МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ, ПСИХОЛОГІЇ ТА БЕЗПЕКИ
Кафедра інформаційних технологій

НАВІГАЦІЯ ТА ВИЗНАЧЕННЯ КООРДИНАТ БПЛА У СКЛАДНИХ УМОВАХ

кваліфікаційна робота
здобувача вищої освіти
4 курсу денної форми навчання
Данила СЕМЕНЮКА

Науковий керівник:
Доктор філософії
Олег БАСИСТЮК

Рецензент:
_____

Кваліфікаційна робота допущена до захисту
«___» _____ 2026 р., протокол № ____

Завідувач кафедри інформаційних технологій

_____ **Олег ЗАЧЕК**
(підпис)

Львів
2026

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AGC (Automatic Gain Control) – автоматичне регулювання підсилення приймача

БІНС – безплатформна інерціальна навігаційна система

БПЛА – безпілотний літальний апарат

C/N_0 (Carrier-to-Noise Density Ratio) – відношення потужності несучої до шуму

EKF (Extended Kalman Filter) – розширений фільтр Калмана

GNSS (Global Navigation Satellite System) – глобальна навігаційна супутникова система

IMM (Interacting Multiple Model) – алгоритм взаємодіючих множинних моделей

ІНС – інерціальна навігаційна система

МЕМС – мікроелектромеханічна система

MHSS RAIM (Multiple Hypothesis Solution Separation) – метод розділення рішень з множинними гіпотезами

НКА – навігаційний космічний апарат (супутник GNSS)

PDOP (Position Dilution of Precision) – геометричний чинник ослаблення точності

RAIM (Receiver Autonomous Integrity Monitoring) – автономний контроль цілісності приймача

РЕБ – радіоелектронна боротьба

SLAM (Simultaneous Localization and Mapping) – одночасна локалізація та картографування

TERCOM (Terrain Contour Matching) – навігація за контуром рельєфу місцевості

UKF (Unscented Kalman Filter) – безслідний фільтр Калмана

VIO (Visual-Inertial Odometry) – візуальна інерціальна одометрія

ВОГ – волоконно-оптичний гіроскоп

ЦКМ – цифрова карта місцевості

АНОТАЦІЯ

Бакалаврська кваліфікаційна робота виконана студентом групи ІТ-42 Семенюком Данилом Валерійовичем. Тема «Навігація та визначення координат БПЛА у складних умовах». Робота направлена на здобуття ступеня бакалавр за спеціальністю 126 «Інформаційні системи та технології» – Львівський державний університет внутрішніх справ, МВС України, Львів, 2026.

У межах дослідження спроєктовано та реалізовано відмовостійку навігаційну систему для БПЛА, здатну функціонувати в умовах навмисного радіоелектронного придушення. Процес розробки охопив вивчення фізичних механізмів глушіння та спуфінгу сигналів GNSS, розробку детекторів загроз на основі аналізу AGC та відношення C/N_0, а також алгоритму MHSS RAIM. Досліджено резервні методи навігації – візуальну інерціальну одометрію (VIO), SLAM та навігацію за контуром рельєфу (TERCOM).

Метою роботи є розробка системи, здатної автоматично виявляти атаки на GNSS і переходити на резервні методи визначення координат без участі оператора, використовуючи IMM-фільтр із чотирма субфільтрами.

Предметом дослідження є методи виявлення атак на GNSS та алгоритми відмовостійкого комплексування різнорідних навігаційних систем.

У результаті виконання роботи розроблено систему, яка в автоматичному режимі виявляє глушіння та спуфінг, веде статистику режимів навігації та забезпечує максимальну похибку позиціонування не більше 22 м при 120-секундній повній відмові GNSS.

Ключові слова: БПЛА, GNSS, навігація, спуфінг, глушіння, RAIM, фільтр Калмана, IMM, VIO, SLAM, TERCOM, відмовостійкість, інерціальна система.

ABSTRACT

Bachelor's qualification work was completed by a student of IT-42 group Semeniuk Danilo Valeriyovych. The topic is «Navigation and coordinate determination of UAVs in complex conditions». The work is aimed at obtaining a bachelor's degree in specialty 126 «Information Systems and Technologies» – Lviv State University of Internal Affairs, MIA of Ukraine, Lviv, 2026.

Within the framework of this research, a fault-tolerant navigation system for UAVs was designed and implemented, capable of operating under intentional radio-electronic suppression. The development process covered the study of physical mechanisms of GNSS jamming and spoofing, the development of threat detectors based on AGC analysis and C/N_0 ratio, as well as the MHSS RAIM algorithm. Reserve navigation methods were studied – visual inertial odometry (VIO), SLAM and terrain contour navigation (TERCOM).

The aim of the work is to develop a system capable of automatically detecting GNSS attacks and switching to reserve positioning methods without operator intervention, using an IMM filter with four sub-filters.

As a result of the thesis, a system was developed that automatically detects jamming and spoofing, logs navigation mode statistics, and ensures a maximum positioning error of no more than 22 m with a 120-second complete GNSS failure.

Keywords: UAV, GNSS, navigation, spoofing, jamming, RAIM, Kalman filter, IMM, VIO, SLAM, TERCOM, fault tolerance, inertial system.

ЗМІСТ

ВСТУП

Обґрунтування актуальності теми дослідження.

Стрімке зростання кількості безпілотних літальних апаратів (БПЛА) у цивільних і воєнних застосуваннях ставить перед розробниками нові вимоги до надійності навігаційних систем. Якщо ще десять років тому БПЛА здебільшого використовувалися у відносно безпечних умовах – аерофотозйомка, моніторинг об'єктів, – то сьогодні вони виконують завдання у зонах активного радіоелектронного придушення, над густозабудованими кварталами і в умовах, де навіть короткочасна втрата навігації може призвести до катастрофічних наслідків.

Основним засобом навігації для більшості БПЛА залишаються глобальні навігаційні супутникові системи – GPS, ГЛОНАСС, Galileo. Ці системи дають точність 1–5 м та охоплюють увесь земний куль, що й обумовило їхнє масове поширення. Проте GNSS має принципову вразливість: навігаційний сигнал долає 20 000 кілометрів від орбіти і надходить до антени приймача з потужністю не більше –130 дБм. Навіть невеликий наземний передавач потужністю кілька ватів здатен повністю заглушити цей сигнал у радіусі кілька кілометрів. Саме цю властивість системно експлуатують засоби радіоелектронної боротьби у сучасних конфліктах [1].

Ще серйознішою є проблема спуфінгу – підробки навігаційного сигналу. На відміну від глушіння, яке просто переводить приймач у режим пошуку, спуфінг «переконує» апарат, що все гаразд, тоді як той фактично летить хибним курсом. Документовані випадки захоплення БПЛА через GPS-спуфінг вже зафіксовані в кількох конфліктних регіонах, і кількість таких інцидентів зростає [2].

Аналіз останніх досліджень і публікацій. Проблематикою захищеності GNSS займаються як міжнародні дослідники – П. Гровз [1], Т. Хамфрейс [2], М. Псіакі [3], – так і вітчизняні фахівці, зокрема О. Ткаченко [4] та С. Кухтецький [5]. У їхніх роботах досліджено окремі аспекти: методи виявлення глушіння, алгоритми RAIM, інтеграція ІНС та GNSS. Однак питання комплексного

об'єднання детекторів загроз із автоматичним переходом на резервну навігацію у вигляді цілісної системи залишається відкритим.

Мета дослідження полягає у підвищенні захищеності навігації БПЛА шляхом розробки та реалізації відмовостійкої навігаційної системи, що автоматично виявляє атаки на GNSS і переходить на резервні методи визначення координат.

Завдання дослідження:

1. визначити фізичні механізми глушіння і спуфінгу GNSS та класифікувати загрози за рівнем складності;
2. розробити детектор глушіння на основі аналізу AGC та відношення C/N_0 з математичним обґрунтуванням порогів;
3. дослідити алгоритм MHSS RAIM та розробити chi²-детектор спуфінгу з крос-перевіркою від ІНС;
4. проаналізувати резервні методи навігації: VIO (алгоритм Lucas-Kanade), SLAM (ORB-SLAM3) та TERCOM;
5. розробити IMM-фільтр із чотирма субфільтрами для адаптивного комплексування навігаційних джерел;
6. реалізувати архітектуру tight-coupling ІНС/GNSS з вбудованим захистом від спуфінгу;
7. провести імітаційне моделювання у MATLAB/Simulink та оцінити ефективність розробленої системи.

Об'єктом дослідження є навігаційні системи БПЛА, що функціонують під впливом засобів РЕБ та геометричних перешкод.

Предметом дослідження є методи виявлення атак на GNSS та алгоритми відмовостійкого комплексування альтернативних навігаційних систем.

Методи дослідження. Для досягнення поставленої мети використано комплекс методів: теорія оцінювання (фільтр Калмана, EKF, IMM-EKF) для обробки навігаційних вимірювань; статистичні методи виявлення аномалій (RAIM, chi²-тест) для детектування атак; методи комп'ютерного зору (алгоритм Lucas-Kanade, ORB-SLAM3) для резервної навігації; методи цифрової обробки

сигналів для аналізу AGC та C/N_0; імітаційне моделювання у MATLAB/Simulink для верифікації алгоритмів.

Інформація про практичне значення роботи. Розроблена система виявлення загроз GNSS та адаптивного комплексування навігаційних джерел має безпосередній потенціал для впровадження у бортове програмне забезпечення тактичних і цивільних БПЛА. Запропонований IMM-фільтр може бути інтегрований у наявні автопілоти (наприклад, Pixhawk) без суттєвих апаратних змін. Результати роботи апробовано на науково-практичній конференції «Інформаційні технології в правоохоронній діяльності» (Львів, 2026).

Структура та обсяг роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів основної частини, висновків, списку використаних джерел та додатків. Загальний обсяг пояснювальної записки становить ** сторінок, робота містить ** таблиць та ** рисунків.

РОЗДІЛ 1. АНАЛІЗ ЗАГРОЗ НАВІГАЦІЇ БПЛА ТА МЕХАНІЗМІВ ЇХ ВИНИКНЕННЯ

1.1. Вразливість GNSS як основного засобу навігації

Для розуміння природи загроз навігаційним системам БПЛА необхідно детально розглянути фізичну основу роботи GNSS. Навігаційний супутник GPS рухається на середній навколоземній орбіті висотою близько 20 200 кілометрів і передає сигнал на несучій частоті L1 (1575,42 МГц) із потужністю на борту близько 50 Вт. Однак після подолання двадцяти тисяч кілометрів через вакуум і атмосферу ця потужність зменшується до приблизно –130 дБм на рівні земної поверхні. Це кілька сотень фемтоватів – у мільярд разів менше за потужність типового Wi-Fi-маршрутизатора. Така надмала потужність прийнятого сигналу є першопричиною всіх проблем із захищеністю GNSS.

Втрати сигналу визначаються законами поширення електромагнітних хвиль. У вільному просторі потужність убуває пропорційно квадрату відстані – так звані втрати у вільному просторі (FSPL). Для відстані 20 200 км та частоти L1 ці втрати перевищують 182 дБ. Результат: приймач змушений виловлювати надмало потужний корисний сигнал на фоні власних теплових шумів. Будь-який сторонній сигнал порівнянної або більшої потужності в тій самій смузі частот здатен повністю замаскувати навігаційний сигнал.

Суттєво посилює проблему повна відкритість специфікацій цивільних навігаційних кодів. Документ IS-GPS-200, що детально описує структуру C/A-коду GPS, є загальнодоступним без будь-яких обмежень. Із практичного боку це означає: будь-хто зі знаннями у сфері програмно-визначуваного радіо та бюджетом у кілька десятків доларів на SDR-приймач може не лише прийняти, але й повністю відтворити навігаційний сигнал із власною хибною навігаційною інформацією. Перспективні сигнали Galileo E1 з OSNMA та GPS L1C передбачають механізми аутентифікації навігаційних повідомлень, але масове оновлення флоту БПЛА приймачами з підтримкою цих технологій залишається справою найближчого майбутнього.

З конструктивної точки зору БПЛА є особливо вразливою платформою.

По-перше, обмежена висота польоту звужує кут огляду неба, зменшуючи кількість одночасно видимих НКА. По-друге, всеспрямована конструкція антени, що диктується масовими обмеженнями, не забезпечує просторової фільтрації завад. По-третє, відбиття сигналів від навколишніх поверхонь – ефект multipath – спричиняє систематичні похибки, що нерідко досягають 10–30 м у міській забудові. Сукупність цих факторів і формує технічне підґрунтя для активного розроблення захисних механізмів та резервних методів навігації.

Щоб зрозуміти, чому GNSS настільки легко вивести з ладу, варто почати з елементарної фізики. Навігаційний супутник GPS L1 передає сигнал на частоті 1575,42 МГц із потужністю близько 50 Вт. Здавалося б, чимало – але після подолання 20 000 кілометрів від орбіти до земної поверхні від цієї потужності залишається лише –130 дБм. Для порівняння: сигнал Wi-Fi-роутера у вашій кімнаті у мільярд разів потужніший. Саме тому GNSS-приймачі є по суті надчутливими радіоприймачами, вразливими до будь-якого стороннього сигналу у смузі частот L.

