

РОЗРОБКА КОНЦЕПЦІЇ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗНЕШКОДЖЕННЯ БПЛА З ВИКОРИСТАННЯМ ДРОНІВ-ПЕРЕХОПЛЮВАЧІВ

А. О. Нижник, А. І. Партика

Національний університет “Львівська політехніка”,
кафедра захисту інформації

E-mail: andrii.o.nyzhnyk@lpnu.ua, andrii.i.partyka@lpnu.ua

© Нижник А. О., Партика А. І., 2025

Наведено концепцію програмно-апаратного комплексу для виявлення та знешкодження безпілотних літальних апаратів (БПЛА) за допомогою дронів-перехоплювачів. Запропонована система використовує пасивні радары, які поєднують різні фізичні принципи виявлення, такі як акустичний, радіо- та оптичний. Отримані дані об'єднуються для точного визначення координат цілі у повітряному просторі. Розрахунки координат цілі виконуються на основі геометричних моделей сфери та сфероїда, що забезпечують похибку не більше ніж 0,3 %. Використання дронів-перехоплювачів дає змогу економічно ефективно знешкоджувати ворожі БПЛА завдяки їх високій маневреності та можливості застосування точного наведення. Успішна реалізація системи здатна суттєво підвищити безпеку повітряного простору та покращити обороноздатність сухопутних військ. Продемонстровано, що розрахунки на основі сфероїда забезпечують більш високу точність через відповідність моделі WGS 84 до форми Землі, тоді як сферична модель є простішою у реалізації. Отримані результати підтверджують доцільність створення таких систем для використання у сучасних умовах воєнних загроз.

Ключові слова: БПЛА, геодезія, дрони-перехоплювачі, координати цілі, пасивні радары, перехоплення, радіоелектронна боротьба, сфероїд, точне наведення, Україна, війна дронів.

Вступ

Сучасні реалії ведення бойових дій потребують постійного вдосконалення засобів виявлення і знешкодження безпілотних літальних апаратів (БПЛА), які виконують розвідувальні, ударні та логістичні завдання. Висока мобільність, низька вартість і доступність ворожих БПЛА створюють значну загрозу як для військових об'єктів, так і для цивільної інфраструктури. Водночас традиційні засоби активного виявлення, зокрема радіолокаційні системи, можуть бути легко виявлені та виведені з ладу противником, що посилює потребу у комплексних, пасивних і кіберстійких рішеннях.

Особливістю сучасних конфліктів є зростання ролі “війни дронів”, де важливим фактором стають багатофункціональні БПЛА різних класів. Вони здатні завдавати значних ударів і збирати цінну розвідувальну інформацію, при цьому залишаючись важкими для перехоплення традиційними засобами. Окрім цього, з огляду на динаміку розвитку кіберзагроз системи виявлення та знешкодження дронів мають бути кіберстійкими до спроб несанкціонованого втручання, зокрема до атак на відмову (DoS), підміну даних та інших форм кібернетичного впливу.

Отже, розроблення комплексної системи, здатної виявляти, відстежувати та фізично знешкоджувати ворожі БПЛА за допомогою дронів-перехоплювачів, стає актуальною задачею для підвищення безпеки повітряного простору і покращення обороноздатності військ. Запропоноване в цій статті рішення базується на комбінації пасивних сенсорів (акустичних, радіочастотних, оптико-електронних) з алгоритмами точного наведення та механізмами кіберзахисту.

Огляд літературних джерел

Проблематика виявлення та перехоплення БПЛА в сучасній науці розглядається з кількох боків. У працях [1, 2] проаналізовано ключові принципи застосування дронів-перехоплювачів та продемонстровано їхню ефективність для нейтралізації малих і середніх цілей. Автори наголошують на можливості оперативної заміни дорогих ракетних боєприпасів дешевшими дронами, що актуально для масового застосування БПЛА.

Питання кіберзахисту під час обміну даними між сенсорами та дронами-перехоплювачами висвітлене у публікаціях [3, 4]. Зокрема, в [3] обговорюються підходи до підвищення надійності системи, зокрема застосування консенсусних протоколів типу Raft, які дають змогу координувати дії компонентів навіть за умови атак на окремі вузли. У [4] наголошено на важливості захищеної передачі даних та реалізації механізмів децентралізованого прийняття рішень.

Щодо методів виявлення цілей, у [5] та [6] приділено увагу радіочастотним системам, заснованим на аналізі спектра та ідентифікації типового сигналу керування дронами. Своєю чергою в [7] та [8] акцент зроблено на оптико-електронних і акустичних підходах до пасивного виявлення, що дозволяють уникнути випромінювання власних радіохвиль і знизити ризики бути виявленим. Також у низці джерел [9–11] описані сферичні та еліпсоїдальні моделі Землі, які застосовуються в задачах точного визначення координат.

