Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

на тему «Кіберфізична система виявлення БПЛА Shahed»

КвРКІП. 190195.22.01.44 ПЗ

Виконав: студент 2 курсу, група КІ2м-22-1 Підпис Присяжнюк О.О. Ініціали, прізвище

Керівник к.т.н., доцент Науковий ступінь, вчене звання Підпис Капустян М.В. Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
23 05 2024 р.

Хмельницький, 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"01" 09 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Присяжнюку Олександру Олександровичу

Прізвище, ім'я, по батькові студента

1. Тема проєкту (роботи) Кіберфізична система виявлення БПЛА Shahed

Керівник проєкту (роботи) Капустян М.В., к.т.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.01.2024 р. № 1

2. Строк подання студентом проєкту (роботи) на кафедру 01.05.2024 р.

3. Вихідні дані до проєкту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих способів та засобів виявлення БПЛА

Моделювання процесу виявлення БПЛА Shahed з використанням AIoT, геолокаційних даних та часу їхньої фіксації

Метод виявлення БПЛА Shahed

Кіберфізична система виявлення БПЛА Shahed

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_01_»_____09_____2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	01.09.2023	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.10.2023	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	01.11.2023	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.12.2023	виконано
5	Робота над науковою статтею	01.02.204	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2024	виконано
7	Робота над розділом 4 – планування та проведення експериментів для вирішення поставленої задачі, аналіз результатів	01.04.204	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2024	виконано
9	Попередній захист ДРМ	29.04.2024	виконано
10	Захист ДРМ на засіданні ЕК	До 23.05.2024	

Студент _____ Присяжнюк О.О.
Підпис Ініціали, прізвище

Керівник роботи _____ Капустян М.В.
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Кіберфізична система виявлення БПЛА Shahed.

Автор роботи: Присяжнюк Олександр Олександрович

Керівник роботи: Капустян М.В., к.т.н., доцент

Пояснювальна записка: 70 с., 26 рис., 2 табл., 2 дод., 83 джерела.

КІБЕРФІЗИЧНА СИСТЕМА, БПЛА, SHAHED, ДРОНИ, AIoT.

Об’єктом дослідження є процес виявлення БПЛА Shahed у повітряному просторі.

Предметом дослідження є метод та кіберфізична система з використанням AIoT для виявлення БПЛА Shahed.

Метою кваліфікаційної роботи магістра є покращення виявлення БПЛА Shahed у повітряному просторі України шляхом створення кіберфізичної системи з використанням AIoT, яка дозволяє ефективно виявляти БПЛА.

Для розв’язання поставлених задач використовувалися основні положення загальної теорії систем, теорії моделювання процесів, системного аналізу. Також при моделюванні процесу виявлення БПЛА використано методи концептуального моделювання, теоретико-множинні підходи, формування лонічного висновку.

Наукова новизна отриманих результатів:

− вперше розроблено архітектуру кіберфізичної системи для виявлення БПЛА Shahed, яка використовує AIoT для обробки геолокаційних даних в процесі виявлення БПЛА;

− вперше запропоновано використання AIoT для якісної та швидкої побудови маршрутів руху виявлених БПЛА.

На основі проведених досліджень розроблена архітектура та компоненти кіберфізичної системи для виявлення БПЛА , які дозволяють ефективно виявляти та відстежувати безпілотні літальні апарати.

Практична значимість отриманих результатів полягає у підвищенні безпеки та захисті важливих об’єктів від незаконного використання БПЛА завдяки вчасному виявленню. Також швидке та точне виявлення БПЛА дозволяє операторам ефективно реагувати на можливі загрози та вживати необхідні заходи безпеки. Швидке виявлення БПЛА дозволяють миттєво реагувати на можливі небезпечні ситуації та мінімізувати можливі наслідки.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

КФС – кіберфізична система

РЛС – радіолокаційна станція

РЕБ – система радіоелектронної боротьби

GPS – (Global Positioning System) система глобального позиціювання

ISM – (Industrial Scientific Medical) частотний діапазон

GNSS – (Global Navigation Satellite System) супутникова система навігації

ОС – операційна система

ЦОТЗ - цифровий оперативно-технологічний зв'язок

ОТЗ - оперативно-технологічний зв'язок

БПЛА – безпілотний літальний апарат

AIoT – (англ. Artificial Intelligence of Things) штучний інтелект речей

БД – бази даних

ШІ- штучний інтелект

ВСТУП

Безпілотний літальний апарат (БПЛА), також відомий як дрон, це повітряний транспортний засіб, який керується дистанційно або автономно без присутності людини на борту. Основні характеристики та опис БПЛА включають:.

1. Конструкція та компоненти:
- корпус;
- крила/гвинти;
- мотори;
- електроніка.
2. Типи БПЛА:
- роторні;
- фіксованого крила;
- гібридні.
3. Функції та застосування:
- військові;
- цивільні;
- наукові;
- комерційні.

Таким чином, БПЛА є універсальним інструментом, який знаходить застосування у різних галузях завдяки своїй здатності виконувати завдання, які раніше були недоступні або складні для виконання традиційними методами.

Актуальність роботи полягає в створені кіберфізичної системи для виявлення БПЛА. Розробка такої системи може сприяти підвищенню безпеки, ефективності та контролю за повітряним простором. Важливими аспектами роботи є розробка методу виявлення та відстеження БПЛА Shahed, інтеграція з існуючими системами безпеки та забезпечення високої точності та надійності системи в умовах реального використання.

Боротьба з БПЛА стає все більш актуальною через широке їх використання в різних галузях, включаючи комерційний сектор, а також ризики, пов'язані з можливими порушеннями безпеки та приватності. Використання штучного інтелекту розуміння речей (AIoT) в цій сфері може значно покращити здатність виявлення, ідентифікації та відстеження БПЛА. AIoT може допомогти в розвитку алгоритмів для розпізнавання патернів, аналізу даних, виявлення аномалій та прийняття швидких та точних рішень у реальному часі. Такий підхід може забезпечити більш ефективну та надійну систему контролю за БПЛА, що є важливим у забезпеченні безпеки та захисту від потенційних загроз.

Метою кваліфікаційної роботи магістра є метод виявлення та індентифікація БПЛА:

- виявлення БПЛА;
- відстеження;
- попередження про можливі загрози;
- інтеграція з існуючими системами безпеки;
- автоматизоване реагування;

Поставлена мета досягається розв’язанням таких основних задач:

- розробка ефективних алгоритмів виявлення;
- оптимізація роботи системи в реальному часі;
- вдосконалення системи через навчання;
- адаптація до змін у середовищі.

Об’єктом дослідження є кіберфізична система виявлення БПЛА Shahed.

Предметом дослідження є методи та технології, спрямовані на виявлення та ідентифікацію БПЛА Shahed у кіберфізичні системі.

Наукова новизна отриманих результатів:

1. Інтеграція сенсорів.
2. Оптимізація алгоритмів.
3. Архітектура системи.
4. Інтеграція з іншими системами.

Практична цінність отриманих результатів. В результаті виконаного наукового дослідження розроблено кіберфізичну систему виявлення БПЛА Shahed. Система включає в себе:

- апаратну частину;
- програмне забезпечення;
- система зв’язку;
- систему управління ресурсами;
- систему зберігання даних.

У даній роботі викладено вимоги до методології такі як:

- ефективність;
- надійність;
- адаптивність;
- безпека;
- ефективне використання ресурсів.

Для вирішення поставлених задач використовуються основні принципи:

1. Інтеграція сенсорів.
2. Обробка даних.
3. Реакція на загрозу.
4. Інтеграція з іншими системами.
5. Оптимізація ресурсів.

За темою кваліфікаційної роботи магістра опубліковано одну публікацію у Збірнику наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2023» (Хмельницький – 2023. – С. 250-251).

1 АНАЛІЗ ВІДОМИХ СПОСОБІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ БПЛА

1.1 Аналіз способів виявлення БПЛА

Принципи виявлення БПЛА можна сформулювати наступним чином:

1) чим менший БПЛА, тим менше площа поверхні, що розсіюється або відбиває, тим складніше техніці і станціям РЛС визначити і виявити дрон;

2) чим менші теплові та звукові сигнатури, тим складніше заздалегідь передбачити підліт техніки до пункту призначення або військової цілі.

Існують принаймні 4 основні способи виявлення та пеленгації БПЛА. Апарати є джерелами звуку, випромінюють енергію у всіх діапазонах, а також віддають спектр електромагнітних та акустичних хвиль у середовище, які засікають налаштовані спеціальні пристрої.

Будь-який БПЛА має ряд ознак, що демаскують. Це теплові (інфрачервоні), радіочастотні сигнатури. Основним джерелом шуму є двигун, гвинти. Джерела випромінювання радіочастотних сигналів - сама станція, що передає польотні дані апарату, та системи приймання та передачі сигналів, встановлених на дроні.

1.1.1 Радіолокаційний спосіб - виявлення радіочастотного rf діапозону

Radio Frequancy (RF) – радіочастоти, тобто виявлення БПЛА відбувається за рахунок випромінювання радіочастот апаратом в частотних діапазонах, в яких працює той чи інший тип повітряного транспорту. Випромінювання фіксується радарними системами, станціями РЛС, пеленгується і контур цілі відображається в радіолокаційному дисплеї. Як правило, звичайні цивільні дрони обмінюються радіосигналами на частотах 2.4 і 5.8 Ггц.

Фахівцями БПЛА розроблений ряд енергетичних показників, таких як показник Херста, дані і статистика також допомагають виявити радіо сигнали дрона.

Однак виявлення даної техніки за допомогою застосування радіолокаційного способу часто ускладнене з наступних причин:

- БПЛА мають малі форми, особливо це стосується апаратів, які запускаються з невеликих катапульт;
- апарати покриваються спеціальною фарбою, що зменшує відбивну здатність корпусу та комплектуючих БПЛА;
- застосовуються композитні матеріали, що значно зменшують випромінювання апарату.

1.1.2 Акустичний спосіб

Акустичний спосіб БПЛА один з найскладніших оскільки датчики і системи виявлення дрона по звуку працюють в невеликому діапазоні, є безліч перешкод в живій природі, при яких дані можуть спотворюватися. Радіус виявлення як правило, становить від 150 до 600 метрів, що дає зовсім небагато часу на відбиття атаки, якщо це буде бойовий дрон.

Політ апарату також визначається по звуковим сигнатурам, які виробляють гвинт, пропелер. Хорошим джерелом шуму є двигун з безперервними по частоті спектрами, системи охолодження, поршневі двигуни, вихлопний тракт глушника. Як правило, бензинові двигуни збільшують шум у міру зростання потужності роботи мотора. Електричні двигуни мають менші звукові характеристики, що значно ускладнює формування акустичного портрету БПЛА.

Виявлення апаратів за допомогою акустичних даних проводиться за допомогою спеціальних сенсорів, модулів акустичної розвідки.

1.1.3 Візуальний спосіб

Візуальний спосіб виявлення – один з найслабших і вразливих способів. Однак дозволяє виявити апарати на підльоті до мети. Особливо, якщо це дрон-камікадзе.

Для виявлення БПЛА в оптичному діапазоні є важливим аспектом сучасних систем безпеки та спостереження для цього використовуються різні методи та технології.

Також є спеціальні оптичні системи розпізнавання БПЛА, що працюють на дальності в 1.5-2 км.за координатами, переданими з радарів, оператор оптичного детектора виробляє виявлення, розпізнавання і підтвердження мети. Оптичний модуль може працювати як під управлінням людини, так і в автоматичному режимі самостійно шукати дрон.

1.1.4 Теплове виявлення

Апарати, особливо ті які працюють на бензинових двигунах, дуже сильно виділяють тепло і утворюють тепловий слід і сигнатуру. Ідентифікуються і виявляються БЛА за допомогою тепловізійних та інфрачервоних камер. Камери на оптичному модулі перемикаються в інфрачервоний режим спостереження за ціллю, шукається теплової рухомий слід в небі, визначаються координати, підтверджуються дані.

Якщо використовується один детектор (одна антена), пристрій може визначити тільки напрямок випромінювання джерела радіосигналу (дрон або пульт керування), відобразивши його у програмному забезпеченні на мапі, це здобувається завдяки вбудованому GPS та компасу у детекторі. Детектор вираховує напрямок джерела випромінювання радіосигналу відносно себе, а також знаючи свої координати та положення в просторі (завдяки GPS та компасу), можна отримати азимут сигналу з певної точки на рисунку 1.1.

Якщо використовується два і більше детекторів, рознесені в просторі на певній відстані, азимути сигналу (одного і того самого джерела випромінювання), на кожному з детекторів будуть не паралельні. Точка перетину цих азимутів буде визначати місцеположення джерела випромінювання, тобто дрона або пульта керування на рисунку 1.2.

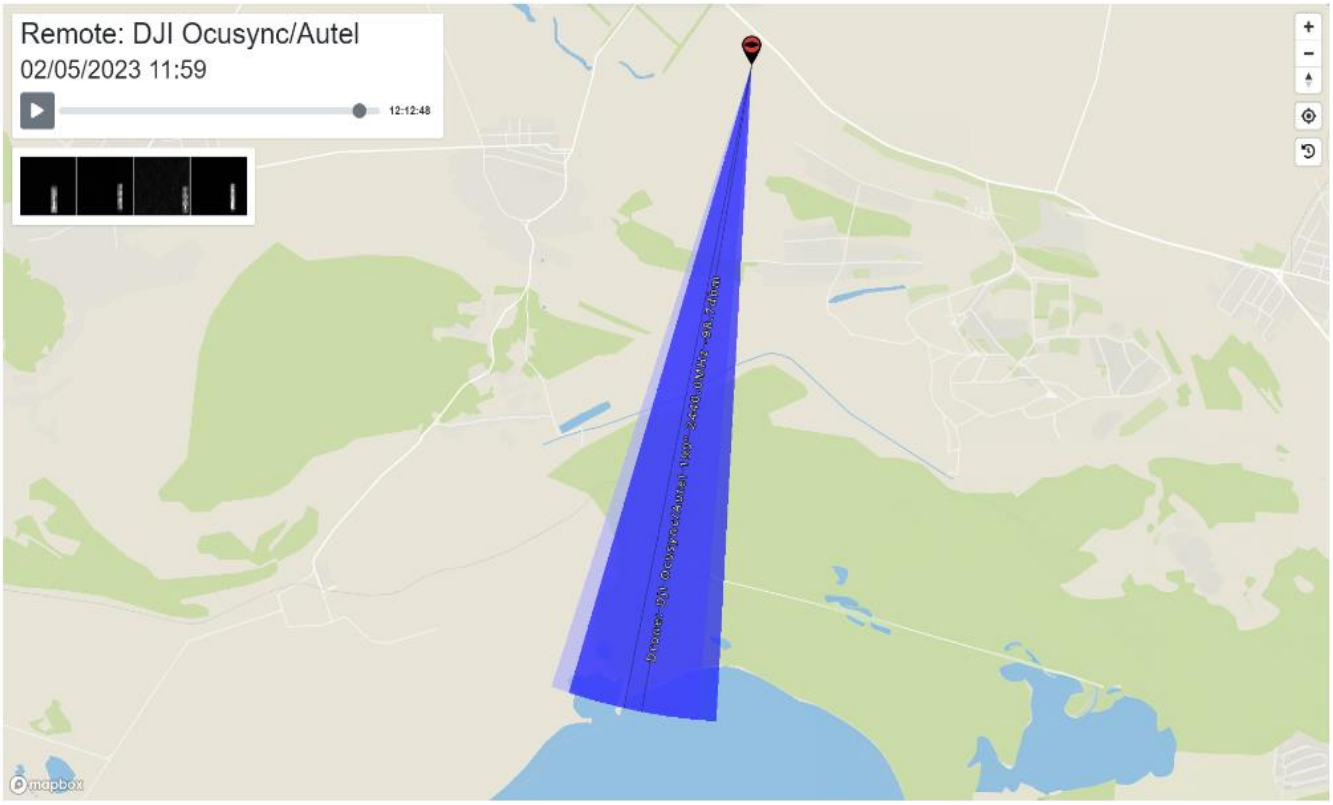


Рисунок 1.1 – Азимут сигналу з певної точки [73]

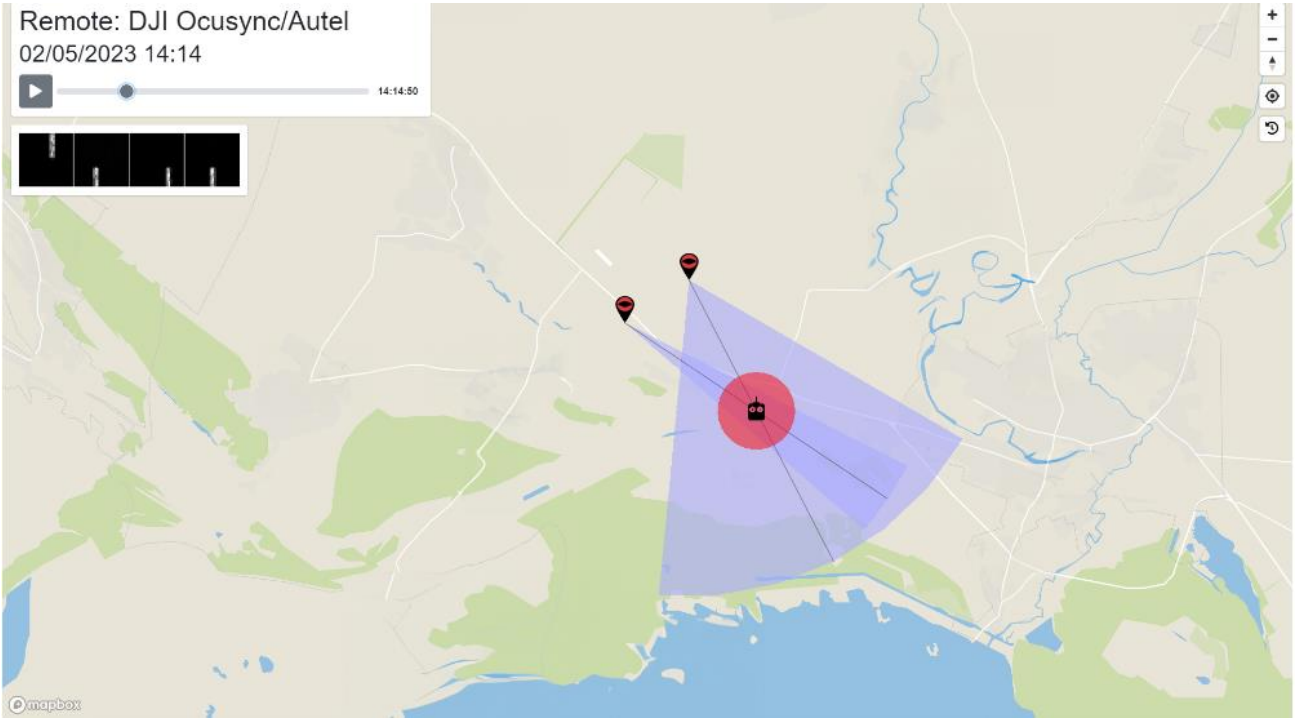


Рисунок 1.2 – Азимут сигналу перетину двох точок [73]

При умові сильної зашумленості радіо ефіру, дуже низьке співвідношення сигнал/шум, через що дуже важко виділити необхідний сигнал.

Для порівняння, візьмемо приклад:

У тихій кімнаті, ви можете чітко розрізнити слова людини з 10-15 метрів, а ось при умові знаходження на шумній вулиці, вам знадобиться скоротити відстань до людини щоб розрізнити слова людини на рисунку 1.3-1.4.

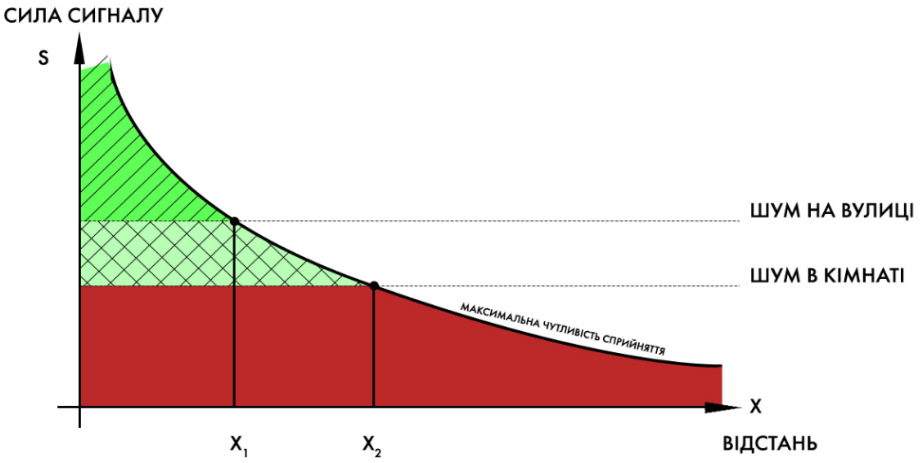


Рисунок 1.3 – Приклад різних сприймань чутливості [73]

X1 - максимальна відстань на якій чутно на вулиці

X2 - максимальна відстань на якій чутно в кімнаті

Рисунок 1.4 – Приклад різних сприймань чутливості [73]

Також, необхідно зазначити, що різні БПЛА мають різну потужність передавача, тому відстань ідентифікації може бути різною.

1.2 Засоби виявлення БПЛА

Радіолокаційні станції можна поділити на кілька видів. Це пасивні прості системи, при виявленні випромінювань і робіт дрона на типових діапазонах частот для комерційного безпілотного транспорту, система виробляє пеленг і передає координати і дані польоту на станцію управління, дальність виявлення до 1 км зображено на рисунку 1.5.

Є більш потужні системи з фазованою решіткою, такі мобільні радари засікають дрон на видаленні до 2 км.більш потужні радари здатні ідентифікувати ціль на видаленні до 3-3. 5 км.