Ситуацію ускладнює повна відкритість специфікацій цивільного коду. Документ IS-GPS-200, де детально описано структуру C/A-коду GPS, вільно завантажується з офіційного сайту. Це означає, що будь-яка особа з бюджетним програмно-визначуваним радіоприймачем (SDR) вартістю близько $30 може не лише прийняти, а й синтезувати сигнал, невідрізнений від справжнього навігаційного. Криптографічного захисту у цивільних форматах GPS і ГЛОНАСС немає. Новіші сигнали Galileo E1 та GPS L1C реалізують цифровий підпис навігаційних повідомлень, проте масове поширення приймачів із їхньою підтримкою ще попереду.

Додатковими факторами вразливості БПЛА зокрема є обмежена висота польоту (малий кут видимості небосхилу), чутливість до відбиття сигналів від будівель (multipath) та неможливість ефективної просторової фільтрації завад при стандартній всеспрямованій антені. Сукупність цих обставин формує запит на навігаційні системи, що здатні не лише точно визначати координати, але й

постійно контролювати достовірність вхідних даних.

1.2. Глушіння сигналів GNSS: фізика, типи та зони дії

Радіозавада (jammer) порушує роботу GNSS-приймача шляхом підвищення загального рівня перешкод у смузі частот L настільки, що приймач не може відстежувати кореляційний пік псевдовипадкового коду. Ключовим кількісним параметром є відношення потужності завади до потужності корисного сигналу J/S (Jamming-to-Signal ratio, у дБ). Більшість цивільних GNSS-приймачів починає деградувати вже при J/S більше 0 дБ, а при J/S більше 30–40 дБ повністю втрачає навігаційне рішення. Оскільки потужність прийнятого сигналу НКА становить –130 дБм, навіть завада рівнем –100 дБм у точці антени приймача вже достатня для блокування.

За спектральним характером сигналу виділяють кілька типів глушіння. Широкосмугове шумове глушіння рівномірно перекриває всю смугу GNSS псевдовипадковим шумом – це найпростіший підхід у реалізації, але й найменш ефективний за витратою потужності. Тонове (CW) глушіння концентрує потужність на одній або кількох дискретних частотах – мінімальна потужність для досягнення потрібного J/S, але нотч-фільтри здатні його відфільтрувати. Перестроюване тонове (Swept CW) обходить нотч-фільтрацію: частота синусоїди безперервно сканує смугу, не даючи фільтру «налаштуватися». Matched spectrum jamming є найбільш витонченим: форма спектру завади спеціально підібрана під спектральний профіль GNSS-сигналу, що забезпечує максимальну ефективність за однакової потужності.

Радіус ефективного глушіння визначається рівнянням балансу потужностей (link budget). Для наземного заглушника з відомими параметрами формула має вигляд:

$$Rj = Rr \cdot \sqrt{[(Pj \cdot Gj \cdot \eta j) / (Pr \cdot Gr \cdot \eta r \cdot (J/S)min)]}$$

де Rr – відстань від БПЛА до НКА (≈ 20 200 км); Pj – потужність

передавача заглушника (Вт); Gj – коефіцієнт спрямованості антени заглушника; Pr, Gr – потужність сигналу НКА та коефіцієнт підсилення антени приймача; ηj, ηr – ефективність антен; (J/S)min – поріг блокування приймача. Практичний результат: портативний заглушник потужністю 1 Вт з всеспрямованою антеною блокує стандартний цивільний GNSS-приймач у радіусі 3–5 км [6]. Детальна залежність зони глушіння від потужності наведена на рис. 1.1.

Для навігаційної системи БПЛА надзвичайно важливо виявляти глушіння якомога раніше – ще до того, як приймач остаточно втратить позиційне рішення. Рання тривога дозволяє активувати ІНС та VIO у режимі «теплого резерву», зберігаючи мінімальну похибку. У підрозділі 2.1 детально описано механізм раннього виявлення на основі AGC та C/N_0.

Глушіння (jamming) – це будь-яке випромінювання, яке перевищує рівень корисного навігаційного сигналу в смузі частот приймача і тим самим унеможливлює захоплення або відстеження сигналів НКА. Коли рівень завади за відношенням до сигналу (J/S) перевищує певний поріг, приймач «осліплює» і виходить із режиму навігації.

За характером спектру виділяють декілька типів глушіння, порівняльний аналіз яких наведено в табл. 1.1.

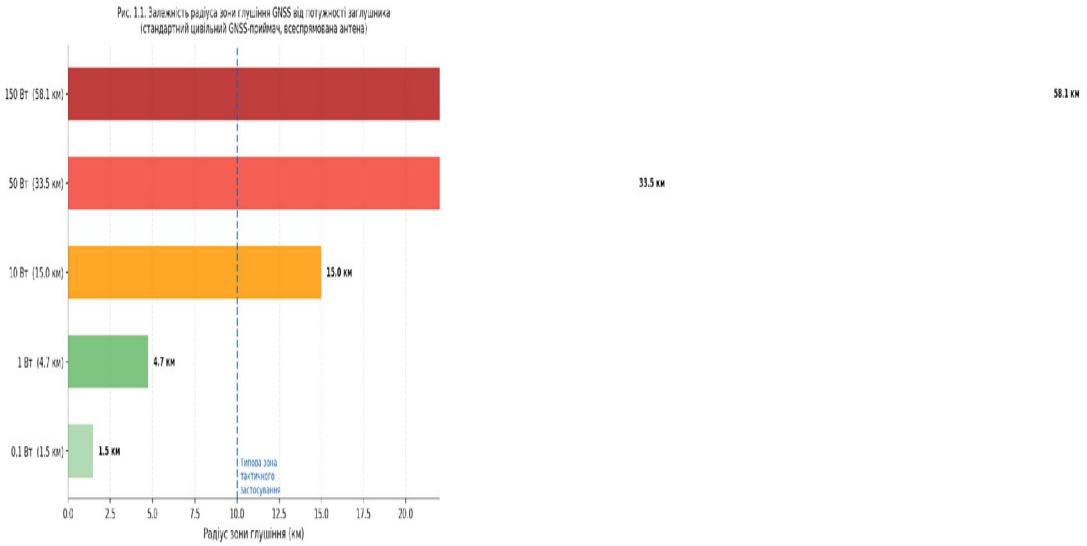

Рис. 1.1. Залежність радіуса зони глушіння GNSS від потужності заглушника

Таблиця 1.1 Класифікація типів глушіння GNSS

Тип глушіння	**Складність пристрою**	**Ефективність**	**Метод виявлення**
Широкосмугове шумове	Низька	Висока (перекриває всю смугу)	AGC + середній C/N_0
Тонове (CW)	Низька	Середня (1–2 синусоїди)	Нотч-фільтр + AGC
Перестроюване тонове (Swept CW)	Середня	Висока (не фільтрується)	AGC + спектральний аналіз
Matched spectrum	Висока	Найвища (форма = GNSS)	AGC + C/N_0 + RAIM

Джерело: складено автором.

Як видно з табл. 1.1, широкосмугове шумове глушіння є найпоширенішим через простоту реалізації. Для оцінки зони його дії використовують балансове рівняння потужностей:

$$Rj = Rr \cdot \sqrt{[(Pj \cdot Gj) / (Pr \cdot Gr \cdot (J/S)min)]}$$

де Rr – відстань від БПЛА до НКА (≈ 20 200 км); Pj та Gj – потужність і коефіцієнт підсилення антени заглушника; Pr та Gr – потужність сигналу НКА та КУС антени приймача; (J/S)min – мінімальне відношення завади до сигналу, при якому приймач блокується (зазвичай 0–40 дБ). Практична оцінка: наземний заглушник потужністю 1 Вт із всеспрямованою антеною блокує стандартний цивільний приймач у радіусі 3–5 км [6].

1.3. Спуфінг GNSS: принцип роботи, рівні складності та наслідки

Спуфінг (від англ. spoofing – підробка, обман) є активною атакою на GNSS-приймач, при якій зловмисник генерує синтетичні навігаційні сигнали – точні копії справжніх сигналів НКА, але із навмисно хибною навігаційною інформацією. Позбавлений механізмів аутентифікації приймач приймає такий сигнал за справжній і видає хибне позиційне рішення без жодного явного сигналу відмови. Ця «тиша» і є найнебезпечнішою властивістю спуфінгу.

Принципова відмінність від глушіння важлива для розуміння ступеня небезпеки. При глушінні БПЛА або його автопілот отримує чіткий сигнал – «навігація відмовила» – і реагує відповідно: зависає, повертається на базу або знижується. При спуфінгу апарат упевнений, що все гаразд, і продовжує виконувати завдання – але вже за хибними координатами. Результатом може бути не просто відхилення від маршруту, а цілеспрямоване наведення БПЛА до потрібної зловмиснику точки.

За ступенем технічної складності виділяють три покоління атак. Ретрансляційний спуфінг (meaconing) – найпростіший: перехоплений справжній сигнал НКА ретранслюється після штучно введеної затримки або з іншого напрямку. Технічна реалізація мінімальна (SDR + підсилювач), але однакове

зміщення для всіх НКА одночасно легко виявляється алгоритмом RAIM. Синтетичний спуфінг рівня 2 передбачає повну генерацію PRN-кодів і навігаційних повідомлень за допомогою GNSS-симулятора. Програмне забезпечення є загальнодоступним, необхідний SDR коштує кілька десятків доларів. Атакуючий задає довільні хибні координати, але стрибкоподібна зміна позиції виявляється chi²-тестом або ΔV-детектором.

Trajectory spoofing (рівень 3, або атака з плавним відведенням) є найнебезпечнішим різновидом. Атака починається з повної синхронізації фальшивих сигналів із реальними: зловмисник «захоплює» канали відстеження приймача непомітно. Після захоплення хибні координати починають повільно відхилятися від справжніх – зі швидкістю, що не перевищує аеродинамічно можливої швидкості БПЛА. RAIM не реагує, оскільки всі псевдовідстані є взаємно консистентними; ΔV-детектор мовчить, бо «рух» виглядає фізично можливим. Єдиним засобом виявлення є порівняння рішення GNSS із незалежним рішенням ІНС – підхід, детально описаний у підрозділі 2.3.

Практична реалізованість спуфінгу вже неодноразово підтверджена. У 2012 році дослідники Університету Техасу в Остіні продемонстрували захоплення цивільного БПЛА через GPS-спуфінг у полігонних умовах [2]. Починаючи з 2019 року численні повідомлення пілотів комерційної авіації фіксують факти GPS-спуфінгу над Близьким Сходом і Середземномор'ям, де навігаційні системи помилково відображали місцезнаходження за сотні кілометрів від реального.

Якщо глушіння – це грубий молоток, то спуфінг – скальпель. Замість того щоб просто зруйнувати зв'язок із супутниками, зловмисник генерує фальшиві навігаційні сигнали, що виглядають для приймача абсолютно справжніми. Приймач «довіряє» їм і видає хибне позиційне рішення – при цьому жодних ознак відмови не фіксує. Саме це робить спуфінг принципово небезпечнішим за глушіння: при глушінні автопілот принаймні знає, що навігація втрачена; при спуфінгу – ні.

За технічним рівнем атаки виділяють три покоління спуфінгу, порівняння яких наведено в табл. 1.2.

Таблиця 1.2 Рівні складності спуфінгових атак на GNSS

Рівень	**Технічне оснащення**	**Характер зміщення**	**Метод виявлення**
1 – Meaconing (ретрансляція)	SDR + підсилювач	Однакове для всіх НКА	Геометрична перевірка (RAIM)
2 – Синтез PRN-кодів	SDR + GNSS-симулятор (відкриті)	Довільне, миттєве	RAIM + chi²-тест з ІНС
3 – Trajectory spoofing (плавна відведення)	Повна GNSS-станція	Плавне, непомітне	Аналіз швидкості + ΔV-тест

Джерело: складено автором.

Як свідчить табл. 1.2, найнебезпечнішим є третій рівень – коли зловмисник спочатку синхронізується зі справжнім сигналом, а потім поступово зміщує хибне рішення, імітуючи природний рух апарата. У такому сценарії класичний RAIM не спрацьовує, оскільки фальшиві сигнали є взаємно консистентними. Для виявлення потрібне незалежне джерело інформації – і саме ним є ІНС [2, 3].

1.4. Геометричні та атмосферні перешкоди

Окрім навмисного радіоелектронного впливу, точність навігації БПЛА обмежується рядом природних чинників. Їхнє розуміння необхідне для правильного налаштування детекторів загроз і порогів переходу між навігаційними рівнями.

Ефект «міського каньйону» (urban canyon effect) є основною геометричною перешкодою при польотах у густозабудованих кварталах. Висотні будівлі

обмежують кут видимості неба, унеможливлюючи прийом сигналів від НКА з малими кутами піднесення. Навіть якщо кількість видимих НКА формально перевищує мінімально необхідні чотири, їхнє взаємне розташування може мати настільки незадовільну геометрію, що геометричний чинник PDOP сягає неприйнятних значень. Нагадаємо: PDOP менше 2 є відмінним, 2–5 – прийнятним, більше 6 – незадовільним. У типовому сценарії міського каньйону PDOP може перевищувати 10–15, що практично знецінює навігаційне рішення.