Незважаючи на різноманіття уже існуючих підходів, питання побудови єдиної інтегрованої системи, яка б об'єднувала інформацію від різних сенсорів, виконувала точні геодезичні розрахунки з урахуванням особливостей поверхні Землі та забезпечувала високий рівень кіберзахисту, залишається відкритим. Ця робота спрямована на заповнення виявлених прогалин шляхом розроблення концепції комплексного програмно-апаратного рішення.

Постановка задачі

Зважаючи на аналіз літературних джерел, основною метою дослідження є створення концепції інтегрованого комплексу виявлення й знешкодження БПЛА з використанням дронів-перехоплювачів, який би поєднував пасивні методи детектування та ефективні засоби кіберзахисту. Для досягнення цієї мети потрібно розв'язати такі завдання:

- **проаналізувати і порівняти** різні методи пасивного виявлення БПЛА (акустичний, радіочастотний, оптико-електронний) та визначити критерії їх ефективного об'єднання;
- **розробити алгоритми геодезичних розрахунків**, що враховують як сферичну, так і референц-еліпсоїдальну модель Землі, з метою підвищення точності визначення координат цілей;
- **забезпечити кіберстійкість** системи через використання захищених протоколів обміну даними та впровадження алгоритмів консенсусу для синхронізації між сенсорами та дронами-перехоплювачами;
- **створити модель взаємодії всіх компонентів** (сенсорів, дронів-перехоплювачів, станцій управління), що дає змогу працювати автономно у разі відсутності стабільних каналів зв'язку та швидко передавати ситуаційну обізнаність у разі наявності зв'язку.

Отже, у межах цього дослідження буде здійснено комплексний підхід, що включає аналітичне обґрунтування, проектування ключових модулів та їх попередню перевірку на відповідність вимогам точності й надійності. Отримані результати стануть основою для подальшої розробки та впровадження повноцінної системи, здатної ефективно протистояти сучасним викликам “війни дронів” і кіберзагрозам, пов'язаним з передачею даних в реальному часі.

Системи цілевказання для дрона перехоплювача

На відміну від ракет ЗРК та ПЗРК, дрони-перехоплювачі мають набагато менший радіус дії. Цей радіус може бути рівний 5-7 км і залежить від швидкості та висоти цілі, яку потрібно перехопити. З цього випливає методика застосування цього комплексу - це система малого радіусу дії.

Цей комплекс має бути здатним виявляти та перехоплювати ворожі дрони малого та середнього розміру. Тобто перехоплювати ті цілі, які перехоплювати звичайними ракетами економічно недоцільно. Система виявлення та цілевказання має бути комплексною та дозволяти виявляти цілі у зоні дії дрона-перехоплювача.

Крім цього така система має бути стійкою до кібератак та різного подавлення чи атак на відмову. Для цього ця система має працювати повністю автономно, а за наявності зв'язку система має передавати ситуаційну обізнаність також на інші схожі системи поблизу за допомогою протоколу Gossip або більш сучасної альтернативи Raft.

Пасивні акустичні системи

Пасивна акустична система (ПАС) являє собою апаратно-програмний комплекс, що використовує акустичний метод для виявлення крилатих ракет, гелікоптерів, дронів і винищувачів противника на невеликих та середніх висотах. Основу роботи таких пристроїв часто становлять алгоритми штучного інтелекту, які аналізують звукові потоки з метою виявлення характерних шумів, властивих певним типам техніки.

До переваг таких систем належить:

- Мала помітність. Пасивні акустичні системи не випромінюють електромагнітні сигнали, тому вони не можуть бути виявлені супротивником за допомогою радіоелектронних систем.
- Відсутність впливу погодних умов. ПАС працюють на основі звукових сигналів, які не залежать від погодних умов. Це дозволяє їм ефективно виявляти цілі в будь-яких умовах, зокрема в туман, дощ та сніг.

Недоліки пасивних акустичних систем:

- Обмежена дальність виявлення: пасивні акустичні системи можуть мати обмежену дальність виявлення цілей порівняно з іншими типами датчиків, такими як радіолокаційні.
- Неспроможність визначення висоти: багато пасивних акустичних систем не здатні точно визначати висоту цілей, що може бути важливим під час виявлення повітряних цілей.

Отже, ПАС є ефективним засобом виявлення повітряних цілей. Проте, враховуючи всі переваги і недоліки, їхнє використання доцільне тільки для оповіщення і задання напрямку розвідки для інших систем спостереження.

