multipath, dynamic interference, as well as the possibility of safe implementation of typical attacks (rogue AP, evil twin, deauthentication) outside productive contours. A system of metrics is proposed that integrates localization quality (mean and median error, 95th percentile), detection and classification indicators (Precision, Recall, F1, ROC-AUC) and SOC operational characteristics (mean time to detection, time to source localization, false positive rate, analyst working time). The data collection protocol and rules for forming training and test subsets taking into account the drift of the radio environment are described. Separately, a model for assessing the practical effect of implementation is presented, which links technical metrics with the risk of incidents, downtime of services and response costs. It is experimentally shown that hybrid localization methods provide a median error of 1.12 m versus 2.7 m for classical RSSI trilateration, and the hybrid attack detector achieves ROC-AUC of 0.962. The results are suitable for testing, implementation in the CII and preparation of materials according to the requirements of professional publications.

Keywords: Wi-Fi cybersecurity; critical information infrastructure; spatial localization; experimental polygon; rogue AP detection; SOC; performance metrics.

Надійшла до редакції (Received): 03.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.056.5:623.746-519 DOI: 10.31673/2409-7292.2026.028613

Ткач Юлія Миколаївна
доктор педагогічних наук, кандидат технічних наук, професор, завідувач кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка», Чернігів, Україна
ORCID: 0000-0002-8565-0525
E-mail: tkachym79@gmail.com

Дюба Ігор Миколайович
аспірант кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка», Чернігів, Україна
ORCID: 0009-0007-3669-6424
E-mail: idyuba@gmail.com

БАГАТОШАРОВИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ КІБЕРФІЗИЧНИХ СИСТЕМ НА ПРИКЛАДІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У статті досліджено комплексний характер уразливостей сучасних безпілотних літальних апаратів (БпЛА) як класу кіберфізичних систем (КФС). Авторами теоретично обґрунтовано та деталізовано концепцію «вакууму безпеки» – системної незахищеності архітектури дронів, що виникає внаслідок стрімкої інтеграції обчислювальних алгоритмів та фізичних процесів за ігнорування базових критеріїв захищеності. У межах теоретико-керівного підходу (Control-Theoretic Approach) проведено пошаровий декомпозиційний аналіз трьох критичних рівнів архітектури БпЛА: навігаційного, мережевого та інформаційного. Математично та емпірично доведено, що відкритість цивільних сигналів GNSS у поєднанні з апаратною архітектурою з однією антеною (Single-Receiver) робить КФС беззахисною перед прихованими атаками ін'єкції помилкових даних (False Data Injection). Досліджено механізми компрометації каналів керування через вразливості протоколу MAVLink за допомогою атак повтору (Replay Attacks). Особливу увагу приділено інформаційному рівню, де продемонстровано можливість деанонімізації стратегії використання системи через аналіз профілю зашифрованого трафіку (Side-Channel Attacks). На основі аналізу провідних світових досліджень сформульовано закон мультиплікативності ризиків КФС та запропоновано системні рекомендації щодо переходу до парадигми Security by Design.

Ключові слова: кіберфізичні системи (КФС), безпілотні літальні апарати (БпЛА), вакуум безпеки, GPS-спуфінг, джаммінг, протокол MAVLink, атака повтору (Replay Attack), ін'єкція хибних даних (FDI), аналіз сторонніх каналів, мультиплікативність ризиків, Security by Design.

Вступ

Стрімкий прогрес у галузі мікроелектроніки, систем автоматичного керування та бездротового зв'язку зумовив масштабну інтеграцію безпілотних літальних апаратів (БпЛА) у цивільний та військовий сектори. Сучасні БпЛА вже не розглядаються як ізольовані механічні пристрої з дистанційним керуванням; вони є повноцінними кіберфізичними системами (КФС), де обчислювальні алгоритми цифрового простору безпосередньо керують динамічними процесами у фізичному середовищі. Безпілотні комплекси виконують широкий спектр критично важливих місій – від автономного моніторингу навколишнього середовища, логістики та охорони державного кордону до виконання високоточних завдань у зонах бойових дій.