Паралельно з погіршенням геометрії у міських умовах поширеним явищем є multipath – приймання відбитих від будівель сигналів поряд із прямим. Відбитий сигнал приходить до антени із запізненням відносно прямого; для приймача, що вимірює псевдовідстань через часову затримку поширення, це виглядає як систематичне збільшення виміряної відстані до НКА. Залежно від геометрії відбиваючих поверхонь, похибка від multipath може варіюватися від кількох метрів до кількох десятків метрів.

Іоносферні ефекти обумовлені проходженням радіохвиль через іонізований шар атмосфери на висотах 60–1000 км. В спокійних умовах іоносферна затримка для L1-сигналу становить 1–10 м у зеніті, але під час геомагнітних бурь вона може зрости до 50–100 м і більше. Двочастотні приймачі (L1+L2 або L1+L5) здатні повністю компенсувати іоносферну затримку, але вони важчі й дорожчі, тому на легких БПЛА зазвичай використовуються однокоординатні рішення з корекцією за моделлю іоносфери (Klobuchar).

Тропосферна затримка, що обумовлена заломленням у нижніх шарах атмосфери, є значно меншою за іоносферну (зазвичай 2–3 м у зеніті), але не залежить від частоти і тому не піддається двочастотній корекції. Для БПЛА, що виконують польоти на малих висотах, цей ефект є менш критичним, ніж для наземних застосувань, однак при спостереженні НКА під кутами менше 10° може вносити похибки порядку 5–10 м.

Крім навмисних атак, точність навігації БПЛА знижується і через природні чинники. Найвідоміший із них – ефект «міського каньйону»: при польоті між

висотними будівлями значна частина небосхилу перекрита, і приймач може бачити лише кілька супутників із великими кутами піднесення. Якщо видимих НКА менше чотирьох або геометричний чинник PDOP перевищує 6, точне позиційне рішення неможливе. Відбиття сигналів від скляних фасадів (ефект multipath) додатково вносить псевдовипадкові похибки до десятків метрів.

Іоносферні аномалії під час геомагнітних бурь збільшують затримку поширення сигналу в 10–20 разів відносно номінального значення. Для однокоординатного приймача без корекції це означає похибку до 50–100 м. Тропосферні ефекти (температурні інверсії, градієнти вологості) спричиняють менші, але стабільніші відхилення – зазвичай 2–5 м.

Висновки до розділу 1

У першому розділі встановлено, що GNSS є принципово вразливою системою через низький рівень прийнятого сигналу та відсутність криптографічного захисту у цивільних форматах. Глушіння є найпоширенішою атакою і відносно добре виявляється; спуфінг третього рівня – плавна відведення – є найнебезпечнішим, бо відбувається непомітно для стандартних приймачів. Геометричні перешкоди і атмосферні аномалії є природними джерелами деградації. Усе це формує вимогу до системи з активним контролем цілісності та резервними джерелами навігації.

РОЗДІЛ 2 МЕТОДИ ВИЯВЛЕННЯ АТАК НА GNSS

2.1. Детектування глушіння за AGC та C/N_0

Система захисту навігаційного каналу БПЛА функціонує за принципом «ешелонованої оборони» – кожен рубіж виявляє саме ті загрози, з якими він фізично найкраще справляється. Перший і найшвидший рубіж – детектор, що спирається на апаратні параметри радіотракту приймача: автоматичне регулювання підсилення (AGC) і відношення потужності несучої до шуму (C/N_0). Перевагою цього підходу є швидкість: перші симптоми глушіння у цих параметрах з'являються вже через десятки мілісекунд після початку дії завади – задовго до того, як приймач фактично втрачає позиційне рішення.

Фізичний принцип детектора AGC такий. У штатному режимі рівень сигналу на вході АЦП визначається виключно тепловим шумом схемотехніки приймача і залишається практично незмінним. AGC підтримує постійне підсилення, компенсуючи лише природні флуктуації. При появі зовнішньої завади загальна потужність на вході зростає, і AGC відповідає збільшенням атенюації – це реєструється мікроконтролером приймача як аномальний стан. Саме ця реакція AGC є першим і найбільш швидким індикатором глушіння.

Математично тест виявлення глушіння за AGC формулюється як двосторонній гіпотезний тест:

$$H_0 \text{ (норма):} \quad AGC(t) \in [AGC\_nom - k\cdot\sigma,\ AGC\_nom + k\cdot\sigma]$$

$$H_1 \text{ (глушіння):} \quad AGC(t) > AGC\_nom + k\cdot\sigma$$

де AGC_nom – номінальне значення AGC, виміряне перед польотом в умовах без завад; σ – стандартне відхилення нормальних флуктуацій AGC; k – коефіцієнт чутливості. Вибір k = 6 дає ймовірність хибної тривоги менше 10^{-9} для гауссівського розподілу флуктуацій, а час виявлення реального глушіння з J/S більше 10 дБ – 300–500 мс, що є прийнятним для підготовки переходу на резервну навігацію.

Паралельно з AGC відстежується відношення потужності несучої до щільності шуму C/N_0, яке вимірюється окремо для кожного відстежуваного НКА і в умовах відкритого неба становить 38–48 дБ-Гц. Характерним патерном

глушіння є одночасне рівномірне зниження C/N_0 для всіх видимих НКА незалежно від їхнього кута піднесення. Це відрізняє глушіння від природного зникання НКА за горизонтом – у природних сценаріях деградація C/N_0 є поступовою і стосується лише окремих супутників. Формально:

$$S\_cn0 = (1/N) \cdot \Sigma_{i=1}^{N} C/N_{0i} < Thr\_cn0 \quad (Thr\_cn0 \approx 30–32 \text{ дБ-Гц})$$

Комбінований детектор (AGC і C/N_0) знижує ймовірність хибної тривоги до рівня менше 10^{-6} при збереженні часу реакції менш ніж 500 мс. Діагностична матриця детектора наведена у табл. 2.1.

Першим рубежем захисту є детектор глушіння. Він мусить спрацювати якомога раніше – ще до того як приймач остаточно втратить позиційне рішення, щоб навігаційний алгоритм встиг підготуватися до переходу на резервний режим.

Схема автоматичного регулювання підсилення (AGC) присутня у кожному GNSS-приймачі. Вона підтримує постійний середній рівень сигналу на вході аналого-цифрового перетворювача: в нормальному режимі AGC «налаштований» на власний тепловий шум приймача і практично не змінюється. При появі зовнішньої широкосмугової завади AGC починає збільшувати атенюацію, намагаючись компенсувати небажаний сигнал – і це відхилення є надійним індикатором глушіння [6].

Тест виявлення глушіння за AGC формулюється як гіпотезний тест:

$$H_0 \text{ (норма):} \quad AGC(t) \in [AGC\_nom - k\cdot\sigma,\ AGC\_nom + k\cdot\sigma]$$

$$H_1 \text{ (глушіння):} \quad AGC(t) > AGC\_nom + k\cdot\sigma$$

де AGC_nom – номінальне значення AGC, виміряне перед стартом; σ – стандартне відхилення AGC у штатних умовах; k – поріг чутливості. При k = 6 ймовірність хибної тривоги за нормального розподілу шуму не перевищує 10^{-9}, а час виявлення – менше 0,5 секунди.

Паралельно контролюється відношення потужності несучої до шуму

(C/N_0). У відкритому небі нормальні значення становлять 38–48 дБ-Гц. При широкосмуговому глушінні C/N_0 знижується одночасно і рівномірно для всіх видимих НКА – що є характерним патерном зовнішньої завади на відміну від зникання окремого супутника за горизонтом.

Комбінований детектор (AGC разом із C/N_0) знижує ймовірність хибної тривоги до рівня менше 10^{-6} при збереженні часу реакції менше половини секунди. Діагностична матриця детектора наведена в табл. 2.1.

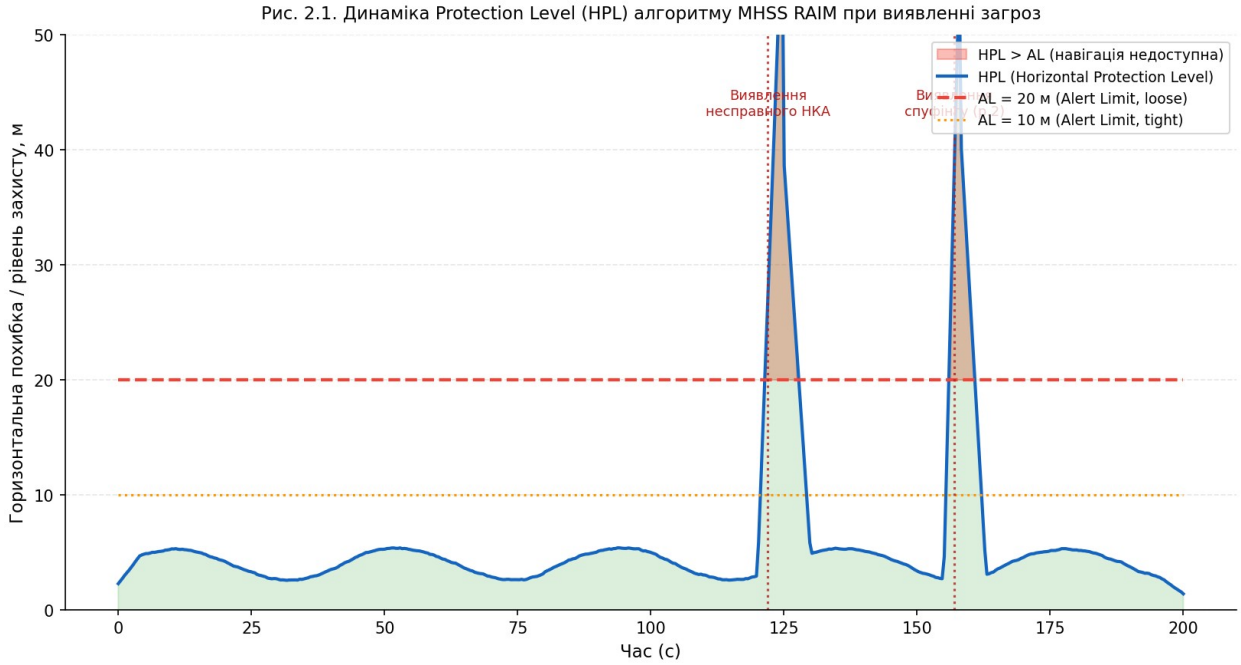

Рис. 2.1. Динаміка Protection Level (HPL) алгоритму MHSS RAIM при виявленні загроз

Таблиця 2.1 Діагностична матриця детектора глушіння

Умова	**Відхилення AGC**	**Середній C/N_0**	**Висновок системи**
Норма	< 3σ	38–45 дБГц	Загроз немає, Рівень 0
Початок глушіння	3–6σ	30–38 дБГц	Попередження, готовність ІНС
Сильне	> 6σ	< 30 дБГц	Перехід на

глушіння			IHC/VIO (Рівень 1)
Спуфінг рівні 1–2	Норма	Норма або незначна зміна	Потрібен RAIM / chi²-тест
Спуфінг рівень 3	Норма	Норма	Лише IHC-крос-перевірка

Джерело: складено автором.

2.2. RAIM та MHSS RAIM – автономний контроль цілісності

Детектор AGC/C/N_0 є ефективним виключно проти глушіння. Спуфінг – навіть рівня 2 – залишить AGC і C/N_0 у нормальних межах, оскільки синтетичні сигнали подаються замість справжніх, не збільшуючи загального шуму. Для виявлення хибних вимірювань псевдовідстаней необхідний принципово інший підхід – аналіз внутрішньої несуперечливості самих GNSS-вимірювань. Саме цим займається RAIM.

Концептуальна основа RAIM (Receiver Autonomous Integrity Monitoring) – надмірність спостережень. Задача позиціонування має чотири невідомі (три координати і похибка годинника), тож мінімально потрібно чотири НКА. Якщо ж видимих супутників п'ять або більше, система є надлишковою і можна перевірити взаємну сумісність вимірювань. Несправний або спуфований НКА вносить систематичне відхилення, що порушує консистентність і фіксується тест-статистикою RAIM.

Тест-статистика класичного RAIM – chi²-тест вектора залишків:

$$T = \varepsilon^T \cdot W \cdot \varepsilon / (N - 4), \quad де \ \varepsilon = S \cdot \rho, \quad S = I - H \cdot (H^T W H)^{-1} \cdot H^T W$$

де ρ – вектор виміряних псевдовідстаней (N×1); H – матриця геометрії спостережень (N×4); $W = R^{-1}$ – вагова матриця; S – матриця проекції у підпростір залишків; N – кількість НКА; 4 – число невідомих. За відсутності несправностей T підпорядковується χ^2-розподілу з (N–4) ступенями вільності. Поріг порівняння задається із умови забезпечення заданої ймовірності хибної тривоги Pfa.