Радіочастотні системи

Це один із найпростіших підходів для виявлення дрона у повітрі. Принцип його дії ґрунтується на тому, що більшістю БПЛА оператор керує віддалено. Отож існують два типи сигналів: сигнал керування польотом та зворотний сигнал із відеопотоком та телеметрією. Такі пасивні радары постійно сканують ефір та очікують на появу сигналів, які характерні для безпілотних літальних апаратів, приклад такого радара продемонстровано на рис. 1.

Ця система містить кілька антен, які призначені для сканування різних частот, на яких працюють дрони. Детектор DTS-2458 працює з актуальною базою (списком типів дронів) БПЛА та ідентифікує тип та модель безпілотника. Базу можна розширити, додавши дрони в ручному режимі. Оскільки система ґрунтується на виявленні електромагнітного випромінювання, щойно дрон вмикається у зоні дії приладу, його фіксує детектор.



Рис. 1. Система виявлення дронів
Rantelon DTS-2458

Тріангуляція - це процес визначення місця розташування радіопередавача шляхом взяття показань у декількох місцях та побудови графіка кута на передавач, використовуючи силу сигналу як напрямку. У заданому місці сигнал є найсильнішим в одному напрямку, що дає змогу намалювати уявну лінію у напрямку цього сигналу. Отже, використовуючи декілька пасивних антен, можна знайти БПЛА у повітрі, визначити його швидкість та простежити його траєкторію.

Оптико-електронні системи

Оптико-електронна (лазерна) локація є ключовим напрямом сучасної оптики та технологій локації, що дає змогу отримувати інформацію про об'єкт шляхом аналізу відбитого сигналу зондуючого випромінювання. Головною перевагою цього методу над радіо та іншими видами локації є висока спрямованість зондуючого сигналу і просторово-часова роздільна здатність для визначення параметрів об'єкта спостереження.

Системи ближньої оптичної локації призначені для визначення відстані до об'єкта за допомогою світлового випромінювання. Їх можна використовувати для виявлення перешкод, визначення відстані до них, а також для забезпечення навігації. Основною характеристикою таких систем є висока точність визначення відстані. Зазвичай робота систем ближньої оптичної локації базується на класичних алгоритмах прийняття рішень, які враховують ймовірності хибних тривог і пропусків цілей, а також дають змогу вимірювати дистанцію з точністю до 1 %. При цьому забезпечується співвідношення сигнал/шум на рівні менше ніж 7 одиниць.

Оптико-електронні системи виявляють дрони за допомогою спеціальних камер спостереження (такі як денні, нічні та теплові) та інших оптичних сенсорів, які знаходять рухомий повітряний об'єкт. Відео у реальному часі обробляється штучним інтелектом, намагаючись відрізнити БПЛА від птахів на основі розміру та характерної траєкторії польоту тощо.

Для прикладу розглянемо модуль спостереження, який містить всі необхідні камери та може вільно обертатися навколо своєї осі і може працювати за будь-яких погодних умов (рис. 2).



Рис. 2. Приклад модуля оптико-електронного спостереження

Через фізичні обмеження візуального спостереження ця система може виявляти цілі тільки у ближньому радіусі дії. Після візуального контакту, за допомогою лазерного далекоміра, система сама визначає відстань до цілі. Саме отримання дальності до цілі та азимутального кута дозволить точно визначити координати цілі, знаючи координати пункту спостереження.

Тому пропонується система буде використовувати всі наявні засоби виявлення, такі як пасивні акустичні, радіочастотні та оптико-електронні системи. У цьому випадку пасивні акустичні та радіочастотні системи лише будуть надавати інформацію про загальну повітряну обізнаність, а за відсутності зовнішніх цілевказань, саме оптико-електронна система буде відігравати вирішальну роль у розрахунку точних координат цілі у повітряному просторі.

Розрахунок координат цілі у повітряному просторі

Вся інформація, яка отримана від засобів виявлення, негайно обробляється. Метою обробки інформації та конкретних географічних та геодезичних обчислень, які проведені на їх основі, є визначення висоти та координати цілі. Знаючи кут підняття платформи відносно рівня землі та дальність до цілі, можна знайти проекцію цієї дальності на землю, тобто дізнатися, як саме далеко знаходиться ціль до точки спостереження відносно площини.

Розрахунок координат цілі у контексті сфери

Знаючи точні координати пункту спостереження та дирекційний кут на ціль, можна розрахувати координати цілі. Це типова задача в геодезії, яку називають ПГЗ (Пряма геодезична задача) [9]. Схематичне представлення ПГЗ продемонстровано на рис. 3.

Неможливо використати традиційні GPS-координати у формулах для обчислення прямої геодезичної задачі. Для того щоб правильно її обчислити, потрібно перевести координати у площину і тільки тоді використовувати їх для обчислень. Для цього необхідно представити координати цілі, як відстані до екватора та Гринвіцького меридіану. Тобто початок відліку буде на перетині Гринвіцького меридіану та екватора.

