в контексті вищезазначеного твердження. Усі UA, незалежно від того, чи є віддаленими, повністю автономними, чи їх комбінація, підпадають під дію положень статті 8. Тільки літаки з дистанційним пілотуванням (RPA), однак, зможуть інтегруватися в міжнародну систему цивільної авіації у передбачуваному режимі. майбутнє Функції та обов'язки віддаленого пілота мають важливе значення для безпечної та передбачуваної експлуатації літального апарату, оскільки він взаємодіє з іншими цивільними літальними апаратами та системою управління повітряним рухом (ATM).

Повністю автономні експлуатації літальних апаратів не розглядаються в рамках цих зусиль, а також безпілотні вільні кулі, а також інші види літальних апаратів, якими не можна керувати в режимі реального часу під час польоту.

Інтеграція віддаленого пілотування UA в несегрегований повітряний простір та на аеродромах може бути досягнута в середньостроковій перспективі. Передумова, що стоїть за нормативно-правовою базою та засобами, за допомогою яких держави-договірники зможуть надати спеціальні дозволи, полягає в тому, що ці АСУ відповідатимуть визначеним мінімальним вимогам безпечно працювати поряд з

пілотованими літальними апаратами. Пілот, що знаходиться віддалено, з основними обов'язками командира є найважливішим елементом для досягнення цього статусу. Не виключено, що держави зможуть розміщувати UA, які не дистанційно пілотуються за допомогою спеціальних положень або у відокремленому повітряному просторі; однак це житло не рівноцінне інтеграції.

Інтеграція ДППС в операції, що виконуються на аеродромах, обумовлює необхідність ідентифікації зовнішнім пілотом в реальному масштабі часу схеми аеродрому і відповідного обладнання, такого як світлотехнічне обладнання, і маркування, що забезпечує можливість безпечного і правильного виконання повітряним судном маневрів незалежно від місця розташування ПДП. Для реалізації цієї мети потрібні передові технології і процедури, наприклад в області спостереження та виявлення, і інші, зовнішні або внутрішні по відношенню до ДППС системи або методи, здатні забезпечити достатній ступінь поінформованості і дозвіл конфліктних ситуацій, для того, щоб зовнішній пілот міг безпечно керувати ДППС, не викликаючи при цьому необґрунтованого порушення руху інших транспортних засобів.

Додаток 14 І ЗАСТОСУВАННЯ аеродромного СПЕЦИФІКАЦІЙ До ДППС.

У Додатку 14 "Аеродроми" містяться специфікації для аеродромів та вимоги, згідно з якими держави повинні проводити сертифікацію аеродромів, використовуваних для виконання міжнародних польотів, відповідно до наявних в Додатку специфікаціями та іншими положеннями, використовуючи для цього встановлені нормативні рамки. Згідно з положеннями Додатка 14 нормативна основа держав повинна передбачати розробку критеріїв і процедур сертифікації, а державам також рекомендується проводити сертифікацію загальнодоступних аеродромів.

Державам потрібно визначити, чи є можливість безпечної інтеграції ДПВС без створення нових видів небезпеки повітряним судам з пілотом на борту або покладання на них нового тягаря. Їм також необхідно провести оцінку прийнятності застосування аеродромних специфікацій до операцій, що виконуються ДППС.

ПИТАННЯ ІНТЕГРАЦІЇ В ОПЕРАЦІЇ, ВИКОНУВАНІ на аеродромі До числа специфічних характеристик ДППС, які можуть вплинути на операції, що виконуються на аеродромах, і які повинні враховуватися державами, експлуатантами аеродромів та виробниками, відносяться:

a) здатність ДППС розпізнавати аеродромні знаки і маркування;

b) здатність ДППС попереджати зіткнення при виконанні маневру;

c) здатність ДППС виконувати вказівки органів УВС в повітрі або на площі маневрування (наприклад, "йдіть за зеленою Сессну 172" або "перетинайте за Ер Франс A320");

d) придатність мінімумів заходу на посадку за приладами до польотів ДППС;

e) необхідність присутності спостерігачів ДППС на аеродромах для надання допомоги зовнішньому пілоту у виконанні вимог, що стосуються попередження зіткнень;

f) наслідки для вимог до сертифікації аеродромів, використовуваних ДППС;

g) інфраструктура, така як засобу забезпечення заходу на посадку, транспортні засоби для наземного обслуговування, засоби забезпечення посадки, засоби для запуску / повернення;

h) вимоги до пошуково-рятувальних і протипожежних служб для ДППС;

i) спільне виконання операцій ДППС і повітряних суден з пілотом на борту в околицях і на робочої площі аеродрому;

j) наслідки використання специфічного обладнання ДППС на аеродромах.

Експлуатаційні УМОВИ на контрольованій аеродрому.

Для інтеграції ДППС в умови аеродромів, на яких надаються служби УПС, що забезпечують безпечне, впорядковане й реальне перевезення повітряних суден і транспортних засобів, ДППС повинні мати можливість здійснювати зв'язок і виконувати маневри аналогічно повітряним судам з пілотом на борту.

Зовнішні пілоти, які використовують контрольовані аеродроми, повинні підтримувати двосторонній зв'язок з органами УПС, підтверджувати отримання вказівок

органів УПС і забезпечувати їх дотримання в повітрі і на землі. Зовнішні пілоти повинні мати можливість виконувати всі вказівки на всіх етапах операцій, пов'язаних з діяльністю аеродромів, наприклад при виконанні зльоту, заходу на посадку і посадки і маневруванні на перонах, РД і ЗПС.

ДППС повинні мати можливість виконувати розпорядження аеродромної маркування, світлових покажчиків і сигналів і, при необхідності, вживати відповідних заходів щодо забезпечення безпеки польотів у зв'язку зі зміною умов на поверхні аеродрому. Будуть потрібні системи попередження зіткнень з людьми, повітряними судами, транспортними засобами, будівлями або перешкодами на спеціально виділених робочих площах або в безпосередній близькості від них, а також для попередження входу в заборонені зони і зони, не призначені для повітряних суден.

Аеродромної служби ПОЛЬОТНОЇ ІНФОРМАЦІЇ (AFIS).

Для інтеграції в AFIS неконтрольованих аеродромів, використовуваних для виконання міжнародних польотів повітряними суднами авіації загального призначення, повинна забезпечуватися можливість експлуатації ДППС таким же чином, як повітряних суден з пілотом на борту. Зовнішні пілоти повинні бути в змозі своєчасно та ефективно здійснювати зв'язок з співробітником AFIS для передачі і отримання пов'язаної з безпекою польотів інформації про повітряний рух. Пред'являються до зовнішніх пілотам вимоги, що стосуються розпізнавання і дотримання приписів аеропортової маркування і покажчиків і безпечного і ефективного маневрування серед інших повітряних суден і користувачів аеропорту, будуть аналогічні вимогам, що застосовуються на контрольованих аеродромах. Додаткова інформація щодо AFIS аеродромів міститься в циркулярі "Аеродромна служба польотної інформації (AFIS)" (Cir 211).

Аеродроми, призначені тільки для ДППС.

Держави можуть прийняти рішення про створення аеродромів, призначених тільки для виробництва польотів ДПАС.

План заходів на випадок аварійної обстановки на аеродромі.

На аеродромах повинні складатися плани заходів на випадок аварійної обстановки, відповідні масштабам операцій, що виконуються повітряними судами, і інших видів діяльності на аеродромі. Цей план повинен передбачати координацію яких необхідно вжити дій на випадок аварійної обстановки на аеродромі і в безпосередній близькості від нього.

Система управління безпекою польотів експлуатанта аеродрому.

Може виникнути потреба у внесенні змін до системи управління безпекою польотів експлуатантів аеродромів для включення в них додаткових вимог, обумовлених експлуатацією ДПАС на аеродромі.

1.4 Вимоги до забезпечення безпеки польотів ДППС у загальному повітряному просторі

У цій главі міститься інформація про функції та обов'язки державних авіаційних організацій та постачальників обслуговування в сфері забезпечення безпеки польотів, передбачених системою контролю за забезпеченням безпеки польотів ДПАС. До числа охоплених областей відносяться: державна програма з безпеки польотів, контроль за реалізацією СУБП постачальників обслуговування і повноваження експлуатантів ДПАС, зокрема повноваження постачальників, що надають обслуговування за контрактом та здійснюють свою діяльність з управління ризиками для безпеки польотів в рамках СУБП експлуатанта ДПАС.

Ці обов'язки безпосередньо пов'язані з положеннями Додатка 19 "Управління безпекою польотів" і інструктивних матеріалів, що містяться в Керівництві з управління безпекою польотів (Рубп) (Doc 9859).

Одна з цілей Програми 19 і відповідного інструктивного матеріалу до нього полягає в гармонізації впровадження практики управління безпекою польотів державами і міжнародними організаціями, які беруть участь в авіаційній діяльності. У зв'язку з цим SARPS Додатки 19 покликані надати допомогу державам в управлінні факторами ризику для безпеки польотів.

Державна програма з безпеки польотів.

Державна програма з безпеки польотів являє собою систему управління, мета якої полягає в регулюванні і адміністративному забезпеченні державою діяльності в області безпеки польотів. Згідно з положеннями Додатка 19 кожна держава приймає ГосПБП з метою досягнення прийнятного рівня ефективності забезпечення безпеки польотів цивільної авіації.

ГосПБП і реалізовані постачальником обслуговування СУБП забезпечують можливість ефективної ідентифікації зафіксованих при виробництві польотів ДПАС системних недоліків і вирішувати питання, що викликають стурбованість в області безпеки польотів.

Положення, що стосуються збору та аналізу даних і обміну ними, обумовлюють необхідність того, щоб система добровільного подання даних про інциденти не носила наказательной характеру і передбачала захист джерел інформації. Кожному державі необхідно створити систему обов'язкового і добровільного уявленнях даних про інциденти, сприяти використанню цих систем представлення даних і заохочувати їх шляхом внесення, у міру необхідності, змін до застосованих законодавство, правила і політику. Експлуатантам ДПАС, зовнішнім пілотам і інші заінтересовані сторони повинні повідомляти про недоліки в області безпеки польотів, використовуючи ці системи.

ЭКСПЛУАТАНТ ДПАС.

Експлуатантом ДПАС є особа, організація або підприємство, що займається експлуатацією ДПАС або пропонує свої послуги в цій галузі.

Незалежно від типів польотів (наприклад, аматорський, корпоративний, комерційний), все експлуатанти ДПАС підлягають сертифікації державою. Передбачається, що одна з вимог, що пред'являються до сертифікації, буде полягати в наявності у експлуатанта ДПАС ефективної СУБП.

Кожна держава в рамках своєї ДПБП вимагає впровадження СУБП постачальником обслуговування, що знаходяться під його контролем. Згідно з

положеннями Додатка 19 експлуатанти повітряних суден є постачальниками обслуговування, тому вони повинні впроваджувати СУБП. Це положення в рівній мірі відноситься до експлуатантам ДПАС.

При впровадженні СУБП необхідно враховувати потенційні наслідки для ефективності забезпечення безпеки польотів, обумовлені взаємним впливом внутрішніх і зовнішніх суб'єктів авіаційної системи. Важливо провести оцінку ризику, пов'язаного з польотами, виконуваними ДПАС, особливо потенційного впливу на інших постачальників обслуговування. Інтеграція ДПВС в несегрегірованное повітряний простір вимагає проведення ретельної оцінки ефективності забезпечення безпеки польотів ДПАС. У зв'язку з цим СУБП експлуатанта ДПАС повинна:

a) створюватися відповідно до елементів концептуальних рамок СУБП, передбаченими додаванням 2 Додатка 19;

b) відповідати масштабам діяльності постачальника обслуговування та складності наданих їм авіаційних продуктів і послуг.

СФЕРА ВІДПОВІДАЛЬНОСТІ ТА ОБОВ'ЯЗКИ В ОБЛАСТІ БЕЗПЕКИ ПОЛЬОТІВ.

У документації по СУБП експлуатанта ДПАС повинні бути чітко обумовлені сфера відповідальності, обов'язки і повноваження всіх відповідних керівників старшої ланки. Обов'язкові функції щодо забезпечення безпеки польотів, що виконуються технічним персоналом, які беруть участь в розробці і впровадженні СУБП експлуатанта, можуть бути відображені в наявних посадових інструкціях, методиках і процедурах. Масштаби, структура і складність діяльності організацій можуть відрізнятися, але функції забезпечення безпеки польотів повинні зберігатися.

Експлуатант ДПАС несе відповідальність за ефективність забезпечення безпеки польотів при наданні продуктів і послуг підрядниками, яким не потрібно окреме узгодження або сертифікат відповідності вимогам безпеки польотів, включаючи надання постачальником обслуговування продуктів і послуг через всесвітню мережу незалежних партнерів-дистриб'юторів і третіми сторонами, що базуються в різних місцях

(наприклад, Инмарсат, CITA, ARINC). В цьому випадку експлуатант ДПАС в рамках своєї СУБП повинен гарантувати ефективність забезпечення безпеки польотів підрядними організаціями, що надають обслуговування .

На відміну від цього, якщо підрядник сертифікований або схвалений державним органом цивільної авіації, оператору RPAS не потрібно включати безпеку наданих послуг або продуктів до своїх SMS. Незважаючи на те, що від усіх підрядників, можливо, не потрібно вимагати отримання SMS-повідомлення, однак оператор RPAS повинен нести свої вимоги щодо забезпечення безпеки.

Виявлення ризику і управління ризиком для безпеки польотів при виробництві польотів ДПАС.

У сфері авіаційної діяльності існують чинники небезпеки. Крім того, в процес виробництва польотів вони можуть бути введені ненавмисно в результаті внесення змін до авіаційну систему. Для виявлення факторів небезпеки, оцінки відповідних ризиків і розробки пом'якшувальних заходів в контексті продуктів і послуг, пов'язаних з ДПАС, необхідно мати задіяну ефективну систему подання інформації. Питання про розробку процедур подання інформації про безпеку польотів і їх затвердження повинен розглядатися в рамках політики експлуатанта ДПАС в області безпеки польотів з урахуванням масштабів, структури і складності виконуваних операцій.

Координація планування заходів на випадок аварійної обстановки.

Сферу застосування здійснюваного експлуатантами ДПАС планування заходів на випадок аварійної обстановки можна поширити на інших постачальників обслуговування, яких торкається пов'язаними з безпекою польотів подіями, викликаними ДПАС або їх експлуатацією. У зв'язку з цим експлуатанту ДПАС слід забезпечити узгодження плану заходів на випадок аварійної обстановки з аналогічними планами тих організацій, з якими він буде взаємодіяти.

1.5 Висновки з розділу

Безпілотний літальний апарат — літальний апарат, який літає та сідає без фізичної присутності пілота на його борту.

Безпілотне повітряне судно — повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким, здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном.

Безпілотне повітряне судно (безпілотний літальний апарат) — повітряне судно, керування польотом якого і контроль за яким здійснюються дистанційно за допомогою пункту дистанційного пілотування, розташованого поза повітряним судном, або повітряне судно, що здійснює політ автономно за відповідною програмою.

Безпілотний авіаційний комплекс (безпілотна авіаційна система) — безпілотне повітряне судно, пов'язані з ним пункти дистанційного пілотування (станції наземного керування), необхідні лінії керування і контролю та інші елементи, вказані в затвердженому проєкті типу цього комплексу. Цей комплекс може охоплювати декілька безпілотних літальних апаратів.

У наш час багато країн виділяють з бюджету чималі гроші на вдосконалення і розробку нових зразків БПЛА - безпілотних літальних апаратів. На театрі військових дій не рідкістю стали випадки, коли при вирішенні бойової або навчальної завдання командування віддавало перевагу цифровій машині, ніж льотчику. І на це була низка вагомих причин. По-перше, це безперервність роботи. Дрони здатні виконувати завдання на протязі до 24 годин без перерви на відпочинок і сон - невід'ємних елементів людських потреб. По-друге, це витривалість.

Безпілотник практично безперебійно працює, в умовах високих перевантажень, і там, де людський організм просто не в змозі витримати перевантаження в 9G, дрон можна продовжувати роботу. Ну а по-третє, це відсутність людського фактора і виконання завдання відповідно до закладеної в комп'ютерний комплекс програми.

Помилитися може хіба що тільки оператор, який вводить інформацію на виконання місії - роботи не помиляються.

Безпілотні літальні апарати - істотно нове слово в століття стрімко розвиваються технологій. Роботи йдуть в ногу з часом, охоплюють не тільки один напрямок, а розвиваються відразу в декількох.

Але все ж, незважаючи на ще далекі від ідеалу, за мірками людини, моделі в області похибок або діяльностей польоту, БПЛА мають один величезний і незаперечний плюс.

2 АРХІТЕКТУРА ДИСТАНЦІЙНО ПІЛОТОВАНОЇ АВІАЦІЙНОЇ СИСТЕМИ (ДПАС)

2.1 Функціональна електромагнітна павутина

Загальна структура системи управління представлена на Рис.2.1.

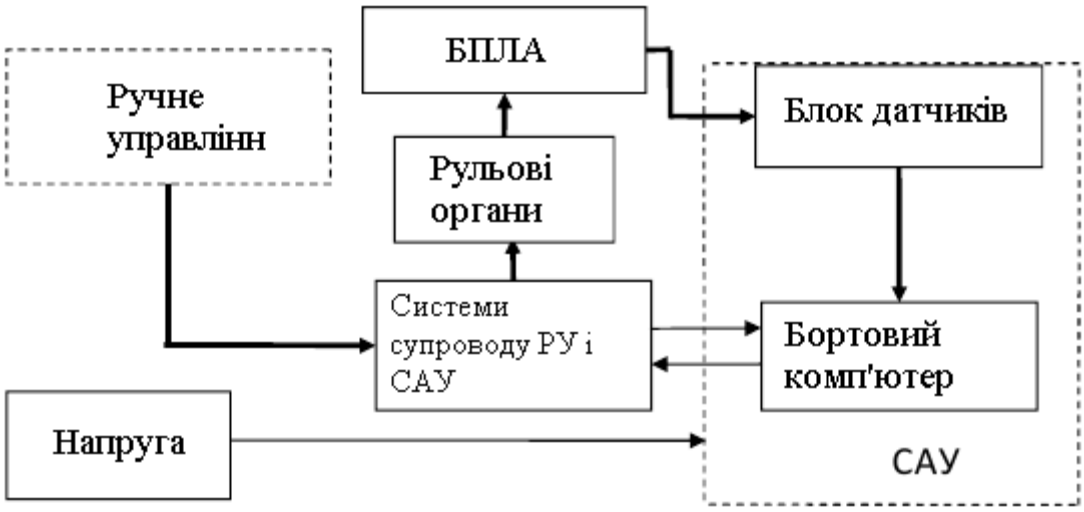


Рис. 2.1 Структура БПЛА з системою управління

Блок датчиків включає інерційних модуль, тривісний магнітометр, приймач супутникових навігаційних сигналів, приймачі статичного і динамічного тиску, ультразвукової висотомір.

Як бортового обчислювача використаний одноплатний комп'ютер. Хоч він і має кілька великі габарити і споживання харчування, ніж більш прості мікропроцесорні системи, проте гнучкість використання і запас обчислювальної потужності дозволяє значно прискорити дослідний процес.

Стабілізація відносної висоти польоту виконується за даними з ультразвукового висотоміра і інформації про поточну вертикальної перевантаження. Вибір саме ультразвукового висотоміра обумовлений його малими габаритами малим споживання енергії, а також невисокою ціною. Проблема невеликого діапазону вимірювання вирішується комплексуванням з сигналом супутникової навігаційної системи і

барометричним висотоміром (при виході за діапазон виміру ультразвукового висотоміра літак виробляє плавне зниження поки висотомір не побачить землю).

Так як рельєф підстильної поверхні невідомий, з даних про вертикальну перевантаження віднімається розрахункове значення перевантаження яке виникає при відпрацюванні нерівностей рельєфу. Це дозволить виділити перевантаження викликану зовнішніми збуреннями і парирувати їх. Також до сигналу перевантаження додається оцінене зміна маси апарату (витрата палива і робочої речовини).

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

2.2 Бортові системи навігації, зв’язку, спостереження і управління ДППС та їх особливості

2.2.1 Системи навігації

Відеонавігація.