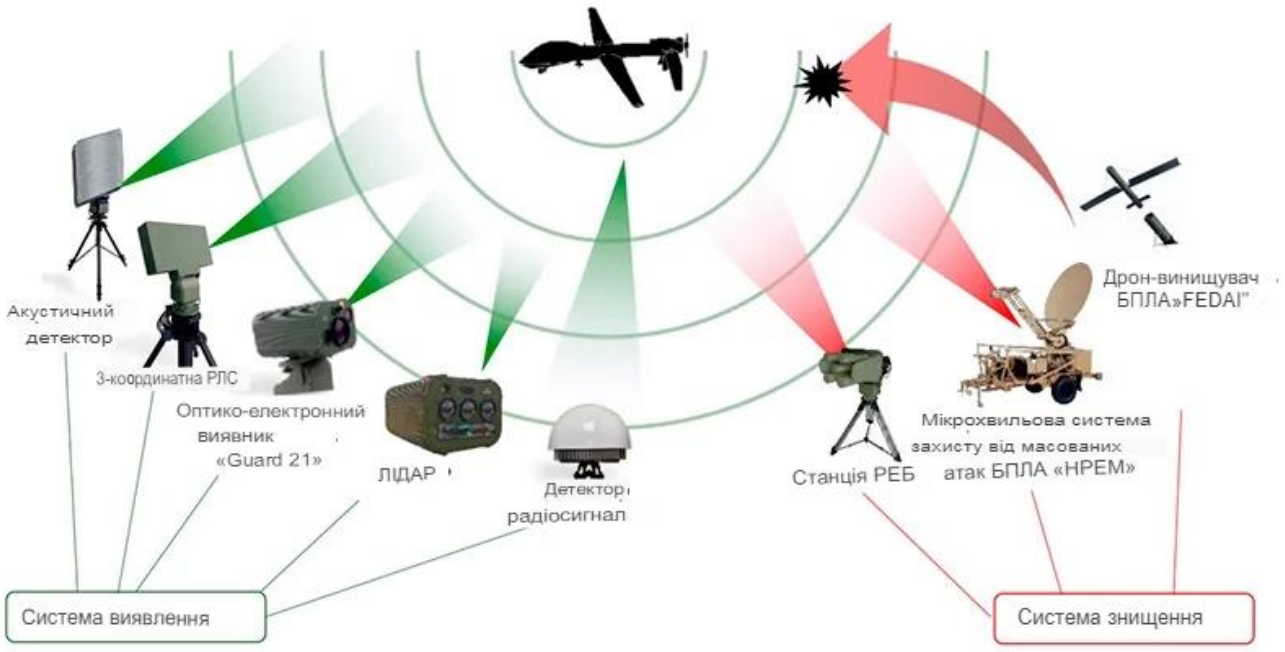


Рисунок 1.5 – Системи виявлення БПЛА [69]

1.2.1 Антидронна система Aaronia

Система Aaronia дозволяє захищати місце від несанкціонованого доступу дронами і є локальним засобом захисту.

Характеристики системи Aaronia:

- діапазон частот: 9 кГц - 20 ГГц;

- дальність виявлення - до 3-4 км;
- тривалість роботи-безперервний моніторинг 24/7 із записом даних на сервер;
- покриття-360 градусів;
- можливість встановити джерело випромінювання сигналу (знаходження оператора);
- є можливість масштабування і установки додаткових підстанцій.

1.2.2 Система RD1000

Ця система зазвичай включають різні сенсори, такі як радари, оптичні камери, тепловізори та інші, щоб виявляти і відстежувати БПЛА в реальному часі.

Характеристики системи RD1000:

- це спеціальний мобільний 2D радар для виявлення БПЛА до 1 км.працює пристрій на частотах 5 -5.8 GHz;
- 2D-радар активна фазована антенна решітка РЛС (імпульсний Допплер);
- радар працює на частотах: C-band (5.5-5.8 ГГц);
- радар працює на відстані від БПЛА-ЕПР≈0.01 м²;
- кут перевищення цілі ±20 градусів;
- точність визначення дистанції ≤5 м;
- точність визначення по азимуту ≤ 1 градуса;
- можливість визначення швидкості дрона від 0,2 м/з до 30 м / з;
- точність визначення швидкості: ≤ 0,2 м / сек;
- пікова випромінювана потужність на панель: 4 Вт;
- розміри станції 775 мм х 775 мм х 1100 мм;
- рівень (клас) захисту: IP65;
- інтерфейс: Ethernet;
- станція працює при температурах від -20 °С до + 60 °С.

1.2.3 Система RD3000

Більш потужні системи виявлення безпілотних об'єктів, що летять, - це спеціальні станції СТОПДРОН-ГОРИЗОНТ і RD3000.2D / 3D радар від компанії Glory Air. Апарати застосовуються для виявлення середніх і міні-дронів на середній віддаленості від мети.

Характеристики системи RD3000:

- 3D активна фазована антенна решітка РЛС (імпульсний, Доплера);
- діапазон частот радара C-band (5,5-5,8 ГГц);
- вилучення об'єкта 2500-3000 км (БПЛА), ЕПР≈0.01 м²;
- кут перевищення мети ±20 градусів;
- азімут мети 360 градусів;
- точність визначення дистанції ≤ 5 м;
- точність визначення азимуту ≤ 1 градуса;
- визначення швидкості БПЛА від 0,2 до 30 м/с;
- точність визначення швидкості ≤ 0,2 м/с;
- пікова випромінювана потужність 120 Вт/панель.

1.2.4 Оптична система виявлення дрона

Оптичні системи також грають не останню роль в роботі по виявленню безпілотників. У просторі, під радаром, яке вже не бачать радарні системи, у підстилає поверхні, оптичні системи допомагають своєчасно виявити і нейтралізувати наближається БПЛА.

Характеристики оптичної системи:

- час безперервної роботи: цілодобово (в т.ч. IR-камера);
- оптична камера: до 2 км (БПЛА);
- тепловізор: БПЛА - до 2800 м, наземні цілі - до 8000 м;
- роздільна здатність тепловізора: 640×512 пікселів;

- роздільна здатність камери: 1920×1080 пікселів;
- дистанція розпізнавання та стеження: до 1200 м;
- збільшення: 36-кратне оптичне;
- кут по азимуту: від 0 до 360 градусів;
- кут по вертикалі: від -50 ° до 40 ° С;
- середнє напрацювання на відмову: більше 10 000 годин;
- потужність: 100 Вт;
- вага: 25 кг;
- розміри: 646×411×330 мм.

1.2.5 Дедрон Сенсор RF-360

Системи виявлення дронів побудовані на тому, що будь-яка техніка випромінює сигнали та приймає сигнали від станції управління. Йде інтенсивний радіо обмін захищеними каналами даними телеметрії, передається відео зображення з дрона на станцію управління.

Від станції управління випромінюються радіосигнали, що містять пакети даних із командами апарату. У будь-якому випадку апарат у пасивному режимі все одно передає на станції свої геодані, дані по висоті, швидкості польоту, прольоту контрольних точок.

DedroneSensor RF-360 - це пасивний, підключений до мережі радіочастотний датчик для виявлення, класифікації та (гео)локації дронів та їх пультів дистанційного керування.

Система знаходить дрони та їх пульти дистанційного керування та відображає їх на карті. Виявлення дронів та пеленгація об'єктів може відбуватися на великих відстанях, до 5 км.

Система дозволяє збирати, накопичувати та зберігати дані на хмарі, в автоматичному режимі підвантажуючи інформацію до хмарного сховища.

Характеристики дедрон сенсора RF-360:

- розпізнавання об'єкта – до 5 км за ідеальних умов, до 2 км виявляє практично всі дрони;
- тип пристрою – вся спрямована система пасивного виявлення;
- розміри (довжина, ширина, висота) - 300 мм х 300 мм х 405 мм;
- маса – 7 кг;
- клас захисту - IP65;
- робоча температура - від -20ºС до +55ºС;
- браузерне програмне забезпечення — DedroneTracker;
- Час розгортання та налаштування – до 3 хвилин.

1.3 Система виявлення дронів Rantelon DTS-2458

Rantelon розробляє технології для виявлення, ідентифікації комерційних БПЛА. Такі БПЛА зазвичай використовують промислові, наукові та медичні (ISM) діапазони радіочастот (РЧ) для дистанційного керування БПЛА із наземної станції. Розроблена технологія протидії безпілотної системи (C-UAS) базується на виявленні, ідентифікації цих сигналів дистанційного керування, а також сигналів, які поширюються в протилежному напрямку, від БПЛА до наземної станції.

Крім того, Rantelon інтегрував у системи C-UAS можливості для запобігання використання БПЛА різних глобальних навігаційних супутникових систем (GNSS), щоб запобігти зловмисним БПЛА виконувати заздалегідь запрограмовані місії, покладаючись на GNSS для навігації на рисунку 1.6.

Управління даними та штучний інтелект є ключовими аспектами досліджень і розробок Rantelon C-UAS. Це пояснюється тим, що основною проблемою виявлення та ідентифікації БПЛА за допомогою радіочастотних датчиків є розрізнення різних форм сигналу, що використовуються різними БАС та іншими користувачами спектру, які не обов’язково є БПЛА. Штучний інтелект забезпечує ефективний і точний метод класифікації різних форм хвиль, які використовуються БПЛА та іншими користувачами спектру. Дійсно, системи на основі штучного інтелекту перевершують класичні системи ідентифікації в

широкому діапазоні застосувань. Управління та збір даних, з іншого боку, дозволяє будувати моделі штучного інтелекту та досягати необхідної точності.

Продовжуючи вибір технологій від виявлення та ідентифікації, радіочастотна ідентифікація є і, швидше за все, буде однією з основних концепцій у протидії ворожим дистанційно керованим БПЛА. Це охоплює прості атаки на відмову в обслуговуванні через перешкоди, а також більш складні підходи через спуфінг.

Система не має випромінювання, тобто працює в пасивному режимі, скануючи певні частоти.

Ключові особливості детектора:

- виявлення в режимі реального часу радіочастотних передач дронів;
- також виявляє пульт дистанційного керування дроном;
- виявляє необмежену кількість дронів;
- дальність виявлення подібна до корисної відстані від оператора до дрона;
- ідентифікація типу дрона (наприклад, DJI Mavic, Autel Evo тощо);
- висока точність відстеження до 10°;
- раннє виявлення (як тільки дрон увімкнувся);
- низький рівень хибнопозитивних результатів (наприклад, не виявляє птахів і повітряні кулі);
- охоплює діапазони частот 2,4 ГГц і 5 ГГц;
- працює в умовах міста;
- актуальна база дронів;
- додавання спеціальних дронів за запитом клієнта;
- вбудовані модулі GNSS і компаса;
- геолокація з кількома системами детекторів;
- інтегрований приймач ADS-B;
- інтеграція з системами перешкод.

Система виявлення дронів Rantelon DTS-2458 попереджає оператора, коли дрони знаходяться поблизу. Система не має обмежень щодо дальності виявлення,

але зазвичай вона порівнюється з максимальною відстанню між дроном і пультом дистанційного керування, тобто дальність виявлення залежить від потужності передавача дрона.

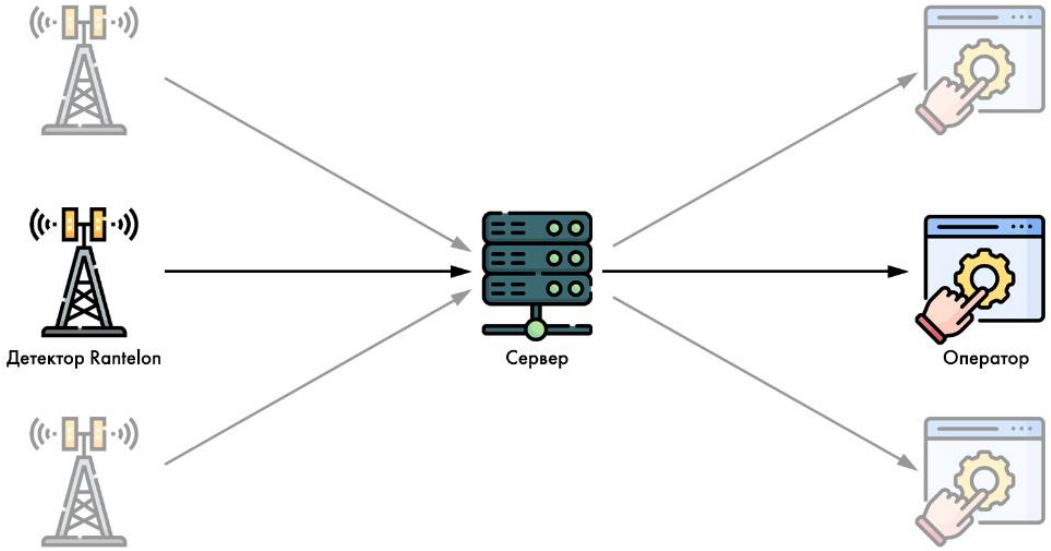


Рисунок 1.6 – Схема обробки даних на прикладі детектора Rantelon [73]

Система виявляє радіочастотне випромінювання, як тільки випромінювач вмикається, що дозволяє виявити дрон до того, як він злетить. Крім того, приймач визначає саме джерело радіовипромінювання тому на нього не впливають інші повітряні об’єкти, такі як птахи, повітряні кулі тощо. Окрім визначення напрямку та присутності дрона, система також здатна визначати напрямок пульта дистанційного керування.

Система складається з антени стеження, програмного забезпечення що має зрозумілий інтерфейс для аналізу. Кілька систем можна з’єднати разом для точного місцезнаходження дронів і пультів.

1.3.1 Принцип роботи детектора Rantelon DTS-2458

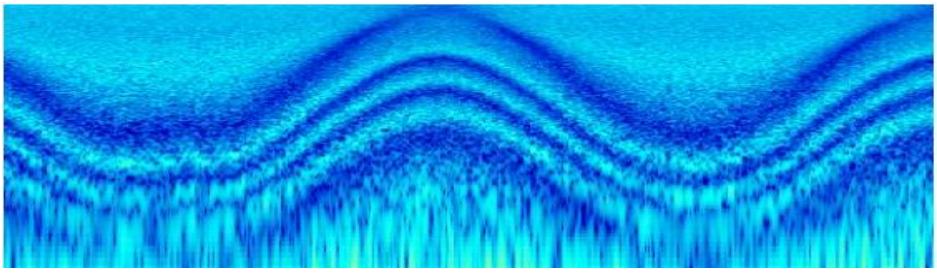
Система виявлення дронів Rantelon DTS-2458 заснована на спрямованому вимірюванні спектрограми та частоти дрона та його дистанційного керування в реальному часі.

Цим методом визначається вже відомі сигнали від дронів та їх пультів (спектрограми) та їх напрямок. Напрямок визначається по силі виділеного сигналу на кожну з восьми секторних антен.

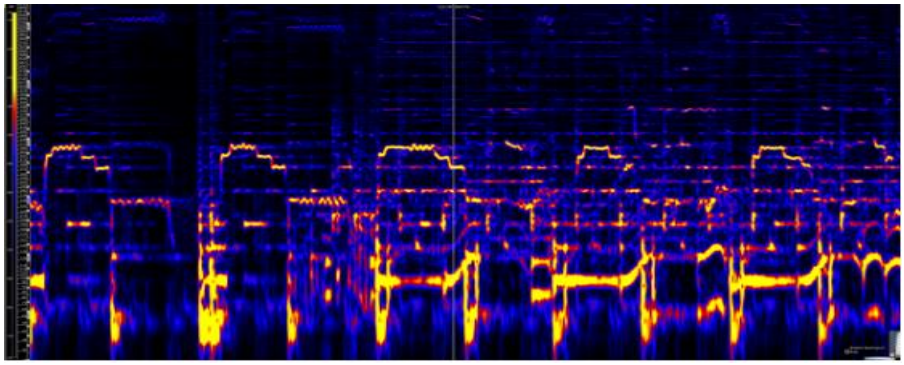
Спектрограма - візуальне зображення спектру частот сигналу в часі. Як аналогію можна взяти за приклад - сонографи, це звуковий «відбиток» того чи іншого звуку що зазвичай використовується для аналізу звуків тварин.

Іншими словами, детектор Rantelon «чує» знайомий йому «голос» в радіоефірі і розрізняє типи та навіть моделі пристроїв, між моделями та виробниками дронів різні «голоси».

На рисунках 1.7 наведено приклади роботи спектограми детектора Rantelon DTS-2458: а) на цьому зображенні видно кілька хвилеподібних візерунків, які можуть бути інтерпретовані як певні частотні моделі, характерні для різних сигналів; б) на цьому зображенні можна бачити складну структуру частотних компонентів з різними рівнями інтенсивності, що вказує на наявність декількох сигналів з різними частотами і змінною інтенсивністю.



а)



б)

Рисунок 1.7 – Приклади роботи спектограми детектора Rantelon DTS-2458 [73]

Детектор Rantelon DTS-2458 працює за принципом виявлення радіочастотних сигналів, що випромінюються дронами та їхніми пультами дистанційного керування. Принцип його роботи:

1. Вимірювання RF-емісій система здійснює спрямоване вимірювання спектрограм та частот у реальному часі, охоплюючи діапазони 2.4 GHz та 5.8 GHz. Це дозволяє виявляти дрони, як тільки їхні передавачі активуються, навіть до зльоту дрона.

2. Виявлення та ідентифікація DTS-2458 здатний не лише визначити наявність дрона, але й ідентифікувати його тип та модель (наприклад, DJI Mavic). Система розрізняє "голоси" різних дронів за їх радіочастотними сигналами.

3. Напрямок та геолокація система складається з антени стеження та програмного забезпечення для аналізу сигналів. Вона визначає напрямок до дрона та пульта керування по силі сигналу, що надходить на кожну з восьми секторних антен. Для точнішого визначення місця розташування дронів можуть бути об'єднані кілька таких детекторів, що дозволяє використовувати метод тріангуляції для геолокації.

4. Інтеграція DTS-2458 може бути інтегрована з системами глушіння дронів та іншими засобами протидії, а також з базами даних для актуалізації інформації про нові моделі дронів.

В таблиці 1.1 представлено характеристики різних видів БПЛА.

Таблиця 1.1 – Характеристика різних типів шахедів

Модель	Радіус дії	Довжина	Максимальна дальність	Розмах крил	Витривалість	Швикість	Висота польоту	Роль
Shahed 136	1000 км	3,5 м	2500 км	2,5 м	11 годин	185 км/год	7620 м	Розвідувально-бойова

Кінець таблиці 1.1 – Характеристика різних типів шахедів

Shahed 141	1300 км	1,9 м	2600 км	5,13 м	12 годин	220 км/год	4572 м	Розвідка
Shahed 161	150 км	1,9 м	300 км	5,13 м	3 години	350 км/год	7620 м	Розвідувально-бойова
Shahed 171	2200 км	4,75 м	4400 км	13 м	10 годин	460 км/год	12000 м	Розвідка
Shahed 181	1150 км	2,7 м	3450 км	7,3 м	13 годин	220 км/год	4572 м	Розвідувально-бойова
Shahed 191	500 км	2,7 м	1500 км	7,3 м	4,5 годин	350 км/год	9144 м	Розвідувально-бойова

Основними варіантами застосування БПЛА Shahed є:

1. Обхід БПЛА зон з розвиненою системою ППО (рисунок 1.8).

2. Можуть бути використані для наведення високоточної зброї, надаючи координати цілей для артилерійських або ракетних ударів.

3. Нанесення ударів великою кількістю БПЛА типу “камікадзе” (рисунок 1.9).

Рисунок 1.8 – Обхід зони роботи ППО противника [43]

БПЛА Shahed-136, також відомі як "дрони-камікадзе", активно застосовуються Росією під час війни в Україні. З початку вторгнення в лютому

2022 року ці дрони використовуються для атак на критичну інфраструктуру України, зокрема енергетичні об'єкти. Їх метою є знищення електромереж, щоб позбавити населення світла та тепла, особливо в зимовий період.

Рисунок 1.9 – Нанесення ударів великою кількістю БПЛА типу “камікадзе” [43]

Організація виявлення БПЛА включає кілька ключових етапів і технологій, які дозволяють ефективно ідентифікувати, відстежувати та реагувати на загрозу від дронів. Основні складові організації виявлення БПЛА:

1. Системи аналізу та обробки даних:

- програмне забезпечення для обробки зображень використовує алгоритми комп'ютерного зору для автоматичного розпізнавання та відстеження дронів на відео та зображеннях;

- машинне навчання та штучний інтелект застосовуються для підвищення точності виявлення та класифікації БПЛА, аналізу радіочастотних спектрів та ідентифікації типу дронів.

2. Інтеграція з іншими системами:

- системи радіоелектронної боротьби можуть бути інтегровані для глушіння сигналів управління дронами або їх навігаційних систем;

- системи протидії включають засоби фізичного знищення дронів, такі як протиповітряні ракети, системи лазерного ураження, мережі для захоплення дронів.

3. Оперативні центри та мережі спостереження:

- центри моніторингу та управління забезпечують централізоване спостереження за повітряним простором, аналіз даних і координацію дій у випадку виявлення загрози;

- інтегровані мережі сенсорів розміщення сенсорів і детекторів на ключових об'єктах та в стратегічних точках для створення мережі спостереження, яка покриває велику територію.

Ці компоненти дозволяють створити ефективну систему виявлення та протидії БПЛА, що забезпечує безпеку як військових об'єктів, так і цивільної інфраструктури.

Виявлення та знищення БПЛА є критично важливими завданнями для забезпечення безпеки військових і цивільних об'єктів зображено на рисунку 1.10. Це досягається за допомогою комплексного підходу, який включає використання різноманітних технологій для виявлення, відстеження та нейтралізації дронів. Основні методи та технології, що використовуються для цих цілей.

Знищення БПЛА:

1. Системи радіоелектронної боротьби (РЕБ):

- глушіння сигналів втручання в радіочастотні канали зв'язку між дроном та його пультом управління, що призводить до втрати управління дроном;

- порушення GPS-навігації глушіння або спотворення сигналів GPS, що використовується дронами для навігації.

2. Кінетичні системи:

- зенітно-ракетні комплекси (ЗРК) використовують ракети для знищення дронів на великій відстані;

- лазерні системи використовують високоенергетичні лазери для знищення або пошкодження дронів на відстані;

- системи з використанням мереж використовують спеціальні мережі для захоплення дронів в повітрі.