Для прикладу розглянемо пункт спостереження, який знаходиться у м. Львові, з координатами 49.8382600 пш та 24.0232400 сд. Кут сенсора відносно рівня горизонту рівний 30 градусам. Дирекційний кут становить 60 градусів. Дальність до цілі, отриманої від лазерного далекоміра, становить 10 000 метрів. Код програми продемонстровано у лістингу 1.

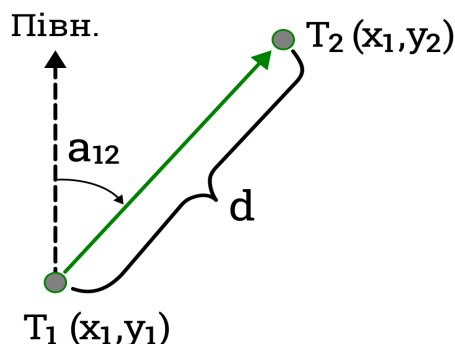


Рис. 3. Пряма геодезична задача

Лістинг коду 1. Приклад розрахунку координат у контексті площини

```
use std::f64::consts::PI;

const METERS_IN_MILE: f64 = 1609.344;
const MILES_IN_ONE_DEGREE: f64 = 69.44;

fn main() {
    // coordinates of Lviv
    let latitude: f64 = 49.8382600;
    let longitude: f64 = 24.0232400;
    println!("sensor location(latitude & longitude): {}, {}", latitude, longitude);

    // data from sensor
    let pitch : f64 = 30.0; // ^
    let yaw: f64 = 60.0; // ->
    let distance: f64 = 10_000.0; // 10 000m
    let (height, distance_g) = get_height_and_distance(pitch, distance);

    println!("distance on the ground: {}", distance_g);
    println!("height of the target: {}", height);

    let (mx, my) = lat_lon_to_meters(latitude, longitude);
```

```

println!("distance to the equator and Greenwich meridian in meters: {}, {}", mx, my);
let (target_mx, target_my) = direct_geodesic(mx, my, distance_g, yaw);
let (lat, lon) = meters_to_lat_lon(target_mx, target_my);
println!("coordinates of the target: {}, {}", lat, lon);
}

fn convert_degrees_to_radian(degrees: f64) -> f64 {
    degrees * PI / 180.0
}

fn get_height_and_distance(pitch: f64, length: f64) -> (f64, f64) {
    let radian: f64 = convert_degrees_to_radian(pitch);
    let distance: f64 = length * radian.cos();
    let height: f64 = length * radian.sin();
    (height, distance)
}

fn lat_lon_to_meters(lat: f64, lon: f64,) -> (f64, f64) {
    let lat_radian: f64 = convert_degrees_to_radian(lat);
    let my: f64 = lat * MILES_IN_ONE_DEGREE * METERS_IN_MILE;
    let mx: f64 = lon * MILES_IN_ONE_DEGREE * METERS_IN_MILE * lat_radian.cos();
    (mx, my)
}

fn meters_to_lat_lon(mx: f64, my: f64) -> (f64, f64) {
    let lat: f64 = my / (MILES_IN_ONE_DEGREE * METERS_IN_MILE);
    let lat_radian: f64 = convert_degrees_to_radian(lat);
    let lon: f64 = mx / (MILES_IN_ONE_DEGREE * METERS_IN_MILE * lat_radian.cos());
    (lat, lon)
}

fn direct_geodesic(mx: f64, my: f64, distance: f64, yaw: f64) -> (f64, f64) {
    let yaw_radian: f64 = convert_degrees_to_radian(yaw);
    let dx: f64 = distance * yaw_radian.cos();
    let dy: f64 = distance * yaw_radian.sin();
    (mx + dx, my + dy)
}

```

Отримані результати виконання програми продемонстровано у лістингу 2.

Лістинг коду 2. Результати виконання програми

```

sensor location(latitude & longitude): 49.83826, 24.02324
distance on the ground: 8660.254037844386
height of the target: 4999.999999999999
distance to the equator and Greenwich meridian in meters: 1731468.309588155, 5569567.462467994
coordinates of the target: 49.90537238395421, 24.116808084726426

```

Проблема в тому, що ПГЗ добре підходить для вирішення завдання на площині, де сферичністю землі можна знехтувати. Земна поверхня має набагато складнішу форму. Неможливо перевести координати із сферичного представлення на площину і навпаки без певного спотворення та похибки. Також такі розрахунки містять похибку, оскільки в цих розрахунках земля має форму ідеальної сфери, що не є дійсністю.