Для використання даного способу необхідно отримання зображення місцевості камерою, потім його аналіз бортовим комп'ютером і, виходячи з цього аналізу, знаходяться координати і орієнтація літального апарату. Ці методи аналогічні методам, використовуємо людиною для орієнтації в просторі.

Виробники безпілотних систем проводять дослідження і розробки, спрямовані на забезпечення автономності застосування БПЛА в умовах відсутності сигналів супутникової навігації на основі альтернативних джерел даних. До таких даних належать, перш за все, видова інформація, яка надходить з бортових фото і відеокамер денного і інфрачервоного діапазонів, синтезоване зображення радара, дані цифрового рельєфу місцевості, космічні знімки, а також так звані «сигнали природного походження»: вектору сили тяжіння, магнітному полю землі, положенню світил. Зокрема, компанія RockwellCollins, яка виробляє апаратуру навігації і управління

польотом для БПЛА різних типів, оголосила про завершення розробки Vision Augmented Inertial Navigation System (VAINS), в якій забезпечується корекція інерціальної системи по швидкості і координат від відеокамери під час відсутності сигналів супутникової навігаційної системи.

В основу принципу покладені 3 базових способу:

1. Числення пройденого шляху на основі аналізу потокового відео, яке надходить із оптикоелектронних приладів спостереження. У першому кадрі відеопотоку знаходяться характерні точки і далі відбувається відстеження їх переміщення в кадрі. За характером переміщення програма визначає, як змінюється положення і орієнтація самої камери. Основним обмеженням методу є можливість тільки відносного визначення координат і орієнтації, що може привести до зростання помилки навігації з часом. Також можуть бути причини, що призводять до неможливості знайти відповідні пари точок на знімках: недостатня освітленість, неможливість використання в разі хмарності, неможливість використання над гладкою поверхнею без характерних особливих точок;

2. Метод точної прив'язки по рельєфу по стереоефект, що виникає при русі камери. Даний спосіб дозволяє частково компенсувати недоліки першого методу. Використовуючи перекриття потоку фото- відеоданих, відновлюється рельєф, він порівнюється з закладеними в пам'ять даними, в разі «впізнавання» визначаються точні координати і орієнтація. Основна перевага перед попереднім методом - можливість знайти не тільки відносне, а й абсолютне положення камери, оскільки знання карти прив'язує камеру до конкретних точок на місцевості з відомими абсолютними координатами. Це веде до того, що помилка навігації не росте з часом. Основний недолік методу - чутливість до занадто великих помилок вихідних координат камери, отриманих від інерційним навігаційних приладів, які метод повинен потім уточнювати. Також зберігається і такий недолік першого методу, як неможливість роботи над водною або піщаної поверхнею і виникнення суттєвої помилки під час відсутності явно вираженого рельєфу;

3. Метод точної прив'язки по еталонним фотографій - кадри відео порівнюються з закладеними в пам'ять зображеннями ділянок маршруту, в разі «впізнавання» визначаються точні координати і орієнтація. Цей метод забезпечує високу точність визначення абсолютних координат навіть при відсутності рельєфу. Він також дозволяє знайти абсолютне положення камери, навіть коли її приблизні координати взагалі невідомі. Це досягається шляхом сканування всієї бази даних зі знімками місцевості і порівняння їх з поточним зображенням. Крім того, маючи «прив'язаний» знімок можна з високою точністю визначати координати наземних об'єктів, виявлених оптико-електронною апаратурою.

Визначення координат БПЛА по пеленгаційної вимірам на спостережуваний об'єкт з відомими координатами.

Зважаючи на відсутність прямих вимірювань дальності до мети, виникає задача визначення її координат тільки на основі кутових вимірювань. Наступним етапом є прив'язка координат цілі до карти місцевості, для чого необхідне точне визначення положення самого БПЛА і в цілому реалізація методу одночасної локалізації і картографування.

Відомий цілий ряд алгоритмів, які використовуються для локалізації цілей по пеленгу. Найбільш поширений алгоритм використовує розширений фільтр Калмана або навіть набір таких фільтрів, що відповідають різним діапазонам дальності. Застосування спеціального рандомізованого тестового сигналу у вхідному каналі дає можливість визначити параметри об'єкта управління, коли розглядається модель об'єкта з майже довільними адитивними перешкодами. Перешкоди можуть бути не випадковими, або типу білого або корельованого шуму з нульовим середнім або зі зміщенням, відношення сигнал / шум може бути високим або низьким. Відновлення невідомих значень параметрів забезпечується властивостями рандомізованих тестових сигналів, які додаються в контурі управління до власних сигналам адаптивного управління, що надходять від зворотного зв'язку. Можливе використання найбільш простого в реалізації Калмановського фільтра, що використовує метод псевдоізмереній.

Цей метод оцінювання зводиться до рекурентному рішенням системи лінійних рівнянь з шумами, залежними від оцінюваних координат. Це завдання може бути приведена до задачі лінійної калмановської фільтрації, рішення якої дає незсунені оцінки координат цілей і значення їх ковариационной матриці, які перераховуються рекуррентно аналогічно стандартному фільтру Калмана. Наявність поточних оцінок матриці ковариаций дозволяє сформулювати завдання планування траєкторії БПЛА, що забезпечує мінімізацію помилок оцінювання координат в умовах обмежених польотних ресурсів.

Для уточнення власних координат БПЛА необхідна прив'язка до будь-яких наземних орієнтирах. Це може бути мережа радіолокаційних вишок, пеленг положення БПЛА і повідомляють йому пеленг на певній заздалегідь фіксованій частоті, або набір характерних елементів ландшафту з точно відомими координатами, які БПЛА розпізнає і визначає кути на елемент, щодо свого положення в просторі. В обох варіантах можливість позиціонування БПЛА зводиться до задачі відновлення координат по пеленгаційної вимірам.

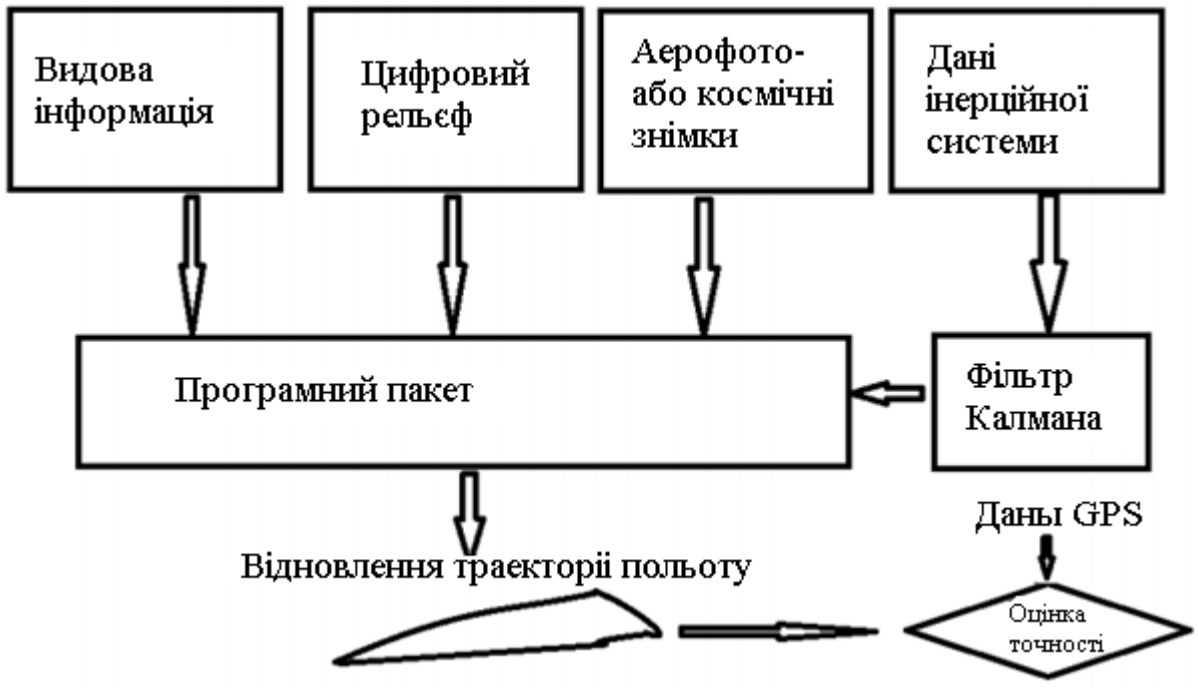


Рис. 2.2 Узагальнена схема навігації БПЛА

Важливо відзначити, що розробка математичних основ зазначених методів вже проведена, і їх реалізація математично обґрунтована і доведена. Попередні оцінки та комп'ютерне моделювання показують, що застосування методів визначення координат об'єкту по видової інформації і цифровим геоданих дозволяє визначати координати місця розташування з помилкою не більше 30 м незалежно від часу. Найкращий результат дає комплексне використання всіх методів в поєднанні з «традиційними» системами навігації, наприклад, з інерціальної навігаційної системою.

2.2.2 Системи 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 сьогоднішній день стало можливим здійснення управління літаками за допомогою автопілоту при повній відсутності зв'язку між бортом літального апарату (ЛА) і НСК. При цьому польотне завдання виконується в автономному режимі. Тим не менш, це не дозволяє говорити про те, що командно-телеметрична радіолінія зв'язку може бути виключена зі складу БПЛА. В силу підвищеної складності і вартості комплексу при його експлуатації потрібен постійний контроль за станом ЛА в повітрі. Крім того, іноді виникає необхідність коригування параметрів польоту БПЛА.

Актуальним завданням також є передача даних корисного навантаження ЛА на НСК. В цьому випадку потрібно забезпечити передачу великого обсягу даних при заданих вимогах по смузі пропускання, ймовірності бітової помилки та ін.

При створенні малих і надмалих БПЛА висуваються вимоги щодо мінімізації розмірів приймально-передавального і антенно-фідерного обладнання.

Підвищені вимоги по відмовостійкості пред'являються до обладнання БПЛА, який здійснює навігацію і літаководіння, що забезпечує режими ручної посадки (якщо це необхідно), до сервоприводу і системі автоматичного порятунку (САП). Перераховане обладнання входить в першу групу класифікації і забезпечує надійність комплексу БПЛА в цілому. Поломка будь-якого елементу обладнання першої групи призводить до негайного припинення виконання льотного завдання та поверненню ЛА на базу. Якщо ж це неможливо, спрацьовує САП і відбувається викид парашута.

Решту обладнання ЛА відносять до другої групи класифікації. При виході з ладу обладнання цієї групи рішення про подальші дії приймається керуючим персоналом комплексу. Взаємодія обладнання першої і другої груп здійснюється за допомогою керуючих інтерфейсів.

В процесі роботи системи зв'язку оцінюються ймовірності бітової помилки для кожного каналу зв'язку і приймається рішення про розподіл командно-телеметричного потоку даних між каналами. Використання декількох каналів зв'язку підвищує надійність системи передачі даних і в той же час є надлишковим з точки зору ефективного використання радіочастотного спектру. Одним із способів підвищення ефективності системи зв'язку є адаптивна робота системи, яка має на увазі передачу по командно-телеметричних каналах зв'язку частини даних корисного навантаження, обсяг яких варіюється в залежності від поточних умов передачі радіосигналу.

Як правило, максимальна відстань для прямого радіозв'язку між БПЛА цивільного призначення та НСК на сьогоднішній день складає не більше 100 км. Для командно-телеметричного зв'язку на великих відстанях можливе використання супутникового зв'язку. У цьому випадку потік даних обмежується мінімально необхідною інформацією про стан БПЛА, інтервал передачі якої може складати, наприклад, від 30 до 300 секунд.

Перспективним напрямком у розвитку систем зв'язку з БПЛА є використання частотних діапазонів вище 5 ГГц. При цьому стає можливою передача великого обсягу даних корисного навантаження в режимі реального часу (наприклад, це можуть бути зображення з датчиків випромінювання різного діапазону довжин хвиль). Факторами, різко обмежуючими радіус дії радіосистеми зв'язку при використанні даних діапазонів, є сильна залежність умов поширення електромагнітних хвиль від погодних умов, необхідність прямої видимості і вплив багатопроменевості.

2.2.3 Системи спостереження

В даний час для спостереження за ПС використовують радіолокаційні некооперативного первинні радіолокатори, кооперативні незалежні вторинні

радіолокатори, системи радіомовного автоматичного спостереження і багатопозиційні системи спостереження. Ці системи відносяться до класу наземного базування з усіма наслідками, що випливають обмеженнями по зоні дії. Всі ці кошти розроблялися для здійснення контролю органами ОПС за польотами пілотованих ПС в контрольованому повітряному просторі. З огляду на можливу зміну класифікації повітряного простору для забезпечення масових польотів малих БПС, моніторинг та відстеження (трекінг) польотів БАС в інтересах ОПС буде здійснюватися не в усьому повітряному просторі. Передбачається, що в класах А і С класифікації повітряного простору Російської Федерації, як і раніше буде здійснюватися контроль і авіаційне спостереження за польотами ПС із використанням традиційних систем спостереження ОВС на основі первинних і вторинних радіолокаторів, систем АЗН-В і МПСН. Відстеження (трекінг) малих БАС буде затребуваний в спеціально виділеному для масових польотів БАС повітряному просторі.

При розробці нових технологічних рішень в галузі зв'язку, навігації і спостереження БАС повинен враховуватися міжнародний досвід, а розробляються системи повинні впроваджуватися з урахуванням використання міжнародної практики і гармонізації з міжнародними стандартами та керівними документами ІКАО, RTCA і EUROCAE з метою забезпечення і гармонізації мінімальних експлуатаційних вимог до технічних характеристик зв'язку (RCP), навігації (RNP) і спостереження (RSP) для виконання всіх видів польотів БВС у всіх класах повітряного простору.

2.2.4 Електронні системи обробки інформації та управління ДППС

Повітряне судно повинно відповідати встановленим компетентними повноважними органами вимогам щодо мінімального складу бортового радіообладнання ближньої та телекомунікації.

В принципі, для виконання цієї вимоги на повітряних судах з пілотом на борту цими правилами мається на увазі можливість використання різних технічних засобів (наприклад, один комплект засобів супутникового зв'язку (SATCOM) і один комплект

ВЧ-обладнання можуть бути затверджені в регіонах, де для ведення регулярного зв'язку на океанічних маршрутах надаються обидва види такого обслуговування).

У випадку з ДПАС зовнішній пілот і ПДП не перебувають на борту ДПВС, тому компетентні повноважні органи можуть розглянути питання про можливість використання вимог до оснащення альтернативними засобами ДВЧ-радіозв'язку з метою УВС. Наприклад, на борту встановлюється один комплект радіообладнання, а необхідне резервування може забезпечуватися другим альтернативним трактом зв'язку між ПДП і органом (ами) УВС.

В принципі, на момент початку польоту встановлене обладнання повинне бути справним. Однак досвід свідчить про те, що в ряді випадків може допускатися тимчасова непрацездатність. У цих випадках слід дотримуватись вимог MMEL. У MMEL міститься перелік обладнання, несправність якого допускається на момент початку польоту, і визначається тривалість такого стану. MMEL затверджується повноважним органом, призначеним державою розробника. Цілком ймовірно, MMEL для ДПАС в частині, що стосується зв'язкового обладнання, буде пов'язаний з прийнятою архітектурою зв'язку. Вимоги до лінії С2 і зв'язку з метою УВС повинні будуть конкретно визначатися окремо, хоча в залежності від архітектури вони не обов'язково повинні бути незалежними.

Зазвичай експлуатантам повітряних суден з пілотом на борту надається право визначати перелік мінімального обладнання (MEL), заснований на MMEL, але не є менш рестриктивним. MEL затверджується компетентним повноважним органом, заснованим державою експлуатанта або державою реєстрації. Можна припустити, що аналогічна процедура буде використовуватися щодо ДПАС.

Якщо для випуску повітряного судна в політ виникає необхідність у внесенні змін до MEL, експлуатант повинен отримати експлуатаційний твердження або, по крайней мере, повідомити про цю зміну держава експлуатанта або держава реєстрації.

2.3 Станція зовнішнього пілота

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.

2.4 Лінії зв’язку та передавання даних ДПАС

Для передачі даних між наземним і повітряним модулями було обрано європейський стандарт наземного цифрового мовлення - DVB-T. DVB-T призначений для передачі єдиного транспортного потоку MPEG-TS з цифровими сервісами (мультиплексу), використовуючи модуляцію COFDM, зі швидкістю до 31 Мбіт/с.

Було обрано компактний повно дуплексний DVB-T передавач, параметри якого задовольняють умовам використання лінії зв’язку (необхідно мати можливість рознести частоти приймачів на наземному і повітряному модулі БПЛА, а також мати значну кількість частот, на які можна налаштувати приймачі, для реалізації алгоритму протидії РЕБ).

Параметр	**Значення**	
Полоса пропускання	Передавач	2/3/4/5/6/7/8 MHz
	Приймач	5/6/7/8 MHz
Frequency range	Передавач	50~950 MHz та 1200~1350 MHz з кроком 1KHz
	Приймач	50~950 MHz з кроком 1KHz
Вихідний рівень RF	0 dBm (108 dBuV)	
Цифрове підсилення	Діапазон: +6/-25 dB , з кроком 1 dB	

Рис. 2.3 Характеристики DVB-T модему

Програмна частина лінії зв’язку є основною і найбільш складною складовою проекту: вона включає в себе мультиплексування/ демультиплексування потоку,

фільтрацію пакетів, інтерфейси для взаємодії із драйвером радіо передавача/приймача, збору статистики та інших компонент.

За допомогою бібліотеки MavLink виконується обмін повідомленнями і сигналами керування між польотним контролером та наземною станцією керування. Всі дані включаючи сигнали керування, телеметрії, відео потік та інші інформаційні об’єднуються у єдиний MPEG-TS потік, також до пакетів прикріплюються додаткові дані для контролю над пакетами, що забезпечує більший захист інформації.

Локальні повідомлення в межах кожного з модулів передаються за допомогою бібліотеки LCM, що забезпечує дуже швидкий обмін даними і, як наслідок малі затримки.

У разі малих БПЛА (злітна маса до 5 кг) внаслідок обмежень за габаритами і масою приймально-передавального обладнання раціональним є використання єдиного радіоканалу зв'язку для передачі команднотелеметричних даних і даних корисного навантаження. Посадка таких ЛА здійснюється, як правило, за допомогою парашута, що не вимагає додаткового радіоканалу зв'язку для передачі зображення з відеокамер ЛА, необхідного при ручній посадці. Додатковим радіоканалом зв'язку є тільки лінія передачі даних САП. Для задоволення вимог по пропускній здатності каналу зв'язку при передачі як даних телеметрії, так і даних корисного навантаження, необхідно розширювати смугу частот приймально-передавального обладнання і використовувати спектрально-ефективні методи модуляції, що призводить до підвищених вимог по відношенню сигнал / шум на вході приймача, зниження дальності дії радіосистеми, підвищення ймовірності бітової помилки і т. д.

Таким чином, додатковий зв'язок обладнання першої і другої груп призводить до погіршення робочих характеристик пристроїв першої групи. Високий ступінь інтеграції пристроїв двох груп призведе до зменшення значення ймовірності безвідмовної роботи життєво важливих елементів комплексу. Виходячи з цього, на комплексах БПЛА із злітною масою більше 5 кг доцільним є використання окремих радіоліній зв'язку для передачі команднотелеметричних даних і даних корисного навантаження. При цьому на

перший план виходять питання електромагнітної сумісності приймальнопередавального обладнання, частотного поділу каналів зв'язку і розміщення антенно-фідерного обладнання на борту БПЛА.

Вибір робочого частотного діапазону радіоканалу зв'язку обумовлюється декількома факторами:

- вимогами до маси, габаритів і споживання приймальнопередавального пристрою БПЛА;

- необхідної дальністю роботи при заданій ймовірності бітової помилки;

- можливістю отримання ліцензії на роботу в необхідному діапазоні або можливістю безліцензійної роботи.