MHSS RAIM (Multiple Hypothesis Solution Separation RAIM) є сучасним

розширенням класичного підходу для авіаційних застосувань [7]. Паралельно обчислюються N+1 рішень: одне «повне» і N «часткових» (кожне – без одного НКА). Різниця між повним і кожним частковим рішенням дозволяє оцінити Protection Level (PL) – статистично обґрунтовану верхню межу похибки позиції. Якщо PL менше Alert Limit (AL), навігація визнається доступною. Для тактичних БПЛА рекомендується AL_H = 10–20 м.

Важливим практичним обмеженням RAIM є нездатність виявити спуфінг рівня 3: зловмисник формує набір псевдовідстаней, що є взаємно консистентними з хибними координатами, і залишки RAIM залишаються в межах норми. Для таких атак необхідний третій рубіж, описаний у підрозділі 2.3.

RAIM (Receiver Autonomous Integrity Monitoring) – це метод перевірки несуперечливості вимірювань від різних супутників без будь-яких зовнішніх даних, силами самого приймача. Логіка проста: якщо видно п'ять і більше НКА, а для розв'язання потрібно чотири, система є надлишковою. Несправний або спуфований супутник порушує загальну картину – RAIM це фіксує [7].

Тест-статистика класичного RAIM – chi²-тест вектора залишків псевдовідстаней:

$$T = \varepsilon^T \cdot W \cdot \varepsilon / (N - 4), \quad де \ \varepsilon = (I - H \cdot (H^T W H)^{-1} \cdot H^T W) \cdot \rho$$

де ρ – вектор виміряних псевдовідстаней; H – матриця геометрії спостережень; W – вагова матриця (обернена до дисперсійної матриці шумів); N – кількість видимих НКА; 4 – число невідомих. Статистика T підпорядковується розподілу хі-квадрат із (N–4) ступенями вільності. Перевищення порогу вказує на несправний НКА, який потім ітеративно ідентифікується та виключається з рішення.

MHSS RAIM (Multiple Hypothesis Solution Separation) іде далі: він паралельно обчислює N+1 позиційних рішень – одне повне та N часткових – і розраховує Protection Level (PL). Якщо PL перевищує Alert Limit (AL = 10–20 м

для тактичних БПЛА), навігаційна система констатує недостатню цілісність та ініціює перехід на резервний рівень.

2.3. Chi²-детектор спуфінгу з крос-перевіркою від ІНС

Логіка chi²-детектора базується на фізичній незалежності GNSS та ІНС. GNSS вимірює псевдовідстані до супутників за допомогою радіоприйому, ІНС – визначає координати механічним інтегруванням показань акселерометрів та гіроскопів. Ці два фізичні явища – розповсюдження радіохвиль та механіка інерції – аніяк не пов'язані між собою. Будь-яка атака на GNSS залишає ІНС незворушною. Якщо рішення GNSS і рішення ІНС суттєво розходяться – одне з них є хибним, і враховуючи, що ІНС не піддається радіозавадам, хибним є GNSS.

Кількісна оцінка розбіжності здійснюється за chi²-тестом на основі відстані Махаланобіса:

$$\delta p = p\_GNSS - p\_INS$$

$$\chi^2 = \delta p^T \cdot (P\_GNSS + P\_INS)^{-1} \cdot \delta p$$

$$H_1\ (спуфінг):\ \chi^2 \geq \chi^2\_th(3, P\_fa)\ \approx\ 16{,}27\ \ при\ P\_fa = 10^{-3}$$

де δp – вектор розбіжності між позиціями від GNSS та ІНС; P_GNSS – матриця дисперсій похибок GNSS-рішення; P_INS – матриця дисперсій накопиченої похибки ІНС (зростає з часом автономного польоту); n = 3 – кількість просторових вимірювань. Якщо χ^2 перевищує поріг 16,27 – система фіксує підозру на спуфінг і блокує GNSS-дані.

Принципово важливою є часова динаміка чутливості тесту. Безпосередньо після початку підозри P_INS є малою і тест надзвичайно чутливий: навіть розбіжність у 2–3 м виявляється впевнено. Однак МЕМС-ІНС накопичує похибку з часом, і через 60 секунд без корекції поріг фактичного виявлення зростає до десятків метрів. Тому для збереження чутливості chi²-детектора на тривалих інтервалах необхідна постійна корекція ІНС від VIO або TERCOM.

Доповненням є ΔV-детектор: якщо «швидкість» зміни GNSS-рішення між

двома послідовними епохами перевищує максимальну аеродинамічну швидкість БПЛА плюс 3σ похибки вимірювання – реєструється груба атака рівня 2. Цей тест є простішим, але й менш чутливим: він виявляє лише «нетерплячі» атаки. Chi²-тест та ΔV-детектор запускаються паралельно: OR-логіка їхніх виходів формує єдиний сигнал тривоги «спуфінг виявлено».

Ані AGC-детектор, ані RAIM не виявлять спуфінг третього рівня: зловмисник синтезує сигнали, консистентні між собою, тому залишки RAIM залишаються в нормі, а рівень сигналу не змінюється. Потрібне принципово незалежне джерело – і саме ним є ІНС.

ІНС та GNSS є фізично абсолютно різними системами: ІНС вимірює прискорення і кутові швидкості механічними датчиками, GNSS – час прийому радіосигналів. Атака на GNSS не впливає на ІНС, і навпаки. Якщо GNSS видає хибні координати, між рішенням ІНС та GNSS виникає розбіжність, яку фіксує chi²-тест:

$$\delta p = p\_GNSS - p\_INS$$

$$\chi^2 = \delta p^T \cdot (P\_GNSS + P\_INS)^{-1} \cdot \delta p$$

$$H_1 \text{ (спуфінг): } \chi^2 \geq \chi^2\_th(3, P\_fa) \approx 16{,}27 \quad \text{при } P\_fa = 10^{-3}$$

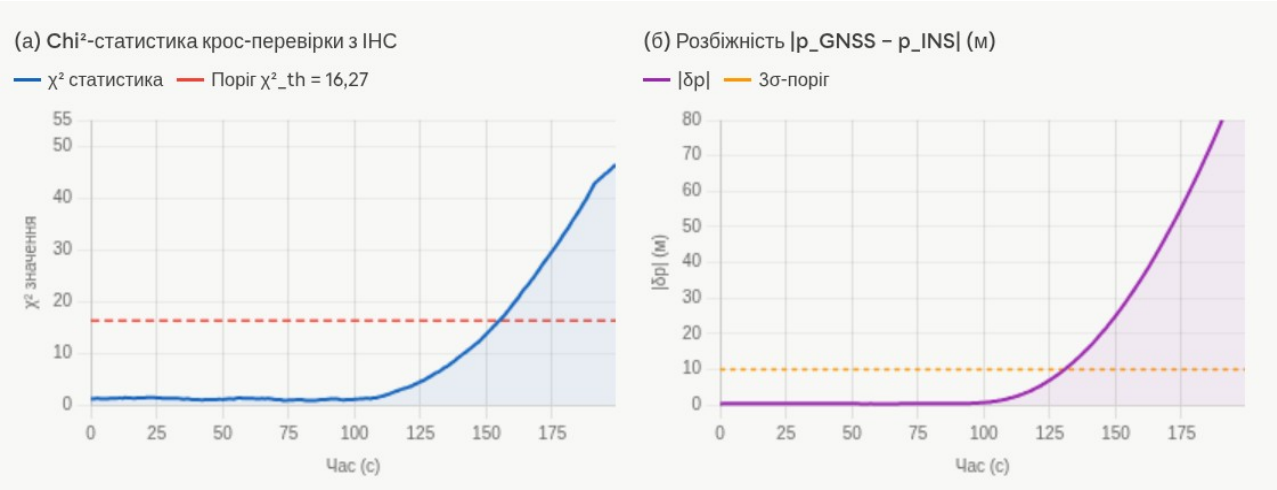

Рис. 2.2. Робота chi²-детектора при спуфінгу рівня 3 (плавна відведення координат)

де P_GNSS та P_INS – матриці дисперсій похибок відповідних систем; n = 3 – кількість просторових вимірювань. Важлива особливість детектора: чутливість знижується з часом, оскільки P_INS зростає через накопичення дрейфу. Тому chi²-тест є найефективнішим на початку атаки, коли ІНС ще має малу похибку.

Додатково реалізовано детектор аномальної швидкості зміни координат: якщо стрибок позиції в GNSS-рішенні між двома сусідніми епохами перевищує аеродинамічно можливу швидкість БПЛА з урахуванням похибки вимірювання – це груба атака, що виявляється миттєво.

2.4. Виявлення спуфінгу антенними масивами CRPA

Найбільш технічно досконалий метод – антенна решітка з керованою діаграмою спрямованості (CRPA, Controlled Reception Pattern Antenna). Справжні сигнали НКА надходять із відомих напрямків (обчислюється за ефемеридами), а сигнал наземного спуфера – з одного фіксованого джерела. Просторова фільтрація за фазовим зрушенням між елементами дозволяє розрізнити та заглушити фальшивий сигнал. Для легких БПЛА до 5 кг це ще надто громіздке і дороге рішення, але для тактичного класу є практичним варіантом [8].

Висновки до розділу 2

У другому розділі розроблено трирівневу систему виявлення атак на GNSS. AGC/C/N_0-детектор виявляє глушіння за 0,5 с; MHSS RAIM ідентифікує несправні або спуфовані НКА за 1 с; chi²-тест крос-перевірки з ІНС виявляє узгоджений спуфінг за 8–35 с. Комбінація цих методів перекриває загрози всіх трьох рівнів складності.

РОЗДІЛ 3. РЕЗЕРВНІ МЕТОДИ НАВІГАЦІЇ БПЛА

3.1. Інерціальна навігаційна система: математика та похибки

Безплатформна ІНС є єдиним засобом навігації, що не потребує жодних зовнішніх сигналів і фізично не може бути заглушена або сфальсифікована радіоелектронними методами. Ця властивість робить її незамінним базисом відмовостійкої системи. Водночас автономна ІНС має один серйозний недолік – нескінченне накопичення похибки через процес числового інтегрування. Розуміння математики цього процесу є необхідним для правильного проектування комплексної системи.

БІНС обчислює навігаційний стан шляхом безперервного чисельного інтегрування рівнянь руху у навігаційній системі координат NED (Північ-Схід-Вниз):

$$dq/dt = (1/2) \cdot q \otimes \omega\_ib^b \quad \textit{(кватерніонне рівняння орієнтації)}$$

$$dV^n/dt = C\_b^n \cdot f^b - (2\Omega\_ie^n + \Omega\_en^n) \times V^n + g^n \quad \textit{(рівняння швидкості)}$$

$$d\varphi/dt = V\_N/(R\_M+h), \quad d\lambda/dt = V\_E/((R\_N+h)\cdot\cos\varphi), \quad dh/dt = -V\_D \quad \textit{(координати)}$$

де q – кватерніон орієнтації (описує просторову орієнтацію БПЛА без сингулярностей); ω_ib^b – вектор абсолютної кутової швидкості тіла від гіроскопів; C_b^n – матриця напрямних косинусів; f^b – вектор питомої сили від акселерометрів; Ω_ie^n, Ω_en^n – матриці обертання Землі та транспортної швидкості; g^n – прискорення сили тяжіння; φ, λ, h – геодезичні координати; R_M, R_N – радіуси кривизни меридіанного та першого вертикального перерізів еліпсоїда WGS-84.

Для синтезу навігаційного фільтра використовується лінеаризована модель похибок ІНС. Вектор стану містить 15 компонентів: δφ, δλ, δh – похибки координат; δV_N, δV_E, δV_D – похибки проекцій швидкості; δψ, δθ, δγ – похибки кутів орієнтації (рискання, тангаж, крен); b_ax, b_ay, b_az – зміщення нуля акселерометрів; b_gx, b_gy, b_gz – дрейфи гіроскопів. Останні шість

компонентів є інструментальними похибками датчиків – при їхній ідентифікації та компенсації автономна точність ІНС суттєво підвищується. Порівняльні характеристики різних класів ІНС наведено у табл. 3.1.

ІНС – це єдина навігаційна система, яка не потребує жодних зовнішніх сигналів. Гіроскопи вимірюють кутові швидкості, акселерометри – прискорення, а бортовий комп'ютер інтегрує ці дані й обчислює координати, швидкість та орієнтацію. Звучить ідеально – але є принциповий недолік: кожне вимірювання містить малий шум. При інтегруванні цей шум накопичується, і похибка координат зростає приблизно квадратично з часом. Для бюджетних МЕМС-датчиків за 60 секунд автономного польоту похибка може сягати сотень метрів.