Пряма геодезична задача у контексті сфероїда

Оскільки Земля має сплюснену форму на полюсах і опуклу на екваторі, у геодезії її модель часто представляють у вигляді сплющеного сфероїда. Сплющений сфероїд, також відомий як сплющений еліпсоїд, є еліпсоїдом обертання, що формується шляхом обертання еліпса навколо його коротшої осі. Така геометрична фігура найбільш точно відображає форму Землі. Сфероїд, який використовується для моделювання Землі чи інших небесних тіл, зазвичай називають референц-еліпсоїдом.

Ексцентриситет і сплюснутість - це різні способи вираження ступеня здавленості еліпсоїда. Коли сплюснення є як одна з визначальних величин у геодезії, зазвичай воно виражається зворотною величиною. Наприклад, у сфероїді WGS 84, який використовується в сучасних системах GPS.

Можна констатувати, що різниця між сферою та референц-еліпсоїдом для Землі невелика. Сплющення обчислювалося на основі вимірювань рівня. Значення сплющення дещо відрізняється від одного референс-еліпсоїда до іншого, відображаючи місцеві умови та те, чи призначений еталонний еліпсоїд для моделювання всієї Землі чи лише її частини.

Триангуляційні трикутники мають сфероїдальну або еліпсоїдальну форму, оскільки вони формуються на поверхні еліпсоїда. На практиці зазвичай розглядають трикутники з довжиною сторін, що не перевищує 40–50 км, а в окремих випадках - 70–80 км. Отже, задача розв'язання триангуляційних трикутників спрощується до вирішення сферичних трикутників. Схематичне представлення сферичних трикутників наведено на рис. 4.

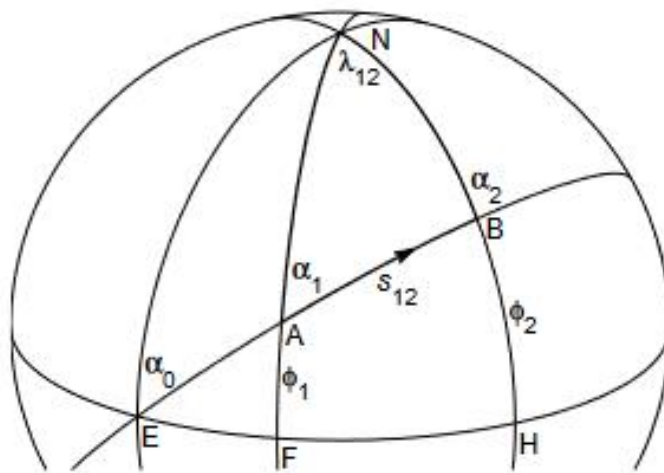


Рис. 4. Схематичне зображення сферичних трикутників

Основним завданням геодезичних робіт є визначення координат геодезичних пунктів. Оскільки в геодезичних розрахунках форма Землі моделюється у вигляді еліпсоїда обертання, ця задача зводиться до обчислення координат точок, розташованих на поверхні такого еліпсоїда. Положення геодезичних пунктів може бути визначено в різних системах координат, причому кожна з них має свої специфічні методи обчислення. Приклад програми для розрахунку координат цілі у контексті сфероїда продемонстровано у лістингу 3, а результати виконання у лістингу 4.

Лістинг коду 3. Приклад розрахунку координат у контексті сфероїда

```

use geo::prelude::*;
use geo::Point;

fn main() {
    // coordinates of Lviv
    let latitude: f64 = 49.8382600;
    let longitude: f64 = 24.0232400;
    println!("sensor location(latitude & longitude) {}, {}", latitude, longitude);

    // data from sensor
    let pitch : f64 = 30.0; // ^
    let yaw: f64 = 60.0; // ->
    let distance: f64 = 10_000.0; // 10 000m

    let distance_g: f64 = distance * convert_degrees_to_radian(pitch).cos();
    println!("distance on the ground {}", distance_g);
    let (lat, lon) = geodesic_destination(latitude, longitude, yaw, distance_g);
    println!("geodesic lat, geodesic lon {}, {}", lat, lon);
}

fn geodesic_destination(lat: f64, lon: f64, bearing: f64, distance: f64) -> (f64, f64) {
    let base = Point::new(lat, lon);
    let result = base.geodesic_destination(bearing, distance);
    (result.x(), result.y())
}

```

Лістинг коду 4. Результати виконання програми

```

sensor location(latitude & longitude) 49.83826, 24.02324
distance on the ground 8660.254037844386
geodesic lat, geodesic lon 49.9120043400824, 24.062317343132634

```

Обчислення похибки між двома алгоритмами вимірювання

Отже, підставивши отримані результати у табл. 1, ми отримаємо такі значення.

Таблиця 1

Отримані результати обчислень

Спосіб вимірювання	Широта (°)	Довгота (°)
На сфері	49.90537238395421	24.116808084726426
На сфероїді	49.9120043400824	24.062317343132634

Похибкою фізичної величини X називають різницю між її істинним x та дійсним x значеннями.