Для систем зв'язку малих БПЛА вирішальними факторами при виборі частотного діапазону є маса і габарити бортового приймача і антенно-фідерного пристрою. Доцільним є вибір діапазону надвисоких частот, при цьому можна використовувати антену малих розмірів, здатну розміститися в профілі крила. Щільна компоновка обладнання всередині малого БПЛА не дозволяє ефективно використовувати приймачі великої потужності з укороченими антенами ультракороткохвильової діапазону внаслідок проблем з електромагнітною сумісністю і великим впливом навколишніх об'єктів на характеристики антени. Одним з відповідних частотних діапазонів є діапазон 2,4 ГГц.

До систем зв'язку БПЛА середнього і великого класу пред'являються більш жорсткі вимоги по дальності роботи, стійкості до заглушення і ймовірності бітової помилки. В цьому випадку є можливим і оптимальним комплексування декількох каналів зв'язку, що працюють в різних частотних діапазонах.

Для оцінки вимог до характеристик зв'язку в цілях УВС при забезпеченні польотів ДПВС слід використовувати принципи, передбачені концепцією RCP, опис яких наводиться в документі Doc 9869. Ця концепція ґрунтується на "важливих з експлуатаційної точки зору" показниках, при досягненні яких є впевненість в тому, що зв'язок з метою УВС буде надійно забезпечувати польоти ДПВС.

Значення RCP для конкретної лінії C2 будуть залежати від:

a) вимог конкретного повітряного простору;

b) етапу польоту;

c) ступеня автоматизації польотів ДПАС.

Оцінка RCP щодо лінії зв'язку УВС для передачі даних виконана, тому, з огляду на можливий вплив різних варіантів архітектур ліній зв'язку ДПАС на час транзакції зв'язку, безперервність, готовність і цілісність системи в цілому, передбачається, що забезпечити зв'язок ДПВС з метою УВС можна буде в рамках діючих вимог.

RCP для УВС визначають вимоги до прямого зв'язку, грунтуючись на припущенні про те, що пілот знаходиться на борту повітряного судна. При проведенні оцінки RCP щодо ДПАС необхідно передбачити додаткову передачу зовнішньому пілотові повідомлень по лінії C2 (якщо вона використовується).

2.4.1 Лінія C2

Лінія C2 - це лінія передачі даних між БВС і станцією зовнішнього пілота з метою управління польотом. Лінії управління і контролю C2 забезпечують можливість зовнішньому пілотові контролювати, управляти БВС, отримувати необхідну телеметрію. У FAA, EUROCAE і MCE лінію C2 відносять до лінії управління та зв'язку, що не відноситься до корисної навантаженні БВС (CNPC). Архітектура лінії C2 RLOS характеризується ситуацією, в якій наземні і бортові системи лінії C2 знаходяться в межах зони дії загальної лінії радіозв'язку і, таким чином, можуть здійснювати прямий зв'язок або зв'язок через наземну мережу. Під архітектурою C2 BRLOS розуміється будь-яка конфігурація, в якій наземні і бортові системи лінії C2 не перебувають в умовах прямої радіовидимості RLOS, що включає в себе всі супутникові системи і, можливо, будь-яку систему, в рамках якої ПДП взаємодіє з однією або декількома наземними радіостанціями через наземну мережу, яка не може забезпечувати передачі в тимчасовому інтервалі, порівнянному з часовим інтервалом C2 RLOS.

Основний варіант застосування лінії С2 для виконання польотів в несегрегірованому повітряному просторі передбачає наявність зв'язку з центрами УВС. Це розширює лінію С2 до С3 (управління, контроль і зв'язок в інтересах УВС). Архітектури лінії С3, що забезпечують польоти БАС, також різняться на RLOS і BRLOS.

Сучасна позиція ІКАО полягає в тому, що в лінії С2 для БАС, що виконують польоти в несегрегірованому повітряному просторі, повинні використовуватися виділені захищені діапазони частот . Отже, при розробці ліній С2 необхідно враховувати управління частотним спектром, який знаходиться під егідою Міжнародного союзу електрозв'язку (МСЕ).

Згідно з чинним Регламентом радіозв'язку МСЕ (видання 2016 року, доопрацьоване за результатами ВКР-12 і ВКР-15), затвердженого Розпорядженням Уряду Російської Федерації від 17 квітня 2018 р № 685-р для ліній С2 ДПАС визначені наступні смуги частот:

а) 117.975 - 137 МГц для RLOS;

б) 960-1164 МГц для RLOS (спільно з маяками DME, вторинними оглядовими радіолокаторами, багатопозиційними системами спостереження (МПСН), і перспективними наземними лініями передачі даних (LDACS);

в) 1545-1555 / 1646,5-1656,5 МГц і 1610-1626,5 МГц для BRLOS (супутникові радіолінії L діапазону);

г) 5030-5091 МГц для RLOS і BRLOS.

д) в якості потенційних для BRLOS визначені смуги діапазонів Ка і Ku Фіксованої супутникової служби: 10,95-11,2 ГГц (Космос-Земля), 11,45-11,7 ГГц (Космос-Земля), 11,7-12 , 2 ГГц (Космос-Земля) в Районі 2, 12,2-12,5 ГГц (Космос-Земля) в Районі 3, 12,5-12,75 ГГц (Космос-Земля) в Районах 1 і 3 і 19, 7- 20,2 ГГц (Космос-Земля), 14-14,47 ГГц (Земля -Космос) і смуги частот 29,5-30,0 ГГц (Земля-Космос) для управління і зв'язку БВС з центрами УВС в несегрегірованном повітряному просторі.

В даний час FAA і EASA для операцій БАС в несегрегірованном повітряному просторі підтримують радиолинию С2 стандарту RTCA DO-362 «Лінія контролю і

управління С2. (Наземна) Вимоги до мінімальних експлуатаційних характеристик (MOPS) ». До основних особливостей радіолінії С2 стандарту RTCA DO-362 відносяться:

- універсальний протокол управління БВС;

- виділені частоти 1040 - 1080 і 1104 - 1150 МГц (Потужність 32 мВт) і 5030-5091 МГц (10 Вт);

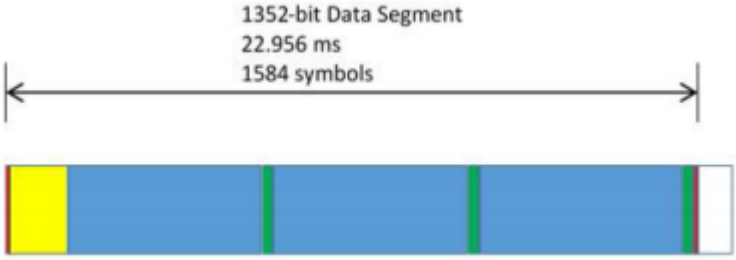
- виділені режими «точка - точка» і «точка - многоточка»;

- дуплексная структура кадру повідомлення (фрейму) з тимчасовим поділом (TDD), тривалість фрейм 50 мс (рисунок 6.2);

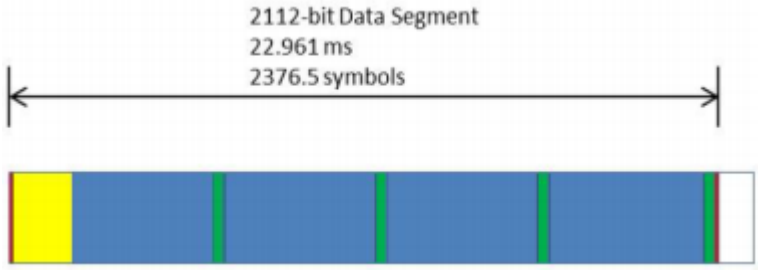
- модуляція сигналу GMSK;

- смуга сигналу 30, 60, 90 або 120 кГц (в залежності від класу)

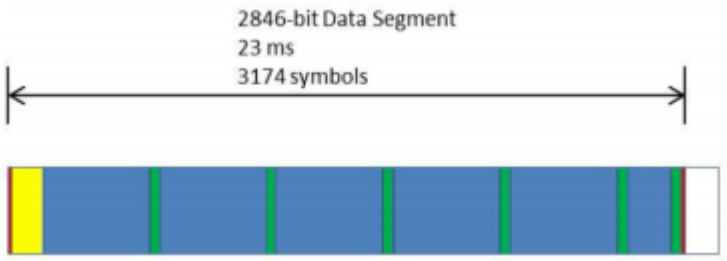
Клас 1. Корисне навантаження 352 біта



Клас 2. Корисне навантаження 800 біт



Клас 3. Корисне навантаження 1280 біт



Клас 4. Корисне навантаження 1 728 біт

Рис. 2.4 Структура кадрів повідомлень стандартної лінії С2

2.4. 2 Лінія С3

Областю, де БАС мають власну технологію, є телекомунікації, технологія наведення та управління, твердотільні гіроскопи та датчики зробили платформи більш надійними з точки зору управління польотом. Сучасні телекомунікаційні технології дозволяють піднімати команди польоту та виконання місій до літака на дуже великих швидкостях і на великих відстанях.

Командування, управління та зв'язок наземної станції (С3): Є кілька ключових аспектів інфраструктури позашляховика С3, які вирішуються, такі як інтерфейси людина-машина, багатолітальний С3, ідентифікація цілей, зменшення наземного обладнання, голосове управління і т. д. Покращення рівня техніки у всіх областях, обговорених вище, дозволить одній людині керувати кількома літаками. БАС під його контролем, щоб забезпечити безпечне та ефективне проведення льотних операцій. Функція управління та управління виконується за допомогою поєднання планування, персоналу, обладнання, зв'язку, навігації та технічних функцій та процедур.

Модель системи С3.

Модель системи С3, показана на операціях UAS на Рис. 2.5, літаки можуть експлуатувати в межах радіочастотної прямої видимості або за межами прямої видимості. Технології та операційні процедури, пов'язані з командуванням, управлінням та зв'язком ПСБ, поділяються на одну з цих двох категорій.

Рис. 2.5 Модель системи С3

За кожною категорією RF LOS та BLOS технічні питання БАС можна розділити на дві категорії: управління та управління (C2) та управління повітряним рухом (ATC). Під C2 та ATC розглядаються різні канали передачі даних, включаючи їх частоту та дані ставки. Перераховано поточні процедури втрати каналів.

2.5 Висновки з розділу

Робота відображає один з підходів до створення програмно-апаратного комплексу управління безпілотними літальними апаратами, як сукупності бортового і наземного сегментів. Для управління бортовим сегментом розроблений блок автопілота. Контроль наземного сегмента комплексу виконує керуюча електронна обчислювальна машина, яка функціонує по уніфікованому програмному забезпеченню з блоком автопілота. Запропонований підхід дозволяє мінімізувати витрати з проектування системи і розробці програмного забезпечення при забезпеченні масштабованості системи.

При проектуванні систем цивільного призначення ключовим є співвідношення функціональності, надійності і ціни. Забезпечення функціональності на початкових етапах життєвого циклу комплексів безпілотних літальних апаратів (БПЛА) ускладнюється слабким розвитком методик їх застосування в господарській діяльності підприємств-споживачів. Можливо, тому активне застосування БПЛА в даний час зводиться до методично простим завданням візуального спостереження і аерофотозйомки.

Для побудови комплексів БПЛА для широкого кола завдань: аероелектророзвідка, аеромагнітометр, аерофотознімання, газоаналізація, патрулювання і т.д. потрібно сформувати комплекс апаратних і програмних засобів, що дозволяють на рівні комплектації і настройки інтегрувати систему з різними корисними навантаженнями на базі планерів БПЛА різних масогабаритних характеристик.

Комплекс управління БПЛА за призначенням поділяється на два сегменти: бортовий комплекс управління (БКУ) і наземний комплекс управління (НКУ).

Завданнями БКУ є:

- Рішення завдання навігації і автоматичного керування літальним апаратом (ЛА);
- Забезпечення командно-телеметричного взаємодії з НКУ;
- Забезпечення функціонування корисного навантаження;
- Забезпечення самодіагностики ЛА.

Основними завданнями НКУ є:

- Забезпечення командно-телеметричного взаємодії з БКУ;
- Забезпечення ручного управління в реальному часі;
- Надання елементів програмування і управління БПЛА;
- Подання телеметричної інформації в графічному вигляді;
- Відображення результатів функціонування корисного навантаження.

За перерахованими основних завдань НКУ одним з очевидних і дешевих рішень є система робочого місця оператора на базі портативної персональної електронної обчислювально машини, підключеної до приймально-передавальної апаратури

командно-телеметричного каналу. Графічне управляє програмне забезпечення (ПО) здійснює програмування маршруту і відображення параметрів польоту. При цьому залишається невирішеною проблема забезпечення ручного управління БПЛА. Завдання підтримки керуючого графічного інтерфейсу і управління в реальному часі (передача сигналів за штатним радіоканалу) на одній ЕОМ є несумісними. Це пов'язано з вимогою забезпечення надійності та детерменірованності часу проходження сигналів ручного управління. Крім цього централізація ПКУ на базі графічної системи вимагає додаткових технічних засобів для забезпечення її автономності протягом тривалого часу.

3 ВИДИ ОРГАНІЗОВАНОЇ РАДІОПРОТИДІЇ НОРМАЛЬНОМУ ФУНКЦІОНУВАННЮ ДПАС

3.1 Шляхи проникнення сторонніх електромагнітних збурень в радіоканали та структурні елементи ДПАС

3.1.1 Види організованих радіозавад

Різноманітні радіоелектронні засоби не можуть бути подавлені завадами лише одного виду. Необхідна ефективність подавлення роботи радіоелектронних засобів (РЕЗ) певного виду може бути досягнута лише при використанні спеціальних видів сигналів завад. Для подавлення РЕЗ одного і того ж виду і класу, але наприклад з різними видами сигналів та способах їх обробки, застосовують відмінні один від одного види сигналів завад. Класифікацію сигналів завад здійснюють за різними критеріями. Один з таких критеріїв це походження сигналів завад. За цим критерієм розрізняють неорганізовані (природні, ненавмисні) та організовані (штучного походження).

Неорганізовані сигнали завад виникають внаслідок відбивання електромагнітної енергії від місцевих предметів, хмар, краплин дощу, а також від блискавок, електромагнітного випромінювання сонця, космічного простору від радіовипромінювання промислових установок і т.д.. Сюди ж відносяться завади створювані власними шумами приймальних пристроїв, взаємні завади РЕЗ, які працюють на близьких або співпадаючих частотах.

Організовані завади створюються спеціальною апаратурою розробленою для подавлення РЕЗ. В подальшому будемо розглядати характеристики організованих завад.

За видом засобів створення завад розрізняють активні і пасивні завади.

Активні завади створюються передавачами завад і випромінюються в ту область простору де розміщені РЕЗ дію яких необхідно подавити.

Пасивні завади формуються за рахунок відбивання сигналів випромінюваних подавлюваними РЕЗ від штучно створюваних відбиваючих об’єктів, наприклад хмара з

відбиваючих диполів (ХВД) або зміна властивостей середовища розповсюдження радіохвиль і т.п. за характером впливу завади підрозділяють на маскуючи, імітуючи та подавляючи.

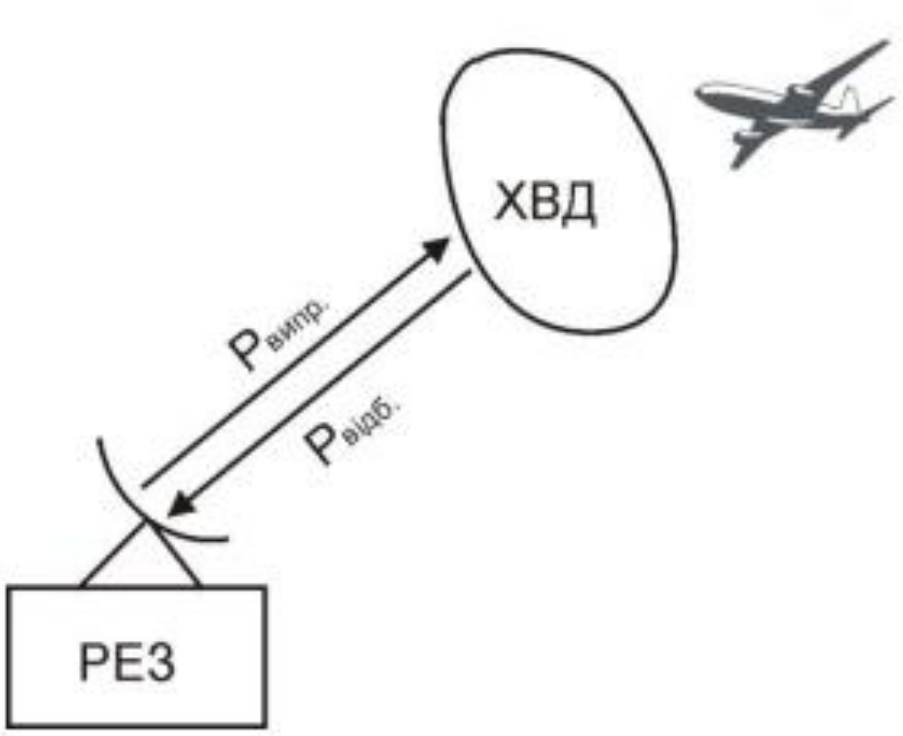


Рис. 3.1. Формування пасивних завад

Маскуючі завади погіршують характеристики подавлюваних РЕЗ. Створюють наприклад на екранах індикаторів маскуючий фон, який утруднює або повністю виключає виявлення об’єктів, виділення корисних сигналів відбитих від цілі. Не позволяє виміряти з потрібною точністю параметри сигналів, які несуть інформацію просторового розміщення, параметри руху і т.д. в термінах теорії виявлення цілей, можна сказати що ймовірність вірного виявлення цілі при дії маскуючи завад може бути знижена практично до нуля. З ростом потужності завади її маскуючи дія зростає.

Імітуючи (дезінформуючі) завади створюють на вході подавлюваного РЕЗ сигнали подібні до корисних, але містять невірну інформацію про той чи інший інформаційний параметр. Це вводить в оману оператора збільшуючи ймовірність помилки в оцінці ситуації наближаючи її до одиниці.

Для подавляючи завад заснована на тому, що підсилювальні тракти реальних РЕЗ характеризуються обмеженим динамічним діапазоном вхідних сигналів. Тому можна створити певний рівень потужності сигналу завади на вході РЕЗ. При якому приймальні канали втрачають можливість виконувати свої функції по відношенню корисної інформації. Особливо сильно при цьому перевантажуються останні каскади підсилювачів проміжної частоти, робоча точка яких внаслідок дії потужної завади виходить за межі лінійної ділянки амплітудної характеристики і корисний сигнал подавляється завадою.

За ознакою використання розрізняють завади сомоприкриття (самозахисту) або групового захисту. В першому випадку, коли об’єкт сам містить джерело завади, реалізується так званий індивідуальний захист (самозахист) об’єкту.