3. БПЛА-перехоплювачі використовують інші дрони, оснащені засобами для захоплення або знищення ворожих БПЛА.

4. Автоматизовані системи виявлення та реагування використовують алгоритми машинного навчання для автоматичного виявлення та реагування на загрозу з боку дронів, координуючи дії різних систем протидії.

Ефективне виявлення та знищення БПЛА потребує інтеграції різних систем і координації між ними. Це включає створення центральних командних центрів, які обробляють дані від різних сенсорів і забезпечують швидке прийняття рішень щодо протидії загрозам.

Завдяки комплексному підходу та використанню передових технологій, сучасні системи виявлення та знищення БПЛА забезпечують високий рівень захисту від цієї зростаючої загрози.

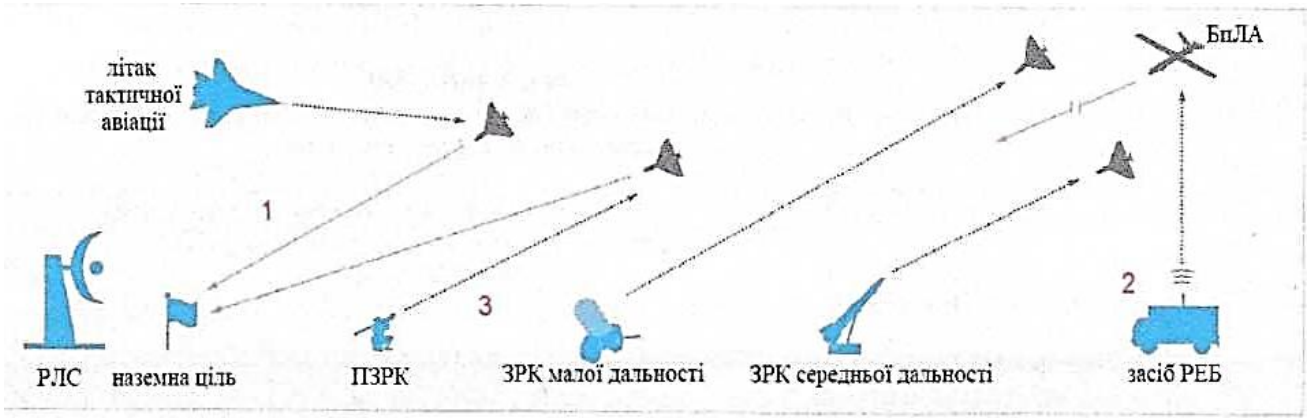


Рисунок 1.10 – Виявлення та знищення БПЛА [43]

БПЛА Shahed-136 є однією з основних загроз, які використовуються під час конфліктів. Щоб ефективно боротися з цими дронами, важливо знати ключові аспекти їх виявлення та знищення. На рисунку 1.11 наведено основні рекомендації та заходи з ураження Shahed-136 такі як:

- знайти ціль;
- визначити випередження;
- визначити напрямок польоту;
- відкрити вогонь по цілі.

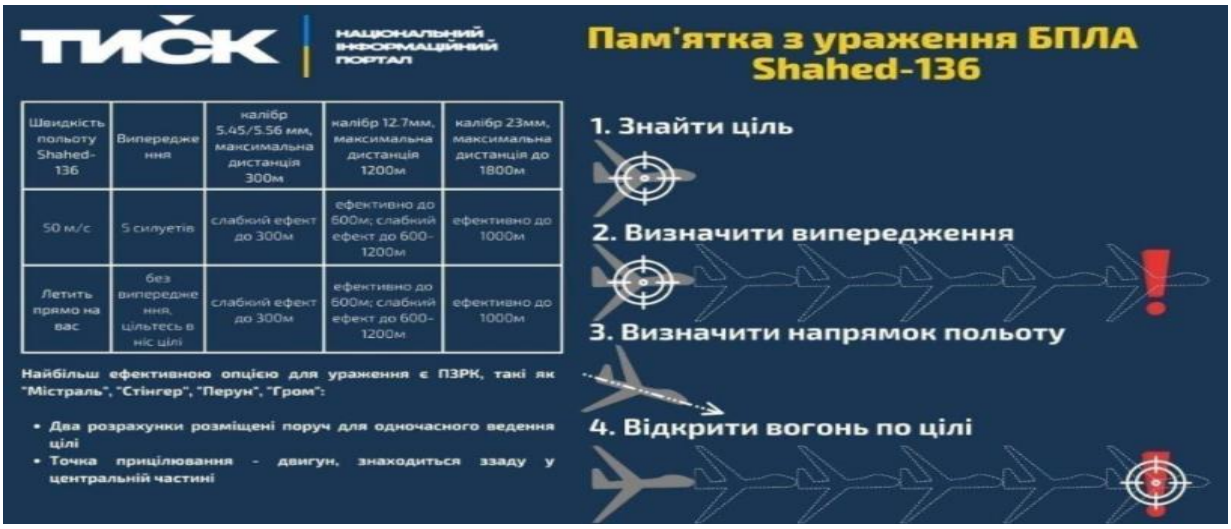


Рисунок 1.11 – Пам’ятка з ураження БПЛА Shahed [43]

1.4 Висновки

У першому розділі розглянуто відомі методи, способи та засоби для виявлення безпілотника Shahed, його характеристики, а також варіанти застосування, виявлення і боротьби з БПЛА.

2 МОДЕЛЮВАННЯ ПРОЦЕСУ ВИЯВЛЕННЯ БПЛА SHAHED З ВИКОРИСТАННЯМ AIoT, ГЕОЛОКАЦІЙНИХ ДАНИХ ТА ЧАСУ ЇХНЬОЇ ФІКСАЦІЇ

2.1 Компоненти для виявлення БПЛА

Архітектура кіберфізичної системи описує структуру, компоненти та взаємозв'язки між програмним та апаратним забезпеченням, що створюють її функціональність. Основні принципи архітектури включають в себе інтеграцію обчислювальних та фізичних процесів, розподіленість, високу надійність та ефективність. Ключові компоненти архітектури кіберфізичної системи:

- сенсори та актуатори;
- мережеві комунікації;
- обчислювальні ресурси;
- програмне забезпечення;
- інтерфейс користувача;
- безпека;
- управління ресурсами.

На рисунку 2.1 представлена архітектура кіберфізичної системи (КФС), яка складається з двох основних частин: кіберсистеми і фізичної системи.

Компоненти кіберфізичної системи:

1. Кіберсистема:

- вбудований контролер - це центральний обчислювальний компонент, який збирає, обробляє і аналізує дані, отримані від сенсорів, і приймає рішення на основі цих даних. Вбудовані контролери можуть включати мікропроцесори, пам'ять і інтерфейси для зв'язку з іншими компонентами;
- виконавчі елементи (ВК) вони отримують команди від вбудованого контролера і виконують фізичні дії, наприклад, переміщення механізмів, регулювання параметрів або запуск виконавчих пристроїв.

Рисунок 2.1 – Архітектура кіберфізичної системи [56]

2. Фізична система:

- сенсори - це пристрої, які збирають дані з фізичного середовища, такі як температура, тиск, вологість, швидкість і т.д. Сенсори передають зібрані дані до вбудованого контролера для подальшої обробки;

- фізичний процес - це реальний об'єкт або явище, що контролюється кіберфізичною системою. Фізичний процес може включати в себе механічні, електричні або хімічні процеси, які відбуваються в системі. Принцип роботи:

1. Збір даних сенсори вимірюють параметри фізичного процесу і передають ці дані до вбудованого контролера.

2. Обробка даних вбудований контролер обробляє отримані дані, використовуючи алгоритми для аналізу і прийняття рішень.

3. Прийняття рішень на основі оброблених даних контролер визначає необхідні дії для керування фізичним процесом.

4. Виконання дій виконавчі елементи виконують команди, змінюючи стан фізичної системи або її параметри.

5. Зворотній зв'язок система отримує зворотній зв'язок про результати виконаних дій, що дозволяє контролеру адаптувати алгоритми і покращувати ефективність керування.

Кіберфізичні системи використовуються в багатьох галузях, таких як:

1. Промисловість:

- промисловість Інтернет речей (IIoT) відстеження стану обладнання, оптимізація виробничих процесів, прогнозування обслуговування та зниження витрат;

- автоматизація виробництва використання роботів та автоматизованих систем для підвищення ефективності та продуктивності.

2. Транспорт:

- автономні транспортні засоби самокеровані автомобілі, які використовують КФС для прийняття рішень у режимі реального часу;

- інтелектуальні транспортні системи (ITS) управління рухом, запобігання аваріям, оптимізація маршрутів та зменшення заторів.

3. Енергетика:

- розумні мережі (Smart Grids) оптимізація виробництва та споживання енергії, інтеграція відновлюваних джерел енергії, підвищення стабільності енергопостачання;

- управління енергоспоживанням відстеження та оптимізація споживання енергії в будівлях і на підприємствах.

4. Охорона здоров’я:

- теле-медицина віддалений моніторинг стану здоров'я пацієнтів, дистанційна діагностика та консультації;

- імплантовані медичні пристрої інтелектуальні сенсори та пристрої для моніторингу та лікування хронічних захворювань.

5. Розумні міста(Smart Cities):

- інфраструктура міста управління освітленням, водопостачанням, відходами та іншими комунальними послугами;

- безпека та моніторинг використання КФС для моніторингу безпеки громадських місць, виявлення та реагування на надзвичайні ситуації.

6. Сільське господарство:

- розумне фермерство моніторинг стану ґрунту, вологи, погодних умов для оптимізації врожайності;

- автономні агродрони використання дронів для посіву, зрошення та збору врожаю.

7. Військова справа:

- Безпілотні літальні апарати (БПЛА) використання дронів для розвідки, спостереження та виконання бойових завдань;

- системи безпеки моніторинг та захист об'єктів критичної інфраструктури.

8. Розваги:

- інтерактивні ігри використання КФС для створення реалістичних та інтерактивних ігрових середовищ;

- віртуальна та доповнена реальність створення інноваційних розваг та навчальних програм.

Ці галузі демонструють широкий спектр застосувань КФС, що сприяє підвищенню ефективності, безпеки та якості життя.

Основними компонентами для виявлення БПЛА Shahed зображено на рис. 2.2.

Основні сенсори, які можуть бути використані для збору даних про навколишнє середовище та рух БПЛА, включають такі:

- радари використовуються для виявлення та вимірювання відстані, швидкості та напрямку руху об'єктів в повітряному просторі. Вони можуть мати різні типи, включаючи метеорологічні радари, навігаційні радари та радари з обліковою функцією;

- камери використовуються для візуального спостереження та записування відео- та фотоматеріалів з повітря. Вони можуть бути обладнані різними об'єктивами та матрицями, забезпечуючи різні поля зору та роздільну здатність;

- теплові датчики (інфрачервоні камери) вимірюють теплове випромінювання об'єктів, що знаходяться в їхньому полі зору. Вони дозволяють

виявляти теплові сліди БПЛА, навіть у темний час доби або за поганих погодних умов;

- лідари вимірюють відстань до об'єктів за допомогою відбивання лазерного променя. Вони можуть забезпечити точне виявлення та розташування об'єктів у тривимірному просторі;
- акустичні сенсори використовуються для виявлення звуків, що можуть бути пов'язані з рухом або роботою БПЛА. Вони дозволяють виявляти апарати, які можуть бути непомітними для інших типів сенсорів;
- гіперспектральні сенсори ці сенсори здатні реєструвати електромагнітне випромінювання в багатьох діапазонах частот, що дозволяє аналізувати характеристики матеріалів та об'єктів на землі.

Ці сенсори можуть використовуватися окремо або в комбінації для забезпечення широкого спектру можливостей збору даних та виявлення БПЛА. Кожна з цих систем має свої переваги і обмеження, які важливо враховувати при розробці системи виявлення БПЛА.

Мережа сенсорів для системи виявлення БПЛА є важливою частиною кіберфізичної системи, оскільки вона забезпечує збір, передачу та обробку даних з сенсорів. Для побудови ефективної мережі сенсорів потрібно врахувати наступні аспекти:

- бездротова комунікація мережа повинна підтримувати бездротову комунікацію між сенсорами та центральним обчислювальним вузлом. Для цього можна використовувати протоколи зв'язку, такі як Wi-Fi, Bluetooth або Zigbee;
- централізоване керування система повинна мати централізоване керування, що дозволяє керувати роботою сенсорів, розподіляти завдання для оптимального використання ресурсів та координувати збір та передачу даних;
- обробка даних на місці деякі сенсори можуть мати можливість обробки даних на місці, що дозволяє зменшити обсяг передаваних даних та знизити вимоги до мережі;

- захист від несанкціонованого доступу мережа повинна мати заходи захисту від несанкціонованого доступу та втручання, такі як шифрування даних та аутентифікація користувачів;
- масштабованість мережа повинна бути масштабованою для можливості додавання нових сенсорів або зміни конфігурації без перерви в роботі системи;

Така мережа сенсорів дозволяє ефективно збирати, передавати та обробляти дані з сенсорів для виявлення та відстеження БПЛА в реальному часі.

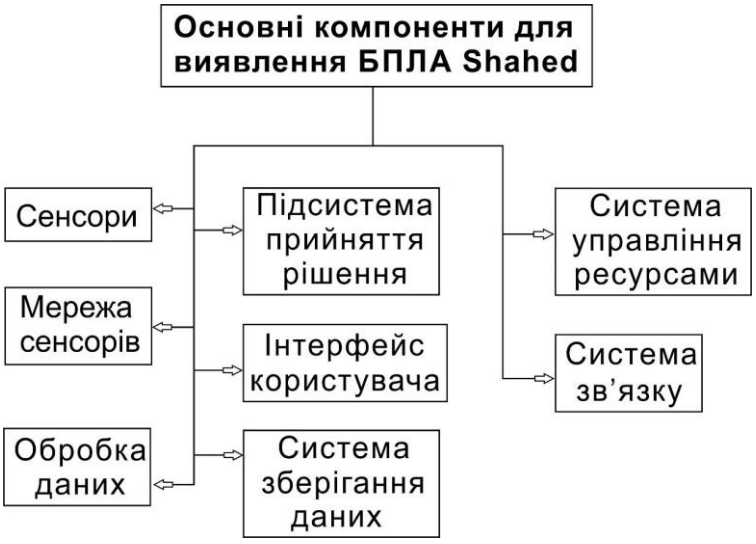


Рисунок 2.2 – Основні компоненти для виявлення БПЛА Shahed

Обробка даних з сенсорів для виявлення та класифікації БПЛА включає в себе кілька важливих етапів та методів:

- попередня обробка даних на цьому етапі дані з сенсорів піддаються попередній обробці, такі як фільтрація шуму, видалення артефактів та нормалізація даних для покращення їхньої якості та готовності для подальшої обробки;
- виділення ознак наступним кроком є виділення ознак з оброблених даних, що можуть вказувати на присутність БПЛА. Це може включати в себе характеристики, такі як розмір, форма, швидкість або тепловий слід, які допоможуть в подальшому виявленні та класифікації;

- класифікація після виділення ознак використовуються алгоритми класифікації для визначення, чи належить об'єкт до класу "БПЛА" або "не БПЛА". Для цього можуть використовуватися методи машинного навчання, такі як нейронні мережі, класифікатори на основі випадкового лісу або метод опорних векторів;
- постановка задачі для оптимального використання алгоритмів необхідно чітко сформулювати задачу, яку вони повинні розв'язувати. Наприклад, визначення мети виявлення та класифікації, обрання метрик оцінки успішності алгоритмів та інше;
- оцінка результатів після застосування алгоритмів необхідно оцінити їхню ефективність та точність за допомогою тестування на валідаційних даних. Це дозволить виявити потенційні проблеми та вдосконалити алгоритми;
- оптимізація на основі результатів тестування може бути виконана оптимізація алгоритмів та параметрів, щоб підвищити їх ефективність та швидкість роботи.

Ці етапи дозволяють ефективно обробляти дані з сенсорів та виявляти та класифікувати БПЛА з високою точністю та швидкістю.

Підсистема прийняття рішень в кіберфізичній системі для виявлення БПЛА відповідає за аналіз та обробку інформації про виявлені та прийняття відповідних рішень щодо реакції на ці об'єкти. Для цього можуть використовуватися наступні етапи та методи:

- аналіз даних підсистема аналізує дані, отримані від сенсорів, для визначення параметрів БПЛА, таких як швидкість, розмір, траєкторія руху тощо;
- класифікація на основі аналізу даних система класифікує об'єкти як БПЛА або інші об'єкти, що перебувають у повітрі;
- прийняття рішень на основі класифікації система приймає рішення щодо подальших дій. Це може бути активація сигналів тривоги, сповіщення операторів або автоматичне ініціювання контрзаходів;

- реакція залежно від прийнятого рішення система може ініціювати реакцію, таку як активація системи захисту, відправлення сигналів тривоги або інші заходи;
- оптимізація підсистема може бути оптимізована для підвищення ефективності та швидкості реакції на виявлені БПЛА.

Ці етапи дозволяють системі ефективно виявляти та реагувати на БПЛА, забезпечуючи надійний та швидкий захист об'єктів від їхнього вторгнення.

Інтерфейс користувача системи для виявлення БПЛА відіграє важливу роль у забезпеченні ефективності та зручності управління системою. Основні функції і можливості такого інтерфейсу можуть включати:

- візуалізація даних інтерфейс повинен відображати дані з сенсорів та інформацію про виявлені БПЛА у зручному для сприйняття форматі, наприклад, на карті або в таблицях;
- керування системою оператор повинен мати можливість керувати роботою системи через інтерфейс, наприклад, активувати сигнали тривоги або ініціювати контрзаходи;
- відображення статусу інтерфейс повинен відображати поточний статус системи, такий як стан сенсорів, результати аналізу даних та стан реагування на виявлені БПЛА;
- налаштування параметрів оператор повинен мати можливість налаштовувати параметри системи через інтерфейс, наприклад, діапазони виявлення БПЛА або чутливість сенсорів;
- журнал подій інтерфейс може включати журнал подій, який відображатиме історію виявлених БПЛА та подій системи для аналізу та відстеження;
- керування доступом інтерфейс може включати засоби керування доступом до системи, щоб забезпечити безпеку та обмежити доступ до функцій для неуповноважених користувачів.

Такий інтерфейс дозволить операторам ефективно взаємодіяти з системою та швидко приймати рішення щодо виявлених БПЛА, що підвищить ефективність та надійність системи.

Система зберігання даних про виявлені БПЛА відіграє важливу роль у забезпеченні доступності та цілісності даних для подальшого аналізу та використання. Для цього можуть використовуватися наступні підходи та технології:

- база даних система може використовувати реляційну базу даних для зберігання структурованих даних про виявлені БПЛА, таких як час виявлення, координати, характеристики БПЛА та інше;
- зберігання даних для забезпечення доступності та резервного копіювання даних можна використовувати Dropbox, Google Drive, Microsoft OneDrive;
- файлове сховище для зберігання великого обсягу неструктурованих даних, таких як відео або зображення, можна використовувати файлові сховища, наприклад, Amazon S3 або Azure Blob Storage;
- інтеграція з аналітичними інструментами для подальшого аналізу даних можна використовувати різноманітні аналітичні інструменти, такі як Python з бібліотеками для обробки даних (pandas, numpy), системи для візуалізації даних (Matplotlib, Seaborn) та інші;
- резервне копіювання важливо мати механізми для резервного копіювання даних, щоб забезпечити їхню доступність у випадку відмови обладнання або інших непередбачуваних подій;

Така система зберігання даних дозволить забезпечити доступність, цілісність та безпеку даних про виявлені БПЛА для подальшого використання та аналізу.

Система управління ресурсами в кіберфізичній системі для виявлення БПЛА включає в себе механізми для ефективного використання апаратних та програмних ресурсів системи. Для цього можуть використовуватися наступні підходи та методи:

- розподіл ресурсів система повинна розподіляти апаратні ресурси, такі як обчислювальна потужність, пам'ять та мережеві ресурси, між різними підсистемами для оптимального використання;
- планування завдань механізми планування допомагають визначити порядок виконання завдань та розподіл ресурсів для їх виконання з урахуванням пріоритетів та обмежень;
- керування пам'яттю система повинна ефективно керувати доступом до пам'яті та використанням нею для забезпечення оптимальної продуктивності;
- керування енергоспоживанням для забезпечення тривалої роботи системи важливо ефективно керувати енергоспоживанням обладнання та виключати неактивні частини системи;
- моніторинг ресурсів система повинна постійно моніторити використання ресурсів та вчасно реагувати на зміни для запобігання перевантаження або неефективного використання;
- автоматизація для підвищення ефективності управління ресурсами можна використовувати автоматизовані механізми та алгоритми.

Ці підходи дозволяють системі ефективно використовувати апаратні та програмні ресурси для забезпечення стабільної та надійної роботи системи виявлення БПЛА.

Система зв'язку в кіберфізичній системі для виявлення БПЛА відіграє ключову роль з іншими системами безпеки та контролю повітряного простору. Для цього можуть використовуватися наступні підходи та технології:

- бездротовий зв'язок система може використовувати бездротові технології, такі як Wi-Fi, Bluetooth, або радіо зв'язок, для забезпечення зв'язку між сенсорами, обчислювальними вузлами та центральною системою управління;
- сполучення з іншими системами система може бути інтегрована з іншими системами безпеки та контролю повітряного простору, такими як радарні системи або системи виявлення загроз, для обміну інформацією та координації дій;

- шифрування для забезпечення безпеки зв'язку можуть використовуватися методи шифрування, що дозволяють захистити передавані дані від несанкціонованого доступу;
- мережеві протоколи для організації зв'язку між компонентами системи можуть використовуватися мережеві протоколи, такі як TCP/IP або MQTT, для надійного та ефективного передавання даних;
- резервне забезпечення для забезпечення надійності зв'язку можуть бути використані механізми резервного забезпечення, такі як дублювання каналів або резервні шляхи зв'язку;

Ці підходи дозволяють системі ефективно забезпечувати зв'язок між компонентами та іншими системами безпеки та контролю повітряного простору, що дозволяє забезпечити ефективну та надійну роботу системи в цілому.