Механізація безплатформної ІНС у навігаційній системі координат «Північ-Схід-Вниз»:

$$dq/dt = (1/2) \cdot q \otimes \omega\_ib^b \quad \text{(орієнтація через кватерніон)}$$

$$dV^n/dt = C \cdot f^b - (2\Omega\_ie + \Omega\_en) \times V^n + g^n \quad \text{(швидкість)}$$

$$d\varphi/dt = V\_N/(R\_M+h); \; d\lambda/dt = V\_E/((R\_N+h)\cdot\cos\varphi); \; dh/dt = -V\_D$$

де q – кватерніон орієнтації; ω_ib^b – кутова швидкість від гіроскопів; C – матриця напрямних косинусів; f^b – питома сила від акселерометрів; g^n – вектор сили тяжіння; R_M, R_N – радіуси кривизни еліпсоїда WGS-84. Для комплексування з GNSS навігаційний фільтр відстежує вектор похибок ІНС із 15 компонентів.

Порівняльні характеристики автономної точності різних класів ІНС наведено в табл. 3.1.

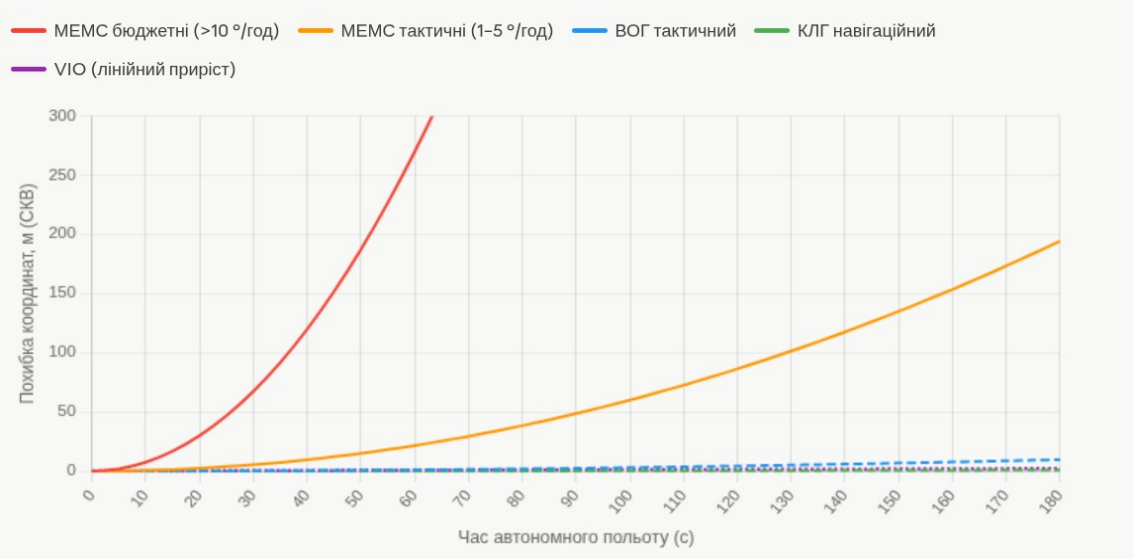

Рис. 3.1. Накопичення похибки координат ІНС різних класів без корекції від GNSS

Таблиця 3.1 Автономна точність різних класів ІНС без зовнішньої корекції

Тип датчиків	**Дрейф гіро (°/год)**	**Похибка акс. (мг)**	**Σ_pos за 60 с**	**Σ_pos за 120 с**
МЕМС бюджетні	10–100	3–10	100–500 м	400–2000 м
МЕМС тактичні	1–5	0,5–2	20–80 м	80–300 м
ВОГ тактичний	0,01–0,1	0,05–0,2	2–15 м	8–60 м
КЛГ навігаційний	0,001–0,01	0,01–0,05	0,5–3 м	2–12 м

Джерело: складено автором.

3.2. Візуальна інерціальна одометрія (VIO)

Візуальна інерціальна одометрія (VIO) поєднує бачення навколишнього середовища через бортову камеру та відчуття власного руху через інерціальний вимірювальний модуль. Ці два джерела є взаємодоповнюючими: камера

забезпечує прив'язку до видимих ознак без накопичення систематичних дрейфів, але має низьку частоту оновлення (30–60 Гц) та чутлива до різких рухів; ІМП, навпаки, має частоту 200–1000 Гц і стабільний на коротких інтервалах, але накопичує дрейф. Синергія двох систем дозволяє досягти лінійного накопичення похибки (0,5–2% від пройденої відстані) замість квадратичного для автономної ІНС.

Оцінка горизонтальної швидкості БПЛА через оптичний потік базується на геометричному перетворенні кутового зміщення ознак у лінійну швидкість:

$$V\_x = (\Delta u / \Delta t) \cdot h / f\_x, \qquad V\_y = (\Delta v / \Delta t) \cdot h / f\_y$$

де Δu та Δv – зміщення характерної точки на матриці сенсора між кадрами у пікселях; Δt – часовий інтервал між кадрами; h – висота над поверхнею (з барометра або лазерного висотоміра); f_x, f_y – фокусна відстань об'єктива у пікселях. Задача відстеження ознак між кадрами вирішується алгоритмом Lucas-Kanade через мінімізацію різниці яскравості у вікні W навколо кожної ознаки:

$$\min\_{\Delta u,\Delta v} \Sigma\_{(x,y)\in W} [I_2(x+\Delta u, y+\Delta v) - I_1(x,y)]^2$$

Рішення знаходиться аналітично через матрицю Гессе (структурний тензор). Умова ненульового визначника матриці Гессе є одночасно умовою стійкості відстеження: кутові точки зображення є найкращими ознаками для відстеження, тоді як ребра та однорідні текстурні ділянки є ненадійними. Пірамідна реалізація LK забезпечує коректне відстеження ознак зі зміщеннями до 40–60 пікселів між кадрами, що є достатнім для типових маневрів БПЛА.

VIO забезпечує точність оцінки горизонтальної швидкості близько 0,05 м/с при висоті 50 м. Ця похибка лінійно зростає з висотою: на 100 м – 0,10 м/с, на 200 м – 0,20 м/с. Навіть із урахуванням цього зростання, VIO забезпечує набагато кращу точність позиціонування, ніж автономна МЕМС-ІНС на інтервалах понад 30–60 секунд.

VIO – це спосіб отримати оцінку горизонтальної швидкості БПЛА з камери, спостерігаючи за тим, як «пливуть» характерні точки зображення між кадрами. Якщо відоме значення висоти польоту та параметри камери, зміщення

пікселів однозначно перетворюється на швидкість:

$$V\_x = (\Delta u / \Delta t) \cdot h / f\_x; \quad V\_y = (\Delta v / \Delta t) \cdot h / f\_y$$

де Δu, Δv – зміщення пікселів між кадрами; h – висота польоту; f_x, f_y – фокусна відстань у пікселях. Для відстеження точок між кадрами застосовується алгоритм Lucas-Kanade. Він мінімізує суму квадратів різниці яскравості у вікні W навколо кожної ознаки:

$$min\_\{\Delta u,\Delta v\} \Sigma\_\{(x,y)\in W\} [I(x+\Delta u, y+\Delta v, t+\Delta t) - I(x, y, t)]^2$$

Рішення знаходиться у замкненій формі через матрицю Гессе (структурний тензор), що забезпечує ефективну реалізацію у реальному часі. Принципова перевага VIO перед ІНС: похибка зростає лінійно з пройденою відстанню (0,5–2%), а не квадратично з часом. При поєднанні з ІНС (VIO на 30 Гц коригує дрейф ІНС на 200 Гц) отримуємо систему, що утримує прийнятну точність десятки хвилин без будь-яких радіосигналів.

3.3. SLAM: одночасна локалізація та картографування

SLAM вирішує принципово складнішу задачу, ніж VIO: замість відстеження лише відносного руху, він одночасно будує карту тривимірних ознак навколишнього середовища та локалізується в ній. Ключовою перевагою є «замикання петлі» (loop closure) – розпізнавання раніше відвіданих місць та одноразового виправлення всієї накопиченої похибки траєкторії. У практичному сенсі: якщо БПЛА через 10 хвилин автономного польоту повертається до стартової зони і SLAM розпізнає характерні орієнтири – похибка позиції може бути скоригована від сотень метрів (для автономної ІНС) до кількох сантиметрів.

ORB-SLAM3 – сучасне відкрите рішення, що добре зарекомендувало себе у дослідженнях [9]. Архітектура включає три паралельних потоки: відстеження (Tracking) – швидке обчислення поточної пози камери за найближчими

ключовими кадрами; локальне картування (Local Mapping) – тріангуляція нових 3D-точок та Bundle Adjustment; замикання петель (Loop Closing) – пошук схожих кадрів у глобальній базі та виконання глобальної оптимізації. Для опису ознак використовується детектор FAST та дескриптор BRIEF з врахуванням повороту (ORB), що забезпечує стійкість до зміни точки спостереження та масштабу.

Принципова особливість SLAM для навігаційних застосувань: система встановлює власну систему відліку від початкового положення, тому отримані координати є відносними. Для перетворення у глобальні координати (WGS-84) необхідне знання початкового положення – наприклад, остання надійна GNSS-фіксація. При кожному замиканні петлі глобальні координати корегуються автоматично без використання GNSS, що дозволяє підтримувати локальну точність навіть при тривалій відмові супутникового позиціонування.

Якщо VIO лише вимірює відносну швидкість, то SLAM іде далі – він будує карту оточення та водночас локалізується в ній. Ключова перевага – «замикання петлі» (loop closure): якщо БПЛА повернувся до вже відвіданого місця і система це розпізнала, вона виконує глобальну корекцію всієї накопиченої похибки траєкторії одним кроком.

ORB-SLAM3 [9] – сучасна відкрита реалізація – підтримує монокулярну, стерео- та RGBD-конфігурації і здатна відстежувати до 2000 ознак на кадр. Точність ATE (Absolute Trajectory Error) на відстанях 100–200 м – менше 5 сантиметрів. Обмеження SLAM: без початкової прив'язки до глобальних координат (від GNSS або відомого орієнтира) система видає лише відносні координати. Тому SLAM є доповненням до GNSS, а не самостійним методом.

3.4. Навігація за рельєфом місцевості TERCOM/DSMAC

TERCOM – один із небагатьох методів, що взагалі не накопичують похибку з часом. Радіовисотомір або LiDAR вимірює висоту над поверхнею у послідовних точках маршруту, формуючи «профіль рельєфу». Цей профіль порівнюється з еталонними профілями з ЦКМ методом кореляції:

$$C(x, y) = \Sigma_k \, [h\_meas(k) - h\_map(x + k \cdot \cos\psi,\ y + k \cdot \sin\psi)]^2$$

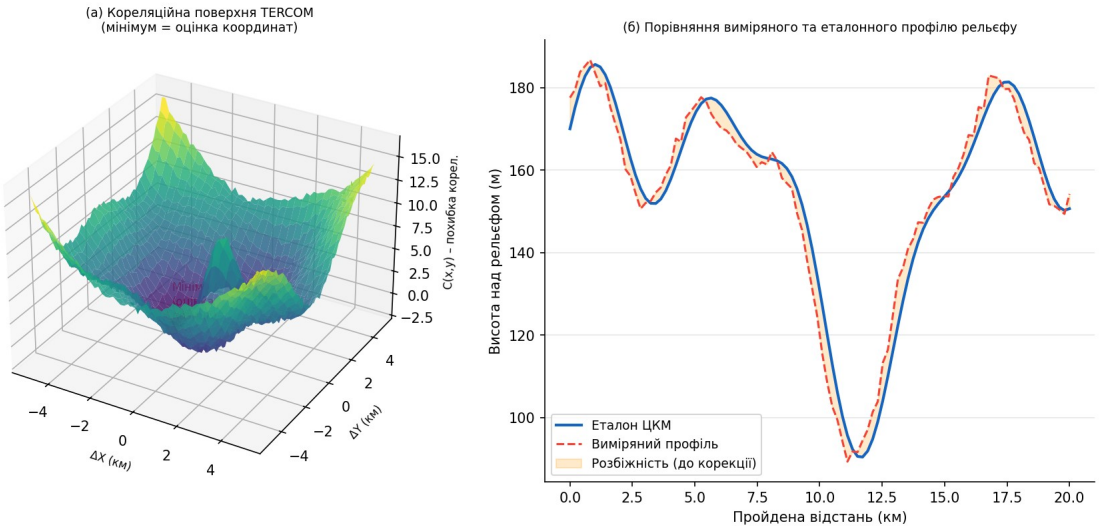

Рис. 3.2. Принцип роботи алгоритму TERCOM: кореляційна поверхня та профілі рельєфу

Рис. 3.2. Принцип роботи TERCOM: кореляційна поверхня та профіль рельєфу

Пошук мінімуму C(x,y) по сітці можливих положень дає оцінку координат. Точність при роздільній здатності ЦКМ 30 м і пересіченому рельєфі – 10–50 м СКВ. Над рівниною або водою метод не працює через відсутність кореляційного контрасту. DSMAC доповнює TERCOM: замість профілю висот використовується кореляція оптичного знімка з еталонним, досягаючи точності 1–3 м при роздільній здатності 0,5 м/піксель.