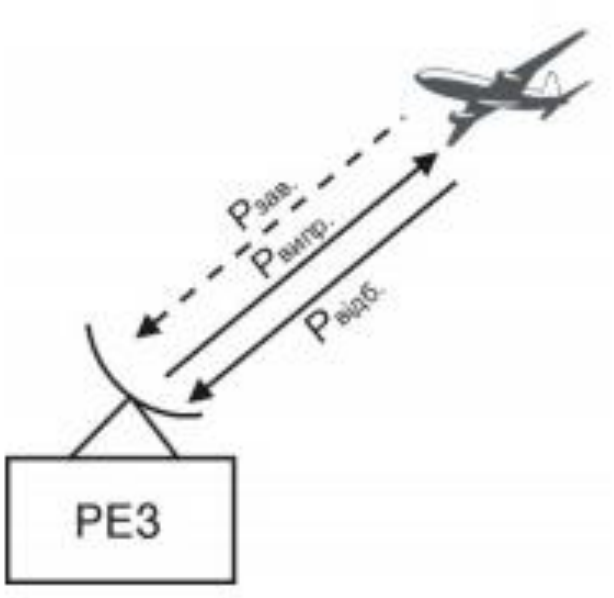


Рис. 3.2. Індивідуальний захист об’єкту

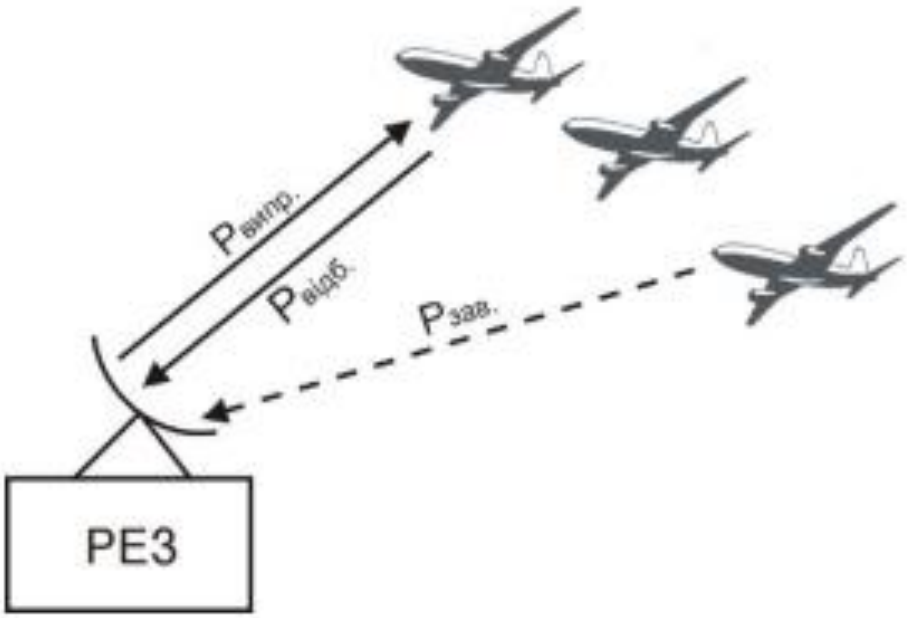


Рис. 3.3. Груповий захист об’єктів

В другому випадку джерело завад розміщують на одному з об’єктів, що входить до групи об’єктів які необхідно захистити. Частіше всього об’єкт з випромінювачем завад розміщують за межами границі його фізичної досяжності. При цьому джерело сигналу (сигналу радіопротидії) групового захист має спеціальну назву, назву джерела „закордонної” завади. При такій методиці організації роботи засобів радіопритидії суттєво підвищується їх живучість.

Особливості тактики застосування засобів радіопротидії.

Отримане використання засобів радіопротидії можливе при умові, що в системі захисту об’єкту є засоби радіотехнічної розвідки інформація якої глибоко і всесторонньо аналізується.

Засоби протидії слід розглядати лише як один з вагомих факторів захисту об’єктів. Захищеність об’єктів суттєво підвищується, якщо прийняті загальні міри по зниженню вразливості об’єкту. Знижено рівень власних радіо- та тепло випромінювань, обмежено

роботу випромінюючих систем, зменшено ефективну поверхню розсіювання і т.д. Сюди ж слід віднести визначення оптимальних моментів ввімкнення засобів радіопротидії. Якщо передавач сигналу радіопротидії буде ввімкнено надто рано то сигнал протидії буде виявлений подавлюваним РЕЗ на більшій віддалі ніж та віддаль на якій подавлюваний РЕЗ може отримувати відбитий від захищуваного об'єкту сигнал. Це пояснюється тим, що в точці розміщення подавлюваного РЕЗ сигнал радіо протидії значно потужніший сигналу відбитого від захищуваного об'єкту. В цьому випадку захищуваний об'єкт буде виявлений набагато раніше ніж би це було можливо з допомогою сигналів подавлюваного РЕЗ. Отже в останнього є часовий запас для прийняття контрмір.

Пізнє ввімкнення засобів радіопротидії може привести до того, що подавлюваний РЕЗ уже виявить захищуваний об'єкт і забезпечить його стійкий супровід. Тобто постійно матиме інформацію наприклад про параметри руху захищуваного об'єкту.

Основним критерієм ефективності роботи засобів радіо протидії є цілісність захищуваного об'єкту. Позитивний кінцевий результат досягається за рахунок оперативної оцінки ефективності засобів радіо протидії в реальному часі, тому необхідно своєчасно адаптувати характеристики сигналів завад до змін обстановки. Для цього необхідно здійснювати неперервний контроль за роботою зондуючи (опромінюючих) РЕЗ (радіолокаторів) тобто приймати зондуючи сигнали під час роботи передавача сигналу РП і по реакції подавлюваних РЕЗ визначати моменти зміни режимів їх роботи.

Інформація отримана при прийомі зондуючи сигналів під час роботи передавачів сигналів РП може бути використана за рахунок таких мір:

1) більш точне налагодження передавача сигналу РП на частоту і напрям зондуючого випромінювання;

2) ввімкнення передавачів сигналів РП тільки на період роботи опромінюючих (зондуючих) РЕЗ;

3) виявлення нових опромінюючих сигналів під час випромінювання сигналів РП;

4) постійне підстроювання параметрів сигналу РП у відповідності із змінами параметрів сигналу опромінення.

Забезпечення можливості прийому опромінюючого сигналу під час роботи передавача сигналу РП може бути здійснене декількома способами. Розглянемо способи які отримали найбільше розповсюдження:

1. Забезпечення надійної „розв'язки" між приймаючою та передаючою антенами. Для забезпечення максимальної „розв'язки" (мінімального впливу випромінюваного сигналу радіо протидій на умови приймання зондую чого сигналу) застосовують самі різноманітні методи і розміщують антени на максимально можливій віддалі одна від одної, використовують екрани між антенами, використовують передаючу і приймаючу антени з гострими діаграмами направленості і т.д. якщо застосовані методом не забезпечують „розв'язки" при якій було б можливо неперервно приймати сигнал зондуючої станції то використовують періодичне вимикання або зміну частоти сигналу радіопротидії.

2. Вимикання передавача сигналу РП здійснюється на короткі інтервали часу, за які здійснюється прийом зондуючи сигналів подавлюваного РЕЗ. Паузи у випромінюванні сигналів завад повинні бути якомога менші, щоб зменшити ймовірність виявлення захищуваних об'єктів. Величина коефіцієнту заповнення $g = \frac{\tau_1}{\tau_1 + \tau_2}$ де 1 τ – часовий інтервал роботи передавача сигналу завади, повинна бути не менше 0,99. слід уникати строго періодичного режиму керування передавачем сигналу завади. Оскільки такий режим позволить синхронізувати роботу подавлюваного РЕЗ.

3. Короткочасна зміна частоти передавача сигналу завади під час якої здійснюється прийом зондую чого сигналу РЕЗ.

4. Компенсація сигналу завади в приймальному тракті системи радіопротидії.

3.1.1.1 Неперервні шумові завади

До неперервних шумових завад відносять електромагнітні коливання з хаотичного (по випадковому закону) зміною амплітуди частоти фази. Часто їх називають флуктуаційними завади. Напругу шумової завади U3(t) на вході подавлюваної РЛС можна розглядати як випадковий процес з нормальним законом розподілу миттєвих значень і рівномірною частотною характеристикою в межах смуги пропускання приймача.

Найбільшими маскуючи ми властивостями з усіх відомих різновидів шумів, характеризується білий шум. Тобто шум в якого спектральна густина інтенсивності не залежить від частоти.

Реальні шумові завади, що створюються передавачами, що володіють паразитними реактивними опорами, за своїми статичними і спектральними характеристиками відрізняються від білого шуму і тому їх реальна маскуючи дія менша.

Безпосереднім результатом дії неперервних шумових завад є маскування корисних сигналів в деякому тілесному куті і відповідному інтервалі віддалей. Оскільки за своєю структурою шумові завади близькі до внутрішніх шумів приймального пристрою, то їх важко виявити і відповідно прийняти міри до ослаблення їх впливу на роботу РЛС. В наслідок дії шумових завад суттєво погіршується роздільна здатність РЛС і знижується точність визначення координат виявлених об’єктів (цілей).

Прямошумові завади як правило формуються в результаті підсилення внутрішніх шумів, які виникають в підсилювальних приладах. Внутрішні шуми виникають в першу чергу в результаті теплового руху вільних електронів в провідниках в резисторах і т.д. це викликає появу шумової напруги, яка складається з великою кількості імпульсів зумовлених рухом окремих електронів. Тривалість імпульсів дуже мала, тому енергетичний спектр теплового шуму зберігає усереднене незмінне значення рівне енергетичному спектру при нульовій частоті в дуже широкій смузі частот. Найбільший внесок у вихідний сигнал шуму здійснюється сигналом шуму на вході підсилювача, оскільки він піддається найбільшому підсиленню.

Прямошумові завади характеризуються власною рівномірністю спектру і тим самим забезпечують можливість перекрити досить широку смугу частот. Характеристики таких завад в найбільшій мірі наближаються за параметрами до білого шуму.

3.1.1.2 Завади модуляційного типу

Такий вид завад створюється з допомогою передавачів, в яких здійснюється модуляція амплітуди, частоти чи фази несучих коливань шумовою напругою. На практиці як правило використовують комбіновану амплітудно-частотну або амплітудно-фазову модуляції, при яких модулююча напруга, діючи на модулюючий каскад передавача змінює одночасно амплітуду і частоту або амплітуду і фазу несучих коливань. Це пояснюється в першу чергу специфікою модуляційної характеристики високочастотних підсилювальних та генераторних приладів. Як правило один з видів модуляції переважає над іншим і саме той переважаючий вид модуляції мають на увазі коли говорять про амплітудну, частотну чи фазову модуляцію сигналу завади.

3.1.1.3 Імпульсні завади

Імпульсні завади відносяться до класу імітаційних. Такі завади створюються радіолокаторами оглядового виду, які працюють в імпульсному режимі випромінювання. Розрізняють синхронні багатократні імпульсні завади і несинхронні хаотичні імпульсні завади (ХІЗ).

Принцип формування синхронних багатократних імпульсних завад полягає в наступному: радіоспектронний пристрій формування сигналу завади приймає зондуючий (випромінюючий) сигнал і пере випромінює його із затримкою в напрямку подавлюваної РЛС на несучій частоті цієї РЛС. На кожний прийнятий зондуючий сигнал може бути сформовано і випромінено декілька радіоімпульсів. Випромінені радіоімпульси повинні бути за формою, тривалістю та потужністю подібними до радіоімпульсів відбитих сигналів.

При дії таких завад на екранах індикаторів подавлюваних РЛС, крім міток від реальних об’єктів (цілей) будуть появлятися другі, аналогічні їм мітки зімітовані передавачем завад. Таким чином, можна зімітувати групу об’єктів (цілей), які характеризуватимуться однаковими кутовими координатами, але розміщеними на різних віддалях. При достатній потужності імітуючи сигналів завад, коли прийом здійснюється боковими пелюстками діаграми направленості антени подавлюваної РЛС, можна зімітувати наявність об’єктів (цілей), кутові координати яких не співпадають з кутовими координатами джерела завад і відповідно об’єкту, який захищають. Введення програмного керування випромінюванним сигналом завади можна імітувати не тільки рух зімітованих об’єктів, практично з довільним курсом, але і різні види їх маневрів.

Радіолокаційна обстановка для подавлюваної РЛС стає дуже складною оскільки приходиться обробляти великі масиви інформації, а отже розпрошувати сили та ресурси призначені для виявлення істиних об’єктів.

Несинхронні хаотичні імпульсні завади реалізуються шляхом формування послідовності радіоімпульсів, несуча частота яких повинна бути близька до несучої частоти зондуючого сигналу, а амплітуда, тривалість та інтервал між імпульсами змінюється за випадковим законом. Такі сигнали створюють на екрані ІКО хаотично розкидані мітки зімітованих об’єктів. Оскільки мітки зімітованих об’єктів можуть переміщуватись за азимутом, віддалю і навіть зникати, щоб знову появитись практично в довільній точці екрану ІКО то виділити сигнал реально об’єкту стає проблематично. Ситуація ще більше ускладнюється якщо сигнали завад прийматимуться боковими пелюстками діаграми направленості приймальної антени подавлюваної РЛС.

Основна складність створення багатократних імпульсних завад полягає в тому, що випромінювання серії імпульсів сигналу завади необхідно здійснювати на несучій частоті зондую чого сигналу і в ті моменти часу коли зондуючи імпульси відсутні на приймальній антені станції завади. Для цього необхідно запам’ятати несучу частоту зондую чого сигналу на відносно великий інтервал часу, співрозмірний з періодом слідування зондуючи імпульсів. Один із способів запам’ятовування частоти полягає у

використані принципу автоматичного підстроювання частоти (АПЧ) гетеродина радіоприймача.

3..2 Загальні аспекти кібербезпеки

3.2.1 Кіберпростір

Кіберпростір – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією.

Деякою мірою, кіберпростір – це віртуальний світ, який базується на реальному матеріальному фундаменті та з реальними наслідками свого “існування та розвитку”.

Кіберпростір є дуже складним явищем, що об’єднує в собі реальність і віртуальність, матеріальне і нематеріальне, абстрактність і дійсність.

Кіберпростір має наступні властивості:

- протяжність;
- єдність дискретності та неперервності;
- матеріальність та нематеріальність;
- абстрактність і дійсність;
- реальність загальнодіючого впливу

Кіберпростір має свою розмірність/протяжність, яка визначаєтьсь кількістю наявних матеріальних і нематеріальних об`єктів на даний період часу. Коли протяжність кіберпростору з точки зору наявності матеріальних об’єктів, обмежена поверхнею земної кулі, то з точки зору наявності нематеріальних об’єктів – протяжність кіберпростору практично необмежена.

Процеси, які відбуваються у кіберпросторі, мають, в основному, як дискретний, так і неперервний характер. Але вони є взаємодоповнюючими один одного, а часто-густо й взаємопов’язаними, які забезпечують існування та розвиток цього простору.

Кіберпростір включає в себе як матеріальну складову, наприклад, засоби обчислювальної техніки, засоби зв`язку, матеріальні складові телекомунікаційних

мереж, написання алгоритмів і кодів та ін., так нематеріальну – інформацію, процеси зчитування кодів, процеси передачі інформації та ін. Але при цьому необхідно зауважити, що під матеріальністю, у даному випадку, ми розуміємо, на відміну від філософського розуміння, все те, що можна побачити, відчути або доторкнутися

Кіберпростір, в цілому, неможливо побачити, відчути, почути або до нього доторкнутися. Він, а особливо процеси, які у ньому відбуваються, людиною сприймається як щось абстрактне. Але окремі складові цього простору можна не тільки побачити, але й доторкнутися.

3.2.3 Види спуфінгу

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.

P-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 нюансу, 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 IP-Спуфінга, але використовуються DNS-протоколи.

ARP-spoofing.

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.

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.

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 GPS-сигналів. 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.

Здавалося б для чого може бути необхідний такий вид спуфинга. Але в житті все може стати в нагоді. Наприклад, є припущення, що захоплення американських безпілотних апаратів на північному сході Ірану в 2011 році був результатом подібної кваліфікованої атаки.

3.2.4 Алгоритмізація процедури виявлення кібератаки

Знання стратегії зловмисників дозволить виявити її на будь-який з стадій і вчасно запобігти. Оператори зв'язку повинні не тільки покладатися на свій досвід побудови захищених мереж, але і використовувати спеціальне обладнання для моніторингу та запобігання вторгнень.

Однією з популярних кібератак є «відмова в обслуговуванні» (DDoS), яка останнім часом не тільки завдає шкоди атакований компанії, але і стає фінансово вмотивованою. За даними дослідження Corero, 62% опитаних респондентів, пов'язаних з мережевою безпекою, допускають можливість передачі хакерам грошей за зупинку DDoS-атаки на ресурси компанії. Якщо раніше такого роду атаки проводилися з метою нанесення шкоди репутації фірми або крадіжки даних, то тепер вони перетворилися на бізнес, як програми вимагачі для персональних комп'ютерів.

Також Corero виявили, що майже три чверті респондентів (73%) очікують посилення заходів безпеки від інтернет-провайдерів і вважають, що ті погано захищають своїх клієнтів від загроз DDoS.

Можна стверджувати, що захист корпоративної інформації лежить цілком на плечах внутрішньої служби безпеки організації, але якщо оператор зв'язку або інтернет-провайдер має інструменти для запобігання DDoS, то їх використання доцільно.

Система глибокого аналізу трафіку СКАТ DPI дозволяє за допомогою інструментів моніторингу та аналізу трафіку в реальному часі відстежувати аномалії і виявляти вторгнення, а також організувати комплекс заходів щодо захисту від DDoS.

Більш детальну інформацію про переваги сучасної системи глибоко аналізу трафіку СКАТ DPI, її ефективне використання на мережах операторів зв'язку, а також про міграцію з інших платформ ви можете дізнатися у фахівців компанії VAS Experts, розробника і постачальника системи аналізу трафіку СКАТ DPI.

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України.

Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

- на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції - здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО,

пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

- на Державну службу спеціального зв'язку та захисту інформації України - формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

- на Службу безпеки України - попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

- на Національну поліцію України - забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;

- на Національний банк України - формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

- на розвідувальні органи України - здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Держава сприятиме залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

3. 3 Висновки з розділу

Різноманітні радіоелектронні засоби не можуть бути подавлені завадами лише одного виду. Необхідна ефективність подавлення роботи радіоелектронних засобів (РЕЗ) певного виду може бути досягнута лише при використанні спеціальних видів сигналів завад . Для подавлення РЕЗ одного і того ж виду і класу, але наприклад з різними видами сигналів та способах їх обробки, застосовують відмінні один від одного види сигналів завад. Класифікацію сигналів завад здійснюють за різними критеріями. Один з таких критеріїв це походження сигналів завад. За цим критерієм розрізняють неорганізовані (природні, ненавмисні) та організовані (штучного походження).

Неорганізовані сигнали завад виникають внаслідок відбивання електромагнітної енергії від місцевих предметів, хмар, краплин дощу, а також від блискавок,

електромагнітного випромінювання сонця, космічного простору від радіовипромінювання промислових установок і т.д.. Сюди ж відносяться завади створювані власними шумами приймальних пристроїв, взаємні завади РЕЗ, які працюють на близьких або співпадаючих частотах.

Організовані завади створюються спеціальною апаратурою розробленою для подавлення РЕЗ. В подальшому будемо розглядати характеристики організованих завад.

За видом засобів створення завад розрізняють активні і пасивні завади.

Активні завади створюються передавачами завад і випромінюються в ту область простору де розміщені РЕЗ дію яких необхідно подавити.

Пасивні завади формуються за рахунок відбивання сигналів випромінюваних подавлюваними РЕЗ від штучно створюваних відбиваючих об’єктів, наприклад хмара з відбиваючих диполів (ХВД) або зміна властивостей середовища розповсюдження радіохвиль і т.д. за характером впливу завади підрозділяють на маскуючи, імітуючи та подавляючи.

4 МЕТОДИ ЗАХИСТУ ДПАС ВІД КІБЕРАТАК

4.1 Організаційні методи протидії кібератакам

У світовій практиці існує кілька понять кібербезпеки. Наприклад, «Збереження конфіденційності, цілісності та доступності інформації в кіберпросторі» (ISO 27032) або «Стан захищеності кіберпростору і здатність запобігти кібератаку в кіберпросторі». Як ви бачите, обидва ці визначення обмежують область дії поняття таким собі «кіберпростором», яке визначено, наприклад, в тому ж NIST SP 800 як: «Глобальна область в інформаційному середовищі, що складається з взаємозалежної мережі систем інформаційної інфраструктури, інформаційних систем, включаючи Інтернет, телекомунікаційних мереж, комп'ютерних систем і вбудованих процесорів і контролерів». Ці визначення змушують ставитися до поняття «кібербезпека», як досить певній сфері загроз, що виникає внаслідок взаємної зв'язності мереж і систем.

Ізольовані від мереж системи, що входять в технологічний контур управління повітряним рухом, забезпечення безпеки інформації в яких має бути гармонізоване з вимогами по інформаційної безпеки системи більш високого рівня (не обов'язково мережевий).