2.2 Моделювання процесу виявлення БПЛА Shahed з використанням геолокаційних даних

В результаті проведеного дослідження було сформовано перелік найпоширеніших БПЛА Shahed, які буде виявляти кіберфізична система моніторингу повітряного простору на предмет наявності БПЛА на рисунку 2.3:

- Shahed 136;
- Shahed 141;
- Shahed 161;
- Shahed 171;
- Shahed 181;
- Shahed 191.

Звісно, що ці моделі можуть змінюватись, а отже, можуть змінюватись і їхні характеристики, технічні параметри, можуть з’являтись нові моделі або принципово нові БПЛА. Тому вкрай важливо враховувати ці зміни, оновлюючи бази даних та підходи до їх виявлення, та навчати AIoT, враховуючи ці оновлені дані.

Рисунок 2.3 – Моделі БПЛА Shahed [82]

Для вирішення задачі виявлення БПЛА немає принципової різниці типу ворожого БПЛА Shahed, адже кожний з них несе загрозу, чи то розвідувальний БПЛА, чи бойовий. Тому в рамках дослідження задача ідентифікації БПЛА не ставилась.

Змоделюємо процес виявлення безпілотних літальних апаратів типу Shahed за допомогою кіберфізичної системи та AIoT. Розглянемо цей процес у контексті розробки кіберфізичної системи виявлення та реагування на появу ворожих БПЛА.

Ось кроки та компоненти, які можна включити до такої моделі:

Крок 1 - сенсорна мережа для виявлення:

- розгортання датчиків;

- встановлення різних типів датчиків (наприклад, радарів, камер, сенсорів руху тощо) на важливих точках території для моніторингу повітряного простору;
- збір та передача даних;
- дані з датчиків збираються та передаються до центральної системи керування через мережу IoT.

Крок 2 - аналіз даних за допомогою штучного інтелекту:

- обробка даних AI;
- використання алгоритмів машинного навчання та глибокого навчання для аналізу потоку даних в реальному часі;
- навчання моделей на основі даних про нормальну поведінку літальних апаратів та виявлення аномалій, які можуть вказувати на присутність небажаного UAV.

Крок 3 - виявлення та реакція:

- виявлення безпілотного літального апарата;
- використання моделі AI для виявлення аномальних паттернів, що вказують на наявність БПЛА, наприклад, неузгоджені польоти або незвичайні маршрути;
- вирішення ситуації;
- після виявлення БПЛА система AIoT може запускати реакцію, таку як відправлення сповіщення оператору, автоматичне висування протиповітряних заходів або інші заходи захисту.

Крок 4 - реагування та моніторинг:

- взаємодія з операторами;
- система AIoT може забезпечувати інформацію операторам або військовим структурам для подальшого реагування на виявлені загрози;
- моніторинг та навчання;
- постійне моніторингове середовище для виявлення нових загроз та навчання моделей штучного інтелекту з урахуванням нових даних.

Ця модель поєднує фізичні компоненти (сенсори, датчики, спеціалізовані системи) з кібернетичними системами (обробка даних AI, передача через мережу IoT) для створення реактивної та ефективної системи виявлення безпілотних літальних апаратів та управління ними.

AIoT дозволяє системі бути більш адаптивною та інтелектуальною, що покращує загальну ефективність інформаційної безпеки.

Критерій надійності джерела повідомлення про модливу присутність БПЛА.

Нехай kn_i - коефіцієнт надійності джерела виявлення БПЛА, адже повідомлення про виявлення може надходити як від сучасних надійних систем наприклад Rantelon DTS-2458 для якого kn_i буде приймати максимальне значення, тобто kn_i =1. А для телефоного дзвінка з нового телефоного номера, якого раніше не було в базі даних або дзвінка з окупованої території kn=0.001.

Нехай систему з різних джерел надійшло I повідомлень про можливу наявність БПЛА. Кожне таке повідомлення містить щонайменше координати цих точок(геодані) та точний час виявлення. Тоді I-множина точок, в яких була зафіксована можлива наявність БПЛА, і для кожної пари найближчих точок з цієї множини система розраховує відстань S_{ij} (де $1 \leq j \leq i$) по прямій між цими точками за допомогою відомих координат.

Поділивши цю відстань S_{ij} на різницю в часі $\Delta t=|t_i-t_j|$, отримаємо швидкість V_{ij} з якою ймовірний БПЛА міг переміститися з однієї точки в іншу по прямій. Логічно припустити, що отримана швидкість не повинна перевищувати максимальну швидкість V_{max} відомих моделей БПЛА. Або ж разі несутєвого перевищення допускається, що ймовірність фіксування нового типу БПЛА з вищою швидкістю, про що повідомляється оператору і маршрут між двома точками є не гарантованим але ймовірним (може зображуватися на карті жовтим кольором) та враховуватися в подальшому розрахунку траєкторії руху БПЛА.

Назвемо цей критерій критерієм максимальної відомої швидкості БПЛА $0 \leq kv_{max} \leq V_{max}$. Варто зазначити, що якщо ймовірна нова швидкість яка перевищує V_{max} підтвердиться на подальшому шляху від точки до точки особливо на маршовому відрізку від кордону з ворогом принаймі кілька разів, то можна і

доречно стверджувати про появу нового типу БПЛА який розвиває нову швидкість і це потрібно враховувати при подальших розрахунках ШІ.

2.3 Висновки

У другому розділі кваліфікаційної роботи описані компоненти кіберфізичних систем та досягнення у їх розробці. Визначені проблеми, які виникають у побудові таких систем, і висунуті принципи створення апаратно-програмної платформи для розробки прикладних кіберфізичних систем. Розглянуті напрямки досліджень у галузі кіберфізичних систем та очікувані результати.

Також у даному розділі розроблено критерії для виявлення БПЛА Shahed залежно від джерела з якого отримано сигнал про можливе виявлення БПЛА, а також критерії максимальної швидкості що базується на відомих технічних характеристиках БПЛА Shahed. Дані критерії надійності джерела та максимальної швидкості буде покладено в основу методу виявлення БПЛА з використанням геолокаційних даних.

3 МЕТОД ВИЯВЛЕННЯ БПЛА SHAHED

3.1 Метод виявлення БПЛА Shahed

Метод виявлення БПЛА Shahed може включати такі кроки і складові:

- розгортання кіберфізичної системи – встановлення датчиків для виявлення БПЛА Shahed; розгортання спеціалізованих систем різного типу для виявлення БПЛА;
- збір даних – отримання геолокаційних даних та часу фіксації можливої наявності БПЛА з датчиків спеціалізованих систем виявлення, зі спеціальних мобільних додатків(наприклад, єППО), а також від поліції з телефоних дзвінків від населення;
- збір та передача даних - полягає в тому, що датчики реєструють інформацію про виявлення БПЛА Shahed, після чого ці дані передаються на центральний сервер або зберігаються в хмарному сховищі;
- обробка даних та їх аналіз - отримані від датчиків дані обробляються на сервері або в хмарному сервісі за допомогою штучного інтелекту речей для подальшого виявлення; вони можуть бути проаналізовані щоб виявляти БПЛА Shahed та відфільтровувати хибні повідомлення випадкові або зловмисні, які можуть вплинути реакцію мобільних груп боротьби з БПЛА;
- візуалізація даних – результати аналізу реалізовуються на мапі, щоб користувачі могли бачити маршрут руху БПЛА Shahed у своєму регіоні та приймати відповідні заходи;
- сповіщення користувачів – у разі виявлення БПЛА Shahed користувачі можуть отримувати сповіщення через мобільний додаток, щоб вживати необхідні заходи;
- пошук та аналіз тенденцій – дані про виявлення БПЛА Shahed можуть бути проаналізовані для виявлення інших типів Shahed в різних регіонах та в різні періоди часу; це дозволить ухвалювати заходи щодо небезпеки Shahed;

- участь цивільного населення – крім збору даних про виявлення БПЛА Shahed є можливість надсилати повідомлення про виявлення БПЛА Shahed у своєму регіоні;
- інформування цивільного населення – зібрані дані про виявлення БПЛА Shahed використовуються для інформування цивільного населення про небезпеку;
- інноваційні рішення для виявлення БПЛА Shahed – на основі зібраних даних моніторингу можуть бути створені та впроваджені нові технологічні рішення для виявлення БПЛА Shahed, які допоможуть краще їх виявляти та збивати;
- дослідження та розвиток можуть використовувати зібрані дані для аналізу виявлення БПЛА Shahed та розробки нових методів, що сприятиме постійному розвитку та удосконаленню системи моніторингу та управління;
- розробка мобільних додатків – створення мобільних додатків для виявлення БПЛА Shahed та надання інформації для безпеки людей на основі геолокаційних даних;
- розвиток системи повідомлень та попереджень – використання автоматичних систем сповіщень та попереджень через смс або мобільні додатки про виявлення БПЛА Shahed;
- використання штучного інтелекту речей – впровадження методів штучного інтелекту речей для аналізу великих обсягів даних з метою прогнозування коли були виявленні БПЛА Shahed.

Можна використати різні методи для виявлення БПЛА Shahed:

1. Акустичний метод - акустичні сенсори розміщуються у визначених точках для фіксування звукових хвиль, створених двигуном БПЛА. Специфічні частотні характеристики шуму, що виникає під час польоту Shahed, можуть бути використані для ідентифікації цього типу безпілотника.

Переваги:

- можливість виявлення на значних відстанях;
- відносно низька вартість обладнання;

- широка зона покриття.

Недоліки:

- високий рівень фонових шумів може ускладнити процес виявлення;
- ефективність залежить від погодних умов.
- технічні обмеження.

2. Радіочастотний метод - радіочастотні сенсори використовуються для перехоплення сигналів управління, що передаються на БПЛА або від нього. Специфічні частоти, на яких працює Shahed, можуть бути використані для його ідентифікації.

Переваги:

- можливість виявлення навіть при наявності перешкод на шляху сигналу;
- висока точність при правильному налаштуванні сенсорів.

Недоліки:

- висока вартість обладнання;
- потреба в спеціалізованих знаннях для налаштування та експлуатації;
- потецийна загроза конфіденційності.

3. Візуальний метод - використання оптичних камер та інфрачервоних сенсорів для виявлення і відстеження БПЛА. Системи комп’ютерного зору можуть автоматично аналізувати зображення для ідентифікації характерних ознак Shahed.

Переваги:

- висока точність в умовах гарної видимості;
- можливість ідентифікації типу БПЛА за зовнішнім виглядом;
- Сумісність із різними технологіями.

Недоліки:

- обмежена ефективність в умовах поганої видимості (туман, ніч);
- висока вартість та складність обслуговування оптичного обладнання;
- проблеми з конфідеційностю.

4. Радіолокаційний метод - використання радарів для виявлення та відстеження руху БПЛА. Радари посилають радіохвилі, які відбиваються від об'єкта, що рухається, і повертаються до приймача, дозволяючи визначити місцезнаходження та швидкість БПЛА.

Переваги:

- можливість роботи в умовах поганої видимості;
- висока точність виявлення та відстеження;
- можливість визначення швидкості і напрямку руху.

Недоліки:

- висока вартість та складність налаштування;
- ефективність залежить від наявності прямих радіолокаційних шляхів;
- помилкове спрацювання.

5. Інтеграція багатьох методів - поєднання кількох методів для підвищення точності та надійності виявлення. Наприклад, використання акустичних сенсорів разом з радіочастотними або радіолокаційними сенсорами для зменшення кількості хибних спрацьовувань.

Переваги:

- підвищення надійності та точності виявлення;
- можливість компенсувати недоліки одного методу за рахунок іншого.

Недоліки:

- висока вартість та складність інтеграції різних систем;
- потреба в складному програмному забезпеченні для обробки даних з різних сенсорів.

Кожен з методів виявлення БПЛА Shahed має свої переваги та недоліки. Використання комбінованого підходу, що включає різні методи, може значно підвищити ефективність виявлення та відстеження таких безпілотників.

Інтеграція різних сенсорних технологій і розробка складних алгоритмів обробки даних дозволяють створити надійну та ефективну систему для захисту від загроз, пов'язаних з використанням БПЛА.

Також застосовуються методи виявлення БПЛА Shahed за допомогою AIoT включають в себе такі етапи:

1. Збір даних за допомогою сенсорів:

- акустичні сенсори;
- оптичні сенсори;
- радіочастотні сенсори;
- лідар.

2. Обробка та аналіз даних:

- алгоритми машинного навчання використання попередньо навчених моделей для ідентифікації та класифікації БПЛА на основі зібраних даних;
- нейронні мережі застосування глибокого навчання для обробки великих обсягів даних і розпізнавання складних шаблонів;
- аналіз великих даних обробка і аналіз даних з сенсорів у реальному часі для виявлення потенційних загроз.

3. Інтеграція з AIoT:

- хмарні обчислення використання хмарних платформ для зберігання, обробки та аналізу даних, забезпечуючи масштабованість і доступність;
- краєві обчислення обробка даних на місці, де вони збираються (на краю мережі), для зменшення затримок і підвищення швидкості реакції;
- мережі IoT об'єднання різних сенсорів і пристроїв в єдину мережу для координації та спільної обробки даних.

4. Забезпечення безпеки та конфіденційності:

- шифрування даних захист даних від несанкціонованого доступу під час їх передачі та зберігання;
- аутентифікація та авторизація перевірка прав доступу до системи для запобігання несанкціонованому використанню;
- моніторинг та реагування на загрози постійний моніторинг системи на предмет виявлення потенційних загроз та швидке реагування на них.

Використання AIoT для виявлення БПЛА Shahed забезпечує точність, швидкість і ефективність у виявленні та нейтралізації потенційних загроз, що значно підвищує рівень безпеки та захисту.

Для виявлення БПЛА Shahed можна використовувати різноманітні типи датчиків, які мають свої переваги і недоліки. Ось порівняння датчиків, які можуть бути ефективними для виявлення БПЛА Shahed:

1) радари

Переваги: висока швидкість виявлення, працездатність у будь-яких погодних умовах, можливість виявлення на великій відстані, висока точність визначення координат.

Недоліки: висока вартість, потреба у великій кількості електроенергії, можливість спричинення перешкод іншим радіоелектронним системам.

2) камери візуального спостереження

Переваги: доступність, можливість використання для ідентифікації та класифікації, можливість віддаленого керування.

Недоліки: залежність від умов освітлення, потреба в стабільності платформи камери, обмежена дальність виявлення.

3) теплові камери

Переваги: здатність виявляти об'єкти за тепловим випромінюванням, ефективність в умовах обмеженої видимості (туман, дим).

Недоліки: обмежена дальність виявлення, можливість спотворення результатів через навколишнє теплове випромінювання.

4) акустичні датчики

Переваги: можливість виявлення БПЛА за звуковим сигналом двигуна або інших джерел шуму, незалежність від видимості.

Недоліки: обмежена дальність виявлення, можливість спричинення помилкових спрацювань іншими джерелами шуму.

5) датчики радіохвиль

Переваги: можливість виявлення БПЛА за радіохвильовим випромінюванням, ефективність при відсутності видимості.

Недоліки: обмежена дальність виявлення, можливість перешкодження радіоелектронними системами.

Кожен з цих датчиків може бути ефективним у виявленні БПЛА Shahed в залежності від конкретних умов використання, таких як область дії, погодні умови, доступність енергії тощо.

Оптимальний вибір датчиків для системи виявлення БПЛА Shahed може бути здійснений шляхом комплексного аналізу цих факторів та врахування потреб системи.

Отже, метод виявлення БПЛА Shahed складається з наступних кроків:

1) навчання системи – задання множини I раніше отриманих повідомлень про можливе виявлення БПЛА що містить геолокаційні дані кожної точки та час фіксації, а також технічні параметри всіх раніше виявлених БПЛА Shahed, основним з яких буде максимальна швидкість, яку може розвивати БПЛА;

2) збір геолокаційних даних при кожній нові атаці ворожими БПЛА;

3) передача отриманих даних на сервер, в базу даних, подальша обробка, виявлення та навчання системи;

4) опрацювання даних, фільтрації хибних повідомлень через використання критеріїв надійності джерела повідомлення та максимальної швидкості руху БПЛА Shahed;

5) передача даних щодо виявлених маршрутів руху БПЛА у конкретному регіоні, передача для аналізу та навчання системи.

Розроблений метод виявлення БПЛА Shahed передбачає використання штучного інтелекту речей, постійне навчання системи на раніше використовуваних маршрутах руху БПЛА, врахування надійності джерела повідомлення, відкидання хибних та сумнівних сигналів, та врахування відомих технічних характеристик БПЛА Shahed.

Завдяки цьому зменшується час на обробку даних, завдяки фільтрації хибних повідомлень зберігається мобільність груп реагування та підвищується рівень безпеки.

3.2 Вимоги до програмних та апаратно-програмних засобів для виявлення БПЛА Shahed

Загальні вимоги для виявлення БПЛА Shahed:

1. Надійність та стабільність роботи:

- система повинна забезпечувати безперервне функціонування без збоїв;
- високий рівень захисту від збоїв і помилок.

2. Реагування в реальному часі:

- система повинна мати здатність обробляти дані та приймати рішення в режимі реального часу;
- мінімальна затримка між виявленням об'єкта та його ідентифікацією.

3. Масштабованість:

- система повинна підтримувати можливість додавання нових сенсорів і компонентів без значних змін у архітектурі;
- підтримка роботи з різними типами сенсорів (акустичні, радіочастотні, оптичні тощо).

4. Гнучкість та адаптивність:

- можливість адаптації під різні сценарії використання та змінні умови навколишнього середовища;
- підтримка оновлень програмного забезпечення без зупинки системи.

5. Безпека:

- захист від кібер-атак та несанкціонованого доступу;
- шифрування даних під час передачі та зберігання.

6. Сумісність з іншими системами:

- сумісність з іншими системами безпеки та мережевими інфраструктурами;
- підтримка стандартних протоколів обміну даними.

Архітектурне проектування програмних та апаратно-програмних засобів включає в себе такі модулі:

1. Сенсорні модулі

Функції:

- збір даних про навколишнє середовище та виявлення потенційних БПЛА;
- попередня обробка даних для зменшення шуму та підвищення точності.

Вимоги:

- висока точність вимірювань та стійкість до зовнішніх перешкод;
- можливість об'єднання даних з кількох сенсорів.

2. Комунікаційні модулі

Функції:

- передача зібраних даних від сенсорів до центрального обчислювального модуля;
- підтримка бездротових та дротових протоколів зв'язку.

Вимоги:

- висока пропускна здатність для передачі великого обсягу даних;
- забезпечення надійного та безпечного каналу зв'язку.

3. Обчислювальний модуль

Функції:

- аналіз даних, отриманих від сенсорів;
- використання алгоритмів машинного навчання та штучного інтелекту для ідентифікації та класифікації БПЛА.

Вимоги:

- висока продуктивність та обчислювальна потужність;
- підтримка паралельної обробки даних.

4. Модуль управління

Функції:

- координація роботи всіх компонентів системи;
- прийняття рішень щодо відповідних дій при виявленні БПЛА.

Вимоги:

- інтуїтивно зрозумілий інтерфейс для операторів;
- можливість ручного втручання у процес управління при необхідності.

5. Модуль зберігання даних

Функції:

- зберігання історичних даних для подальшого аналізу та тренування алгоритмів;
- забезпечення надійного резервного копіювання даних.

Вимоги:

- висока місткість та швидкодія;
- захист даних від несанкціонованого доступу та втрат.

6. Інтерфейс користувача

Функції:

- надання користувачу інформації про стан системи та виявлені об'єкти;
- інструменти для налаштування та моніторингу системи.

Вимоги:

- зрозумілий та зручний інтерфейс;
- підтримка віддаленого доступу через веб-інтерфейси або мобільні додатки.

Отже, розробка кіберфізичної системи для виявлення БПЛА Shahed вимагає врахування різноманітних технічних та програмних аспектів.

Інтеграція сенсорних, комунікаційних, обчислювальних та керуючих компонентів у єдину систему забезпечить високу ефективність та надійність роботи системи.

Використання сучасних методів обробки даних, таких як машинне навчання та штучний інтелект, дозволить підвищити точність виявлення та ідентифікації БПЛА, а також забезпечити надійний захист від можливих загроз.

3.3 Алгоритм виявлення БПЛА Shahed

Основні кроки алгоритму виявлення БПЛА включають зображено на рисунку 3.1:

1. Збір даних - система повинна збирати дані з усіх доступних джерел, включаючи вимірювання з датчиків, отримання повідомлень від операторів чи систем моніторингу.

2. Попередня обробка - отримані дані можуть потребувати попередньої обробки для фільтрації шумів, видалення артефактів або нормалізації до одного формату.

3. Інтеграція і об'єднання - дані з різних джерел повинні бути інтегровані і об'єднані для створення повнішого зображення ситуації.

Це може включати синхронізацію часових міток, об'єднання географічної інформації тощо.

4. Аналіз і обробка даних - опрацювання даних включає використання алгоритмів обробки сигналів, комп'ютерного зору, машинного навчання та інших методів для виявлення та аналізу БПЛА. Наприклад, можуть застосовуватися алгоритми виявлення об'єктів на зображеннях або аналізу акустичних сигналів.

5. Формування зведених даних - на основі оброблених даних формуються зведені дані або звіти, які відображають виявлені об'єкти БПЛА, їх місцезнаходження, швидкість, напрямок руху тощо.

6. Перевірка і валідація - сформовані дані перевіряються на достовірність і валідність. Цей етап включає перевірку відповідності отриманих даних до очікуваного стандарту та можливих помилок обробки.

7. Представлення і передача результатів - остаточні результати обробки можуть бути представлені в інтерфейсі для операторів або інших систем для прийняття рішень.

Результати також можуть автоматично передаватися до інших систем для подальшого використання.