Проте швидкість комерціалізації та нарощування функціональних можливостей БпЛА увійшли в гостру суперечність із вимогами їхньої безпеки. Історично склалося так, що базові архітектурні стандарти, які використовуються в цивільних дронах, розроблялися в умовах обмежених обчислювальних ресурсів і були оптимізовані для мінімізації затримок та зниження вартості обладнання, а не для протидії цілеспрямованим кіберзагрозам. Внаслідок цього виник феномен, який автори окреслюють як системний «вакуум безпеки». Його сутність полягає в тому, що сучасні БпЛА функціонують у режимі абсолютної, апріорної довіри до вхідних даних навколишнього середовища та командних каналів.

Наукова актуальність цієї проблеми посилюється тим, що класична парадигма IT-безпеки, заснована на тріаді CIA (конфіденційність, цілісність, доступність), виявляється недостатньою для захисту КФС. Як зазначається у фундаментальних працях із теоретико-керівної безпеки [1], специфіка кіберфізичних систем вимагає аналізу того, як інформаційні деструкції в цифровому контурі трансформуються у незворотні фізичні аномалії у реальному просторі. Безпека КФС є мультиплікативною величиною: якщо хоча б один рівень архітектури – навігаційний, мережевий або інформаційний – має критичну прогалину, загальна захищеність системи прямує до нуля.

Аналіз літературних джерел

У фундаментальній праці Тейшейри та ін. (Teixeira et al., 2015) [1] безпека кіберфізичних систем розглядається через призму теорії керування. Автори доводять, що відсутність автентифікації даних на рівні сенсорів (що відповідає навігаційному вакууму безпеки БпЛА) дозволяє зловмиснику реалізувати так звані "приховані атаки" (stealthy attacks). За таких умов бортові системи виявлення аномалій не здатні ідентифікувати підміну координат, оскільки хибні дані генеруються з урахуванням фізичної моделі динаміки апарату.

Імплементація теорії безпеки КФС Тейшейри в архітектурні рівні БпЛА

У фундаментальній праці Тейшейри та ін. (Teixeira et al., 2015) безпека кіберфізичних систем виводиться за межі класичної парадигми захисту інформації (конфіденційність, цілісність, доступність – триада CIA) і розглядається через призму теоретико-керівного підходу (Control-Theoretic Approach). Автори доводять, що специфіка КФС полягає в синергетичній взаємодії між цифровим та фізичним просторами, де будь-яка інформаційна деструкція неминуче трансформується у фізичні аномалії. У контексті аналізу «вакууму безпеки» БпЛА, запропонована авторами математична матриця загроз дозволяє детально експлікувати кожен із трьох критичних рівнів уразливості:

1. Деструкція навігаційного контуру як прихована атака на сенсори (Stealthy Sensor Attacks). Тейшейра та співавтори математично описують клас атак типу FDI (False Data Injection – ін'єкція хибних даних), які здатні обходити стандартні бортові алгоритми детектування аномалій (Bad Data Detection, BDD). У випадку цивільних БпЛА, навігаційний вакуум безпеки (відсутність автентифікації сигналів GNSS) надає зловмиснику необмежені ресурси для модифікації сигналів (Disruption Resources). Якщо різкий джаммінг одразу фіксується автопілотом як втрата зв'язку, то інтелектуальний GPS-спуфінг діє за принципом «прихованої атаки» (stealthy attack). Зловмисник впроваджує хибні координати не хаотично, а

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613

з урахуванням матриці стану системи та фізичних законів динаміки польоту БпЛА. Бортовий контролер (наприклад, Pixhawk) отримує топологічно коректні, але фальшиві дані, внаслідок чого коригує траєкторію апарата у хибному напрямку, залишаючись повністю «впевненим» у легітимності свого курсу аж до моменту фізичного знищення чи перехоплення борту;

2. Мережевий рівень у контексті компрометації каналів керування (Actuator & Channel Attacks). Аналізуючи мережеві вразливості, монографія фокусується на загрозах для каналів передачі команд від контролера до актюаторів (приводів двигунів та поверхонь керування). Відкритість і відсутність криптографічного підпису у базових профілях протоколу MAVLink забезпечує атакуючій стороні повні ресурси моніторингу (Disclosure Resources). Згідно з Тейшейрою, це дозволяє реалізувати атаку повтору (Replay Attack) з високим рівнем руйнівності: зловмисник записує пакети телеметрії стабільного польоту, а потім транслює їх в ефір для наземної станції (GCS), паралельно перехоплюючи реальне керування за допомогою ін'єкцій шкідливих команд. Оператор бачить на моніторі стабільні телеметричні показники нормального польоту, тоді як безпілотник виконує закладені зловмисником деструктивні дії;