Історично інформаційна безпека в авіації та аеронавігації в більшій мірі базувалася на організаційних процедурах (наприклад - дотримання фразеології радіообміну) і людський фактор, практично не спираючись на технології. Для відносно ізольованою системи це не погано працювало і навіть продовжує працювати, але з приходом нових парадигм і підходів (елементи IoT, розподілені системи, CDM, SWIM) системи перестають бути ізольованими. І цими погрозами все не обмежується. Сьогодні багато технологій доступні всім бажаючим. Наприклад, недорогий радіомодуль, який використовує методи SDR, дозволяє не тільки прийняти і декодувати практично будь-яке аеронавігаційне повідомлення силами і знаннями студента, а й синтезувати сигнали аеронавігаційних систем в діапазоні від 100 кГц до 6 ГГц. А є і готові OpenSource програми, декодуючі сигнали систем АЗН-В, ACARS, CPDLC. Вразлива більшість

систем спостереження, навігації та зв'язку, починаючи з первинних радіолокаторів і закінчуючи системами, що використовують сигнали супутникових навігаційних систем. Деяким особняком стоїть БПСС (багатопозиційна система спостереження), для якої, внаслідок архітектурних особливостей, це зробити складніше, так як потрібно кілька синхронно працюючих передавачів.

Як правило, більшість заходів щодо забезпечення безпеки чинять негативний вплив на сам технологічної процес. Забезпечення захисту - це певний компроміс між впливом на технологічний процес і рівнем захищеності. Щоб чіткіше визначити основні загрози і правильно спланувати протидію їм, формується так звана «модель порушника», яка визначає його вигляд: цілі, мотивацію, обсяг залучених ресурсів, знання і можливості. Адже діапазон потенційних порушників досить широкий: від охочого самоствердитися підлітка, збройного радіостанцією і інформацією з Інтернету, до великого терористичного співтовариства або спецслужби, здатних проводити систематичні дослідження і створювати спеціальні засоби проведення атак.

Питання захисту від кіберзагроз в аеронавігаційної галузі, вирішується індивідуально кожним провайдером на основі існуючих практик або стандартів. У провідних країнах ці питання регулює держава.

Як приклад можна привести вимоги американського стандарту NIST SP 800-53 (rev 4 04-2013) «Security and Privacy Controls for Federal Information Systems and Organizations», прийнятого за основу не тільки в США, але і в Європі. В основі життєвого циклу безпеки взято деякий каркас управління ризиками, який передбачає безперервну оцінку ризиків, прийняття заходів по їх нейтралізації, моніторингу ефективності вжитих заходів і знову оцінку ризиків (внаслідок перманентної зміни ландшафту, оточення безпеки) - і так безперервно. Важливо не зупиняти цей процес і постійно актуалізувати моделі можливих загроз, удосконалювати (це не завжди означає посилювати, ускладнювати) комплекс забезпечення інформаційної безпеки, забезпечуючи стійкість захищеного стану. Це типова модель забезпечення інформаційної безпеки, на основі якої будуються системи в усьому світі. Однак є нюанс:

де саме проходить межа, що захищається системи? Можна провести межу по комплексу засобів автоматизації диспетчерського центру, збудувавши ефективний захист від зовнішніх впливів, але не включаючи в контур зовнішні засоби зв'язку, спостереження, навігації, які винесені на сотні кілометрів по каналах зв'язку, часто знаходяться поза контрольованою зоною і без гарантій відсутності доступу до ним з боку порушника. Можна включити в контур і всі наземні засоби, передбачивши необхідні заходи щодо захисту розподілених об'єктів і каналів зв'язку, пов'язавши їх в єдину систему управління безпеки, але залишивши поза контуром захисту бортове обладнання повітряного судна і сам канал (як правило, радіо). Однак найбільш цілісним буде застосування такого підходу, коли всередині контуру захисту будуть знаходитися всі технологічні елементи для виконання функції, а якщо це з яких-небудь причин неможливо, то повинні застосовуватися заходи з управління цими ризиками, а в стратегічному плані - по технологічних змін, що дозволяють в подальшому повністю вирішити цю проблему.

Проблеми забезпечення інформаційної безпеки в авіації стоять найгостріше в поточний момент:

- швидка зміна ландшафту безпеки, викликане такими факторами, як:

1. Збільшення складності і відкритості аеронавігаційних систем (більше потенційних вразливостей; більше залучених людей, які здатні ними скористатися);

2. Розширення можливостей зловмисників;

3. Тенденція переходу до розподіленої моделі аеронавігаційної інфраструктури.

Варто додати, що в структурі надання аеронавігаційних сервісів очевидний один з найменш охоплених засобами безпеки сегментів - радіоканал. На відміну від бортового обладнання, безпеку якого забезпечується дотриманням ряду спеціальних заходів, безпеку радіоканалу продовжує базуватися на припущенні «це нікому не цікаво», «пілот / диспетчер виявить і вживе заходів». Насправді цей комплекс заходів помітно глибше.

Одна з головних вимог в галузі - забезпечення міжнародної інтероперабельності з урахуванням реальної оснащеності повітряних суден, наземної інфраструктури. А це серйозно обмежує використання технологій забезпечення інформаційної безпеки. Для

захисту передбачається застосування криптографічних засобів, включаючи відкритий розподіл ключів. Некриптографічні методи, як показує аналіз стандарту VDL-4, часто залишають помітні уразливості в системі безпеки.

Перспективи розвитку інформаційної безпеки в авіації насамперед, це вдосконалення моделі загроз, як стратегічне цілепокладання в сфері забезпечення інформаційної безпеки, що дозволить ефективніше будувати комплекс заходів захисту. Друге - гармонізація підходів під егідою ІКАО. На жаль, динаміка тут залишає бажати кращого, але це необхідно, так як на процес накладаються особливості національних вимог щодо захисту критичної інфраструктури. Третє - прихід в аеронавігації абсолютно нових технологій, пов'язаних з безпілотної авіації та забезпеченням безпеки її застосування. Технології, обрані відразу повинні враховувати вимоги інформаційної безпеки. Від захисту каналів управління і захисту від несанкціонованого доступу до станції зовнішнього пілота до технології контролю дотримання обмежень повітряного простору.

Безумовно, значимість питань забезпечення інформаційної безпеки буде зростати, а необхідність впровадження методології наскрізного управління безпекою на всіх етапах життєвого циклу (від формування вимог, розробки систем до їх утилізації) ні в кого не викликатиме сумнівів.

4.2 Криптографічні методи захисту

За визначенням відомого американського криптолога У. Фрідмана «криптоаналіз включає визначення використовуваної мови, типу криптосистеми, ключа і вихідного тексту; зазвичай саме в цьому порядку». Хоча визначення криптоаналіза було введено порівняно недавно, першим відомим писемною згадкою про криптоаналіз є «Книга про великий прагненні людини розгадати загадки древньої писемності», написана арабським ученим Абу ВАКР бен Алі бен Вахшем ал-Набаті в середні століття. В даний час криптоаналіз активно розвивається, хоча єдина математична теорія криптоаналіза ще не розроблена, і на ринку вже з'явилися пакети прикладних програм з криптоаналізом.

Зокрема, розробкою таких програмних продуктів займається американська фірма Access Data Recovery.

Слід зауважити відразу, що основна мета криптоаналіза полягає не стільки в отриманні інформації, що приховується, а в оцінці стійкості існуючих і розроблюваних криптосистем. Оцінка стійкості криптосистем представляється у вигляді кількості операцій, необхідних для злому криптосистеми або у вигляді часу, який потрібен для злому.

Наведемо основні принципи, які були «вистраждані» криптології:

1. Принцип Керкхоффом. Тільки криптоаналітик може судити про криптостійкість системи.

2. Принцип Керкхоффом-Шеннона. Противник знає використовувану криптосистему з точністю до ключової інформації.

3. Принцип Жеверже. Поверхневі ускладнення криптосистеми можуть бути ілюзорні, так як породжують помилкові оцінки її криптостійкості.

4. При оцінці криптостійкості необхідно враховувати можливі криптографічні помилки і інші порушення дисципліни безпеки.

З наведених вище принципів випливає, що основне завдання криптоаналітика полягає в оцінці ключової інформації, за умови, що сама використовувана криптосистема відома. Алгоритм оцінки ключової інформації називається кріптоатакой. Залежно від умов взаємодії криптоаналітика з криптосистемою розрізняють наступні основні типи криптоатак:

- криптоатака з використанням тільки криптограми;

- криптоатака з використанням відкритих текстів і відповідних їм криптограми;

- криптоатака з використанням обираних криптоаналітиків відкритих текстів і відповідних їм криптограми;

- криптоатака з використанням апаратного впливу на криптосистему (криптоатака по стороннім каналам).

Останній тип криптоатак передбачає не дослідження теоретичного опису криптографічного алгоритму, а аналіз даних, отриманих в результаті спостереження за фізичним процесом роботи пристрою, що реалізує криптографічний алгоритм. До цього типу криптоатак відносяться: криптоатака за часом, криптоатака по енергоспоживанню, криптоатака по електромагнітному випромінюванню, криптоатака на основі акустичного аналізу.

Системи блочного шифрування.

Ідея, що лежить в основі більшості ітераційних блокових шифрів, полягає в побудові криптографічно стійкї системи шляхом послідовного застосування відносно простих криптографічних перетворень.иПринцип багаторазового шифрування за допомогою простих криптографічних перетворень був вперше запропонований Шенноном: він використовував з цією метою перетворення перестановки і підстановки. Перше з цих перетворень переставляє окремі символи перетворюється інформаційного блоку, а друге - замінює кожен символ (або групу символів) з преутвореного інформаційного блоку іншим символом з того ж алфавіту (відповідно групою символів того ж розміру і з того ж алфавіту). Вузли, що реалізують ці перетворення, називаються, відповідно, P-блоками (P-box, permutation box) і S-блоками (S-box, substitution box).

DES, Triple DES і AES. У 1973-74 рр. Національне Бюро Стандартів США (NBS) опублікувало документи, що містять вимоги до криптографічним алгоритмом, який міг би бути прийнятий в якості стандарту шифрування даних в державних і приватних установах. У 1976 р в цій іпостасі стандарту був затверджений алгоритм, розроблений фірмою IBM. У 1977 р цей стандарт був офіційно опублікований і набрав чинності як федеральний стандарт шифрування даних - Data Encryption Standard або скорочено DES.

У самому схематичному вигляді DES являє собою 16-циклової ітераційний блоковий шифр. DES працює з блоками даних розрядністю 64 біта з використанням 56 - розрядного ключа. Застосовувані перетворення - порозрядно додавання по модулю два, підстановки і перестановки. Алгоритм вироблення 48-бітових циклових ключів з 56 - бітового ключа системи і ряд перетворень служать для забезпечення необхідного

перемішування і розсіювання переробляється, однак при аналізі DES найчастіше грають не саму істотну роль.

Системи потокового шифрування.

Основна ідея поточного шифрування полягає в тому, що кожен з послідовних знаків відкритого тексту піддається своєму перетворенню. В ідеалі різні знаки відкритого тексту піддаються різним перетворенням, таким чином перетворення, якому піддаються знаки відкритого тексту, має змінюватися з кожним наступним моментом часу. Реалізується ця ідея в такий спосіб. Деяким чином виходить послідовність знаків k_1, k_2, ... , звана ключовим потоком (keystream) або біжать ключем (running key, RK). Потім кожен знак x_1 відкритого тексту піддається оборотного перетворення, залежному від k_i - відповідного знака ключового потоку.

Хоча переважна більшість існуючих шифрів з секретним ключем з певністю можна віднести або до потокових або до блокових шифрів, теоретично межа між цими класами залишається досить розмитою. Так, наприклад, допускається використання алгоритмів блочного шифрування в режимі потокового шифрування (наприклад, режими CBF і OFB для алгоритму DES або режим гамування для алгоритму ГОСТ 28147-89).

Потокові шифри майже завжди працюють швидше і зазвичай вимагають для своєї реалізації набагато менше програмного коду, ніж блокові шифри. Найбільш відомий потоковий шифр був розроблений Р. Рівестом; це шифр RC4, який характеризується змінним розміром ключа і байт-орієнтованими операціями. На один байт потрібно від 8 до 16 дій, програмна реалізація шифру виконується дуже швидко. Незалежні аналітики досліджували шифр, і він вважається захищеним. RC4 використовується для шифрування файлів в таких виробах, як RSA SecurPC. Він також застосовується для захисту комунікацій, наприклад, для шифрування потоку даних в Інтернет-сполуках, що використовують протокол SSL.

Криптосистеми з відкритим ключем.

У асиметричної криптографії для шифрування і розшифрування використовуються різні функції. Асиметричні алгоритми засновані на ряді математичних проблем, на яких і базується їх стійкість. Ще не знайдений поліноміальний алгоритм вирішення цих проблем, дані алгоритми будуть стійкі. У цьому полягає ще одна відмінність симетричного і асиметричного шифрування: стійкість першого є безпосередньою і науково доказовою, стійкість другого - імовірною.

Найбільш відомі криптосистеми з відкритим ключем:

• рюкзачной криптосистема (Knapsack Cryptosystem);

• Криптосистема RSA;

• Криптосистема Ель-Гамаля - EGCS (El Gamal Cryptosystem);

• Криптосистема, заснована на властивостях еліптичних кривих - ECCS (Elliptic Curve Cryptosystems). Застосування алгоритмів шифрування з відкритим ключем дозволяє:

• позбутися необхідності секретних каналів зв'язку для попереднього обміну ключами;

• звести проблему злому шифру до вирішення важкої математичної задачі, тобто в кінцевому рахунку, принципово по-іншому підійти до обгрунтування стійкості криптосистеми;

• вирішувати засобами криптографії завдання, відмінні від шифрування, наприклад, задачу забезпечення юридичної значимості електронних документів.

Автоматизація (без якої неможливий розвиток організацій) призводить до зростання загроз несанкціонованого доступу до інформації, як наслідок, до необхідності постійної підтримки і розвитку системи захисту. Захист інформації є не разовим заходом і навіть не сукупністю заходів, а безперервним процесом, який повинен протікати в часі на всіх етапах життєвого циклу автоматизованої системи обробки інформації. Підвищення продуктивності обчислювальної техніки і поява нових видів атак на шифри веде до зниження стійкості відомих криптографічних алгоритмів. Таким чином, використовувані криптографічні засоби повинні постійно оновлюватися. Підтримка і

забезпечення надійного функціонування механізмів системи захисту інформації пов'язане з рішенням специфічних завдань і тому може здійснюватися лише фахівцями - висококваліфікованими криптографами і криптоаналітиків, які можуть гарантувати надійність використовуваних алгоритмів і програмних засобів, що реалізують функції захисту інформації.

4.3 Алгоритмічні методи захисту

Було доведено, що в криптографії існують тільки два основних типи перетворень - заміни і перестановки. Таким чином, є криптографічні алгоритми, побудовані на основі заміни, перестановки і об'єднання цих двох перетворень. У перестановки шифри символи відкритого тексту змінюють своє місце розташування.

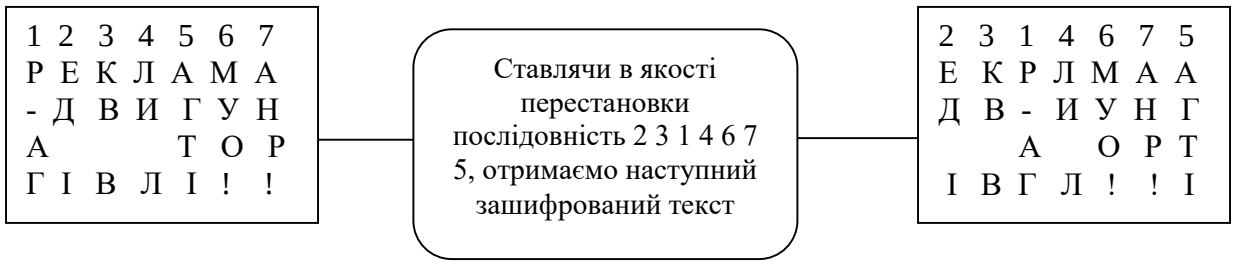


Рис.4.1 Загальна схема перестановки

З іншого боку, в шифри заміни один символ відкритого тексту замінюється І символом зашифрованого тексту. У класичній криптографії розрізняють чотири типи шифрів заміни:

Шифри простої заміни. Один символ відкритого тексту замінюється одним символом зашифрованого тексту;

Шифри складної заміни. Один символ відкритого тексту замінюється одним або декількома символами зашифрованого тексту, наприклад: А може бути замінений З або РО4Е;

Шифри блокової заміни. Один блок символів відкритого тексту замінюється блоком закритого тексту, наприклад: ABC може бути замінений CPT або КАР;

Поліалфавітних шифри заміни, в яких до відкритого тексту застосовуються кілька шифрів простої заміни.

Класична криптографія, зокрема теорія зв'язку в секретних системах, заснована К. Шенноном, виходила з того, що ключі 1 і 2 (рис.4.1), що використовуються відповідно для шифрування і розшифрування, є секретними і однаковими, і передача їх повинна здійснюватися по надійному каналу обміну ключової інформації. Подібні алгоритми були названі симетричними, так як зашифрування і розшифрування відбувається на однакових ключах. Однак розвиток теорії побудови алгоритмів шифрування з відкритим ключем, родоначальниками якої стали Діффі і Хеллмана, поклало початок повсюдного використання асиметричних алгоритмів шифрування, в яких ключі шифрування і розшифрування різні. Залежно від застосування один з ключів буде відкритим, тобто загальнодоступним, а інший необхідно зберігати в секреті.

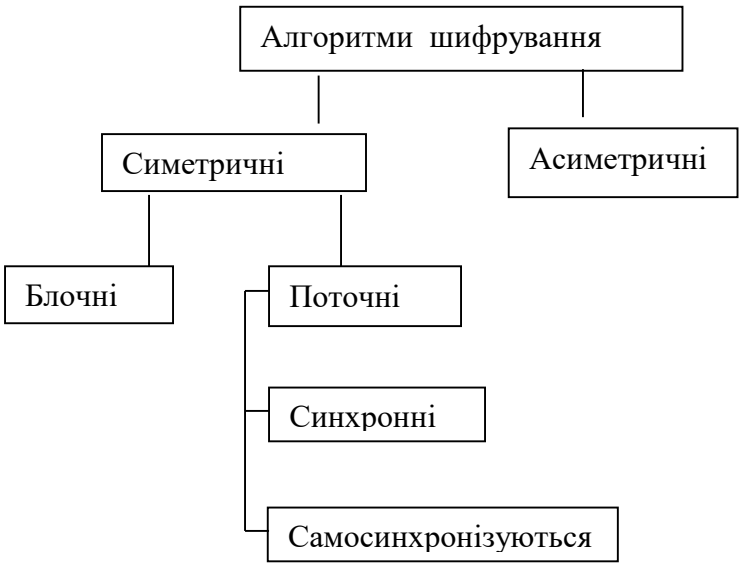


Рис.4.2 Класифікація алгоритмів шифрування

Через деякий час симетричні алгоритми були розділені на два великі класи - блокові і потокові. У перших відкритий текст розбивається на блоки відповідної довжини і фактично кожен блок шифрується, хоча існують різні варіанти застосування алгоритмів блочного шифрування. У поточних алгоритмах кожен символ відкритого тексту зашифровується незалежно від інших і розшифровується таким же чином. Інакше кажучи, перетворення кожного символу відкритого тексту змінюється від одного символу до іншого, в той час як для блокових алгоритмів в рамках шифрування блоку використовується один і той же криптографічне перетворення. Головна ідея, втілена в алгоритмах поточного шифрування, полягає у виробленні на основі секретного ключа послідовності символів з вхідного алфавіту, з яким працює алгоритм шифрування.

Алгоритм RSA.

Піонерська стаття Діффі і Хеллмана знаменувала появу нового підходу в криптографії та насправді кинула виклик криптологам пропозицією знайти криптографічний алгоритм, який відповідав би всім вимогам, що висуваються криптосистемам із загальним ключем. Одними з перших на цей виклик відповіли в 1977 році Рон Ривест, Аді Шамір і Льон Адлеман з MTI, а відповідна публікація з'явилася в 1978 році. Схема Ривеста-Шаміра-Адлемана (RSA) стала з тих пір єдиною отримала широке визнання і практично застосовуваної схемою шифрування з відкритим ключем. Схема RSA є блоковий шифр, в якому і відкритий текст, і шифрований текст представляються цілими числами з діапазону від 0 до n-1, для деякого n.

Опис алгоритму.