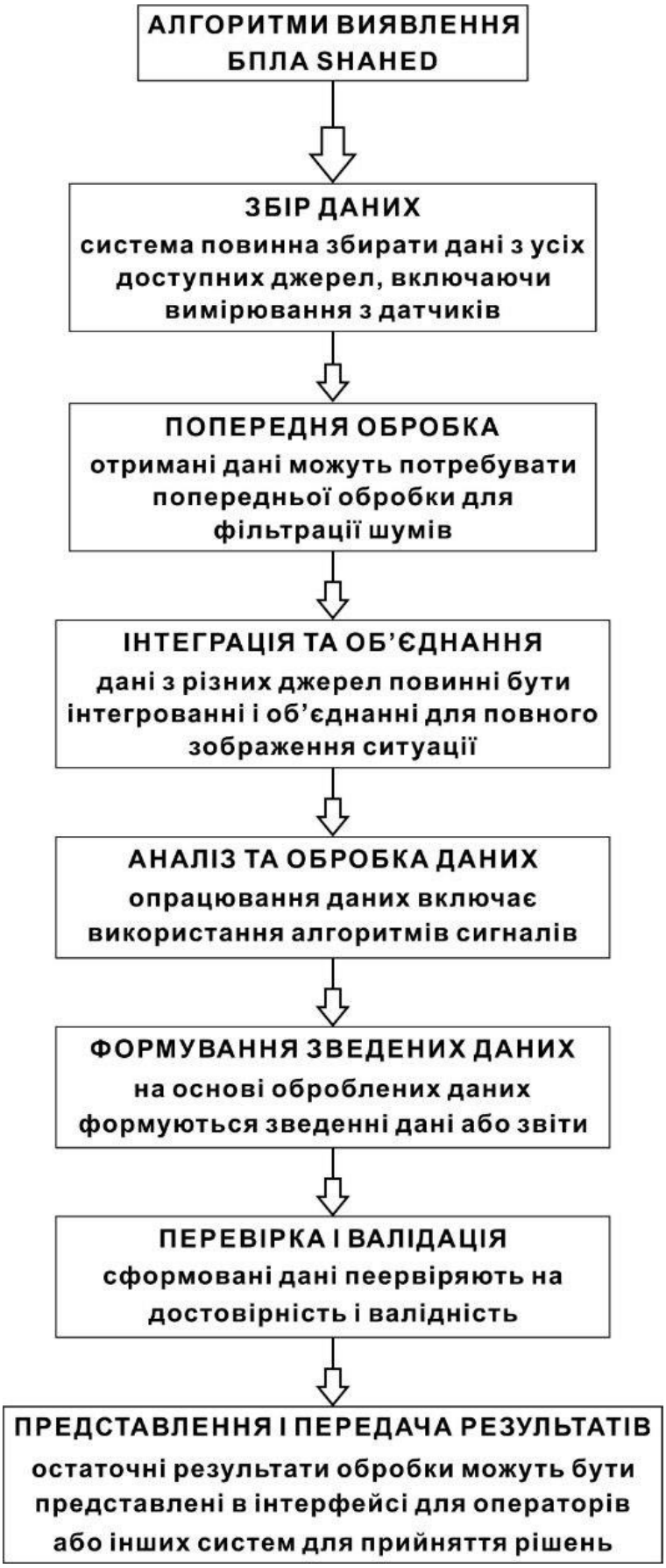


Рисунок 3.1 –Алгоритми виявлення БПЛА Shahed

8. Цей процес опрацювання даних має на меті забезпечити швидку та якісну обробку інформації з різних джерел для ефективного виявлення і відстеження БПЛА та інших об'єктів у повітряному просторі.

Кожен крок важливий для забезпечення надійної роботи системи виявлення.

3.3 Висновки

У третьому розділі кваліфікаційної роботи було запропоновано метод виявлення БПЛА Shahed, з використанням штучного інтелекту речей, для обробки геолокаційних даних та точного часу фіксації ймовірного виявлення БПЛА Shahed, завдяки фільтрації хибних повідомлень зберігається мобільність груп реагування та підвищується рівень безпеки.

Окрім цього у розділі 3 кваліфікаційної роботи розроблено алгоритм виявлення БПЛА Shahed з використання геолокаційних даних, за яким буде здійснюватися виявлення БПЛА Shahed, буде прийматися рішення щодо кількості ворожих БПЛА у повітряному просторі, та візуалізація їхніх маршрутів руху.

Розроблений алгоритм забезпечує комплексний підхід до виявлення БПЛА Shahed оскільки передбачає отримання інформації з різних джерел, з різним ступенем надійності, а також враховує накопичений досвід та передбачає постійне навчання системи.

4 КІБЕРФІЗИЧНА СИСТЕМА ВИЯВЛЕННЯ БПЛА SHAHED

4.1 Кіберфізична система виявлення БПЛА Shahed

Дослідження у галузі кіберфізичних систем (КФС) включає нові розробки у сферах комп'ютерної архітектури, програмного забезпечення, комп'ютерних систем, мереж та інших інженерних галузях. Ця область відкриває нові можливості і створює додаткові виклики, такі як:

1. Забезпечення взаємодії між розподіленими кіберфізичними системами.
2. Забезпечення надійності та захисту інформації.
3. Забезпечення контролю над гібридними системами.
4. Розроблення архітектури.

Традиційні вбудовані системи потребують більш високого рівня безпеки, ніж платформи загального призначення. У перехідний період до кіберфізичних систем вимоги до безпеки мають зрости, щоб захистити фізичні системи від зростаючої кількості загроз, спрямованих на їхнє пошкодження через кібератаки. Без підвищення рівня безпеки КФС не можуть застосовуватись у таких галузях, як охорона здоров'я, та в інших системах, де вимоги до безпеки є критичними.

Незалежно від середовища КФС мають такі властивості:

1. Інтенсивна взаємодія з фізичними системами.
2. Наявність програмного забезпечення у всіх вбудованих або фізичних компонентах.
3. Взаємодія з різними мережами, включаючи дротові та бездротові (Wi-Fi, Bluetooth).
4. Взаємодія з різноманітними ресурсами з різноманітними властивостями.
5. Динамічна реорганізація / реконфігурація для адаптації до змін.

Взаємодія з фізичним світом визначає поведінку кіберфізичних систем, які часто виступають як системи управління зі зворотним зв'язком. Це означає, що зміна у фізичній системі може призвести до відповідної зміни в кіберсистемі і

навпаки. Взаємодія з фізичним світом відбувається у реальному часі і повинна бути стійкою до несподіваних змін і збоїв. Оскільки ця взаємодія збільшується, зростає і вразливість до кібератак, що вимагає вдосконалення безпеки системи.

Різноманіття компонентів відрізняє кіберфізичні системи (КФС) від традиційних вбудованих систем, які можна розглядати як їх підсистеми. Незважаючи на велику кількість компонентів у КФС, всі вони об'єднуються для єдиного обслуговування фізичних систем. КФС характеризуються різноманітністю компонентів і взаємодій, а також різноманітністю цілей і завдань.

Вони мають жорсткі зв'язки між обчислювальною технікою і фізичними компонентами, які можуть бути фізично розділені й розподілені на великі відстані за допомогою мережевих взаємодій у різних мережевих доменах. Це відрізняє КФС від традиційних вбудованих систем, які зазвичай зосереджені на одній платформі.

Вразливості КФС можуть бути спричинені ненавмисними або спеціальними змінами у роботі системи, що може призвести до втрати конфіденційності, цілісності та доступності. Система є найвразливішою у режимах:

- моніторинг;
- передача інформації через мережу;
- опрацювання інформації.

Моніторинг фізичних процесів є ключовою функцією кіберфізичних систем (КФС), яка використовує безліч датчиків для постійного збору інформації про фізичну систему. Ця інформація передається до керуючих модулів кіберсистеми. Датчики перетворюють фізичні параметри, такі як температура чи тиск, на електричні сигнали. Системи зворотного зв'язку в основному ґрунтуються на даних з датчиків фізичних процесів. Помилки датчиків є типовими для всіх фізичних систем. Для захисту від кібератак у цьому режимі було розроблено багато методів і алгоритмів, оскільки кіберзлочинці намагаються отримати або змінити інформацію, що передається датчиками.

КФС складаються з декількох датчиків і вбудованих контролерів, що взаємодіють між собою, переважно за допомогою мереж. Обмін інформацією між

елементами КФС є вразливим до різних кіберзагроз, таких як прослуховування, атаки з відмовою в обслуговуванні (DOS), модифікація даних тощо. Для забезпечення безпечного обміну інформацією через мережу застосовуються методи шифрування, аутентифікації і авторизації.

На цьому етапі вбудовані контролери обробляють інформацію від датчиків і відправляють зворотний зв'язок до системи. Вбудовані контролери об'єднують в собі апаратну та програмну частини, зберігальні елементи, пристрої вводу/виводу та пристрої зв'язку. Пристрої обробки інформації включають прості мікроконтролери, одно- та багатоядерні процесори, цифрові сигнальні процесори, спеціалізовані інтегральні схеми та програмовані логічні матриці. Особлива увага приділяється використанню "ненадійних компонентів" у КФС, тобто тих, безпека яких не є гарантованою. Стандартні методи захисту, такі як фізичний поділ потоку інформації, застосовуються рідше через їх високу вартість, і можуть лише зменшити, а не усунути загрози безпеці систем

Бездротові сенсорні мережі є важливим компонентом, що сприяв формуванню концепції кіберфізичних систем (КФС). Дослідження у цій галузі спрямовані на створення нових принципів побудови мереж на основі інтелектуальних агентів та систем розподілених контактних вимірювань з використанням автономних мобільних інтелектуальних агентів. Ці дослідження дозволяють розробляти автономні розподілені системи, що самостійно оптимізують процеси збору та обробки вимірювальної інформації.

Також важливим елементом є сучасні засоби телекомунікацій, які забезпечують взаємодію компонентів системи незалежно від їх розташування. Проекти з розробки просторових засобів телекомунікацій дозволяють створювати системи попередження про катастрофи та цифрового оперативно-технологічного зв’язку.

Наприклад, система цифрового оперативно-технологічного зв’язку для залізничного транспорту працює у цифрових і цифро-аналогових мережах, організованих по волоконно-оптичних і мідних кабельних лініях, забезпечуючи стійке з'єднання та використання наявної аналогової мережі.

Створення кіберфізичних систем (КФС) включає в себе деякі ключові проблеми, серед яких можна виділити наступні:

1. Інтеграція різноманітних компонентів необхідно забезпечити ефективне поєднання різнотипних компонентів у складі КФС. Це вимагає дослідження різних підходів до побудови та організації роботи системи.

2. Взаємодія з фізичним середовищем важливо забезпечити ефективну взаємодію кібернетичних засобів з фізичним середовищем, враховуючи синергетичні процеси, що відбуваються в ньому.

3. Управління потрібно ефективно поєднати централізовані та децентралізовані методи управління функціонуванням системи, враховуючи принципи самоконфігурування та самоорганізації.

4. Прийняття рішень важливо забезпечити таку швидкість прийняття рішень кібернетичними засобами, яка дозволить досягти потрібної якості функціонування КФС.

5. Структурна організація необхідно поділити КФС на незалежні ієрархічні рівні та розробити принципи взаємодії між ними для спрощення структурної організації системи.

6. Безпека важливо забезпечити розпізнавання та ефективне захищене функціонування компонентів та системи в цілому.

Дослідження у цій області орієнтовані на створення узагальненої моделі вимірювально-обчислювальних технологій, технологій управління та прийняття рішень, комунікаційних технологій та технологій захисту інформації.

Описаний підхід базується на розробці теоретичних основ побудови прикладних кіберфізичних систем та їх функціонування, які реалізовані у вигляді універсальної, масштабованої, гнучкої та розширюваної апаратно-програмної платформи.

Ця платформа забезпечує захищену взаємодію різних компонентів, таких як вимірювально-обчислювальні, керуючі, комунікаційні та виконавчі, для досягнення функціональної повноти та синергетичного ефекту від їх взаємодії на

рисунку 4.1. Це дозволить підняти процеси дослідження та управління фізичними процесами на новий рівень якості.

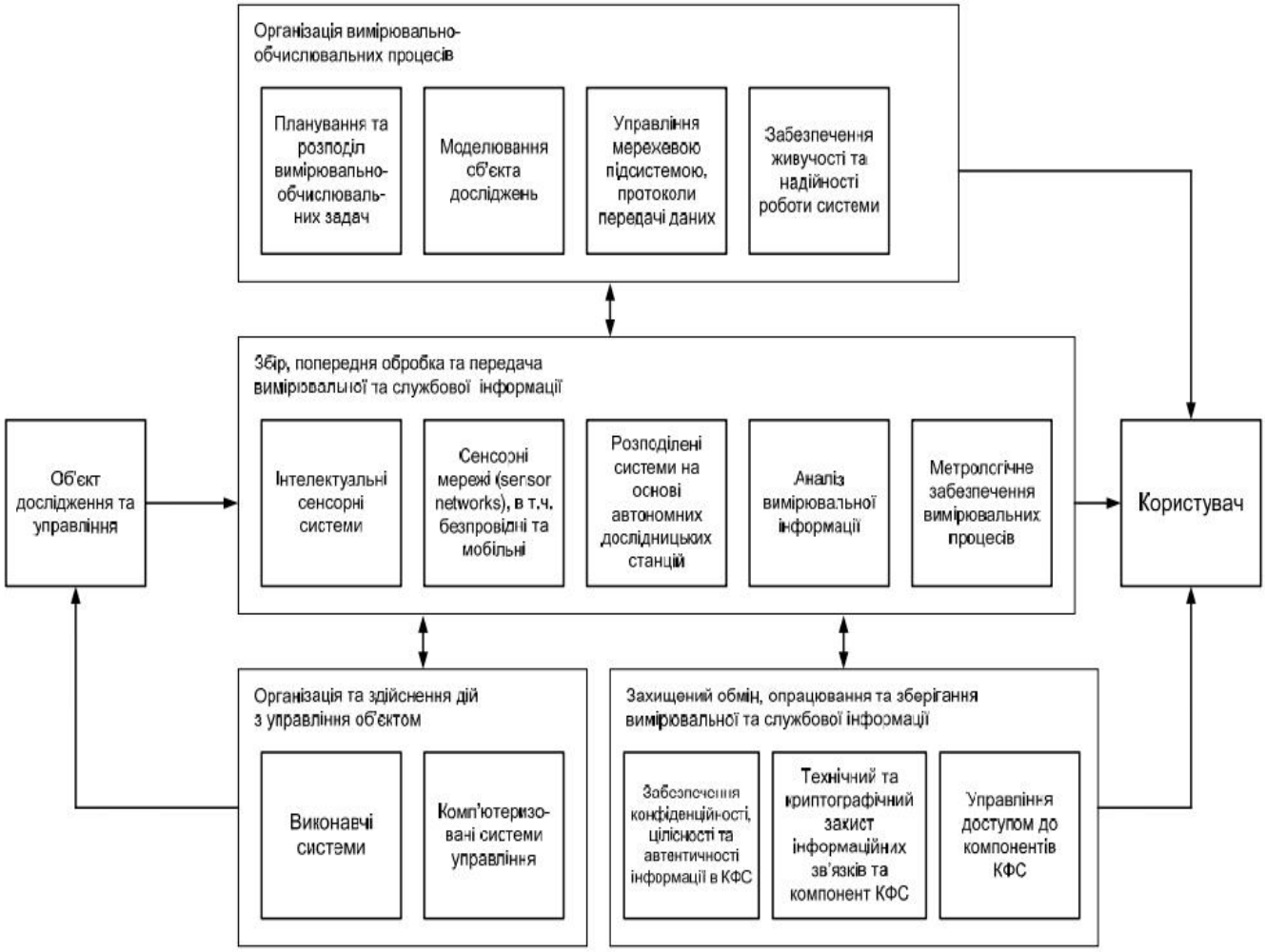


Рисунок 4.1 – Платформа для розробки інтегрованих кіберфізичних систем

Основні завдання дослідження кіберфізичних систем включають:

- розробка нових методів поєднання та організації захищеної взаємодії компонентів КФС для ефективного планування та виконання складних завдань з дослідження та управління, включаючи масштабованість, гнучкість, нарощуваність та реконфігуруваність.

- розвиток принципів організації вимірювально-обчислювальних процесів, таких як планування та розподіл завдань, структурна адаптація, децентралізоване управління та самоорганізація автономних вимірювально-обчислювальних вузлів.

- використання технологій та інструментів моделювання і високорівневого проектування комп'ютерних систем.

- розробка принципів управління цільовим об'єктом, включаючи системи управління, пристрої автоматики та обчислювальну техніку, і створення нових математичних моделей та алгоритмів для обробки та компресії інформації.

- розробка принципів безпечного обміну, опрацювання та зберігання вимірювальної та службової інформації, включаючи забезпечення конфіденційності, цілісності та автентичності інформації, технічного та криптографічного захисту інформаційних зв'язків та управління доступом до них.

Результатом досліджень будуть нові підходи до організації вимірювально-обчислювальних процесів у кіберфізичних системах, розроблені на основі самоорганізації та адаптації, що сприятиме ефективному плануванню та виконанню завдань з управління. Також будуть розроблені нові принципи планування та розподілу завдань, а також технології моделювання комп'ютерних систем.

Дослідження дозволять синтезувати нейронні контролери для управління складними об'єктами, де інформація про об'єкт керування є неповною, а також розробити принципи організації вимірювальних пристроїв та засобів захисту інформації.

Ці результати досліджень стануть основою для створення нових поколінь кіберфізичних систем для різних сфер, включаючи промислове та військове застосування.

Спроектуємо архітектуру кіберфізичної системи БПЛА Shahed з використанням геолокаційних даних на основі розробленого методу(рисунок 4.2):

1. Дані, необхідні для роботи КФС, можуть надходити з різних джерел: радари, оптичні системи, теплові датчики, акустичні датчики, сенсори. Ці різні типи датчиків та систем дозволяють створити комплексну систему виявлення та відстежування БПЛА.

2. Також окремим джерелом є дані з мобільних додатків, таких як єППО, та дзвінків адже при підтвердженні вони модуть бути надзвичайно корисним

джерелом інформації для виявлення БПЛА. Ці дані можуть містити інформацію про місцезнаходження користувачів, яка може бути використана для виявлення БПЛА в області появи повідомлення.

3. Дані зі спеціалізованих систем можуть бути додатковим джерелом інформації для виявлення БПЛА. Ці системи можуть включати радари, камери спостереження, теплові датчики та інші сенсори. Дані з цих систем можуть бути використані для підтвердження виявлення отриманих від інших джерел та для отримання додаткової інформації та дії БПЛА.

4. Передача даних різними каналами зв'язку важливе для забезпечення надійності та ефективності системи виявлення БпЛА. Канали зв'язку які можна використовувати: бездротові канали, кабельні канали, інтернет-зв'язок. Використання різних каналів зв'зку дозволяє забезпечити надійність та ефективність передачі даних у кіберфізичні системі виявлення БПЛА.

5. Сервер в кіберфізичні системі виявлення БПЛА може виконувати різні функції, такі як зберігання та обробка даних, керування системою, комунікація з іншими компонентами системи та надання інтерфейсу для взаємодії з операторoми.

6. База даних у кіберфізичній системі БПЛА може використовуватися для зберігання різноманітної інформації, такої як дані від сенсорів, відомості про виявлення БПЛА, журна подій конфігураційні дані.

7. Обробка та аналіз сигналів в кіберфізичній системі дозволяє ефективно аналізувати та використовувати дані від сенсорів для виявлення для виявлення та відстежування БПЛА в реальному часі.

AIoT (Artificial Intelligence of Things) та кіберфізичні системи мають великий потенціал у виявленні та відстеженні БПЛА, таких як Shahed. AIoT поєднує в собі штучний інтелект (AI) та Інтернет речей (IoT), що дозволяє системам збирати, аналізувати та використовувати дані для прийняття рішень та автоматизації процесів. У випадку системи виявлення БПЛА, AIoT може бути використаний для оптимізації роботи сенсорів, алгоритмів виявлення та прийняття рішень.

Наприклад, система може використовувати дані з різних датчиків (наприклад, радарів, оптичних систем, акустичних датчиків) та мобільних додатків для виявлення та відстеження БПЛА. AI може допомогти у виявленні закономірностей у цих даних та удосконаленні алгоритмів виявлення, що дозволить системі більш ефективно реагувати на наявність БПЛА.

Крім того, кіберфізичні системи можуть використовувати AIoT для підтримки рішень на основі даних з сенсорів та інших джерел. Наприклад, система може автоматично відправляти сигнали тривоги або ініціювати контрзаходи у випадку виявлення БПЛА, що допомагає підвищити швидкість реакції та зменшити втрати.

Таким чином, поєднання AIoT та кіберфізичних систем може стати потужним інструментом у виявленні та відстеженні БПЛА, забезпечуючи високу ефективність та точність системи.

Для розробки вищеописаної кіберфізичної системи виявлення БПЛА Shahed користувачам знадобляться геолокаційні дані, отримані з різних джерел, а також актуальні технічні характеристики всіх відомих БПЛА на момент роботи КФС.

Для цього використаємо моделювання процесу руху БПЛА по кількох раніше зафіксованих траєкторіях руху БПЛА Shahed територією України з точки зору визначення точного часу фіксації та координат БПЛА в цей момент. Ці дані опрацьовуються та готуються до картування за допомогою відповідного AIoT.

При цьому враховується надійність джерела, з якого були отримані дані, відкидаються сумнівні та ненадійні дані. Результати моделювання порівнюються та узгоджуються з фактичними підтвердженими виявленими БПЛА та їхніми маршрутами, отриманими з відкритих джерел.

Крім того, кіберфізична система, що розробляється, буде розраховувати верхню граничну швидкість руху виявленого БПЛА в режимі реального часу, що допоможе вчасно виявляти появу нового БПЛА поблизу виявленого, враховуючи, що БПЛА міг раніше бути невиявлений через особливості місцевості чи несприятливих погодних умов.