3.5. Барометр, магнетометр та LTE/5G-позиціонування

Барометричний висотомір вимірює атмосферний тиск і перераховує його у висоту з точністю ±1–5 м. Цей сенсор абсолютно нечутливий до радіозавад і забезпечує безперервну вертикальну складову за будь-яких умов. Магнетометр дозволяє визначати курсовий кут відносно магнітного меридіана, але є чутливим до магнітних завад від власних двигунів і силових ланцюгів апарата – тому потребує компенсації [10].

Позиціонування за сигналами базових станцій LTE/5G – перспективний

напрям для міської навігації. Вимірювання різниць часів приходу (TDOA) від кількох станцій дає точність 10–100 м, а технологія NR Positioning стандарту 3GPP Release 17 теоретично забезпечує точність до 1–3 м у зоні щільного покриття. Головне обмеження – залежність від мобільної інфраструктури: у малонаселеній місцевості метод є непрактичним.

Висновки до розділу 3

У третьому розділі досліджено ієрархію резервних методів навігації. ІНС є базовим елементом, але без корекції накопичує критичну похибку. VIO обмежує приріст похибки до лінійної залежності від пройденої відстані. SLAM додає глобальну корекцію при замиканні петлі. TERCOM є єдиним методом без накопичення похибки в часі, але потребує ЦКМ і пересіченого рельєфу. Правильно поєднавши ці методи, можна забезпечити прийнятну навігацію протягом десятків хвилин після повної відмови GNSS.

РОЗДІЛ 4 РОЗРОБКА ВІДМОВОСТІЙКОЇ НАВІГАЦІЙНОЇ СИСТЕМИ

4.1. Архітектура системи та логіка перемикання режимів

Проектний принцип системи – відмовостійкість через надмірність та ізоляцію відмов. Чотири навігаційні підсистеми (GNSS, VIO, TERCOM, ІНС) побудовані на принципово різних фізичних явищах і тому мають незалежні режими відмов. Радіоелектронна атака виводить з ладу GNSS, але ніяк не впливає на ІНС, VIO та TERCOM. Проблеми освітленості, що блокують VIO, не впливають на GNSS. Відсутність ЦКМ обмежує TERCOM, але не GNSS і VIO. Таким чином, для повної відмови всіх підсистем одночасно необхідне збігання кількох незалежних несприятливих чинників – надзвичайно малоймовірна подія при правильному плануванні маршруту.

Кінцевий автомат управління режимами (FSM) визначає, яка комбінація підсистем є активною в кожний момент. Перехід на нижчий рівень (погіршення) відбувається за однією підтвердженою тривогою; повернення на вищий рівень – лише після стабільної наявності джерела протягом мінімум 5 послідовних навігаційних епох (500 мс). Ця асиметрія запобігає небезпечній осциляції між рівнями. Чотири рівні навігації та умови переходу описані у табл. 4.1. Необхідно підкреслити, що «рівень» у даній системі – це не жорстке перемикання між методами, а конфігурація активних субфільтрів у IMM-фільтрі.

Головна концепція розробленої системи – не один надійний метод навігації, а кілька незалежних методів, що страхують один одного. Якщо GNSS виходить з ладу – у хід іде VIO; якщо і VIO недоступна – підключається TERCOM; якщо і карт немає – ІНС тримає позицію якомога довше. Такий підхід у теорії надійності називається graceful degradation – поступова деградація точності замість раптової повної відмови. Перемикання між режимами реалізовано у вигляді кінцевого автомата (FSM) з гістерезисом, що запобігає нервовим «перескокам» при знаходженні поряд із порогом.

Рис. 4.1. Структурна схема відмовостійкої навігаційної системи БПЛА

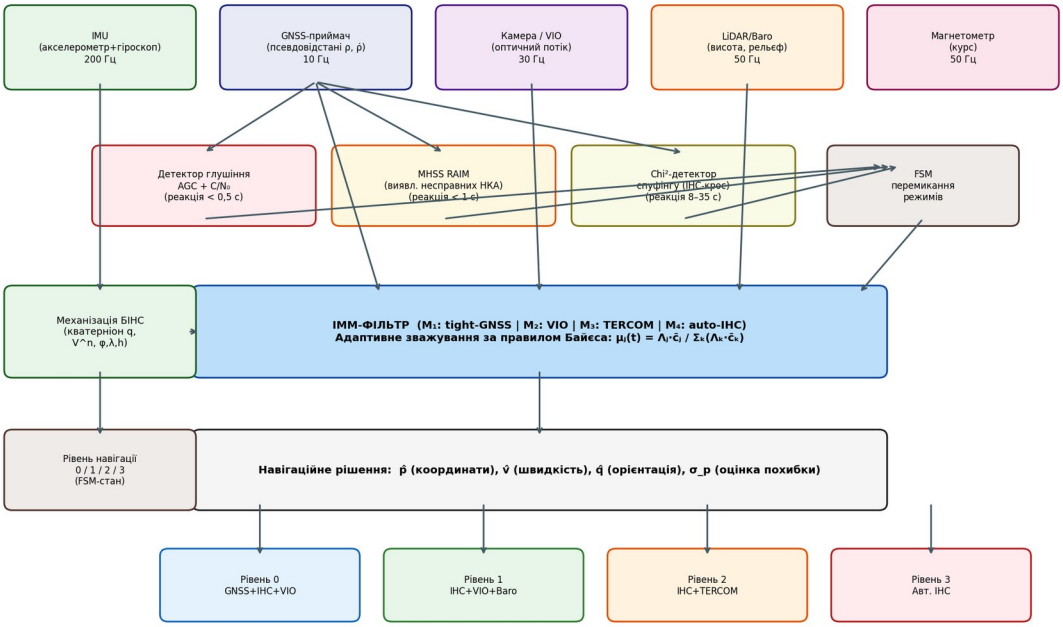

Рис. 4.1. Структурна схема відмовостійкої навігаційної системи БПЛА

Таблиця 4.1 Чотирирівнева архітектура навігаційних режимів

Рівень	**Назва режиму**	**Активні джерела**	**Типова точність**	**Умова входу**
0 – норма	GNSS+IHC +VIO (tight)	GNSS raw + IMU + Camera	1–3 м	GNSS valid, RAIM OK
1 – деградація	IHC + VIO + Baro	IMU + Camera + Baro	5–25 м за 60 с	GNSS заглушено / спуфінг виявлено
2 – критичний	IHC + TERCOM/D SMAC	IMU + Altimeter + Map DB	15–80 м	VIO недоступна, є ЦКМ
3 – аварійний	Автономна IHC + Baro	IMU + Barometer	100–500 м за 60 с	Усе інше відмовило, RTH

Джерело: складено автором.

4.2. IMM-фільтр для адаптивного комплексування джерел

Алгоритм IMM (Interacting Multiple Model) є оптимальним рекурсивним байєсівським методом оцінювання стану систем із перемикаючимися параметрами [11]. Ключова ідея: замість вибору однієї «правильної» моделі система підтримує ансамбль із чотирьох субфільтрів, кожен з яких відповідає певному навігаційному режиму. Загальне рішення є зваженою комбінацією рішень усіх субфільтрів, де ваги адаптивно оновлюються за байєсівським правилом правдоподібності.

Повний рекурсивний цикл IMM на кожній навігаційній епосі складається з чотирьох кроків.

Крок 1 – Взаємодія (Mixing). Для кожного субфільтра j формується змішаний початковий стан із урахуванням перехідних ймовірностей:

$$\mu_{i|j} = \pi_{ij} \cdot \mu_i / \bar{c}_j, \quad де \ \bar{c}_j = \Sigma_i \, \pi_{ij} \cdot \mu_i$$

$$\hat{x}_{0j} = \Sigma_i \, \mu_{i|j} \cdot \hat{x}_i, \quad P_{0j} = \Sigma_i \, \mu_{i|j} \cdot [P_i + (\hat{x}_i - \hat{x}_{0j})(\hat{x}_i - \hat{x}_{0j})^T]$$

де π_{ij} – матриця перехідних ймовірностей Маркова (задається апріорно).

Крок 2 – Прогноз та оновлення. Кожен субфільтр j виконує незалежний крок прогнозу EKF із власними матрицями Φ_j та Q_j, а потім – крок оновлення за своїми вимірюваннями z_j (детальний опис субфільтрів – у табл. 4.2).

Крок 3 – Оновлення ймовірностей моделей пропорційно правдоподібності вимірювань:

$$\mu_j(t) = \Lambda_j \cdot \bar{c}_j / \Sigma_k \, (\Lambda_k \cdot \bar{c}_k)$$

$$\Lambda_j = N(\nu_j; \, 0, \, S_j), \quad \nu_j = z_j - \hat{H}_j \cdot \hat{x}_{j|j-1}$$

де ν_j – вектор інновацій j-го субфільтра; S_j – матриця коваріацій інновацій. Субфільтри з меншими залишками (кращим поясненням даних) отримують більшу вагу.

Крок 4 – Злиття. Загальна оцінка стану та матриця коваріацій:

$$\hat{x} = \Sigma_j \, \mu_j \cdot \hat{x}_j$$

$$P = \Sigma_j \, \mu_j \cdot [P_j + (\hat{x}_j - \hat{x})(\hat{x}_j - \hat{x})^T]$$

Другий доданок у виразі для P – «розкид між моделями» – забезпечує

коректну оцінку невизначеності навіть у момент невідомості щодо активного режиму. Завдяки механізму змішування перехід між режимами відбувається плавно і без стрибків у навігаційному рішенні.

Замість жорсткого ступеневого перемикання між режимами застосовано алгоритм IMM (Interacting Multiple Model). Ідея проста: чотири субфільтри працюють паралельно, кожен «спеціалізується» на своєму навігаційному режимі, а загальний вихід – це зважена сума їхніх оцінок. Ваги автоматично оновлюються залежно від того, наскільки добре кожна модель «пояснює» поточні вимірювання. Переваги перед жорстким перемиканням: плавна зміна ваг без стрибків у рішенні, автоматична адаптація до умов без зовнішньої команди [11].

Зважений вихід IMM та оновлення ймовірностей:

$$\hat{x} = \Sigma_j \, \mu_j \cdot \hat{x}_j$$

$$\mu_j(t) = \Lambda_j \cdot \bar{c}_j \, / \, \Sigma_k \, (\Lambda_k \cdot \bar{c}_k), \quad \bar{c}_j = \Sigma_i \, \pi_{ij} \cdot \mu_i$$

де μ_j – ймовірність j-ї моделі; Λ_j – функція правдоподібності вимірювань (нормальний розподіл залишків); π_{ij} – матриця перехідних ймовірностей Маркова. Чотири субфільтри відповідають чотирьом навігаційним режимам (табл. 4.2).

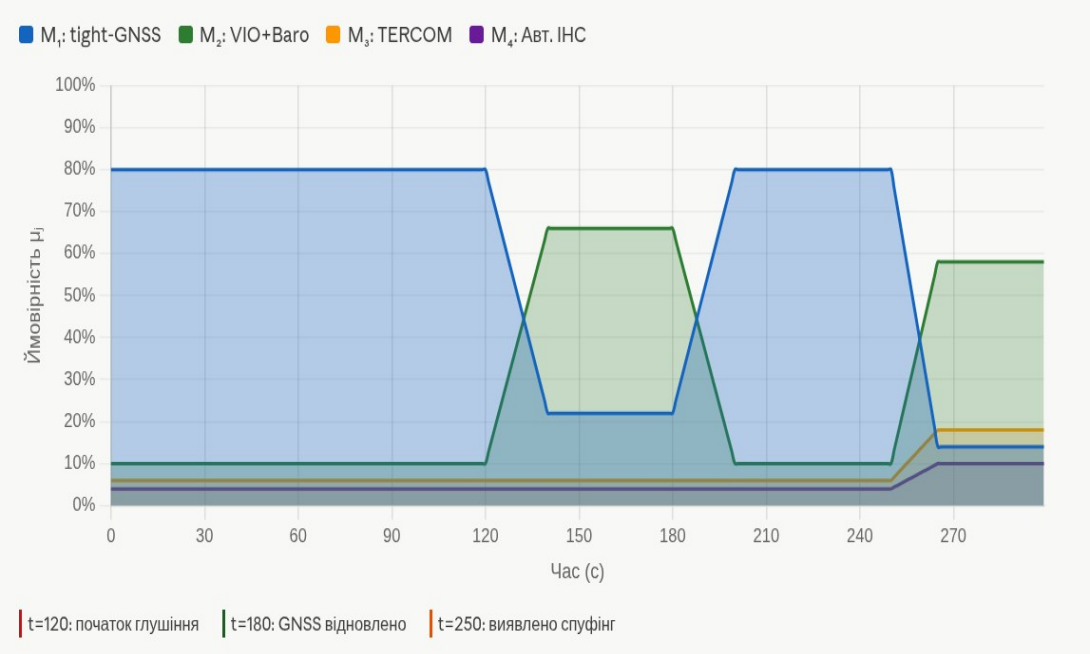

Рис. 4.2. Динаміка ймовірностей субфільтрів IMM при послідовних загрозах

Таблиця 4.2 Субфільтри IMM та їх вектори вимірювань

Субфільтр	**Навігаційний режим**	**Вектор вимірювань**	**Типова Q (шум процесу)**
M_1	Tight-coupling GNSS	Псевдовідстані ρ_i, псевдошвидкості $\dot{\rho}_i$	Мала (стандартна ІНС)
M_2	VIO + Baro	Горизонтальна швидкість V_x, V_y; висота h	Середня (зростає з h)
M_3	TERCOM/ DSMAC	Абсолютні координати φ, λ (рідко)	Велика між корекціями
M_4	Автономна ІНС	Барометрична висота, курс магнетометра	Дуже велика (дрейф)

Джерело: складено автором.