Схема, розроблена Ривестом, Шамір і Адлеманом, заснована на вираженні зі ступенями. Відкритий текст шифрується блоками, кожен з яких містить двійкове значення, менше деякого заданого числа n. Це означає, що довжина блоку повинна бути менше або дорівнює log2 (n). Шифрування / дешифрування для блоку відкритого тексту M і блоку шифрованого тексту можна представити у вигляді наступних формул:

$$C=M^e \bmod n, \quad (4.1)$$

$$M=C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n. \quad (4.2)$$

Захищеність алгоритму RSA.

Трьома можливими підходами до криптоанализу алгоритму RSA є наступні:

1. Простий перебір. Передбачає перевірку всіх можливих особистих ключів.

2. Математичний аналіз. Існує кілька підходів такого роду, але всі вони по суті еквівалентні знаходженню множників твори двох простих, позитивних, взаємно простих чисел.

3. Аналіз тимчасових витрат. Спирається на аналіз часу виконання алгоритму дешифрування.

Захист проти простого перебору - використання великого простору ключів, тобто чим більше бітів в e і d, тим краще. Однак через складність обчислень, як при генеруванні ключів, так і при шифруванні / дешифрування, чим більше виявляється розмір ключа, тим повільніше працює система.

4.4 Програмні методи захисту

Робота з будь-якими даними завжди пов'язана з потенційною можливістю їх втрати. Дані можуть бути втрачені в результаті різних факторів: людських помилок (як користувачів, так адміністраторів мережі), фізичної крадіжки, в результаті деструктивних дій шкідливих програм, поломки пристроїв зберігання даних. Якщо були втрачені особисті дані (наприклад, архів з фотографіями), то збитки є суб'єктивним і буде виражатися в негативних емоціях користувача. А, в разі втрати службової інформації, збиток може проявитися в економічній сфері - в фінансові збитки, втрати конкурентних переваг, зриви або невиконанні контрактів і навіть розорення організації.

Для захисту від втрати інформації використовуються системи резервного копіювання та відновлення даних (Backup & Recovery). Система резервного копіювання та відновлення даних - це програмний або програмно-апаратний комплекс для створення копій даних з певною періодичністю для їх подальшого відновлення. Крім захисту від втрати даних системи резервного копіювання також дозволяють забезпечити організувати безперервність роботи співробітників за рахунок швидкого відновлення

операційної системи (при наявності її образу) або відновлення даних на іншому комп'ютері.

Як працюють системи резервного копіювання та відновлення даних.

Створення копії даних є досить простим процесом, проте реальні потреби користувачів часто бувають дуже різні і складні. Наприклад, багато користувачів хочуть мати можливість робити резервні копії з довільної точки або зберігати дуже великі обсяги даних. Для підприємств актуальною є проблема управління великою кількістю даних, їх зберіганням і швидким відновленням. Для вирішення кожного класу задач і існують різні системи резервного копіювання та відновлення даних.

Головні розділові лінії між різними системами резервного копіювання та відновлення даних проходять по сферам їх використання - для персональних потреб, в невеликих компаніях і «домашніх офісах» (SMB / SOHO / ROBO) або в середніх (Enterprise) і великих компаніях (Large Enterprise). Залежно від цього розрізняється ціна систем резервного копіювання і відновлення даних, що використовуються типи сховищ, типи платформ, що надаються функції і т.д. Розглянемо деякі з цих критеріїв.

Одне з основних відмінностей для систем резервного копіювання і відновлення даних - це тип носіїв для зберігання даних. Для зберігання резервних копій може використовуватися стрічка, оптичні диски (CD, DVD, Blu-Ray і т.д.), «жорсткі» диски (HDD), твердотільні диски (SSD), мережеві сховища. Кожен з них має свої переваги і недоліки. Наприклад, зберігання даних на стрічках тільки на перший погляд здається анахронізмом. Сучасні стрічкові пристрої досить дешеві і гарантують тривале зберігання даних. Але ось відновлення даних з таких носіїв може бути дуже довгим. Тому вони більше підходять для архівації даних. «Жорсткі» диски дозволяють виконувати резервне копіювання і відновлення досить швидко, однак у них висока ціна і не найдовше час життя.

Альтернативою «жорстким» дискам є використання «хмарних» сховищ, в яких тип систем зберігання прихований від користувачів. Звичайно, в якості «заліза» в них використовуються будь-які диски, але проблема збереження дисків лягає на

постачальника послуг. А що ж ціна? Забезпечення додаткових гарантій збереження вимагає великих грошей на утримання «хмарної» інфраструктури (може підтримуватися дублювання даних, «гаряча» заміна дисків, RAID-масиви). Однак при цьому ефективність використання дискового простору може бути вище, тому що «Хмарою» може користуватися кілька клієнтів і ефективність його використання буде вище, ніж у системи резервного копіювання та відновлення даних, встановленої безпосередньо в компанії. В результаті цього ефективність тієї чи іншої системи складно порахувати апріорно, тому в кожній конкретній ситуації вибору системи зберігання повинен передувати економічний розрахунок.

Ще одна відмінність - це тип використовуваних платформ. Система резервного копіювання та відновлення даних може бути реалізована у вигляді програмного забезпечення, програмно-апаратного комплексу або у вигляді послуги (software-as-a-service). Програмне забезпечення коштує дешевше і вимагає окремих систем зберігання. Тому такі системи підходять для персонального використання і невеликих компаній. Для великих компаній такі системи можуть використовуватися в зв'язці зі спеціальними сховищами даних. Для середніх і великих підприємств більше підходять системи резервного копіювання та відновлення даних, виконані у вигляді програмно-апаратних комплексів (PBBA, Purpose-Built Backup Appliance). Дані пристрої підрозділяються на дві категорії:

1. PBBA target systems (целевиесістеми). Дані комплексивиступает тільки в якості цільового пристрою для резервного копіювання. Таке рішення вимагає використання додаткового програмного забезпечення для автоматизації, управління і консолідації резервного копіювання, яке, в свою чергу, повинно бути розміщено на додатковому серверному обладнанні з розгорнутою операційною системою для інтеграції всіх перерахованих компонент. До таких пристроїв відносяться EMC Data Domain, HP StoreOnce і т.д.

2. PBBA integrated systems (інтегровані системи). Це повністю закінчені рішення, яке не потребує додаткових складових для повноцінної роботи. Вони включають в себе

сервера, дискові масиви і програмне забезпечення для здійснення резервного копіювання. Такі системи мають більшу інтеграцію між апаратурою і програмним забезпеченням і можуть включати додаткові інструменти для роботи з мережею (наприклад, балансування навантаження). Такі рішення не вимагають додаткових інвестицій в інфраструктуру, мають менші витрати на розгортання і інтеграцію, а також простіше супроводжувати і адмініструвати. До таких пристроїв відносяться EMC Avamar, Symantec Appliance BE + NBU і т.д.

Системи резервного копіювання і відновлення даних відрізняються і за функціями, які вони надають. Умовне можна виділити «базові» і «розширені» функції. До базових функцій можна віднести роботу за розкладом, стиснення і шифрування резервних копій. Додаткові функції різноманітніші:

1. Дублювання дозволяє здійснювати одночасне копіювання на кілька джерел, що збільшує надійність зберігання даних.

2. Дедуплікація дозволяє проводити аналіз і стиснення дубльованих даних. В результаті зменшується навантаження на канали передачі даних і місце для зберігання даних.

3. Створення образів системи. Періодичне копіювання не тільки даних, але і образів системи дозволяє швидко відновити робоче місце співробітника навіть в разі пошкодження операційної системи або персонального комп'ютера, що забезпечує безперервність його роботи.

4. Балансування навантаження. Дозволяє оптимізувати навантаження на кілька сховищ для найбільш швидкого виконання операцій з резервними копіями.

5. Сумісність з програмним забезпеченням (операційними системами і СУБД). Дозволяє створювати «зліпки» файлів і баз даних, які можуть змінюватися в процесі створення резервної копії, для їх коректної цілісної передачі і відновлення.

6. Різні інструменти для віддаленого адміністрування. Це досить різноманітний набір функцій, що дозволяють автоматизувати роботу адміністратора. До них може

ставитися віддалена установка агентів на комп'ютери користувачів, перевірка створених архівів, ручне або автоматичне злиття резервних копій і т.д.

7. Робота з віртуальними пристроями.

8. абота з «хмарними» сховищами.

9. Алгоритми відновлення даних.

При втраті даних для збільшення швидкості відновлення даних використовуються різні алгоритми, що дозволяють відновлювати тільки потрібні дані, виключати дублювання при відновленні і т.д.

4.5 Висновки з розділу

В даному розділі були розглянуті методи захисту ДПАС.

Ізольовані від мереж системи, що входять в технологічний контур управління повітряним рухом, забезпечення безпеки інформації в яких має бути гармонізоване з вимогами по інформаційної безпеки системи більш високого рівня (не обов'язково мережевий).

Історично інформаційна безпека в авіації та аеронавігації в більшій мірі базувалася на організаційних процедурах (наприклад - дотримання фразеології радіообміну) і людський фактор, практично не спираючись на технології. Для відносно ізольованою системи це не погано працювало і навіть продовжує працювати, але з приходом нових парадигм і підходів (елементи IoT, розподілені системи, CDM, SWIM) системи перестають бути ізольованими. І цими погрозами все не обмежується. Сьогодні багато технологій доступні всім бажаючим.

Як правило, більшість заходів щодо забезпечення безпеки чинять негативний вплив на сам технологічної процес. Забезпечення захисту - це певний компроміс між впливом на технологічний процес і рівнем захищеності. Щоб чіткіше визначити основні загрози і правильно спланувати протидію їм, формується так звана «модель порушника», яка визначає його вигляд: цілі, мотивацію, обсяг залучених ресурсів, знання і можливості. Адже діапазон потенційних порушників досить широкий: від охочого

самоствердитися підлітка, збройного радіостанцією і інформацією з Інтернету, до великого терористичного співтовариства або спецслужби, здатних проводити систематичні дослідження і створювати спеціальні засоби проведення атак.

Питання захисту від кіберзагроз в аеронавігаційної галузі, вирішується індивідуально кожним провайдером на основі існуючих практик або стандартів. У провідних країнах ці питання регулює держава.

5 Охорона праці

5.1 Вступ

Система заходів з охорони праці займається розробкою засобів для забезпечення безпеки життя і здоров’я працівників в процесі їх трудової діяльності, тобто ця система вміщує в собі заходи, які поодинці або в сукупності спрямовані на створення умов праці, що відповідають вимогам збереження життя та здоров’я працівників в процесі трудової діяльності.

Охорона праці спирається на комплекс державних законодавчих актів.

Загальними законами України, що визначають основні положення щодо охорони праці є Конституція України, Кодекс законів про працю, Закон України «Про охорону праці», Закон України «Про загальнообов›язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності» та підзаконні акти щодо охорони праці.

Технічна експлуатація електроустаткування літаків і аеропортів пов›язана з небезпекою ураження інженерно-технічного персоналу електричним струмом.

У державному стандарті України ДСТУ 2293-99 «Система стандартів безпеки праці. Охорона праці. Терміни та визначення» встановлені терміни і визначення основних понять з охорони праці. Наведемо деякі з них:

Охорона праці система правових, соціально-економічних, організаційно-технічних, гігієнічних або лікувально-профілактичних заходів і засобів спрямованих на збереження здоров›я і працездатності людини в процесі праці;

Шкідливий (виробничий) фактор виробничий фактор вплив якого може призвести до погіршення стану здоров›я та зниження працездатності працівника;

Небезпечний (виробничий) фактор виробничий фактор вплив якого в певних умовах може призвести до травм або іншого раптового погіршення здоров'я працівника;

Нещасний випадок на виробництві раптовий вплив на працівника небез печного виробничого фактора чи середовища, внаслідок яких заподіяна шкода здоров›ю або наступила смерть;

Виробнича травма порушення анатомічної цілісності організму людини або його функцій внаслідок впливу виробничих факторів;

Виробниче середовище сукупність фізичних, хімічних, біологічних, соціальних факторів, що діють на людину в процесі трудової діяльності;

Міжгалузеві і галузеві акти з охорони праці закони, міжгалузеві і галузеві стандарти, норми, правила, положення, інструкції та інші документи з охорони праці, яким надається сила правових норм обов›язкових для виконання;

Нагляд за охороною праці одна з форм діяльності державних органів по дотриманню вимог законів та інших нормативних актів з охорони праці встановлених державною владою.

5.2 Аналіз умов праці на робочому місці

Організація робочого місця

Для створення сприятливих умов зорової роботи, які б виключали швидку втомлюваність очей, виникнення професійних захворювань і сприяли підвищенню продуктивності праці, виробниче освітлення повинне відповідати вимогам СНиП II-4-79 «Естественное и искусственное освещение. Нормы проектирования”, ДБН В.2.5-28-2006 «Природне і штучне освітлення», де основною вимогою є необхідність створення на робочій поверхні освітленості, що відповідає характеру зорової роботи і знаходиться в межах встановлених норм. Освітлення у приміщенні з ВДТ має бути суміщеним, при якому недостатнє за нормами природне освітлення доповнюється штучним. Природне освітлення повинне бути боковим, бажано одностороннім. Найкраще, коли вікна зорієнтовані на північ чи північний схід, це дасть змогу усунути небажану засліплюючу дію сонячних променів. Вікна необхіно обладнати регульованими пристроями (жалюзі, завіски, зовнішні козирки тощо).

Поверхня підлоги приміщення з ВДТ має бути рівною, неслизькою, зручною для очищення та вологого прибирання, мати антистатичні властивості. Площа, на якій розташовується одне робоче місце з комп'ютером, повинна становити не менше ніж 6,0 кв.м , а об'єм приміщення - не менше ніж 20,0 куб.метрів. Приміщення з ВДТ мають бути оснащені аптечками першої медичної допомоги.

Правильна організація робочих місць сприяє усуненню загального дискомфорту, зменшенню втомлюваності працівника, підвищенню продуктивності його праці. Організація робочого місця передбачає :

- правильне розміщення робочого місця у виробничому приміщенні;
- вибір ергономічного обгрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;
- раціональне компонування обладнання на робочих місцях;
- урахування характеру та особливостей трудової діяльності.

На робочому місці присутні стіл, стілець, та комп’ютер разом з монітором в реальному часі, що знаходяться на столі.

Розмір приміщення для ВДТ довжиною а = 7 м, шириною в = 4,5 м, висотою h = 3.5 м.

Відповідно до ДНАОП 0.00-1.3 1-99 є неприпустимим розташування приміщень, призначених для роботи з ВДТ у підвалах та на цокольних поверхах. Також забороняється розташовування вибухонебезпечних приміщень категорії А і В (ОНТП 24-86) та виробництв з «мокрими» технологічними процесами поряд з приміщеннями, де розташовуються ЕОМ, а також над такими приміщеннями або під ними. Окрім того, виробничі приміщення для роботи з ВДТ не повинні межувати з приміщеннями, в яких рівень шуму і вібрації перевищує допустимі значення.

Оскільки площа приміщення S = ахв=7х4,5=5кв.м, а площа на якій розташовується одне робоче місце з ВДТ, повинна становити не менше 6,0 кв.м., то в даному приміщенні можна розмістити не більше п' яти комп'ютеризованих робочих місць.

Об'єм приміщення становить Sxh= 31,5 х 3,5 = 110,25 куб.м. а об'єм,що припадає на одне робоче місце – 110,25: 5 = 22,05 куб.метрів.

Планування розміщення комп'ютеризованих робочих місць у приміщенні проводимо з урахуванням наступних вимог:

-робочі місця з ВДТ розміщуються на відстані не менше 1 м від стіни зі світловими прорізами (вікнами);

-відстань між бічними поверхнями ВДТ має бути не меншою за 1,2 м;

-відстань між тильною поверхнею одного ВДТ та екраном іншого не повинна бути меншою за 2,5 м;

-прохід між рядами робочих місць має бути не меншим за 1м;

Необхідно також врахувати розміри меблів на комп'ютеризованих робочих місцях, зокрема, робочого столу. Відповідно до ДНАОП 0.00-1.31-99 рекомендовані розміри столу для робочого місця з ВДТ становлять: висота - 725 мм, ширина- 600- 1400 мм, глибина 800-1000 мм. Приймаємо, що робочий стіл має такі розміри: ширина- 1200 мм, глибина- 800 мм.

Найкраще розмістити комп'ютеризовані робочі місця рядами вздовж стіни з вікнами. Це дасть змогу виключити дзеркальне відбиття на екрані ВДТ джерел природного світла (вікон) та потрапляння останніх у поле зору операторів, що погіршує їх зорову роботу.

Наводимо план виробничого приміщення з комп'ютеризованими робочими місцями (рис. 5.1).

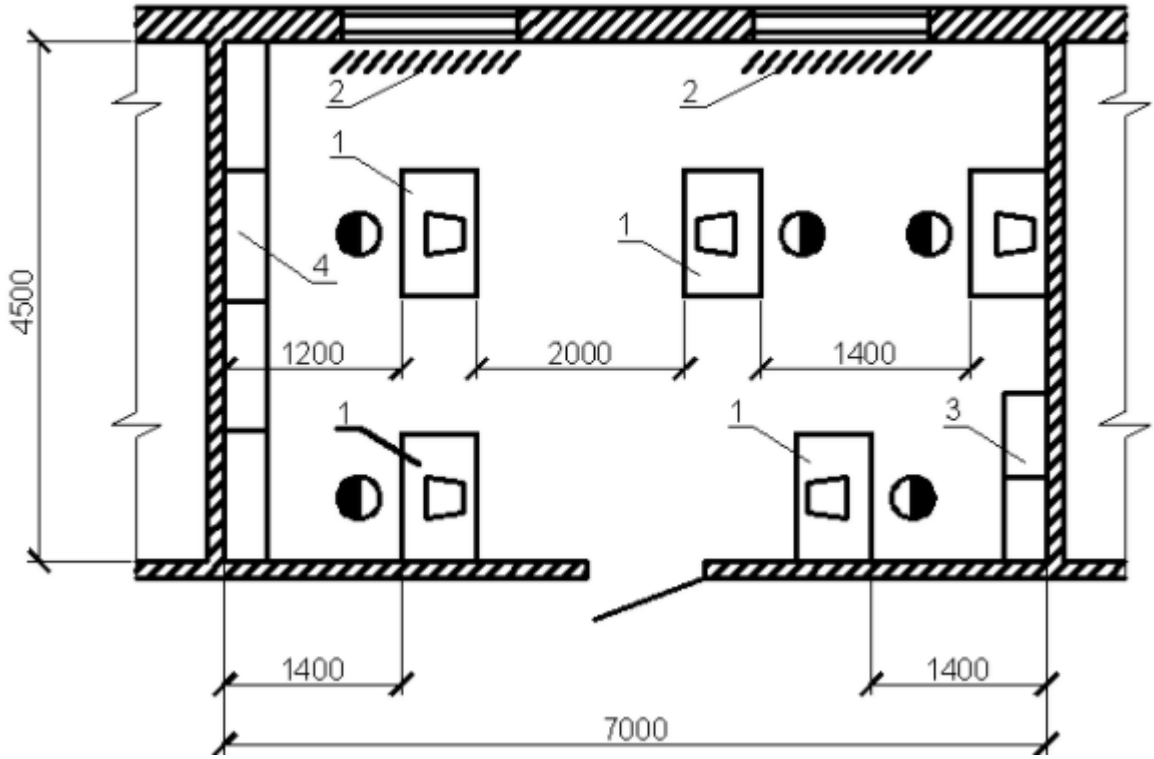


Рис 5.1 План виробничого приміщення з комп'ютеризованими робочими місцями

1 - комп'ютеризоване робоче місце з ВДТ;

2 - сонцезахисні жалюзі;

3 - шафи для зберігання дискет та програмного забезпечення;

4 – шафи для зберігання документації та фахової літератури.

5.3 Аналіз шкідливих та небезпечних виробничих факторів

На суб’єкта охорони праці в межах лабораторії та його робочого місця діють такі шкідливі та небезпечні виробничі чинники:

1) неіонізуючі електромагнітні поля і випромінювання;

2) виробничий шум;

3) штучне освітлення;

4) електрична мережа та підвищене значення напруги в електричному ланцюзі, замикання якого при певних ситуаціях може відбутися через тіло людини;

5) шкідливі речовини в повітрі робочої зони.