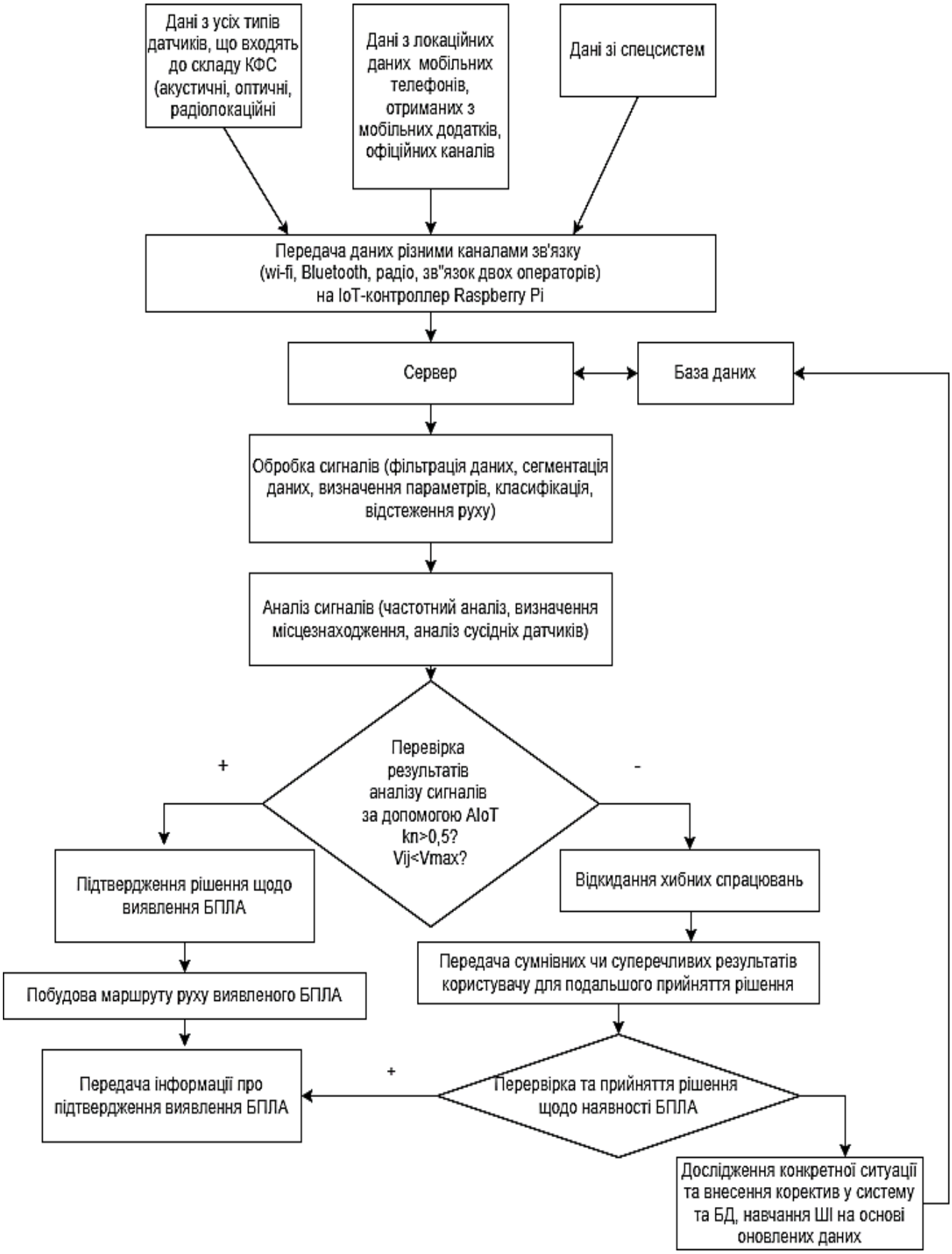


Рисунок 4.2 – Архітектура кіберфізичної системи виявлення БПЛА

Адже, БПЛА не завжди рухається по прямій, і маючи координати двох точок та точний час фіксації цих геолокаційних даних, потрібно зважати, що швидкість руху може бути меншою, траєкторія може змінюватись, і не завжди це є той самий БПЛА.

Отже, виявлення БПЛА Shahed складається з наступних кроків:

1) навчання системи – встановлення набору порогових значень для максимальної швидкості різних БПЛА HS, у випадку виявлення швидкості переміщення між двома сусідніми точками геолокації, яка вище максимального значення множини відомих параметрів, система попереджає про можливе виявлення нового БПЛА та враховує його можливу наявність при подальшому аналізі нових даних; встановлення набору вагових коефіцієнтів для всіх джерел нижче якого рівень алергенів вважається низьким і безпечним;

2) збір геолокаційних даних – визначення розташування кожного датчика, який передав дані про фіксування БПЛА за допомогою системи геолокаційного моніторингу, для створення карти руху виявлених БПЛА;

3) відправлення геолокаційних даних на сервер для подальшого аналізу та обробки;

4) передача даних про виявлення БПА Shahed у певному регіоні,та відправленні на сервер для аналізу та обробки;

5) аналіз даних геолокації, даних про виявлення БПЛА Shahed у певному регіоні, отриманих із карт датчиків кіберфізичної системи, використовуючи аналітичні методи для обробки даних;

6) створення доступної в мобільному додатку кіберфізичної системи карти для виявлення БПЛА Shahed в певному регіоні в заданий час з графічним відображенням Shahed;

Дані в обробленому вигляді одразу відображаються на моніторах операторів.

4.2 Приклади функціонування кіберфізичної системи БПЛА Shahed

Розглянемо приклади використання кіберфізичної системи БПЛА Shahed.

На жаль масові атаки безпілотників відбуваються доволі часто протягом останніх двох років, тому доцільно використати маршрути руху БПЛА Shahed, які вже використовувалися ворогом. На рисунка 4.3-4.10 представлені приблизні маршрути БПЛА Shahed в період з вересня 2023-березень 2024р.

По кожному маршруту було сформовано базу даних з множини I геолокаційних даних, які могли бути отримані з різних джерел, а також точний час їхнього ймовірного виявлення. Ці дані були відповідним чином відсортовані залежно від джерела, з якого були отримані, та оцінені за критерієм надійності.

Наприклад, сигнал від системи Rantelon DTS-2458 отримував коефіцієнт надійності kn_i =0,999, сигнал від радарних датчиків kn_i =0,995, повідомлення від постійного користувача мобільного додатку (єППО), який вже раніше повідомляв виявлення БПЛА чи ракети, і воно було підтверджене, kn_i =0,800, повідомення від нового користувача (єППО), або телефоний дзвінок до поліції від особи що відсутня в базі даних, або знаходиться наокупованій території kn_i =0,200.

Крім точок, які дійсно знаходяться на маршруті руху БПЛА, до множини геолокаційних даних зумисно додаються хибні повідомлення, які можуть мати місце в реальних ситуаціях, коли цивільні особи помилково сприймають схожі звуки від мотоцикла або інших приладів за звуки Shahed, або ж помилкове спрацювання датчиків.

Також в систему вносяться технічні характеристики БПЛА Shahed. В даному дослідженні враховується лише максимальна швидкість серед усіх відомих БПЛА Shahed. В подальшому можна враховувати інші параметри. Система на основі сформованої множини геолокаційних даних отримала задачу побудувати маршрут виявлених БПЛА, відфільтрувавши всі хибні сигнали.

В якості критеріїв, які вливали на результат роботи системи, були коефіцієнт надійності джерела сигналу та максимальна швидкість, яку здатні розвивати відомі БПЛА.

Система аналізувала кожну пару найближчих просторі та часі точок з отриманої множини правдивих та хибних сигналів, і для кожної пари найближчих точок з цієї множини система розраховує відстань S_{ij} (де $1 \leq j \leq i$) по прямій між цими точками за допомогою відомих координат. Поділивши цю відстань S_{ij} на різницю в часі $\Delta t = t_i - t_j$, отримаємо швидкість V_{ij}, з якою ймовірний БПЛА міг переміститися з точки j в точку i по прямій.

Далі система перевіряє чи отримана швидкість не перевищує максимальну швидкість V_{max} відомих моделей БПЛА. В такому випадку точку j і точку i можна з'єднувати. Або ж разі несуттєвого перевищення допускається ймовірність фіксування нового типу БПЛА з вищою швидкістю, про що повідомляється оператору і маршрут між двома точками є не гарантованим але ймовірним (може зображуватися на карті жовтим кольором) та враховуватися в подальшому розрахунку траєкторії руху БПЛА.

Варто зазначити, що якщо ймовірна нова швидкість, яка перевищує V_{max} підтвердиться на подальшому шляху від точки до точки, особливо на маршовому відрізку від кордону з ворогом принаймні кілька разів, то можна і доречно стверджувати про появу нового типу БПЛА який розвиває нову швидкість і це потрібно враховувати при подальших розрахунках ШІ.

Рисунок 4.3 – Приблизний маршрут руху Shahed 26.09.2023 [83]

Рисунок 4.4 – Приблизний маршрут руху Shahed 30.09.2023 [83]

Рисунок 4.5 – Приблизний маршрут руху Shahed 06.10.2023 [83]

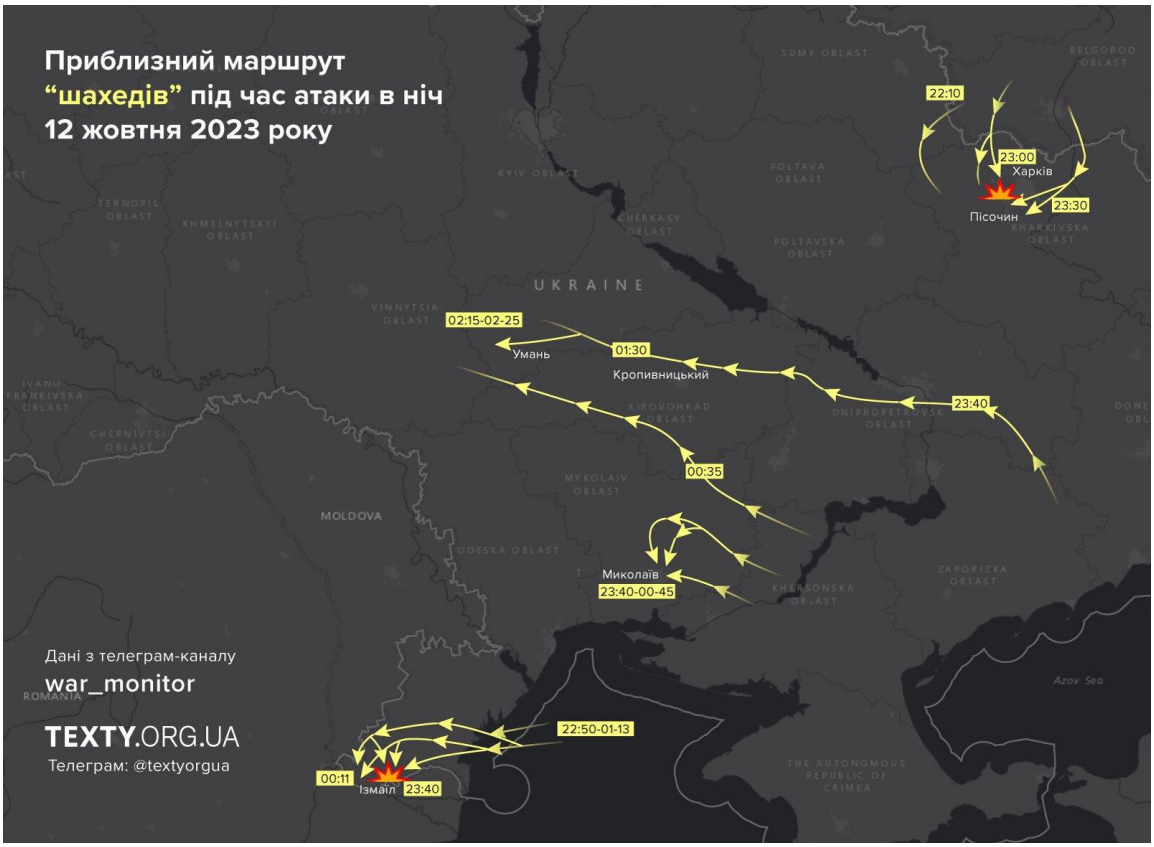


Рисунок 4.6 – Приблизний маршрут руху Shahed 12.10.2023 [83]

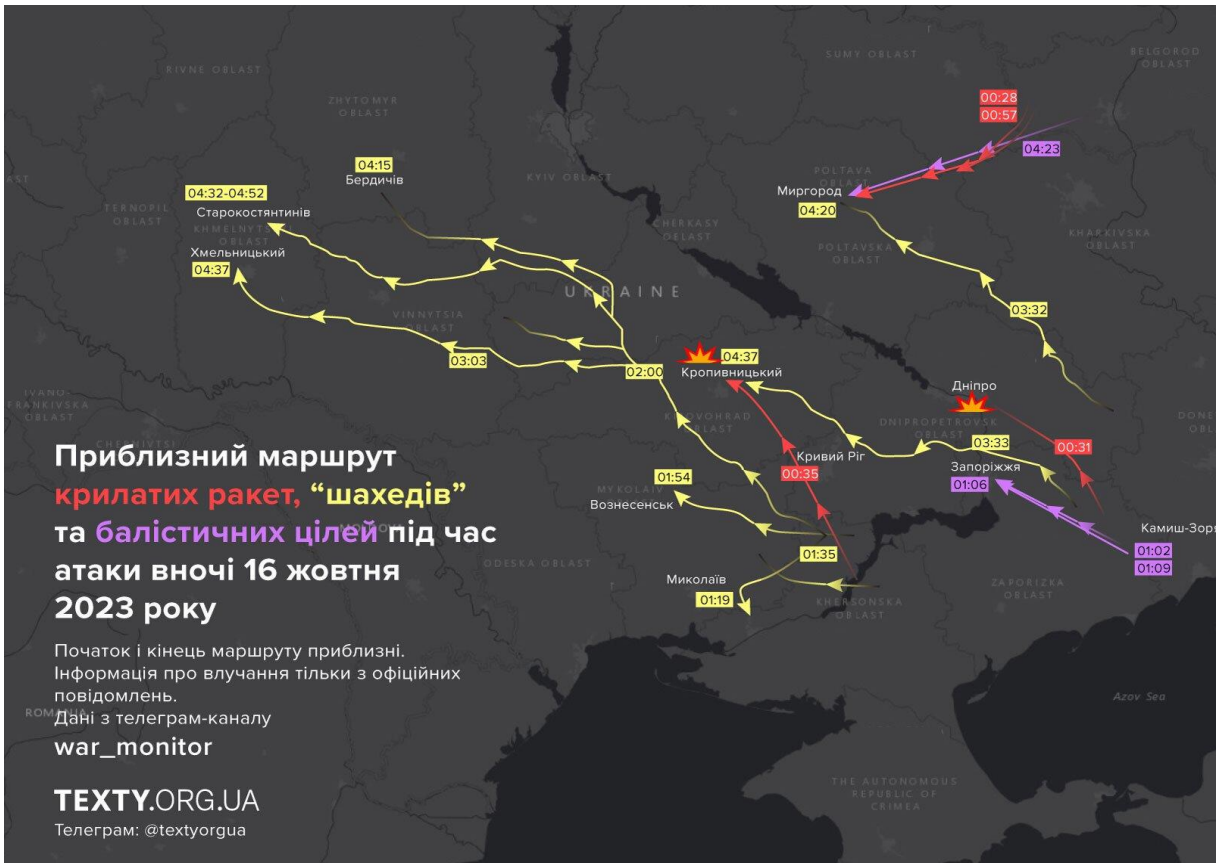


Рисунок 4.7 – Приблизний маршрут руху Shahed 16.10.2023 [83]

Рисунок 4.8 – Приблизний маршрут руху Shahed 2-3.11.2023 [83]

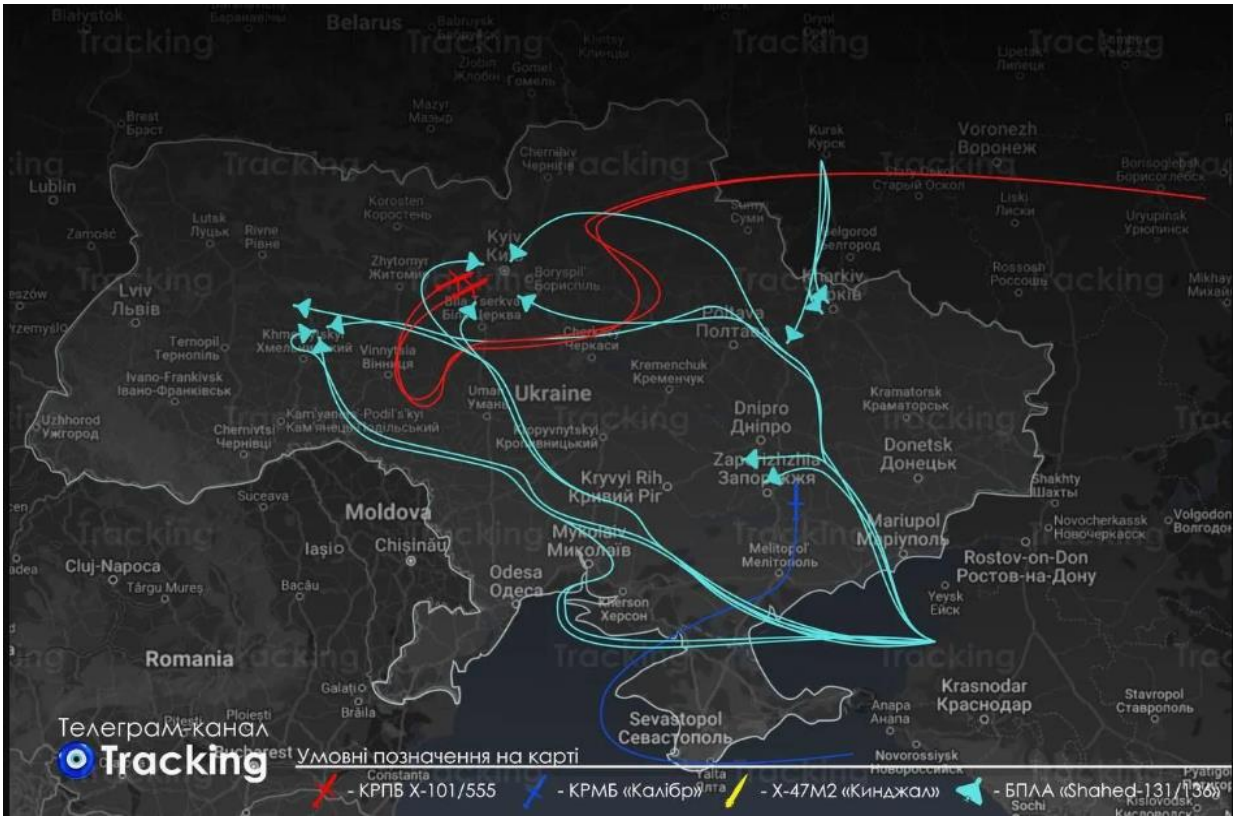


Рисунок 4.9 – Приблизний маршрут руху Shahed 10.11.2023 [83]

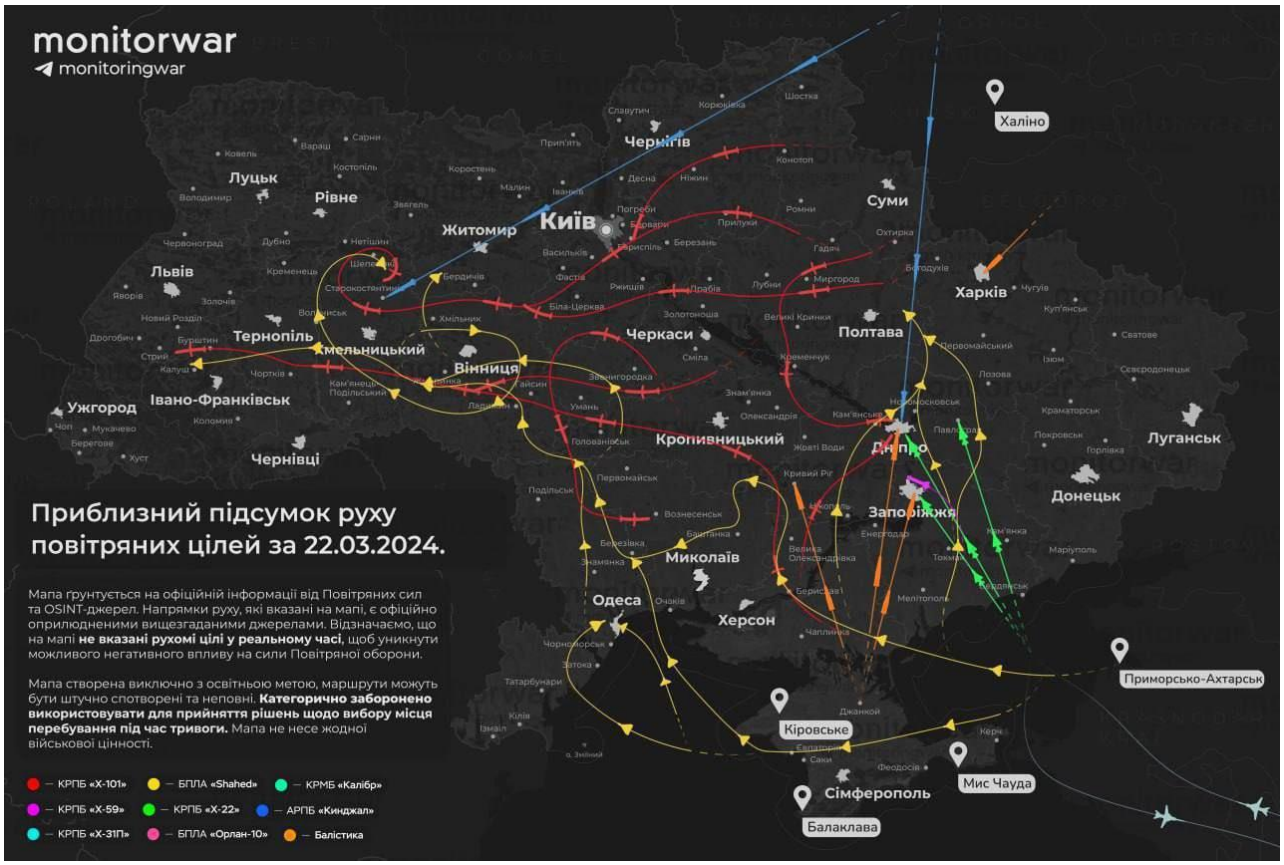


Рисунок 4.10 – Приблизний маршрут руху Shahed 22.03.2024 [83]

Для розробленої кіберфізичної системи виявлення БПЛА Shahed можна створити confusion матрицю, щоб оцінити її ефективність. Модель класифікації буде визначати наявність або відсутність Shahed на основі даних з датчиків, confusion матриця буде використана в якості інструменту для оцінки того, наскільки часто створена модель правильно класифікує наявність БПЛА і як часто будуть виникати помилки.