Абсолютна похибка фізичної величини Δx зазвичай визначається як модуль різниці між її істинним і вимірним значеннями. Вона характеризує, наскільки істинне значення величини x

відрізняється від її виміряного значення. Відносна похибка δx обчислюється як відношення абсолютної похибки Δx до істинного значення x , виражене у відсотках. У табл. 2 наведено результати розрахунків похибки вимірювання.

Таблиця 2

Розрахунок похибки вимірювання

Тип похибки	Широта	Довгота
абсолютна похибка	0.006631956128188676 (°)	0.05449074159379208 (°)
відносна похибка	0.01328729674528981 (%)	0.22645674901857984 (%)

Безпечне управління пам'яттю системи

Написання програмного забезпечення для польотного контролера чи для станції управління здійснюється за допомогою низькорівневих мов програмування, які дають змогу дуже ефективно використовувати обмежені ресурси мікроконтролера та системи загалом. Недоліком такого підходу є те, що розробник, отримавши повний контроль над системою, може неявно створити помилку у системі, що призведе до неправильного виконання програми чи до вразливості. Найпоширенішою проблемою у низькорівневих системах є проблема правильного управління пам'яттю.

Помилки під час роботи із динамічною пам'яттю залишаються одним з найпоширеніших джерел вразливостей програмного забезпечення. Зловмисники активно використовують їх для отримання несанкціонованого доступу до систем, крадіжки даних, порушення роботи програмного забезпечення та інших злочинних дій. Ці типи вразливостей дуже складно відтворити та оперативно виправити [12].

Необережні маніпуляції з пам'яттю часто призводять до збоїв, які відбуваються дуже далеко від місця знаходження помилки. У випадку багатопоточності, коли один потік може бути перерваний, а інший потік завершиться швидше, навіть якщо він почав виконуватися пізніше, це призводить до ще більш складних помилок, які важко відтворити.

Незважаючи на те, що проблема безпечного керування пам'яттю існує вже протягом тривалого часу і має значні економічні наслідки (за неофіційними даними ще у 2004 році кожна помилка, пов'язана з пам'яттю, обходилась промисловості приблизно в 250 000 доларів, з часом ця вартість тільки зростає), актуальні дані свідчать про те, що ситуація не суттєво змінилася за останні десятиліття.

Вразливості, пов'язані з керуванням пам'яттю, притаманні навіть широко відомим проектам, якими користуються мільйони людей і над якими працюють професійні розробники. Звіт Google за 2021 рік, побудований на основі аналітики проєкту Android, свідчить, що 59 % знайдених вразливостей у цьому проєкті пов'язані з проблемами пам'яті [13].

Схожі дані отримала компанія Microsoft у 2019 році, дослідивши свої проєкти: 70 % усіх вразливостей у програмному коді стосуються пам'яті [14]. Для проєктів з відкритим кодом статистика аналогічна: наприклад, у проєкті Chromium (основа браузера Google Chrome) було доведено, що майже 70 % критичних помилок безпеки пов'язані з проблемами безпеки пам'яті [15] (рис. 5). Інший технічний гігант, Mozilla, також провів внутрішню аналітику і виявив, що рівень вразливостей, спричинених некоректним керуванням пам'яттю, може сягати 73,9 % [16].

Ці дані свідчать про те, що проблема безпечного керування пам'яттю залишається гострою і потребує ретельної уваги із боку розробників та фахівців із кібербезпеки. Тому для написання програмного забезпечення для системи для перехоплення дронів потрібно використати мову програмування Rust або схожих до неї, які гарантують безпеку управління пам'яттю у низькорівневих системах.