Неіонізуючі електромагнітні поля і випромінювання

На інженера-дослідника на його робочому місці діють електромагнітні випромінювання промислової частоти від техніки та устаткування і електромагнітні випромінювання радіочастотного діапазону.

Згідно з ДСНіП 3.3.6.096-2002 «Державні санітарні норми і правила при роботі з джерелами електромагнітних полів» напруженість електромагнітного поля промислової частоти (50 Гц), що діє на інженера-дослідника не повинна перевищувати 5 кВ/м .

Граничні значення для неіонізуючого випромінювання радіочастотного діапазону наведені в табл. 5.1 .

Таблиця 5.1 Граничні значення для неіонізуючого випромінювання радіочастотного діапазону

Параметри та одиниці вимірювання	Граничні значення в діапазонах частот				
	1-10кГц	10-60кГц	0,06-3 МГц	3-30 МГц	30-300 МГц
$E_{гд}$, В/м	1000	700	500	300	80
$ЕН_{E_{гд}}$, $(В/м)^2 \cdot год$	1200000	40000	20000	7000	800
$H_{гд}$, А/м	75	57	50	-	3,0*
$ЕН_{H_{гд}}$, $(А/м)^2 \cdot год$	675	390	200	-	0,72*

* ГДР енергетичного навантаження магнітного поля поширюється на діапазон частот 30-50 МГц.

Виробничий шум

Згідно з ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку» рівні шуму в дослідницькій лабораторії, що діє на інженера-дослідника, мають складати 50 дБ, а фактичне значення рівня шуму складає 55-65 дБ. Це пов’язано з наявністю у приміщенні установок кондиціонування повітря, вентиляції та повітряного опалення, які утворюють шум. На робочому місці наявні такі види шумів як механічний, ультразвук, електромагнітний та аеродинамічний; інфразвук відсутній.

Рівні звукового тиску, що характеризують ступінь перевищення звукового тиску над певним порогом сенсорного сприйняття даного фактору, для виробничого шуму наведені у табл. 5.2 .

Таблиця 5.2 Рівні звукового тиску в дБ для працівників лабораторії

Вид трудової діяльності, робоче місце	Рівні звукового тиску в дБ в октавних смугах з середньогерметичними частотами, Гц									
	31,5	63	125	250	500	1000	2000	4000	8000	Еквівалентні рівні шуму, Дб А
Наукова діяльність, робочі місця – лабораторії для теоретичних робіт та обробки даних	86	71	61	54	49	45	42	40	38	50

Природне і штучне освітлення

Згідно з ДБН-В.2.5.-28-2006 «Природне і штучне освітлення» нормовані показники освітленості на робочому місці інженера-дослідника мають складати 300-500 лк, а фактичне значення освітленості складає 250-430 лк. Це пов’язано з застарілістю системи освітлення. Найменша освітленість робочих поверхонь у виробничих приміщеннях визначається, в основному, характеристикою зорової роботи. Нормовані показники носять міжгалузевий характер.

Місцеве освітлення – це освітлення, що додається до загального, що створюється світильниками, які концентрують світловий потік безпосередньо на робочих місцях.

Чергове освітлення – освітлення за відсутності основного робочого процесу. Аварійне освітлення поділяється на освітлення безпеки та евакуаційне. Евакуаційне освітлення: у приміщеннях 0,5 лк, на відкритих ділянках – 0,2 лк.

На робочому місці використовується змішане освітлення. В якості природного освітлення в даному приміщенні використовується одностороннє освітлення за допомогою трьох вікон.

Для штучного освітлення в даному випадку необхідні джерела світла з досить великим ККД у світильниках загального освітлення, що розташовуються рівномірно по всій площі приміщення. Найкраще підходять в такому випадку світлодіодні (LED) лампи, які мають один з найвищих показників світловіддачі.

При правильно розрахованому і виконаному освітленні виробничих приміщень, очі працюючого протягом тривалого часу зберігають здатність добре розрізняти предмети, не стомлюючись. Такі умови сприяють зниженню виробничого травматизму і професійного захворювання очей. Раціональне освітлення має задовольняти ряд вимог та умов.

Воно має бути:

- достатнім, щоб мати можливість без напруги розрізняти предмети;
- постійним для цього напруга в мережі живлення не повинна коливатися більше ніж на 5%;
- рівномірно розподіленим по робочих поверхнях;
- таким, що не здійснює осліплюючу дію на око людини як від самого джерела світла, так і від поверхонь, що віддзеркалюють його та знаходяться в полі зору інженера;
- не викликати різких тіней на робочих місцях. Цього можна уникнути при правильному розташуванні світильників.

5.3 Розробка заходів з охорони праці

Основним нормативним документом, який визначає вимоги до безпечної експлуатації обчислювальної техніки, є ДНАОП 0.00-1.31 -99 „Правила охорони праці під час експлуатації електронно-обчислювальних машин”.

До роботи з комп'ютерною технікою можуть бути допущені особи, які засвоїли відповідний практичний курс, ознайомилися з інструкцією і отримали інструктаж з охорони праці на робочому місці, пройшли медичний огляд і не мають протипоказань щодо роботи з ВДТ.

Слід дотримуватись встановлених вимог щодо безпеки перед початком роботи, наприклад, перед ввімкненням ЕОМ в мережу необхідно переконатись у наявності заземлення обладнання, у справності шнура живлення та інших провідників. Перевірити надійність і правильність встановлення апаратури на робочому столі, увімкнути систему кондиціонування робочого приміщення, відрегулювати освітленість робочого місця тощо.

У разі виявлення будь-яких несправностей роботу розпочинати не можна і слід повідомити про це керівника або іншу відповідальну особу.

Під час виконання роботи забороняється працювати без належного освітлення, закривати вентиляційні отвори апаратури, залишати без нагляду ввімкнене обладнання, допускати до роботи на обладнанні сторонніх осіб.

І з метою профілактики негативного впливу на здоров'я шкідливих виробничих факторів необхідно дотримуватися режимів праці та відпочинку. Після кожної години роботи за дисплеєм необхідно робити перерву для відпочинку тривалістю 10-15 хвилин. Під час регламентованих перерв рекомендується виконувати спеціальні вправи та самомасаж кистей рук та очей, а також проводити сеанс психофізіологічного розвантаження у спеціально обладнаному приміщенні.

Після закінчення роботи слід вимкнути принтер, дисплей, процесор і інше обладнання, витягнути з розеток штепсельні вилки, прибрати робоче місце, ретельно вимити руки теплою водою з милом, вимкнути також кондиціонер, освітлення і загальне

електроживлення підрозділу.

5.4 Пожежна безпека виробничого приміщення

Основним нормативним документом, що регламентує вимоги щодо пожежної безпеки є Закон України „Про пожежну безпеку". Цей Закон визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності.

Відповідно до Закону України „Про пожежну безпеку", забезпечення безпеки підприємства, установи покладено на керівника або уповноважену особу. Керівники зобов'язані :

1 Розробляти комплекс заходів щодо забезпечення пожежної безпеки (в даному випадку в приміщеннях з обчислювальною апаратурою);

2 Розробляти і затверджувати інструкції, положення, правила щодо пожежної безпеки і здійснювати контроль за їх виконанням ;

3 Організовувати навчання працівників щодо пожежної безпеки ;

4 Утримувати в справному стані засоби протипожежного захисту і зв'язку, пожежну техніку, обладнання та інвентар, не використовувати його не за призначенням.

5 Проводити службове розслідування випадків пожеж.

Осіб, які не пройшли інструктаж з пожежної безпеки, не можна допускати до роботи. Кожен працівник зобов'язаний виконувати вимоги щодо пожежної безпеки, а також вживати заходів щодо усунення порушень правил пожежної безпеки, ліквідації пожеж і загорянь. Кожен працівник повинен знати місце розташування первинних засобів пожежогасіння і вміти ними користуватися, працівники повинні знати правила поведінки під час пожежі, шляхи евакуації. У разі виникнення пожежі працівники повинні негайно повідомити про це пожежну охорону (зателефонувати) та керівництво установи і розпочати ліквідацію пожежі всіма наявними засобами.

Крім загальних вимог пожежної безпеки, здійснюються спеціальні протипожежні

заходи. Для споруд та приміщень, в яких експлуатуються відео-термінали та ЕОМ такі заходи визначені Правилами з пожежної безпеки в Україні НАПБ А.01.001-2004, Правилами з охорони праці під час експлуатації електронно-обчислювальних машин ДНАОП 0.00-1.31-99 та іншими норма тивними документами.

Будівлі та їх частини, в яких розташовуються ЕОМ, повинні бути не нижче П ступеня вогнестійкості. Над та під приміщеннями, де розташовуються ЕОМ, а також у суміжних з ними приміщеннях не дозволяється розташування приміщень категорій А і Б з метою запобігання вибухопожежній небезпеці. Приміщення категорії В слід відділяти від приміщень з ЕОМ протипожежними стінами. Для всіх споруд і приміщень, в яких експлуатуються відеотермінали та ЕОМ, повинна бути визначена категорія з вибухопожежної і пожежної небезпеки відповідно до НАПБ Б.07.005-86 (ОНТП 24-86 МВД СССР Общесоюзные нормы технологического проектирования. Определение категорий помещений и зданий по взрывопожарной и пожарной опасности), та клас зони згідно з Правилами влаштування електроустановок. Відповідні позначення повинні бути нанесені на вхідних дверях приміщення.

Сховища носіїв інформації, важливої документації, зопасної техніки слід розміщати у відокремлених приміщеннях, обладнаних негорючими стелажами і шафами. В приміщеннях, де знаходяться робочі комп'ютери, слід зберігати лише ті носії інформації, які необхідні для поточної роботи.

Звукопоглинальне облицювання стін та стель у приміщеннях ЕОМ слід виготовляти з негорючих або важкогорючих матеріалів.

Приміщення з ЕОМ рекомендується оснащувати вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 кв.м площі приміщення з урахуванням гранично - допустимої концентрації вогнегасної речовини. Відстань від можливого осередку пожежі до місця розташування вогнегасника не повинна перевищувати згідно з нормами 20 метрів.

5.6 Висновки з розділу

Необхідність дотримання описаних в розділі заходів охорони праці необхідна для виконання.

В першу чергу тому, що найвищою цінністю завжди є людина, її життя і здоров'я. Ні розмір заробітної плати, ні рівень рентабельності підприємства, ні цінність виробленого продукту не можуть служити підставою для зневаги правилами безпеки і виправданням існуючих загроз життю або здоров'ю працівників. Крім того, в даному випадку мова також йде про цінності конкретної людини як співробітника з властивими йому знаннями, навичками і досвідом.

По-друге, правильно організована робота по забезпеченню безпеки праці підвищує дисциплінованість працівників, що, в свою чергу, веде до підвищення продуктивності праці, зниження кількості нещасних випадків, поломок устаткування і інших позаштатних ситуацій, тобто підвищує в кінцевому підсумку ефективність виробництва.

По-третє, охорона праці має на увазі не тільки забезпечення безпеки працівників під час виконання ними службових обов'язків. Насправді сюди також відносяться найрізноманітніші заходи: наприклад, профілактика професійних захворювань, організація повноцінного відпочинку і харчування працівників під час робочих перерв, забезпечення їх необхідним спецодягом і гігієнічними засобами і навіть виконання соціальних пільг і гарантій. Правильний підхід до організації охорони праці на підприємстві, грамотне використання різних нематеріальних способів стимулювання працівників дають останнім необхідне почуття надійності, стабільності і зацікавленості керівництва в своїх співробітниках. Таким чином, завдяки налагодженій охороні праці знижується також плинність кадрів, що теж благотворно впливає на стабільність всього підприємства.

6 ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1 Вступ

Охорона навколишнього середовища — система заходів щодо раціонального використання природних ресурсів, збереження особливо цінних та унікальних природних комплексів і забезпечення екологічної безпеки. Це сукупність державних, адміністративних, правових, економічних, політичних і суспільних заходів, спрямованих на раціональне використання, відтворення і збереження природних ресурсів землі, обмеження негативного впливу людської діяльності на навколишнє середовище.

Основними принципами охорони навколишнього природного середовища є (стаття 3 Закону):

- пріоритетність вимог екологічної безпеки, обов'язкове додержання екологічних стандартів, нормативів та лімітів використання природних ресурсів при здійсненні господарської, управлінської та іншої діяльності;

- гарантування екологічно безпечного середовища для життя і здоров'я людей;

- запобіжний характер заходів щодо охорони навколишнього природного середовища;

- екологізація матеріального виробництва на основі комплексності рішень у питаннях охорони навколишнього природного середовища, використання та відтворення відновлюваних природних ресурсів, широкого впровадження новітніх технологій;

- обов’язковість екологічної експертизи;

- гласність і демократизм при прийнятті рішень, реалізація яких впливає на стан навколишнього природного середовища, формування у населення екологічного світогляду;

- науково обґрунтоване нормування впливу господарської та іншої діяльності на навколишнє природне середовище;

- компенсація шкоди, заподіяної порушенням законодавства про охорону навколишнього природного середовища;

- встановлення екологічного податку, збору за спеціальне використання води, збору за спеціальне використання лісових ресурсів, плати за користування надрами відповідно до податкового кодексу України.

Законодавством України встановлюються нормативи використання природних ресурсів та інші екологічні нормативи.

Екологічні нормативи встановлюють гранично допустимі викиди та скиди у навколишнє природне середовище забруднюючих хімічних речовин, рівні допустимого шкідливого впливу на нього фізичних та біологічних факторів (стаття 33 Закону).

Нормативи гранично допустимих концентрацій забруднюючих речовин у навколишньому природному середовищі та рівні шкідливих фізичних та біологічних впливів на нього є єдиними для всієї території України. Підприємства, установи й організації, діяльність яких пов'язана з шкідливим впливом на навколишнє природне середовище, незалежно від часу введення їх у дію повинні бути обладнані спорудами, устаткуванням і пристроями для очищення викидів і скидів або їх знешкодження, зменшення впливу шкідливих факторів, а також приладами контролю за кількістю і складом забруднюючих речовин та за характеристиками шкідливих факторів (стаття 51 Закону).

6.2 Аналіз основних джерел впливу та їх наслідків на людину та її оточення

Електромагнітне поле - це сукупність електричного і магнітного полів, що породжують один одного при взаємодії електрично заряджених тіл. Хвилею називають зміну стану електромагнітного поля, що поширюється в просторі. Вони бувають: наддовгими (радіохвилі), терагерцеві, інфрачервоні, видиме світло, ультрафіолетові, рентгенівські й жорсткі (гамма). Хвилі поширюються всюди, в тому числі і в вакуумі. Випромінювання - це характеристика загасання поля в міру віддалення від джерела

виникнення. Залежить від довжини хвилі. Воно практично без загасання поширюється на величезні відстані, навіть в просторі, заповненим речовиною.

Навколо Землі існують електричне та магнітне поля, інтенсивність яких не залишається постійною. Спостерігаються річні, добові коливання цих полів під дією грозових розрядів, опадів, вітрів, а також під дією сонячної активності (магнітні бурі).

Біосфера впродовж своєї еволюції знаходилась під впливом електромагнітних полів (ЕМП), фонового випромінювання, викликаного природними чинниками. Навколо Землі існують електричне та магнітне поля, інтенсивність яких не залишається постійною. Спостерігаються річні, добові коливання цих полів під дією грозових розрядів, опадів, вітрів, а також під дією сонячної активності (магнітні бурі).

Можливі механізми біологічної дії електромагнітного поля.

Механізм дії електромагнітного випромінювання на живі організми то сих пір остаточно не розшифрований. Існує декілька гіпотез, що пояснюють біологічну дію електромагнітного поля. В основному вони зводяться до індиціюванню струмів в тканинах і безпосередньому впливу поля на клітковому рівні, в першу чергу з його впливом на мембранні структури. Вважається, що під дією електромагнітного поля може змінюватися швидкість дифузії через біологічні мембрани, орієнтація і конфірмація біологічних макромолекул, крім того, стан електронної структури вільних радикалів. Вочевидь, механізми біологічної дії електромагнітного поля мають, в основному, неспецифічний характер і пов’язані зі зміною активності регуляторних систем організму.

Вплив електромагнітного випромінювання на хімічні реакції.

Живі організми являють собою складні гетерогенні системи, в яких біоколоїдам і фізико-хімічним реакціям належить головна роль. На підставі неперервних багаторічних досліджень декількома вченими було показано, що швидкість реакції в колоїдних системах залежить від сонячної активності і розташування відносно геомагнітних полюсів, причому основна причина цього – зміна під впливом електромагнітного поля властивостей води – загального компонента реакцій в живих і неживих об’єктах.

Вплив електромагнітного поля на клітину.

Мішенню для ініціації будь-якого адаптуючого ефекту, в першу чергу, є мембрани, плазматичні і внутріклітинні, обмежуючі різні органели і внутріклітинні компоненти. Відома велика чутливість кліткових мембран до дії самих різних хімічних і фізичних агентів, у тому числі до опромінення. Морфологічні і функціональні порушення мембран виявляються практично відразу після опромінення і при дуже малих дозах. Зміна іонного складу, що виникає при цьому, може ініціювати в клітині проліферативні процеси. Окрім зміни проникності біологічних мембран і прискорення активного транспорту катіонів натрію, під впливом електромагнітного випромінювання відбувається активація перекисного окислення ненасичених жирних кислот і розгалуження процесів окислення і фосфорилірування в мітохондріях.

Вважається, що всі ці зміни на рівні клітини розвиваються з наступних причин:

Електромагнітне поле впливає на заряджені частинки і струми, внаслідок чого енергія поля на рівні клітини перетворюється в інші види енергії. Атоми і молекули в електричному поле поляризуються, полярні молекули орієнтуються по напрямку розповсюдження магнітного поля. В електролітах, якими є рідкі складові тканин, після впливу зовнішнього поля виникають іонні струми. Змінне електричне поле викликає нагрівання тканей живих організмів як за рахунок змінної поляризації діелектрика (суглобів, хрящів, кісток), так і за рахунок виникнення струмів провідності. Тепловий ефект є наслідком поглинання енергії електромагнітного поля. Чим більше напруженість поля і час впливу, тим сильніше виражені вказані ефекти. До величини в 10 мВт/м, умовно прийнятій за тепловий поріг, надлишкове тепло відводиться за рахунок механізму терморегуляції. Крім того, чутливість органів до перегрівання визначається їх будовою. Найбільш чутливими до перегрівання є органи зору, мозок, нирки, жовчний і сечовий міхур.

Вплив електромагнітного поля на нервову систему.

Перші експериментальні дослідження по впливу електромагнітного поля на нервову систему були проведені в СРСР. В монографіях професора Ю.А. Холодова

опубліковані результати його багаторічних досліджень по проблемі впливу електромагнітних і магнітних полів на центральну нервову систему. Було встановлено наявність прямої дії електромагнітного поля на мозок, мембрани нейронів, пам'ять, умовно-рефлекторну діяльність. В модельних експериментах показана можливість впливу слабких електромагнітних полів на процеси синтезу в нервових клітинах. Отримані чіткі зміни імпульсації коркових нейронів, що приводять до порушення інформації що передається в більш складні структури мозку. Р.І. Крутиковим виявлено, що при впливі електромагнітного поля в надвисокочастотному діапазоні може розвитися порушення короткочасної пам'яті.

Вплив електромагнітного випромінювання на імунну систему.

На теперішній час накопичено достатньо даних, що вказують на те, що при впливі електромагнітного поля порушуються процеси імуногенезу. Встановлено, що під впливом електромагнітного поля змінюється характер інфекційного процесу, виникають порушення білкового обміну, спостерігається зниження вмісту альбумінів і підвищення гамма-глобулінів в крові. Крім того, електромагнітне поле може виступати в якості алергену або пускового фактора, викликаючи важкі реакції у хворих алергіків при контакті з електромагнітним полем.

Вплив електромагнітного поля на статеву систему.

Під впливом електромагнітного випромінювання знижується функція сперматогенезу, змінюється менструальний цикл, уповільнюється ембріональний розвиток, виникають вроджені вади у новонароджених дітей і зменшення лактації у годуючих мам.