Тобто, вона покаже кількість правильних і неправильних класифікацій, зроблених запропонованим алгоритмом, порівняно з фактичними класами даних.

Матриця має чотири можливі випадки:

- True Positive (TP) - правильно класифіковані позитивні приклади;
- False Positive (FP) - неправильно класифіковані позитивні приклади;
- True Negative (TN) - правильно класифіковані негативні приклади;
- False Negative (FN) - неправильно класифіковані негативні приклади.

На основі цих значень можна розрахувати різноманітні показники, такі як точність, чутливість, специфічність і т. д., які допомагають оцінити ефективність алгоритму класифікації.

Для експерименту було використано інструменти Open AI, для розробки рішень зі штучного інтелекту, які можна використовувати для аналізу даних з IoT.

Для оцінки отриманих результатів пропонується також розрахувати їхню точність(Accuracy) – відсоток правильно класифікованих прикладів:

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}. \quad (4.1)$$

Результати проведених експериментів на основі Open AI

Таблиця 4.2 – Результати проведених експериментів на основі OpenAI

Номер маршруту	Кількість геоточок	TP	TN	FN	FP	Загальна точність, %
1	500	490	5	2	3	0.984
2	500	490	1	5	4	0.99
3	500	490	4	3	3	0.986
4	500	490	2	2	6	0.984
5	1000	950	0	9	1	0.9989583333
6	1000	950	3	4	3	0.99375
7	1000	950	6	2	2	0.9916666667
8	1000	950	1	7	2	0.996875

Отримані результати допоможуть зрозуміти, наскільки ефективно працює розроблена кіберфізична система виявлення БПЛА Shahed.

4.3 Висновки

У четвертому розділі було розроблено кіберфізичну систему виявлення БПЛА Shahed описано та розгянуто функціонування цієї системи. Також було проведено аналіз приблизних маршрутів руху Shahed та був проведений експеремент в якому використали інструменти Open AI, для розробки рішень зі штучного інтелекту.

За допомогою результатів можна оцінити ефективність роботи кіберфізична система виявлення БПЛА Shahed.

ВИСНОВКИ

В результаті проведених теоретичних та практичних досліджень була створена кіберфізична система для виявлення безпілотних літальних апаратів Shahed.

У першому розділі розглянуто відомі методи, способи та засоби для виявлення безпілотника Shahed, його характеристики, а також варіанти застосування, виявлення і боротьби з БПЛА.

У другому розділі кваліфікаційної роботи описані компоненти кіберфізичних систем та досягнення у їх розробці. Визначені проблеми, які виникають у побудові таких систем, і висунуті принципи створення апаратно-програмної платформи для розробки прикладних кіберфізичних систем. Розглянуті напрямки досліджень у галузі кіберфізичних систем та очікувані результати.

Також у даному розділі розроблено критерії для виявлення БПЛА Shahed залежно від джерела з якого отримано сигнал про можливе виявлення БПЛА, а також критерії максимальної швидкості що базується на відомих технічних характеристиках БПЛА Shahed. Дані критерії надійності джерела та максимальної швидкості буде покладено в основу методу виявлення БПЛА з використанням геолокаційних даних.

У третьому розділі було запропоновано метод виявлення БПЛА Shahed, з використанням штучного інтелекту речей, для обробки геолокаційних даних та точного часу фіксації ймовірного виявлення БПЛА Shahed, завдяки фільтрації хибних повідомлень зберігається мобільність груп реагування та підвищується рівень безпеки.

Окрім цього у розділі 3 кваліфікаційної роботи розроблено алгоритм виявлення БПЛА Shahed з використання геолокаційних даних, за яким буде здійснюватися виявлення БПЛА Shahed, буде прийматися рішення щодо кількості ворожих БПЛА у повітряному просторі, та візуалізація їхніх маршрутів руху. Розроблений алгоритм забезпечує комплексний підхід до виявлення БПЛА Shahed

оскільки передбачає отримання інформації з різних джерел, з різним ступенем надійності, а також враховує накопичений досвід та передбачає постійне навчання системи.

У четвертому розділі було розроблено кіберфізичну систему виявлення БПЛА Shahed описано та розгянуто функціонування цієї системи. Також було проведено аналіз приблизних маршрутів руху Shahed та був проведений експеремент в якому використали інструменти Open AI, для розробки рішень зі штучного інтелекту.

За допомогою результатів можна оцінити ефективність роботи кіберфізична система виявлення БПЛА Shahed.

Набула подальшого розвитку інформаційна технологія кіберфізичної системи виявлення БПЛА Shahed.

Впровадження результатів роботи дозволили розробити кіберфізичну систему виявлення БПЛА Shahed.

За темою кваліфікаційної роботи магістра опубліковано одну публікацію у Збірнику наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2023» (Хмельницький – 2023. – С. 250-251).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. 10 технологій виявлення та протидії БПЛА. URL: https://bezpeka.club/10-technologies-for-detecting-countering-drones/. (дата звернення: 24.03.2024).

2. Darabseh A., Freris N. M. A software defined architecture for cyberphysical systems. *Fourth International Conference on Software Defined Systems (SDS)*, 2017. pp. 54-60.

3. Al-Haija Abu. Q., Badawi Al.A. High-performance intrusion detection system for networked UAVs via deep learning. *Neural Comput*. Appl. 2022. pp. 34.

4. Alladi T., Bansal G., Chamola V., Guizani M. SecAuthUAV: A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication. *IEEE Trans. Veh. Technol*. 2020. pp. 69.

5. Altawy. R., Youssef A.M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber-Phys*. Syst. 2016. pp. 1–25.

6. Mohammad Fadilah Bin, Balachandran M.S., Loh V., Chua P. M. DRAT: A Drone Attack Tool for Vulnerability Assessment. *In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA*, 16–18 March 2020. pp. 153–155.

7. Bisio I., Garibotto C., Lavagetto F., Sciarrone A., Zappatore S. Unauthorized amateur UAV detection based on WiFi statistical fingerprint analysis. *IEEE Commun*. Mag. 2018. pp 106–111.

8. Bouafif H., Kamoun F., Iqbal F., Marrington A. Drone forensics: Challenges and new insights. *In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 26–28 February 2018. pp. 1–6.

9. Chiper F.L., Martian A., Vladeanu C., Marghescu I., Craciunescu R., Fratu O. *Drone detection and defense systems: Survey and a software-defined radio-based solution*. Sensors 2022. pp. 22.

10. Choudhary G., Sharma V., You I., Yim K., Chen R., Cho J.H. Intrusion detection systems for networked unmanned aerial vehicles: A survey. *In Proceedings of the 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*, Limassol, Cyprus, 25–29 June 2018. pp. 560–565.

11. Čisar P., Pinter R., Čisar S.M., Gligorijević M. Principles of Anti-Drone Defense. *In Proceedings of the 2020 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom)*, Mariehamn, Finland, 23–25 September 2020. pp. 19–26.

12. Condomines J.P., Zhang R., Larrieu N. *Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation*. Ad Hoc Netw. 2019. pp. 90.

13. Dey V., Pudi V., Chattopadhyay A., Elovici Y. Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. *In Proceedings of the 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, Pune, India, 6–10 January 2018. pp. 398–403.

14. Elands P., de Kraker J., Laarakkers J., Olk J., Schonagen J. *Technical Aspects Concerning the Safe and Secure Use of Drones*. TNO: Den Haag, The Netherlands, 2016.

15. Fei F., Tu Z., Yu R., Kim T., Zhang X., Xu D., Deng X. Cross-layer retrofitting of UAVs against cyber-physical attacks. *In Proceedings of the 2018 IEEE International Conference on Robotics and Automation (ICRA)*, Brisbane, QLD, Australia, 21–25 May 2018. pp. 550–557.

16. Fotouhi A., Qiang H., Ding M., Hassan M., Giordano L.G., Garcia-Rodriguez A., Yuan J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor*. 2019. pp. 3417–3442.

17. Fu R., Ren X., Li Y., Wu Y., Sun, H., Al-Absi M.A. Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection. *IEEE Internet Things J*. 2023. pp. 1.

18. Gope P., Sikdar B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. *IEEE Trans. Veh. Technol*. 2020. pp. 69.

19. GÜLATAŞ İ., BAKTIR S. Unmanned aerial vehicle digital forensic investigation framework. *J. Nav. Sci. Eng*. 2018. pp. 32–53.

20. Hadi H.J., Cao Y., Nisa K.U., Jamil A.M., Ni Q. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *J. Netw. Comput*. Appl. 2023 pp. 213.

21. Hamza A., Akram U., Samad A., Khosa S.N., Fatima R., Mushtaq M.F. Unmaned Aerial Vehicles Threats and Defence Solutions. *In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 5–7 November 2020. pp. 1–6.

22. Hosseinzadeh M., Sinopoli B. Active attack detection and control in constrained cyber-physical systems under prevented actuation attack. *In Proceedings of the 2021 American Control Conference (ACC)*, New Orleans, LA, USA, 25–28 May 2021. pp. 3242–3247.

23. Khan A.A., Beg O.A., Alamaniotis M. Ahmed S. Intelligent anomaly identification in cyber-physical inverter-based systems. *Electr. Power Syst. Res*. 2021. pp. 193.

24. Khan, N.A., Brohi S.N., Jhanjhi, N. UAV's applications, architecture, security issues and attack scenarios: A survey. In Intelligent Computing and Innovation on Data Science. *Springer*: Singapore, 2020. pp. 753–760.

25. Khan N.A., Jhanjhi N.Z., Brohi S.N., Nayyar, A. Emerging use of UAV's: Secure communication protocol issues and challenges. *In Drones in Smart-Cities; Elsevier: Amsterdam*, The Netherlands, 2020. pp. 37–55.

26. Kim K., Kang Y. Drone security module for UAV data encryption. *In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Republic of Korea, 21–23 October 2020. pp. 1672–1674.

27. Motlagh N.H., Taleb T., Arouk O. Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. *IEEE Internet Things J*. 2016. pp. 899–922.

28. Nagarajan S.M., Deverajan G.G., Bashir A.K., Mahapatra R.P., Al-Numay M.S. IADF-CPS: Intelligent Anomaly Detection Framework towards Cyber Physical Systems. *Comput. Commun*. 2022. pp. 81–89.

29. Park S., Kim H.T., Lee S., Joo H., Kim H. Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access* 2021. pp. 635–659.

30. Pojsomphong N., Visoottiviseth V., Sawangphol W., Khurat A., Kashihara S., Fall D. Investigation of Drone Vulnerability and its Countermeasure. *In Proceedings of the 2020 IEEE 10th Symposium on Computer Applications Industrial Electronics (ISCAIE)*, Penang, Malaysia, 18–19 April 2020. pp. 251–255.

31. Praveena V., Vijayaraj A., Chinnasamy P., Ali I., Alroobaea R., Alyahyan S.Y., Raza M.A. Optimal Deep Reinforcement Learning for Intrusion Detection in UAVs. *Comput. Mater. Contin*. 2022. pp. 2639–2653.

32. Rana T., Shankar A., Sultan M.K., Patan R., Balusamy B. An intelligent approach for UAV and drone privacy security using blockchain methodology. *In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, Noida, India, 10–11 January 2019. pp. 162–167.

33. Rani C., Modares H., Sriram R., Mikulski D., Lewis F.L. Security of unmanned aerial vehicle systems against cyber-physical attacks. *J. Def. Model. Simul*. 2016. pp. 331–342.

34. Renyu Z., Kiat S.C., Kai W., Heng Z. Spoofing attack of drone. *In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 7–10 December 2018, pp. 1239–1246.

35. Restituyo R., Hayajneh T. Vulnerabilities and attacks analysis for military and commercial iot drones. *In Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 8–10 November 2018. pp. 26–32.

36. Rodday N.M., Schmidt R.d.O., Pras A. Exploring security vulnerabilities of unmanned aerial vehicles. *In Proceedings of the NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey, 25–29 April 2016. pp. 993–994

37. Salamh F.E., Mirza M.M., Karabiyik U. UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. *Electronics* 2021 pp. 733.

38. Sciancalepore S., Ibrahim O.A., Oligeri G., Di Pietro R. Detecting drones status via encrypted traffic analysis. *In Proceedings of the ACM Workshop on Wireless Security and Machine Learning*, Miami, FL, USA, 15–17 May 2019. pp. 67–72.

39. Shafique A., Mehmood A., Elhadef M. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access* 2021.pp. 927–948.

40. Shahed 136 та Shahed 131. URL: https://nv.ua/ukr/ukraine/events/shahedi-shahed-136-i-131-u-chomu-riznicya-harakteristiki-nedoliki-ta-infografika-novini-ukrajini-50327025.html. (дата звернення: 01.04.2024).

41. SHAHED-131. URL: https://defence-ua.com/weapon_and_tech/ne_tilki_shahed_136_zjavilos_detalne_doslidzhennja_sche_odnogo_iranskogo_drona_kamikadze_jakij_vikoristovuje_rf-9033.html. (дата звернення:16.04.2024).

42. SHAHED-136. URL: https://osvitoria.media/experience/koly-atakuyut-drony-kamikadze-shahed-136-yak-rozpiznaty-ta-zahystytys/. (дата звернення: 14.04.2023).

43. SHAHED-136. URL: https://sprotyvg7.com.ua/lesson/rekomendacii-pidrozdilam-shhodo-borotbi-z-bezpilotnimi-litalnimi-aparatami-kamikadze-shahed-136-geran-2. (дата звернення: 06.04.2024).

44. SHAHED-136. URL: https://suprotyv.com/bpla/shahed-136/. (дата звернення 19.04.2024).

45. SHAHED-136. URL: https://uk.wikipedia.org/wiki/Шахед-136. (дата звернення: 15.04.2024).

46. SHAHED-136. URL: https://www.ukrinform.ua/rubric-ato/3580083-iranski-droni-shahed136-zbivati-ih-uze-mozna-ale-ce-se-ne-prosto.html. (дата звернення: 10.04.2024).

47. Shin J.M., Kim Y.S., Ban T.W., Choi S., Kang K.M., Ryu J.Y. Position tracking techniques using multiple receivers for anti-drone systems. *Sensors* 2021, pp. 21-35.

48. Shrestha R., Omidkar A., Roudi S.A., Abbas R., Kim S. Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks. *Electronics* 2021. pp. 1549.

49. Shulepov A., Novikova E., Murenin I. Approach to Anomaly Detection in Cyber-Physical Object Behavior. In Intelligent Distributed Computing XIV. Camacho D., Rosaci D., Sarné G.M.L., Versaci M., Eds. *Springer International Publishing: Cham*, Switzerland, 2022. pp. 417–426.

50. Siddappaji B., Akhilesh K. Role of cyber security in drone technology. *In Smart Technologies*. Springer: Berlin/Heidelberg, Germany, 2020. pp. 169–178.

51. Teng L., Jianfeng M., Pengbin F., Yue M., Xindi M., Jiawei Z., Gao C., Di L. Lightweight security authentication mechanism towards uav networks. *In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA)*, Daegu, Republic of Korea, 10–13 October 2019. pp. 379–384.

52. Yaacoub J.P., Noura H., Salman O., Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* 2020. pp. 11-18.

53. Zhang G., Wu Q., Cui M., Zhang R. Securing UAV communications via trajectory optimization. *In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference*, Singapore, 4–8 December 2017. pp. 1–6.

54. АЕРОСКОП: СИСТЕМА ВИЯВЛЕННЯ ДРОНІВ. URL: https://elitebike.ua/aeroskop-sistema-viyavlennya-droniv. (дата звернення: 14.04.2024).

55. БПЛА. URL: https://boryviter.org.ua/multirotor-drones/. (дата звернення 10.04.2024).

56. Кіберфізична система. URL: https://ieeexplore.ieee.org/document/10368002. (дата звернення 06.04.2024).

57. Кіберфізична система. URL: https://moodle.znu.edu.ua/course/view.php?id=15556. (дата звернення: 27.02.2024).

58. Кіберфізична система. URL: https://pharmsfera.com/blog/15/. (дата звернення: 29.02.2024).

59. Кіберфізична система. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2018/sep/14522/06st.pdf. (дата звернення: 26.02.2024).

60. Кіберфізична система. URL: https://uk.wikipedia.org/wiki/. (дата звернення: 05.02.2024).

61. Кіберфізична система. URL: https://www.wikidata.uk-ua.nina.az. (дата звернення: 22.02.2024).

62. Комплекс виявлення дронів “Плутон”. URL: https://mil.in.ua/uk/blogs/kompleks-vyyavlennya-droniv-pluton/. (дата звернення: 21.03.2024).

63. Протидронові системи. URL: https://prodrone.com.ua/sistemi-bezpeki/. (дата звернення: 17.04.2024).

64. Радіолокаційна система виявлення дронів. URL: https://ua.alasartech-security.com/drone-detection/radar-drone-detection-system/c-band-radar-detection.html. (дата звернення: 09.04.2024).

65. Система Виявлення БПЛА AARTOS DDS X3. URL: https://airunit.com.ua/aartos-dds-x3/. (дата звернення: 19.03.2024).

66. Система виявлення БПЛА ARDRONIS. URL: https://inkotel.com.ua/ru/sistema-avtomaticheskogo-obnaruzheniya-i-podavleniya-bpla-dr/. (дата звернення: 23.04.2024).

67. Система виявлення БПЛА ARonia AG. URL: https://airunit.com.ua/aaronia-ag/. (дата звернення: 12.04.2024).

68. Система виявлення БПЛА. URL: https://defence-ua.com/people_and_company/v_ukrajini_rozrobili_pasivnu_sistemu_jaka_zdatna_vijav

ljati_bud_jaki_bpla_zalishajuchis_nepomichenoju-4647.html. (дата звернення: 20.03.2024).

69. Система виявлення БПЛА. URL: https://uav-bpla.com/obnaruzhenie_bpla/?ysclid=lt099jqoaq375382069. (дата звернення: 18.02.2024).

70. Система виявлення БПЛА FENEK. URL: https://fenek.com.ua/. (дата звернення: 14.04.2024).

71. Система виявлення БПЛА. URL: https://goobkas.com/ua/p1167896025-sistema-viyavlennya-bezpilotnih.html. (дата звернення: 12.04.2024).

72. Система виявлення БПЛА. URL: https://life.pravda.com.ua/society/2023/09/2/256312/. (дата звернення: 15.03.2024).

73. Система виявлення БПЛА. URL: https://store.quadro.ua/detektor-droniv-rantelon-dts-2458-opis-mozhlivostey-ta-printsip-roboti/. (дата звернення: 14.04.2024).

74. Система виявлення БПЛА. URL: https://uav-bpla.com/obnaruzhenie_bpla/?ysclid=lt099jqoaq375382069. (дата звернення: 06.04.2024).

75. Система виявлення дронів DDSR1 V2. URL: https://www.kseonics-technology.com.ua/ddsr1/. (дата звернення: 14.03.2024).

76. Система виявлення дронів DRONELYZER. URL: https://store.drone.ua/systema-vyiavlennia-droniv-dronelyzer/. (дата звернення: 10.04.2024).

77. Система виявлення дронів аероскоп Rantelon DTS-2458 Aeroscop. URL: https://elitebike.ua/sistema-obnaruzheniya-dronov-detektor-rantelon-dts-245. (дата звернення: 17.04.2024).

78. Система захисту від БПЛА SurveilSPIRE. URL: https://armyinform.com.ua/2023/10/17/systema-zahystu-vid-bpla-surveilspire-velyki-sposterezhni-mozhlyvosti-j-minimum-personalu/. (дата звернення: 15.04.2024).

79. Системи виявлення дронів DJI Aeroscope. URL: https://airunit.com.ua/dji-aeroscope/. (дата звернення: 20.03.2024).

80. Системи виявлення дронів і протидронні системи. URL: https://www.bezpeka-shop.com/ua/blog/obzor/sistemy-obnaruzheniya-dronov-i-protivodronnye-sistemy/. (дата звернення: 08.04.2024).

81. Системи для перехоплення Shahed. URL: https://dev.ua/news/shahid-1665663459. (дата звернення: 11.04.2024).

82. Технічні характеристики Shahed. URL: https://focus.ua/uk/digital/606703-zlitaye-z-pikapa-u-merezhi-pokazali-virobnictvo-ta-viprobuvannya-reaktivnogo-shahed-171-video (дата звернення: 15.04.2024).

83. Типові маршрути БПЛА Shahed. URL: https://texty.org.ua/fragments/110886(дата звернення 19.04.2024).

ДОДАТОК А
(обов’язковий)

КОПІЯ СТАТІ У ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ XV ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «АКТУАЛЬНІ ПРОБЛЕМИ КОМП’ЮТЕРНИХ НАУК АПКН-2023»

УДК 004.4

Присяжнюк О.О.

Хмельницький національний університет

ДОСЛІДЖЕННЯ ТА ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект – це сукупність раціональних, логічних і формалізованих інструментів правила, розроблені та закодовані людьми, які організовують процеси та діяльність наслідування раціональних/інтелектуальних структур та створюють та відтворювати цілеспрямовані практики, а також механізми побудови подальшого кодування та прийняття рішень.

Artifcial Intelligence is an ensemble of rational, logical, and formalized instrumental rules developed and coded by human beings that organize the processes and activities to emulate rational/intellectual structures and fabricate and reproduce goal-oriented practices as well as the mechanisms for constructing further coding and decision making.

Штучний інтелект з'являється у свідомості людей як комбінація трьох тверджень - явища, проблеми і фрази (або концепції).