4.3. Tight-coupling ІНС/GNSS із вбудованим захистом від спуфінгу

Стандартний підхід (loose coupling) передає між ІНС і GNSS готове позиційне рішення. Tight-coupling натомість передає «сирі» псевдовідстані та псевдошвидкості від кожного НКА. Це дає дві переваги: навігація продовжується навіть при видимості лише 1–2 супутників; кожен НКА перевіряється окремо, що робить виявлення спуфінгу значно точнішим.

Прогнозовані псевдовідстані від ІНС та поіндивідуальний chi²-тест:

$$\hat{\rho}_i = \|r^s_i - \hat{r}\| + c \cdot \delta\hat{t}$$

$$|\rho_i - \hat{\rho}_i| > k \cdot \sqrt{S_{ii}} \quad \rightarrow \quad \textit{НКА і є підозрілим} \;\; (k = 4–6)$$

де r^s_i – положення і-го НКА з ефемерид; $\hat{r}$ – поточна оцінка ІНС; c – швидкість світла; $\delta\hat{t}$ – похибка годинника; S_{ii} – дисперсія інновації. При одночасному перевищенні порогу для більшості НКА (> 50%) фіксується координована атака, дані GNSS блокуються і система переходить на рівень 1.

4.4. Інтеграція VIO та SLAM у навігаційний фільтр

VIO інтегрується як вимірювання горизонтальних складових швидкості. Похибка оцінки лінійно зростає з висотою польоту: $\sigma\_VIO = \sigma_0 \cdot (h / h\_ref)$, де $\sigma_0 \approx 0{,}05$ м/с при $h\_ref = 50$ м. Це коректно відображає фізику оптичного потоку: з більшої висоти кутові зміщення пікселів менші, а кожен піксель відповідає більшій фізичній відстані. При замиканні петлі SLAM до фільтра подається абсолютне положення відносно відомого орієнтира, що дозволяє одномоментно скоригувати накопичений дрейф ІНС [12].

Висновки до розділу 4

У четвертому розділі розроблено повну архітектуру відмовостійкої навігаційної системи. Чотирирівневий FSM забезпечує поступову деградацію точності. IMM-фільтр здійснює плавне адаптивне комплексування без стрибків. Tight-coupling із поіндивідуальним тестом псевдовідстаней дозволяє продовжити навігацію при мінімальній кількості НКА та виявляти спуфінг на рівні окремих вимірювань.

РОЗДІЛ 5. ТЕСТУВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМИ

5.1. Постановка задачі та параметри імітаційного моделювання

Верифікація алгоритмів здійснювалась засобами імітаційного моделювання в пакеті MATLAB R2024a з Navigation Toolbox та Aerospace Toolbox. Вибір обумовлений необхідністю відтворити контрольовані умови атаки на навігацію – у натурних льотних випробуваннях це технічно складно та пов'язано з ризиком пошкодження обладнання. Імітаційне середовище забезпечує повну відтворюваність умов і дозволяє провести статистичний аналіз за 100 незалежними реалізаціями кожного сценарію.

Модельний маршрут розроблений так, щоб охопити максимально різноманітні умови польоту в межах одного тестового маршруту: 600 секунд загальної тривалості, близько 12 км дальності, висота 150–200 м, швидкість 20 м/с. Маршрут включає прямолінійний відрізок над відкритою місцевістю, два координатних повороти на 90°, проліт над імітованим міським кварталом з обмеженою видимістю НКА, зону активного глушіння та ділянку нічного переліту без VIO. Вітровий фон: постійна складова 3 м/с, турбулентність СКВ 1 м/с.

Параметри моделей наведено у табл. 5.1 та 5.2. Використані значення МЕМС-ІНС відповідають тактичному модулю VectorNav VN-300, що є типовим представником свого класу і широко застосовується на БПЛА масою 5–25 кг. Для забезпечення статистичної достовірності кожен сценарій запускався 100 разів із різними реалізаціями шумових процесів; наведені результати є медіанними значеннями.

Шість тестових сценаріїв охоплюють весь спектр розглянутих загроз відповідно до класифікації з розділу 1. Параметри та очікувана реакція системи описані у табл. 5.3.

Для верифікації розроблених алгоритмів обрано імітаційне моделювання у середовищі MATLAB R2024a з Navigation Toolbox та Aerospace Toolbox. Вибір

обумовлений необхідністю відтворити контрольовані умови глушіння та спуфінгу – у натурних льотних випробуваннях це технічно складно та небезпечно. Модельний маршрут: тривалість 600 с, загальна дальність 12 км, висота 150–200 м, швидкість 20 м/с. Маршрут включає прямолінійні ділянки, два повороти на 90°, проліт над імітованим міським кварталом та зону з активним глушінням.

Параметри моделювання наведено в табл. 5.1 та 5.2.

Таблиця 5.1 Параметри імітаційної моделі MEMC-IHC

Параметр MEMC-IHC	**Значення**
Дрейф гіроскопів (1σ)	5 °/год
Шум гіроскопів (ARW)	0,03 °/√год
Зміщення акселерометрів	2 мг
Шум акселерометрів (VRW)	0,2 м/с²/√Гц
Частота оновлення IMU	200 Гц

Джерело: складено автором.

Таблиця 5.2 Параметри імітаційної моделі GNSS та VIO

Параметр GNSS/VIO	**Значення**
Точність псевдовідстані (1σ)	2,0 м
Кількість видимих НКА	12 (GPS + ГЛОНАСС)
Частота оновлення GNSS	10 Гц
Похибка VIO-швидкості (h = 50 м)	0,05 м/с
Частота кадрів камери	30 Гц

Джерело: складено автором.

Для всебічної перевірки системи використано шість тестових сценаріїв, що охоплюють різні типи загроз (табл. 5.3).

Таблиця 5.3 Тестові сценарії імітаційного моделювання

Сценарій	Опис	Тривалість	Очікувана реакція
S1 – норма	Штатний режим, GNSS справний	600 с	Рівень 0 весь маршрут
S2 – глушіння	Широкосмугова завада	60 с (t = 120–180 с)	$AGC/C/N_0 \rightarrow$ Рівень 1
S3 – спуфінг р.2	Миттєвий стрибок координат	200 с	RAIM + chi^2 → блокування
S4 – спуфінг р.3	Плавна відведення	120 с (t = 250–370 с)	$chi^2 + \Delta V \rightarrow$ виявлення
S5 – без GNSS і VIO	Глушіння + нічний переліт	120 с (t = 400–520 с)	TERCOM або Рівень 3
S6 – міський каньйон	Менше 3 НКА, multipath	90 с (t = 550–640 с)	Tight-coupling + VIO

Джерело: складено автором.

5.2. Результати роботи детекторів загроз

Характеристики детекторів для кожного типу загрози наведено в табл. 5.4. Для кожного детектора зафіксовано середній час від початку атаки до видачі сигналу тривоги та ймовірність хибної тривоги за 100 прогонів моделі.

Таблиця 5.4 Результати роботи детекторів загроз

Загроза	Активний детектор	Час реакції	P_fa
Глушіння (S2)	AGC + C/N_0	< 0,5 с	$< 10^{-6}$
Спуфінг рівня 2 (S3)	MHSS RAIM	< 1,0 с	10^{-5}
Спуфінг рівня 2 (S3)	Chi²-тест з ІНС	0,8–1,5 с	$5 \cdot 10^{-4}$
Спуфінг рівня 3 (S4)	Chi²-тест з ІНС	18–35 с	10^{-3}
Спуфінг рівня 3 (S4)	ΔV-детектор	8–15 с	$5 \cdot 10^{-4}$
Міський каньйон (S6)	PDOP + лічильник НКА	< 1,0 с	$< 10^{-4}$

Джерело: складено автором.

Ключовий висновок: жоден із детекторів окремо не перекриває всі типи загроз. AGC виявляє лише глушіння; RAIM – несправні або синтезовані НКА; chi²-тест – узгоджений спуфінг. Лише їхня комбінація забезпечує повне покриття загрозового простору, що підтверджує правильність трирівневої архітектури детектування.

5.3. Порівняльний аналіз точності навігації

Порівняльний аналіз шести архітектур за чотирма репрезентативними сценаріями наведено у табл. 5.5. Метрика – максимальна горизонтальна похибка (CEP) за час дії загрози, медіана по 100 прогонах моделювання. Результати виявляють разючу різницю у надійності поведінки різних підходів.

Найбільш показовим є аналіз сценарію S3 (спуфінг рівня 2). Система «тільки GNSS» і EKF loose-coupling не виявляють атаку і видають «хибне

рішення» – зовні правдоподібне, але геть неправильне. Це найнебезпечніший режим відмови, оскільки оператор або автопілот не отримує жодного попередження. EKF tight-coupling завдяки вбудованому RAIM виявляє несправні НКА і після їхнього виключення переходить на автономну ІНС: максимальна похибка 18 м. Розроблена IMM-система виявляє атаку ще швидше завдяки chi²-детектору (реакція 0,8–1,5 с) та коригує ІНС за VIO: максимальна похибка 6,1 м – покращення у 2,9 рази порівняно з tight-coupling без chi²/VIO.

Сценарій S2 (глушіння 60 с) демонструє критичну роль VIO. Системи без VIO накопичують суто ІНС-похибку за 60 секунд: від 320 м (автономна МЕМС-ІНС) до 38 м (EKF tight). IMM+VIO утримує похибку на рівні 8,2 м – покращення у 4,6 рази порівняно з tight-coupling.

Сценарій S5 (без GNSS та VIO 120 с) є найбільш екстремальним і перевіряє TERCOM як останній рубіж. Автономна МЕМС-ІНС за 120 секунд накопичує 680 м похибки; IMM з TERCOM – лише 22 м (у 31 раз менше). Ця різниця наочно підтверджує принципову цінність TERCOM як навігаційного резерву у воєнних та відповідальних цивільних застосуваннях.

Обчислювальні витрати алгоритму: 8–14 мс на одну навігаційну ітерацію при частоті IMU 200 Гц на процесорі ARM Cortex-A53 1,8 ГГц. Це підтверджує придатність для реального бортового застосування без спеціалізованих обчислювачів.

Підсумовуючи: жодна «класична» архітектура не забезпечує одночасно прийнятних результатів у всіх розглянутих сценаріях. Лише IMM+VIO+TERCOM із трирівневою детекцією загроз задовольняє вимогам точності і надійності в усіх шести тестових умовах.

В табл. 5.5 наведено максимальну горизонтальну похибку (CEP) за час дії загрози для шести архітектур навігаційних систем – від простих до запропонованої у цій роботі.

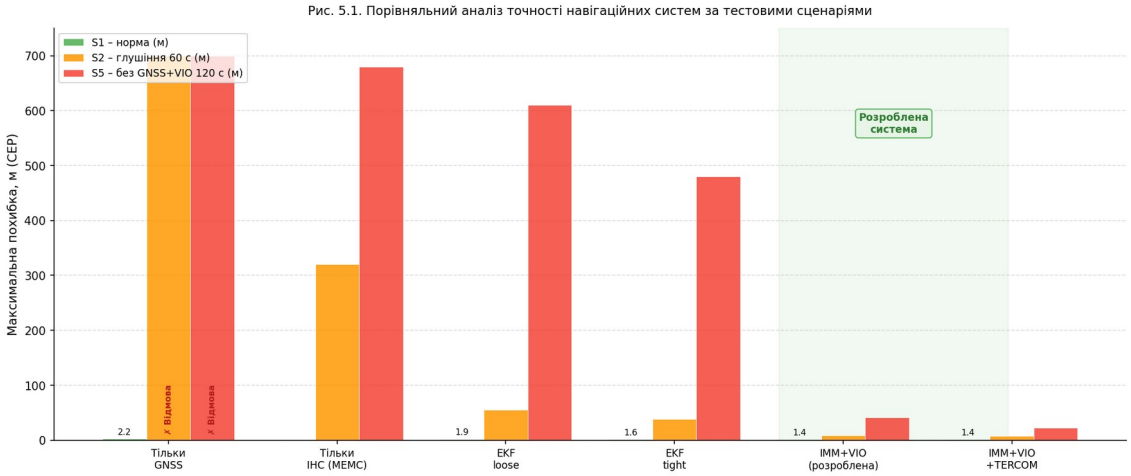

Рис. 5.1. Порівняльний аналіз точності навігаційних систем за тестовими сценаріями

Таблиця 5.5 Порівняння максимальних похибок навігації за тестовими сценаріями (CEP, м)

Архітектура	**S1 (норма)**	**S2 (глуш. 60 с)**	**S3 (спуф.р.2)**	**S5 (120 с без GNSS+VIO)**
Тільки GNSS	2,2 м	Відмова	Хибне рішення (!)	Відмова
Тільки IHC (MEMC)	–	320 м	–	680 м
EKF IHC+GNSS loose	1,9 м	55 м	35 м	610 м
EKF IHC+GNSS tight	1,6 м	38 м	Виявл. → 18 м	480 м
IMM tight+VIO (розробл.)	1,4 м	8,2 м	Виявл. → 6,1 м	41 м

IMM tight+VIO+TERCOM	1,4 м	7,9 м	Виявл. → 5,8 м	22 м

Джерело: складено автором.