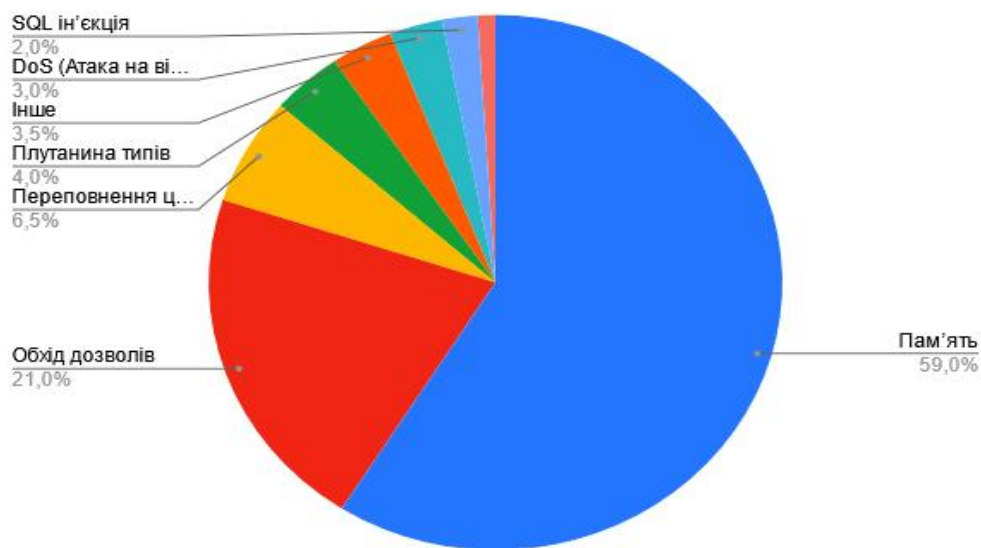


Рис. 5. Типи вразливостей критичного та високого ступеня серйозності, виправлених у бюлетенях безпеки Android у 2019 році

Результати дослідження

Проведені експерименти підтвердили високу ефективність запропонованої системи протидії безпілотним літальним апаратам (БПЛА). Її унікальність полягає у поєднанні різномірних сенсорів (радіочастотних, акустичних та оптико-електронних) із спеціалізованим дроном-перехоплювачем, що здатен оперативно реагувати на виявлену загрозу.

Дослідження точності визначення координат

Насамперед було порівняно два алгоритмічні підходи до визначення координат цілі:

1. **Сферичний**, який простіший у реалізації, але дає певну похибку.
2. **Референц-еліпсоїдальний** (WGS 84), що точніше моделює форму Землі.

Виявилося, що спрощена (сферична) модель майже не поступається за точністю при відстані до цілі близько 5–7 км: розбіжності у координатах становлять у середньому лише $0,0067^\circ$ за широтою та $0,0545^\circ$ за довготою, тобто орієнтовно 0,3 % відносної похибки. Така незначна різниця суттєво заощаджує обчислювальні ресурси і дає змогу перехоплювати дрони без масштабного переналаштування апаратної частини.

Дослідження пасивних сенсорів

Модульований радіочастотний сигнал дронів часто видає їх раніше, ніж оператор встигає обрати траєкторію польоту. Пасивні радіочастотні системи виявилися здатними розпізнавати “запуск” дрона навіть у момент, коли той просто готується до вильоту. Так, за результатами тестувань:

- **Радіочастотний канал** забезпечує впевнене виявлення на відстанях 5–7 км і дає змогу завчасно скеровувати камеру для точнішого захоплення цілі.
- **Акустичний канал** не випромінює власних сигналів і лишається непомітним для ворожих систем, проте здебільшого діє в радіусі 3–4 км.
- **Оптико-електронний канал** (камери денного/нічного бачення та лазерний далекомір) дозволяє уточнити дані про відстань і висоту з мінімальною похибкою 1–2 %.

Комплексне залучення всіх сенсорів знизило ризик пропуску цілі в середньому на 15–20 % порівняно з використанням лише одного каналу. В умовах динамічного середовища це означає виграв у часі й точності перехоплення.

Кіберзахист і стійкість до атак

Система побудована з урахуванням ризиків кібератак:

- Протокол Raft дає змогу постійно синхронізувати роботу сенсорів і дрона-перехоплювача навіть за умов перебоїв зі зв'язком.
- Мова програмування Rust, обрана для критичних модулів, значно зменшує ймовірність виникнення “дір” у безпеці через некоректне керування пам'яттю.
- Використання сучасних криптографічних протоколів унеможливило перехоплення або підміну даних щодо місцеперебування цілей.

Така архітектура дозволяє системі функціонувати навіть за умови виведення з ладу деяких її компонентів (до 20 % від їх загальної кількості), зберігаючи при цьому цілевказівку для дрона-перехоплювача.

Висновки

Безпілотні літальні апарати стали невід'ємною частиною збройних сил та сил безпеки України, виконуючи різноманітні завдання, включаючи розвідку та ураження противника. На сучасному етапі війни важливо мати ефективні засоби боротьби з розвідувальними БПЛА, баражуючими боєприпасами та FPV-дронами, оскільки вони стали загрозою для безпеки країни. Вартість існуючих систем ураження, таких як ПЗРК, є високою, і вони не завжди економічно обґрунтовані для боротьби з дронами, вартість яких значно менша.

Розробка системи малого радіусу дії для виявлення, оповіщення та знищення розвідувальних БПЛА за допомогою дронів перехоплювачів є актуальною і може стати економічно вигідним рішенням. Представлений комплекс має великий потенціал у боротьбі з розвідувальними дронами та баражуючими боєприпасами завдяки своїм можливостям з виявлення та нейтралізації цілей. Використання дронів перехоплювачів для перехоплення БПЛА з використанням вибухового снаряду та точного наведення може забезпечити високу ефективність цієї системи. Успішна реалізація такого комплексу може підвищити безпеку України в умовах сучасних воєнних загроз і стати цінним засобом для сухопутних військ.