Вплив слабких електромагнітних полів на живі організми.

Слабкі електромагнітні поля при інтенсивності менш порогу теплового ефекту також впливають на зміни в живій тканині. Дослідження по біологічному впливу мобільного телефону, комп'ютерного блока і інших електронних засобів проведені в ряді російських наукових центрів, у тому числі - і на біологічному факультеті Московського державного університету. При цьому шкідливість електронних засобів

перевірялась як в робочому, так і у вимкненому стані пристрою, у тому числі і без джерел живлення.

Результати проведених досліджень по оцінці впливу мобільного телефону, комп'ютера і інших сучасних радіоелектронних засобів на різні організми як в робочому, так і у вимкненому стані виявились невтішними і показали вкрай негативний їх вплив на стан біологічних об'єктів, що виявилось:

- в зменшенні рухомої активності і виживаності мікроорганізмів;
- в збільшенні смертності мікроорганізмів;
- в погіршенні регенерації тканин;
- в порушенні ембріонального і личиночного розвитку;
- в зниженні біохімічних реакцій, порушенні метаболізму;
- в зниженні енергетичного потенціалу в усіх життєво важливих системах організму.

У процесі науково-технічного розвитку людство додало до фонового випромінювання цілий ряд факторів, які підсилили це випромінювання в декілька разів (антропогенні ЕМП). У побуті та промисловості набули масового застосування обладнання та прилади, робота яких пов'язана з утворенням електромагнітних випромінювань широкого діапазону частот. Зростання рівня ЕМП різко підсилилось з початку 30-х років XX століття. В окремих районах їх рівень в сотні разів перевищує рівень полів природного походження. Джерелами випромінювань електромагнітної енергії є потужні радіо та телевізійні станції, ретранслятори, засоби радіозв'язку різного призначення, в тому числі і супутникового, промислові установки високочастотного нагрівання металів, високовольтні лінії електропередач, електротранспорт, вимірювальні прилади, персональні комп'ютери (ПК).

В аеропортах та на військових об'єктах працюють потужні радіолокатори, які випромінюють в навколишнє середовище потоки електромагнітної енергії. Потужність та кількість джерел ЕМП постійно зростає.

Відомо, що навколо провідника, по якому протікає електричний струм, виникають електричне та магнітне поля. Якщо струм постійний, то ці поля існують незалежно одне від одного.

При змінному електричному струмі електричне та магнітне поля пов'язані між собою, становлячи єдине електромагнітне поле. При появі електричної напруги на струмоведучих частинах з’являється електричне поле (ЕП). Якщо електричне коло замкнуте, тобто по ньому протікає струм, це супроводжується появою магнітної складової поля, і в цьому випадку говорять про існування електромагнітного поля (ЕМП). Для характеристики ЕМП введено поняття напруженості його складових — електричного та магнітного полів. Одиницею вимірювання електричної складової поля Е прийнято $[{}^{\text{В}}/_{\text{м}}]$, а магнітної – Н -$[{}^{A}/_{\text{м}}]$.

Електрична та магнітна складові поля визначаються за формулами (6.1) та (6.2):

$$E = \frac{U}{l}, \tag{6.1}$$

$$H = \frac{I}{2\pi * R}, \tag{6.2}$$

де U — величина напруги, B; — відстань від джерела випромінювання до точки, в якій ведеться вимірювання, м; I - сила струму, А; R — радіус кола силової лінії поля провідника, м.

Оскільки струм, який викликає появу ЕМП, характеризується частотою, то електромагнітне поле також характеризується частотою коливань — f довжиною хвилі — λ . Між ними існує зв’язок, показаний у формулі (6.3):

$$\lambda = \frac{C}{f} = C * T \tag{6.3}$$

де C — 3*108 м/с — швидкість поширення радіохвиль; — частота коливань Гц; Т — період коливань, с.

Електромагнітні випромінювання з частотою від 3 до 3*10 Гц належать до радіочастотного діапазону.

У табл. 6.1 наведена номенклатура діапазонів частот ЕМП.

Таблиця 6.1 —Номенклатура діапазонів частот ЕМП

Назва діапазону	Діапазон частот	Довжина хвилі	Назва діапазону довжини хвиль
Низькі частоти НЧ	0.003…0.3 Гц 0.3…3.0 Гц 3.0…300 Гц 300 Гц…30 кГц	107…106 км 106…104 км 104…102 км 102…10 км	Інфранизькі Низькі Промислові Звукові
Високі частоти ВЧ	30…300 кГц 300 кГц…3 МГц 3…30 МГц	10…1 км 1 км…100 м 100…10 м	Довгі (кілометрові) Середні (гектаметрові) Короткі (декаметрові)
Ультрависокі частоти УВЧ	30…300 МГц	10…1 м	Ультракороткі
Надвисокі частоти НВЧ	300 МГц…3 ГГц 3…30 ГГц 30…300 ГГц	100…10 см 10…1 см 10… 1 мм	Дециметрові Сантиметрові Міліметрові

Електромагнітні поля діапазону частот 30 кГц — 300 ГГц поширюються у просторі без наявності провідника із струмом зі швидкістю, близькою до швид кості світла (300 000 км/с).

Інтенсивність поля в діапазоні частот 30 кГц — 300 МГц оцінюється напруженістю поля. У діапазоні 300 МГц — 300 ГГц поле оцінюється поверхневою густиною потоку енергії (ГПЕ), тобто кількість енергії, яка припадає в одиницю часу на одиницю площі. Одиницею виміру ГПЕ є $1\ {}^{\text{Вт}}/_{\text{м}^2}$.

6.3 Рекомендації щодо зниження негативних чинників електромагнітного поля

Вибір того чи іншого способу захисту від дії електромагнітних випромінювань залежить від робочого діапазону частот, характеру виконуваних робіт, напруженості та щільності потоку енергії ЕМП, необхідного ступеня захисту.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають таке розташування джерел ЕМП, яке б зводило до мінімуму їх вплив на працюючих, використання в умовах виробництва дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання, застосування засобів індивідуального захисту (халатів, комбінезонів із металізованої тканини, з виводом на заземлюючий пристрій). Для захисту очей доцільно використовувати захисні окуляри ЗП5-90. Скло окулярів вкрито напівпровідниковим оловом, що послаблює інтенсивність електромагнітної енергії при світлопропусканні не нижче 75%.

Взагалі, засоби індивідуального захисту необхідно використовувати лише тоді, коли інші захисні засоби неможливі чи недостатньо ефективні: при проходженні через зони опромінення підвищеної інтенсивності, при ремонтних і налагоджувальних роботах в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання трудових операцій, погіршують гігієнічні умови.

У радіочастотному діапазоні засоби індивідуального захисту працюють за принципом екранування людини з використанням відбиття і поглинання ЕМП. Для захисту тіла використовується одяг з металізованих тканин і радіопоглинаючих матеріалів. Металізовану тканину роблять із бавовняних ниток з розміщеним всередині

них тонким проводом, або з бавовняних чи капронових ниток, спірально обвитих металевим дротом. Така тканина, наче металева сітка, при відстані між нитками до 0,5 мм значно послаблює дію випромінювання. При зшиванні деталей захисного одягу треба забезпечити контакт ізольованих проводів. Тому електрогерметизацію швів здійснюють електропровідними масами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок неконтактуючих проводів.

Найбільш ефективним способом захисту є екранування. Електромагнітне поле послаблюється екраном внаслідок створення в його товщі поля протилежного напрямку. Ступінь ослаблення електромагнітного поля залежить від глибини проникнення високочастотного струму в товщу екрану. Чим більша магнітна проникність екрана і вище частота екрануючого поля, тим менша глибина проникнення і необхідна товщина екрана. Екранують або джерело випромінювань, або робоче місце.

Крім виконання своєї прямої функції, екранування значно знижує шкідливий вплив електромагнітних випромінювань на організм людини. Воно дозволяє також зменшити вплив електромагнітних шумів на роботу пристроїв.

Під час налагоджування, ремонту, випробування та експлуатації радіоелектронної апаратури електротермічних установок існує можливість опромінення обслуговуючого персоналу.

В зв'язку з цим необхідно здійснювати попередній розрахунок інтенсивності опромінення електромагнітного поля та передбачати використання засобів захисту від випромінювань.

При ізотропному випромінюванні напруженість електричної Е та магнітної Н складових поля у ближній зоні:

$$E = \frac{Il}{2\pi\omega\varepsilon r^3}; \tag{6.4}$$

$$\text{H} = \frac{Il}{4\pi r^2}; \tag{6.5}$$

де I - сила струму в провіднику (антені), А; l - довжина провідника (антени), м; ω - кругова частота поля; ε - діелектрична проникність середовища; r - відстань від джерела випромінювання до робочого місця, м.

В дальній зоні напруженість електричної та магнітної складових:

$$E = \frac{\sqrt{30P\sigma}}{r}; \tag{6.6}$$

$$H = \frac{\sqrt{P\sigma/30}}{4\pi r}; \tag{6.7}$$

де P - потужність випромінювання, Вт; σ - коефіцієнт підсилення антени.

При напрямленому випромінюванні щільність потоку енергії в ближній зоні по осі діаграми направленості випромінювання:

$$\psi_{\text{Б.З.}} = \frac{3\text{P}_{\text{СЕР}}}{S}; \tag{6.8}$$

де $P_{СЕР}$ - середня потужність випромінювання, Вт; S - площа випромінювальної системи, м^2.

Для установок, котрі працюють в імпульсному режимі, середня потужність:

$$\text{P}_{\text{СЕР}} = \frac{\text{P}_{\text{ІМП}}{}^{\tau}}{\text{T}_1}; \tag{6.9}$$

де: $P_{ІМП}$ - потужність випромінювання в імпульсному режимі; τ - тривалість імпульсу; T - період чергування імпульсів.

У проміжній зоні щільність потоку енергії:

$$\psi_{\text{П.З.}} = \frac{3\text{P}_{\text{СЕР}}}{S} \cdot \left(\frac{r_{\text{Б.З.}}}{r}\right); \tag{6.10}$$

де r - відстань від центра розкриття антени до даної точки, розташованої в проміжній зоні.

В дальній точці щільність потоку енергії по осі випромінювання:

$$\psi_{\text{Д.З.}} = \frac{\text{P}_{\text{СЕР}} \cdot \sigma}{4\pi r^2}; \tag{6.11}$$

Визначаємо допустиму величину магнітної складової поля з врахуванням, що допустима напруженість поля $\text{E}_{\text{П.Д.}}$= 5 В/м (за санітарними нормами):

$$\text{Н}_{\text{П.Д.}} = 1{,}27 \cdot 10^5 \frac{\text{Е}_{\text{П.Д.}}}{Xf} = 1{,}27 \cdot 10^5 \frac{5}{0{,}8 \cdot 6 \cdot 10^4} = 13{,}2\ \text{А/м}$$

Напруженість на робочому місці при відсутності екрана:

$$\text{Н}_{\text{х}} = \frac{\omega I a^2}{4X^2} = \frac{14 \cdot 380 \cdot 0{,}1^2}{4 \cdot 0{,}8^2} = 20{,}7\ \text{А/м}$$

Необхідна ефективність екранування на робочому місці:

$$\text{Н}_{\text{Х.Н.}} = \frac{\text{Н}_{\text{х}}}{\text{Н}_{\text{П.Д.}}} = \frac{20{,}7}{13{,}2} = 1{,}57.$$

Дійсна ефективність екранування на робочому місці:

$$\text{Е}_{\text{Х.Д.}} = \frac{Re^{\frac{d}{\delta}}}{2\sqrt{2}\delta\mu_e^1} = \frac{0{,}35 \cdot 0{,}3^{\frac{1}{0{,}32}}}{2\sqrt{2} \cdot 3{,}2 \cdot 10^{-4} \cdot 1} = 10{,}5,$$

де d - товщина екрана, мм; δ - глибина проникнення поля в екран, м; $\mu^1{}_e$ - відносна магнітна проникність екрана $\left(\mu_e^1 = \frac{\mu_e}{\mu_0}\right)$.

$$\delta = \frac{1}{\sqrt{\mu_\text{e}\gamma_\text{e}\omega f}} = \frac{1}{\sqrt{4\pi \cdot 10^{-7} \cdot 3{,}55 \cdot 10^7 \cdot 314 \cdot 6 \cdot 10^4}} = 0{,}32\text{мм}.$$

З конструктивних міркувань приймаємо d = 1 мм.

Таким чином, вибраний екран забезпечує необхідний захист на місці, оскільки $E_{х.д.} > E_{х.н.}$ *(10,5 > 1,57)*.

Лікарсько-профілактичні заходи передбачають проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП, обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань, видачу працюючим безкоштовного лікарсько-профілактичного харчування, перерви санітарно-оздоровчого характеру.

Таким чином, усвідомлення небезпеки дії електромагнітних полів та обізнаність у методах захисту від них є необхідною умовою для людини, що здійснює виявлення наявності електромагнітних полів у приміщенні.

6.4 Висновки з розділу

У зв'язку зі стрімким зростанням числа технологій виробництва радіолокаційних станцій уникнути впливу ЕМП в сучасному світі практично неможливо.

Вплив електромагнітних полів на біо-об’єкти залежить від багатьох чинників: типу поля і його характеристик, самого біо-об’єкта, а також від властивостей середовища, що його оточує. Сам вплив електромагнітних полів багатогранний, але можна зробити висновки, що найбільші зміни відбувається на клітинному рівні. Причому нагрівання тканин організму, за досить високої інтенсивності випромінювання, не значне. Тому можна стверджувати, що вплив на біо-об’єкти обумовлений взаємодіями електромагнітного поля з інформаційними електричними полями організму, що призводить до порушення природних ритмів і спричиняє фізіологічні порушення у вигляді радіохвильової хвороби.

Різні організації як державні, так і міжнародні розробили безліч стандартів і вимог для запобігання якого б то не було впливу електромагнітного поля на людину від радіолокаційних станцій. Майже всі РЛС, що реалізуються в ринкових умовах відповідають цим вимогам. Таким чином, можна зробити висновок, що дотримання санітарних і гігієнічних норм при містобудуванні і виконання необтяжливих рекомендацій з використання РЛС практично нівелює вплив електромагнітних полів на людину. Хоча це питання має і буде досліджуватися далі.

Окрім цього велике значення має дотримання правил дотримання електромагнітного захисту на підприємствах, враховуючи вік працівника, індивідуальні особливості, стан здоров′я.

ВИСНОВКИ

Відповідно до мети дипломної роботи у першому розділі було розглянуто типи дистанційно пілотовані повітряні судна та їх впровадження у загальний повітряний простір.

Відповідно до мети дипломної роботи у другому розділі було розглянуто архітектуру дистанційно пілотованих авіаційних систем, бортові системи зв'язку, навігації, спостереження, електронні системи обробки інформації та управління, ліній зв'язку та передавання дистанційно пілотованих авіаційних систем.

Відповідно до мети дипломної роботи у третьому розділі було розглянуто види організованої протидії нормальному функціонуванню дистанційно пілотованих авіаційних систем, види організованих радіозавад, загальні аспекти кібербезпеки.

Відповідно до мети дипломної роботи у четвертому розділі було наведено методи захисту дистанційно пілотованих авіаційних систем від кібератак, організаційні методи протидії кібератакам, криптографічні методи захисту, алгоритмічні методи захисту, програмні методи захисту.

Історично інформаційна безпека в авіації та аеронавігації в більшій мірі базувалася на організаційних процедурах і людський фактор, практично не спираючись на технології. Для відносно ізольованою системи це не погано працювало і навіть продовжує працювати, але з приходом нових парадигм і підходів (елементи IoT, розподілені системи, CDM, SWIM) системи перестають бути ізольованими. І цими погрозами все не обмежується. Сьогодні багато технологій доступні всім бажаючим. Наприклад, недорогий радіомодуль, який використовує методи SDR, дозволяє не тільки прийняти і декодувати практично будь-яке аеронавігаційне повідомлення, а й синтезувати сигнали аеронавігаційних систем в діапазоні від 100 кГц до 6 ГГц. А є і готові OpenSource програми. Вразлива більшість систем спостереження, навігації та зв'язку, починаючи з первинних радіолокаторів і закінчуючи системами, що використовують сигнали супутникових навігаційних систем.

Як правило, більшість заходів щодо забезпечення безпеки чинять негативний вплив на сам технологічної процес. Забезпечення захисту - це певний компроміс між впливом на технологічний процес і рівнем захищеності. Щоб чіткіше визначити основні загрози і правильно спланувати протидію їм, формується так звана «модель порушника», яка визначає його вигляд: цілі, мотивацію, обсяг залучених ресурсів, знання і можливості.

Питання захисту від кіберзагроз в аеронавігаційної галузі, вирішується індивідуально кожним провайдером на основі існуючих практик або стандартів.

В основі життєвого циклу безпеки взято деякий каркас управління ризиками, який передбачає безперервну оцінку ризиків, прийняття заходів по їх нейтралізації, моніторингу ефективності вжитих заходів і знову оцінку ризиків - і так безперервно. Важливо не зупиняти цей процес і постійно актуалізувати моделі можливих загроз, удосконалювати комплекс забезпечення інформаційної безпеки, забезпечуючи стійкість захищеного стану. Це типова модель забезпечення інформаційної безпеки, на основі якої будуються системи в усьому світі.

В структурі надання аеронавігаційних сервісів очевидний один з найменш охоплених засобами безпеки сегментів - радіоканал. На відміну від бортового обладнання, безпеку якого забезпечується дотриманням ряду спеціальних заходів, безпеку радіоканалу продовжує базуватися на припущенні «це нікому не цікаво», «пілот / диспетчер виявить і вживе заходів».

Одна з головних вимог в галузі - забезпечення міжнародної інтероперабельність з урахуванням реальної оснащеності повітряних суден, наземної інфраструктури. А це серйозно обмежує використання технологій забезпечення інформаційної безпеки. Для захисту передбачається застосування криптографічних засобів, включаючи відкритий розподіл ключів. Некриптографічні методи, як показує аналіз стандарту VDL-4, часто залишають помітні уразливості в системі безпеки.

Перспективи розвитку інформаційної безпеки в авіації насамперед, це вдосконалення моделі загроз, як стратегічне цілепокладання в сфері забезпечення

інформаційної безпеки, що дозволить ефективніше будувати комплекс заходів захисту. Друге - гармонізація підходів під егідою ІКАО. Третє - прихід в аеронавігації абсолютно нових технологій, пов'язаних з безпілотної авіації та забезпеченням безпеки її застосування. Технології, обрані відразу повинні враховувати вимоги інформаційної безпеки. Від захисту каналів управління і захисту від несанкціонованого доступу до станції зовнішнього пілота до технології контролю дотримання обмежень повітряного простору.

ПЕРЕЛІК ВИКОРИСТАНИ Х ДЖЕРЕЛ

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

3. Glossary and Acronyms (Archived) / European Commission. – (Accessed 03 Nov 2009). Режим доступу : //www.ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c

4. Haas E. Aeronautical channel modeling// IEEE Transactions on Vehicular Technology. 2002. V. 51. № 2.

5. National Military Strategy for Cyberspace Operations. – Режим доступу: //www.dod. gov/pubs/foi/ojcs/07-F-2105doc1.pdf

6. Richard V.N., Prasad R. OFDM wireless multimedia communication. Artech House Boston London. 2000.

7. Автономна некомерційна організація «Аналітичний центр« АЕРОНЕТ »(АНО« ЦЕНТР «АЕРОНЕТ»). Аналіз міжнародних і національних програм, нормативних актів і сучасних технологічних рішень, що відносяться до інтеграції безпілотних авіаційних систем в контрольоване і неконтрольоване повітряний простір, і пропозиції щодо їх вдосконалення в Російській Федерації.

8. Амелін К., Міллер А. Алгоритм уточнення місцезнаходження легкого БПЛА на основі калмановської фільтрації вимірів пеленгаційної типу // Інформаційні процеси, 2013.

9. Браїловський В.В., Гресь О.В., Косован Г.В. Радіомоніторинг та радіопротидія на об'єктах інформаційної діяльності. 2016.

10. В. Фурашев Сутність та визначення понять "інформаційна безпека" і "безпека інформації" // "Правова інформатика". – № 2(34)/2012.

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).