Як явище повсякденного життя, штучний інтелект не може бути розкритий іншим способом, крім як у формі матеріалізованих (відчутних) продуктів/пристроїв. Таким чином, ці пристрої мають подвійне призначення — технічне і соціальне. З одного боку, штучний інтелект постає як технологічний пристрій, призначений для вирішення завдання, яке неможливе для людини. З іншого боку, штучний інтелект існує не тільки в технічному середовищі. Технології, спочатку орієнтовані на інструментальні завдання, стають середовищем існування і учасниками людських взаємодій. Цю тенденцію називаємо “штучною соціальністю”[1].

Як дослідницька проблема, штучний інтелект: (1) піднімає філософські (світоглядні) питання; (2) по-новому характеризує соціальну реальність; проливає нове світло на специфіку і потенціал соціальної реальності; закликає переглянути панівні уявлення про соціальну реальність; (3) проявляється по-різному в різних науках. Для природничих та інженерних наук проблеми штучного інтелекту пов'язані з вирішенням технічних та інструментальних завдань. Для соціології та інших суспільних наук питання про штучний інтелект, по суті, є маргінальним, побічним питанням. У філософії, як і в гуманітарних науках в цілому, штучний інтелект обговорюється у зв'язку зі світоглядними проблемами, які по-різному вирішувалися в різні історичні епохи і в різних інтелектуальних традиціях.

Як словосполучення (концепція) в науковій літературі, штучний інтелект ще не визначений але має загальноприйняте значення.

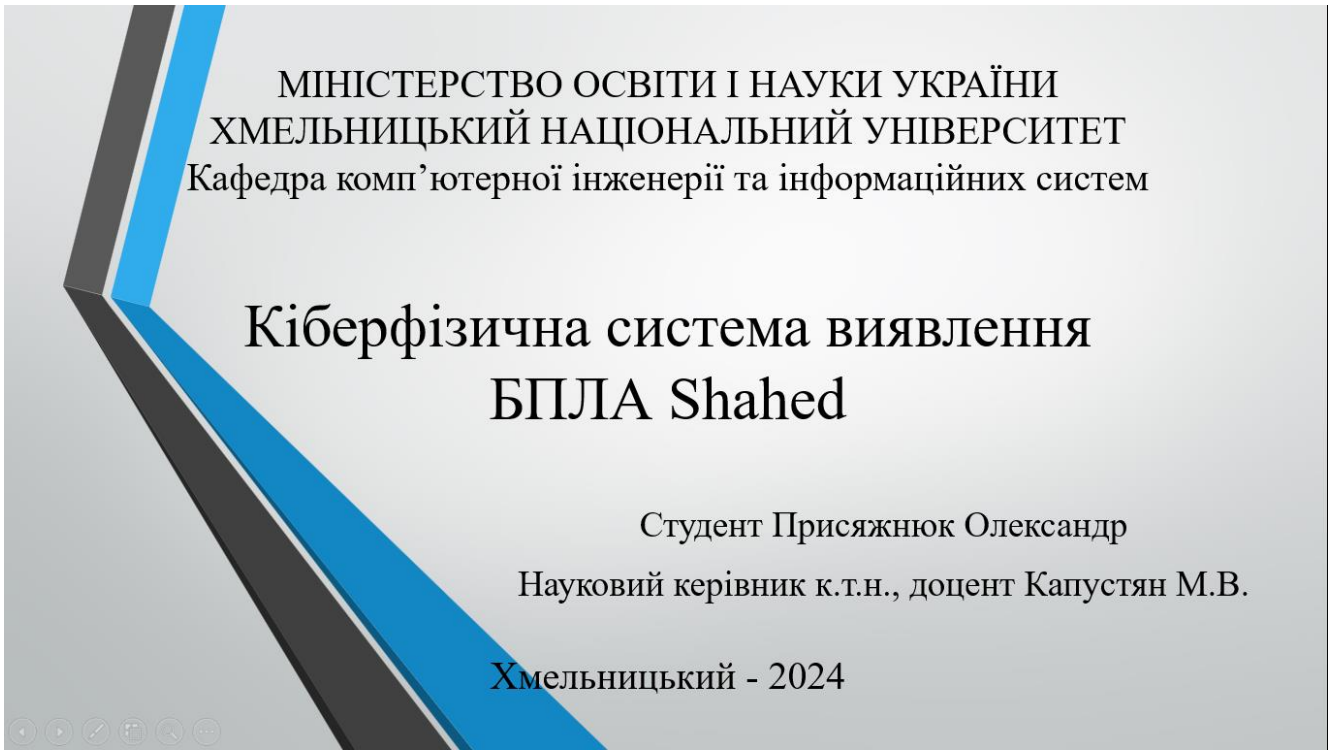
Однак вчені повинні прийти до згоди у визначенні ШІ, щоб перейти до раціонального мислення про впровадження ШІ в реальність людського життя і суспільного розвитку.

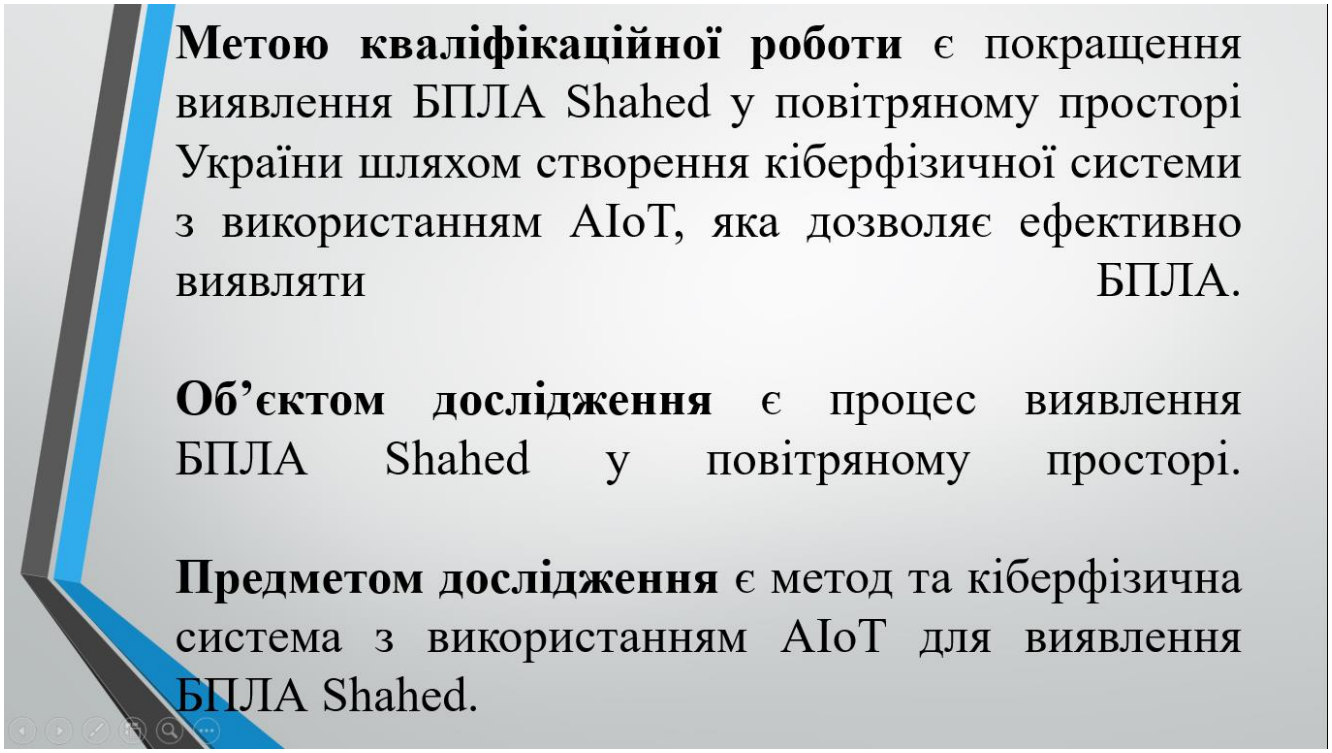
Перелік посилань

1. Rezaev A. V. (2021) Twelve thoughts on Artifcial Intelligence and Artifcial Sociality.
2. Pigge E., Tzudnowski I. Kuenstliche Intelligenz: Continental staerkt weltweites Experten-Netzwerk bis 2021.
3. Як створюється штучний інтелект. URL: https://lemon.school/blog/yak-stvoryuyetsya-shtuchnyj-intelekt
4. Штучний інтелект та artificial intelligence ACT. URL: https://cedem.org.ua/analytics/artificial-intelligence-act/
5. Історія розвитку «Штучного інтелекту в ІК». URL: https://web.archive.org/web/20131203002125/http://www.iprinet.kiev.ua/gf/serg1.htm

ДОДАТОК Б
(обов'язковий)

ПРЕЗЕНТАЦІЯ ДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ





НАУКОВА НОВИЗНА ОТРИМАНИХ РЕЗУЛЬТАТІВ

- вперше розроблено архітектуру кіберфізичної системи для виявлення БПЛА Shahed, яка використовує AIoT для обробки геолокаційних даних в процесі виявлення БПЛА.
- вперше запропоновано використання AIoT для якісної та швидкої побудови маршрутів руху виявлених БПЛА.

Практична значимість отриманих результатів

- полягає у підвищенні безпеки та захисту важливих об'єктів від незаконного використання БПЛА завдяки вчасному виявленню. Також швидке та точне виявлення БПЛА дозволяє операторам ефективно реагувати на можливі загрози і небезпечні ситуації та вживати необхідні заходи безпеки щоб мінімізувати можливі наслідки.

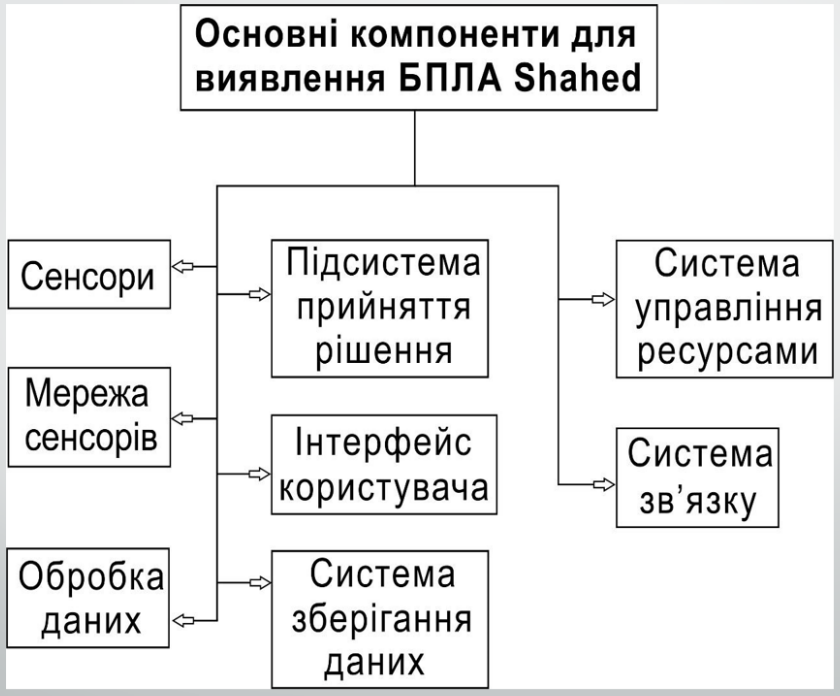
ПУБЛІКАЦІЯ

Опубліковано публікацію у Збірнику наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023» (Хмельницький – 2023. – С. 250-251)

Актуальність роботи полягає в створенні кіберфізичної системи для виявлення БПЛА. Розробка такої системи може сприяти підвищенню безпеки, ефективності та контролю за повітряним простором. Важливими аспектами роботи є розробка методу виявлення та відстеження БПЛА Shahed, інтеграція з існуючими системами безпеки та забезпечення високої точності та надійності системи в умовах реального використання.

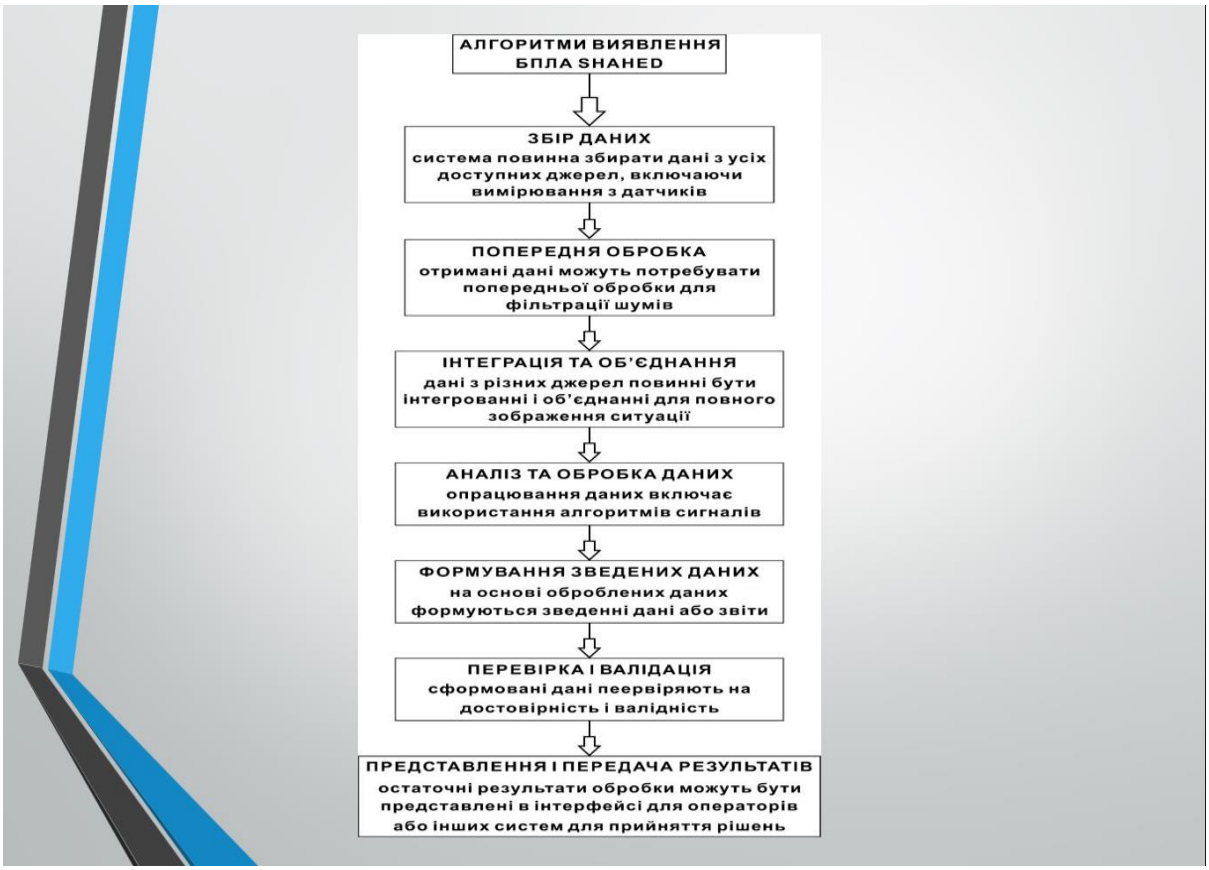
Безпілотний літальний апарат (БПЛА) - це повітряний транспортний засіб, який керується дистанційно або автономно без присутності людини на борту.

БПЛА є універсальним інструментом, який знаходить застосування у різних галузях завдяки своїй здатності виконувати завдання, які раніше були недоступні або складні для виконання традиційними методами.



Використовуються такі методи для виявлення БПЛА Shahed:

- Акустичний
- Радіочастотний
- Візуальний
- Радіолокаційний



Архітектура кіберфізичної системи виявлення БПЛА

ВИСНОВКИ

В результаті проведених теоретичних та практичних досліджень була створена кіберфізична система для виявлення безпілотних літальних апаратів Shahed.

- У першому розділі розглянуто відомі методи, способи та засоби для виявлення безпілотника Shahed, його характеристики, а також варіанти застосування, виявлення і боротьби з БПЛА.
- У другому розділі кваліфікаційної роботи описані компоненти кіберфізичних систем та досягнення у їх розробці. Визначені проблеми, які виникають у побудові таких систем, і висунуті принципи створення апаратно-програмної платформи для розробки прикладних кіберфізичних систем. Розглянуті напрямки досліджень у галузі кіберфізичних систем та очікувані результати. Також у даному розділі розроблено критерії для виявлення БПЛА Shahed залежно від джерела з якого отримано сигнал про можливе виявлення БПЛА, а також критерії максимальної швидкості що базується на відомих технічних характеристиках БПЛА Shahed. Дані критерії надійності джерела та максимальної швидкості буде покладено в основу методу виявлення БПЛА з використанням геолокаційних даних

- У третьому розділі було запропоновано метод виявлення БПЛА Shahed, з використанням штучного інтелекту речей, для обробки геолокаційних даних та точного часу фіксації ймовірного виявлення БПЛА Shahed, завдяки фільтрації хибних повідомлень зберігається мобільність груп реагування та підвищується рівень безпеки.

- Окрім цього у розділі 3 кваліфікаційної роботи розроблено алгоритм виявлення БПЛА Shahed з використання геолокаційних даних, за яким буде здійснюватися виявлення БПЛА Shahed, буде прийматися рішення щодо кількості ворожих БПЛА у повітряному просторі, та візуалізація їхніх маршрутів руху. Розроблений алгоритм забезпечує комплексний підхід до виявлення БПЛА Shahed оскільки передбачає отримання інформації з різних джерел, з різним ступенем надійності, а також враховує накопичений досвід та передбачає постійне навчання системи.

- У четвертому розділі було розроблено кіберфізичну систему виявлення БПЛА Shahed описано та розгянуто функціонування цієї системи. Також було проведено аналіз приблизних маршрутів руху Shahed та був проведений експеремент в якому використали інструменти Open AI, для розробки рішень зі штучного інтелекту.

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016265517

Дата перевірки:
20.05.2024 17:32:34 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
20.05.2024 19:12:58 EEST

ID користувача:
100005591

Назва документа: Присяжнюк_2_Кіберфізична система виявлення БПЛА Shahed

Кількість сторінок: 82 Кількість слів: 13911 Кількість символів: 108884 Розмір файлу: 6.72 MB ID файлу: 1016055449

1.11%
Схожість

Найбільша схожість: 0.63% з джерелом з Бібліотеки (ID файлу: 1011153750)

0.98% Джерела з Інтернету 17 ..... Сторінка 84

0.78% Джерела з Бібліотеки 41 ..... Сторінка 84

0.78% Цитат

Цитати 5 ..... Сторінка 85

Не знайдено жодних посилань

71.8%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

11.7% Вилучення з Інтернету 852 ..... Сторінка 86

71.8% Вилученого тексту з Бібліотеки 60 ..... Сторінка 88

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Заміжені символи 1

Wed May 15 06:25:47 EEST 2024, Медзатий Дмитро Миколайович, Хмельницький національний університет, Т

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 16%**

ID: 126266 Назва: МКР Кіберфізична система виявлення БПЛА Shahed Додано в БД: 2024-05-15 Автора: Присяжнюк О.О. Керівники: Капустян М.В. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	89094	693	1817 (2%)	17 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Присяжнюк Олександр Олександрович

Тема: Кіберфізична система виявлення БПЛА Shahed

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість сторінок записки 70 стор.

1. Короткий зміст роботи та прийнятих рішень: метою кваліфікаційної роботи є створення кіберфізичної системи виявлення БПЛА Shahed шляхом використання AIoT.

2. Висновок про відповідність роботи дипломному завданню: робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки та передових методів роботи: проведено огляд різних способів та засобів виявлення БПЛА Shahed. Кожний спосіб має свої переваги та недоліки, які потрібно враховувати при виборі оптимального рішення конкретної системи. Звісно, тематика має пряме відношення до систем, які використовуються військовими, та доступ до них дуже обмежений. Тому глибоке дослідження за даною тематикою неможливе, або вимагає спеціального доступу та грифу роботи. Однак перспектива використання штучного інтелекту речей є беззаперечною, тому дослідження в цьому напрямку є доцільними, особливо для таких актуальних задач як виявлення безпілотних літальних апаратів.

В роботі проведено огляд відомих способів та засобів виявлення безпілотних апаратів типу Shahed. Запропоновано архітектуру кіберфізичної системи та метод виявлення БПЛА Shahed з використанням AIoT.

В результаті проведення експерименту з двома системами, а саме Google Cloud IoT та OpenAI, які надають інструменти для розробки рішень з штучного інтелекту, та які можна використовувати для аналізу даних з IoT, виявлено, що системи ефективно використовують результати навчання на основі бази даних. Також для кожної системи обчислено точність отриманих результатів, проведено порівняльний аналіз. Запропонований метод демонструє високу ефективність, забезпечуючи достатню точність виявлення безпілотних літальних апаратів.

4. Позитивні сторони кваліфікаційної роботи: отримання наукової новизни.

5. Негативні сторони роботи: специфіка теми, яка створює істотні обмеження при проведенні глибокого дослідження.

6. Оцінка графічного оформлення та пояснювальної записки роботи: пояснювальна записка оформлена коректно, згідно з діючими стандартами оформлення документації.

7. Відгук про роботу в цілому: робота виконана на достатньому науково-технічному рівні.

8. Інші зауваження: в робота присутні граматичні помилки, різні варіанти скорочення термінів.

9. Оцінка кваліфікаційної роботи: задовільно/D.

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Мартинюк Валерій Валентинович, дтн, професор, завідувач кафедри АКІТ, ХНУ

«14» травня 2024 р. _____ (підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Присяжнюка Олександра Олександровича
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

22 квітня 2024 року

О. [signature]

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Кіберфізична система виявлення БПЛА Shahed

Автор: Присяжнюк Олександр Олександрович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Капустян М.В., к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості Unicheck, складає 1.11% і адресується до 17 першоджерела; та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ М. В. Капусятн

Гарант ОП _____ О. С. Савенко

Завідувач кафедри КІІС _____ Т. О. Говорущенко