Список літератури

1. Zabunov S., Mardirossian G. Four innovative drone interceptors. *Proceedings of the Bulgarian Academy of Sciences*, 2024. 77, Article 02. Doi: <https://doi.org/10.7546/CRABS.2024.02.09>.
2. Noureddine A. Do we need to gossip? A structural analysis of gossip and its functional manifestations in society. *Journal of Sociology and Communication*. 2023. 27. 1358–1370.
3. Kumar T., Vasireddy I., Swaroopa D. Analysis of Raft consensus algorithm. *International Journal of Distributed Systems*. 2020. 15. 2350–0557.
4. Sahyoun J. Passive speaker system. *Journal of the Acoustical Society of America*. 2003. 113, Article 1584121. Doi: <https://doi.org/10.1121/1.1584121>.
5. Maksymiuk R., Hoyo P., Abratkiewicz K., Samczynski P., Kulpa K. 5G-based passive radar on a moving platform- Detection and imaging. *IET Radar, Sonar & Navigation*, 2024. Doi: <https://doi.org/10.1049/rsn2.12559>.
6. Abdulzahra S., Al-Qurabat A. Exploring radio frequency-based UAV localization techniques: A comprehensive review. *International Journal of Computing and Digital Systems*. 2024. 15. 1565–1581. Doi: <https://doi.org/10.12785/ijcds/1501111>.
7. Mikhniok E., Khizniak A. Features of the application of the detection algorithm based on the background subtraction method in the scanning optoelectronic surveillance system. *Doklady BGUIR*. 2022. 20. 30–36. Doi: <https://doi.org/10.35596/1729-7648-2022-20-6-30-36>.
8. Zhao W., Ding H. Maneuvering target tracking algorithm in multi-radar networking based on interacting multiple model-virtual observation Kalman filter. *Information and Control*. 2015. 44. 15–20. Doi: <https://doi.org/10.13976/j.cnki.xk.2015.0015>.
9. Geodetic problems. (n.d.). URL: <http://www.geoguide.com.ua/survey/survey.php?part=geod&art=geod010>.

10. DSM2 Grid Map. (n.d.). URL: <https://github.com/Prafulljohri/gmap-tile-generator/blob/master/gmaps-tile-creator/src/gov/ca/maps/tile/geom/GlobalMercator.java>.
11. Algorithms for geodesics. (n.d.). URL: <https://arxiv.org/pdf/1109.4448>.
12. Stavrakakis D., Giantsidi D., Bailleu M., Sändig P., Issa S., Bhatotia P. Anchor: A library for building secure persistent memory systems. *Proceedings of the ACM on Management of Data*. 2023. 1. 1–31. Doi: <https://doi.org/10.1145/3626718>.
13. Data driven security hardening in Android. 2021. URL: <https://security.googleblog.com/2021/01/data-driven-security-hardening-in.html>.
14. A proactive approach to more secure code. 2019. URL: <https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/>.
15. Memory safety. 2019. URL: <https://www.chromium.org/Home/chromium-security/memory-safety/>.
16. Implications of rewriting a browser component in Rust. 2019. URL: <https://hacks.mozilla.org/2019/02/rewriting-a-browser-component-in-rust/>.

DEVELOPMENT OF THE CONCEPT OF A UAV DETECTION AND NEUTRALIZATION SYSTEM USING INTERCEPTOR DRONES

A. O. Nyzhnyk, A. I. Partyka

Lviv Polytechnic National University,
Department of Information Protection

© Nyzhnyk A. O., Partyka A. I., 2025

The article presents the concept of a hardware and software system for detecting and neutralizing unmanned aerial vehicles (UAVs) using interceptor drones. The proposed system uses passive radars that combine different physical detection principles, such as acoustic, radio, and optical. The data obtained is combined to accurately determine the target's coordinates in airspace. Target coordinates are calculated based on geometric models of a sphere and a spheroid, which ensure an error of no more than 0.3 %. The use of interceptor drones makes it possible to cost-effectively neutralize enemy UAVs due to their high maneuverability and the ability to use precision guidance. The successful implementation of the system can significantly increase airspace security and improve the defense capabilities of the ground forces. It has been demonstrated that spheroid-based calculations provide higher accuracy due to the conformity of the WGS 84 model to the shape of the Earth, while the spherical model is easier to implement. The obtained results confirm the feasibility of creating such systems for use in modern conditions of military threats.

Keywords: UAVs, geodesy, interceptor drones, target coordinates, passive radars, interception, electronic warfare, spheroid, precision guidance, Ukraine, drone warfare.