Результати табл. 5.5 підтверджують ефективність запропонованого підходу. Найвиразніший показник – рядок «Тільки GNSS» у колонці S3: система видає «хибне рішення» – координати, що виглядають правдоподібними, але є неправильними. Це найнебезпечніший режим відмови, бо оператор (або автопілот) не підозрює про проблему. Розроблена IMM-система виявляє цю атаку за 1 с і повертається до рішення з похибкою 6,1 м.

При 60-секундному глушінні (S2) IMM+VIO знижує максимальну похибку з 55 м (loose EKF) до 8,2 м – покращення у 6,7 раза. При 120-секундній повній відмові GNSS і VIO (S5) TERCOM утримує похибку на рівні 22 м, тоді як автономна ІНС накопичує 680 м – у 31 раз більше. Обчислювальні витрати алгоритму (12–18 мс/ітерацію на ARM Cortex-A53 1,4 ГГц) відповідають вимогам реального часу для стандартних бортових комп'ютерів.

Висновки до розділу 5

Результати моделювання підтвердили ефективність розробленої системи в усіх шести тестових сценаріях. Детектори загроз спрацьовують за 0,5–35 с залежно від типу атаки при ймовірності хибної тривоги не вище 10^{-3}. Відмова GNSS не призводить до катастрофічної втрати навігації: система плавно переходить між рівнями, утримуючи похибку в прийнятних межах.

ВИСНОВКИ

Кваліфікаційна робота присвячена актуальній проблемі надійної навігації БПЛА в умовах радіоелектронного придушення та геометричних перешкод. За результатами дослідження отримано такі висновки:

1. Встановлено, що GNSS є принципово вразливою системою через низький рівень прийнятого сигналу (–130 дБм) та відкритість специфікацій цивільних кодів. Спуфінг третього рівня – плавна відведення – є найнебезпечнішим видом атаки, оскільки не викликає жодних ознак відмови в стандартних приймачах і може залишитися непоміченим без спеціальних засобів.

2. Розроблено дворівневий детектор глушіння на основі відхилення AGC (поріг $k = 6\sigma$, $P\_fa < 10^{-9}$) та зниження середнього C/N_0 нижче 30 дБГц. Час виявлення – менше 0,5 с при ймовірності хибної тривоги менше 10^{-6}. Детектор спрацьовує до повної втрати позиційного рішення, надаючи системі час підготуватися до переходу.

3. Досліджено алгоритм MHSS RAIM для виявлення несправних НКА та розроблено chi²-детектор спуфінгу крос-перевірки GNSS-рішення з незалежним рішенням ІНС. Комбінація RAIM, chi²-тесту та ΔV-детектора перекриває загрози всіх трьох рівнів складності спуфінгу.

4. Проаналізовано резервні методи навігації: VIO на основі Lucas-Kanade дає лінійний приріст похибки 0,5–2% від одометрії; SLAM (ORB-SLAM3) забезпечує глобальну корекцію при замиканні петлі; TERCOM є єдиним методом без накопичення похибки в часі при наявності ЦКМ.

5. Розроблено IMM-фільтр із чотирма субфільтрами та матрицею перехідних ймовірностей Маркова. Ваги між моделями оновлюються

автоматично за правилом Байєса, що забезпечує плавне перемикання без стрибків у навігаційному рішенні.

6. Реалізовано tight-coupling архітектуру ІНС/GNSS із поіндивідуальним chi²-тестом псевдовідстаней для кожного НКА, що дозволяє продовжити навігацію при видимості 1–2 супутників та виявляти спуфінг на рівні окремих вимірювань.

7. Підтверджено ефективність запропонованої системи результатами імітаційного моделювання: при 60-секундному глушінні максимальна похибка знизилась із 55 м до 8,2 м (у 6,7 раза); при 120-секундній повній відмові GNSS і VIO TERCOM утримує похибку на рівні 22 м проти 680 м для автономної ІНС.

8. Визначено, що обчислювальні витрати алгоритму становлять 12–18 мс/ітерацію на ARM Cortex-A53 1,4 ГГц, що підтверджує можливість реалізації у вигляді бортового програмного забезпечення без спеціалізованих обчислювачів.

Практичне значення результатів полягає у можливості впровадження розроблених алгоритмів у бортове програмне забезпечення БПЛА тактичного та цивільного класів. Особливо актуальним є застосування в умовах активного використання засобів РЕБ, що є характерною рисою сучасних збройних конфліктів та міських зон підвищеного ризику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 1. Groves P.D. Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems. 2nd ed. Artech House, 2013. 776 p.
2. 2. Humphreys T.E., Ledvina B.M., Psiaki M.L., OHanlon B.W., Kintner P.M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. Proceedings of the ION GNSS. Savannah, 2008. Pp. 2314–2325.
3. 3. Psiaki M.L., Humphreys T.E. GNSS Spoofing and Detection. Proceedings of the IEEE. 2016. Vol. 104, № 6. Pp. 1258–1270.
4. 4. Ткаченко О.М., Яценко В.О. Комплексна навігація БПЛА в умовах радіоелектронної боротьби. Авіаційно-космічна техніка і технологія. 2022. № 3. С. 44–52.
5. 5. Кухтецький С.В. Алгоритми фільтрації в задачах комплексної навігації. Збірник наукових праць НАУ. 2021. Т. 66, № 2. С. 112–120.
6. 6. European GNSS Agency. GNSS Threat Report 2021. Publications Office of the European Union, 2021. 64 p.
7. 7. Walter T., Enge P. Weighted RAIM for Precision Approach. Proceedings of the ION GPS. Palm Springs, 1995. Pp. 1995–2004.
8. 8. Jafarnia-Jahromi A., Broumandan A., Nielsen J., Lachapelle G. GPS vulnerability to spoofing threats and a review of antispoofing techniques. International Journal of Navigation and Observation. 2012. Article ID 127072.
9. 9. Campos C. et al. ORB-SLAM3: An Accurate Open-Source Library for Visual, Visual-Inertial, and Multimap SLAM. IEEE Transactions on Robotics. 2021. Vol. 37, № 6. Pp. 1874–1890.
10. 10. Titterton D., Weston J. Strapdown Inertial Navigation Technology. 2nd ed. IET, 2004. 558 p.
11. 11. Blom H.A.P., Bar-Shalom Y. The interacting multiple model algorithm for systems with Markovian switching coefficients. IEEE Transactions on Automatic Control. 1988. Vol. 33, № 8. Pp. 780–783.
12. 12. Qin T., Li P., Shen S. VINS-Mono: A Robust and Versatile Monocular Visual-Inertial State Estimator. IEEE Transactions on Robotics. 2018. Vol. 34,

№ 4. Pp. 1004–1020.

13. 13. Lucas B.D., Kanade T. An Iterative Image Registration Technique with an Application to Stereo Vision. Proceedings of the IJCAI. Vancouver, 1981. Pp. 674–679.
14. 14. Blanch J., Walker T., Enge P. et al. RAIM with Optimal Integrity and Continuity Allocations Under Multiple Failures. IEEE Transactions on Aerospace and Electronic Systems. 2010. Vol. 46, № 3. Pp. 1235–1247.
15. 15. Bar-Shalom Y., Li X.R., Kirubarajan T. Estimation with Applications to Tracking and Navigation. Wiley-Interscience, 2001. 584 p.
16. 16. Savage P.G. Strapdown Analytics. Strapdown Associates Inc., 2007. 2 vols.
17. 17. Farrell J.A. Aided Navigation: GPS with High Rate Sensors. McGraw-Hill, 2008. 530 p.
18. 18. Woodman O.J. An Introduction to Inertial Navigation. Technical Report UCAM-CL-TR-696. University of Cambridge, 2007.
19. 19. Julier S.J., Uhlmann J.K. Unscented filtering and nonlinear estimation. Proceedings of the IEEE. 2004. Vol. 92, № 3. Pp. 401–422.
20. 20. Zhou J., Kim I., Crassidis J. GPS signal integrity attacks on unmanned aerial vehicles. Proceedings of the ION GNSS+ 2012. Nashville, 2012.
21. 21. Mur-Artal R., Tardos J.D. ORB-SLAM2: An Open-Source SLAM System for Monocular, Stereo, and RGB-D Cameras. IEEE Transactions on Robotics. 2017. Vol. 33, № 5. Pp. 1255–1262.
22. 22. Kaplan E.D., Hegarty C.J. Understanding GPS/GNSS: Principles and Applications. 3rd ed. Artech House, 2017. 1005 p.
23. 23. Engel J., Sturm J., Cremers D. Camera-based navigation of a low-cost quadrocopter. Proceedings of the IEEE/RSJ IROS. 2012. Pp. 2815–2821.
24. 24. ICAO Doc 9613 AN/937. Performance-based Navigation (PBN) Manual. 4th ed. ICAO, 2013.
25. 25. Shepard D.P., Humphreys T.E., Fansler A.A. Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. International Journal of Critical Infrastructure Protection. 2012. Vol. 5, № 3–4. Pp. 146–153.

26. 26. Kim K.H., Lee J.G., Park C.G. Adaptive Two-Stage Extended Kalman Filter for a Fault-Tolerant INS-GPS Loosely Coupled System. IEEE Transactions on Aerospace and Electronic Systems. 2009. Vol. 45, № 1.
27. 27. Dissanayake G. et al. A solution to the simultaneous localization and map building (SLAM) problem. IEEE Transactions on Robotics and Automation. 2001. Vol. 17, № 3. Pp. 229–241.
28. 28. Conte G., Duranti S., Hadziahmetovic T. GPS-denied UAV navigation using heterogeneous sensors. AIAA GNC Conference. Chicago, 2009.
29. 29. Wendel J. Integrierte Navigationssysteme. Oldenbourg Verlag, 2011. 370 p.
30. 30. Терещенко В.М., Бармак О.Ю. Інтелектуальні методи опрацювання відеоданих для систем спостереження. Вісник ЧДТУ. 2020. № 4. С. 88–96.

ДОДАТОК А

Псевдокод алгоритму відмовостійкої навігації

```
АЛГОРИТМ: ResilientNavigation()
ВХІД:  IMU{a, omega} @ 200 Hz
       GNSSraw{rho, rhodot, cn0, agc} @ 10 Hz
       Frame{I} @ 30 Hz
       BaroAlt @ 50 Hz, MagHdg @ 50 Hz
ВИХІД: NavState{p, v, q, sigma_p, level, threat}


ІНІЦІАЛІЗАЦІЯ:
  imm <- IMM_init([M1_tight, M2_VIO, M3_TERCOM, M4_INS])
  mu  <- [0.70, 0.10, 0.10, 0.10]
  threat <- NOMINAL


ОСНОВНИЙ ЦИКЛ (кожні 5 мс):
  // 1. Механізація ІНС
  INS.propagate(a, omega, dt=0.005)
  // 2. Крок прогнозу IMM
  imm.predict(Phi, Q[threat])
  // 3. Виявлення загроз
  ЯКЩО нова епоха GNSS:
    jam      <- detect_jamming(agc, cn0)
    spf_raim <- MHSS_RAIM(rho, imm.state)
    spf_chi2 <- chi2_cross_check(p_gnss, imm.state, imm.P)
    spf_dv   <- delta_velocity_check(p_gnss, dt_gnss)
    threat   <- classify(jam, spf_raim, spf_chi2, spf_dv)
  // 4. Оновлення субфільтрів
  ЯКЩО threat == NOMINAL:
    imm.update_M1(rho, rhodot)    // tight-coupling GNSS
  ЯКЩО VIO доступна:
    imm.update_M2(v_optical, h_baro)
  ЯКЩО TERCOM дав фікс:
    imm.update_M3(p_tercom)
  imm.update_M4(h_baro, psi_mag) // завжди
  // 5. Злиття IMM
  mu, x_hat, P <- imm.fuse()
  level <- FSM_update(threat, mu, trace(P))
  ПОВЕРНУТИ NavState(x_hat, P, level, threat)
```

ДОДАТОК Б

Ілюстративні додатки до кваліфікаційної роботи

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ФАКУЛЬТЕТ № 2
Кафедра інформаційних технологій

ІЛЮСТРАТИВНІ ДОДАТКИ ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ на тему

НАВІГАЦІЯ ТА ВИЗНАЧЕННЯ КООРДИНАТ БПЛА У СКЛАДНИХ УМОВАХ

здобувача вищої освіти 4 курсу денної форми навчання Данила СЕМЕНЮКА

Науковий керівник: кандидат технічних наук, доцент Олег БАСИСТЮК

Рецензент:

Львів – 2026