3. Інформаційний рівень та деанонімізація через атаки на розкриття (Disclosure Attacks). Найбільш латентний аспект безпеки, описаний у монографії – це атаки, спрямовані на порушення конфіденційності стану КФС. Автори доводять, що навіть за умов використання стійкого шифрування вмісту пакетів (коли зловмисник не може прочитати сухі цифри координат), сам факт спостереження за динамікою системи, інтенсивністю випромінювання та частотою зміни мережевих патернів дозволяє сторонньому спостерігачу повністю реконструювати структуру системи. Для БпЛА це означає, що аналіз профілю зашифрованого трафіку дає змогу зловмиснику математично вирахувати поведінкові алгоритми дрона, деанонімізувати стратегію місії та локалізувати зони особливого інтересу оператора (наприклад, виявити точний час і місце виявлення тактичних цілей чи екологічних об'єктів), спираючись виключно на непрямі метрики радіообміну.

Таким чином, праця Тейшейри та ін. (2015) підтверджує, що безпека БпЛА є мультиплікативною величиною. Наявність архітектурного «вакууму» хоча б на одному рівні повністю нівелює захисні механізми інших рівнів, трансформуючи локальну цифрову вразливість у тотальний фізичний контроль над кіберфізичною системою.

Автори [2] починають із констатації факту: світ увійшов в епоху масової «дронізації». БпЛА стрімко інтегруються у цивільний сектор (логістика, сільське господарство, моніторинг). Однак Вессон і Гамфріс висувають тривожну тезу: цивільні безпілотники абсолютно сліпо довіряють навколишньому середовищу, оскільки їхня навігаційна архітектура базується на відкритих, незахищених технологіях, розроблених ще у 1970-х роках. Це створює глобальний кіберфізичний ризик.

У статті детально розбирається фізика і логіка роботи супутникової навігації. Автори пояснюють, що супутники GPS знаходяться на орбіті висотою близько 20 000 км. Коли їхній сигнал долітає до поверхні Землі, його потужність є надзвичайно малою — вона менша, ніж фоновий космічний шум. Бортовий приймач БпЛА має виокремити цей слабкий сигнал та розшифрувати його.

Головна проблема, яку підкреслюють Вессон і Гамфріс, полягає в архітектурному розділенні GPS:

- військовий сигнал (M-code / P(Y)-code): зашифрований, має криптографічну автентифікацію. Підробити його цивільними засобами неможливо;
- цивільний сигнал (C/A code, частота L1): повністю відкритий. Структура його кодів та повідомлень детально описана у загальнодоступних технічних специфікаціях. Жодних цифрових підписів чи шифрування у ньому немає.

Автори класифікують методи придушення та перехоплення БпЛА, що безпосередньо доводить вашу тезу про навігаційний вакуум безпеки:

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613

- брутальний джаммінг (Jamming): просте "заглушення" ефіру потужним радіошумом на частоті 1575,42 МГц. Дрон втрачає супутники. Зазвичай це призводить до спрацювання алгоритму Fail-Safe (дрон зависає або летить додому за інерціальною системою). Це створює незручності, але не дає зловмиснику контролю;

- інтелектуальний спуфінг (Spoofing): саме цьому методу присвячено ядро статті. Гамфріс та Вессон описують створений ними «імітатор сигналів» (spoofer). Процес перехоплення відбувається у три етапи:

1) синхронізація: спуфер генерує копію справжніх GPS-сигналів і транслює їх у бік БпЛА, ідеально вирівнюючи їх за часом та фазою з легітимними сигналами супутників;

2) захоплення контуру: спуфер плавно збільшує потужність свого сигналу (всього на кілька децибел). Бортовий приймач БпЛА через особливості своєї схемотехніки автоматично перемикається на сильніший сигнал, «не помічаючи» підміни;

3) маніпуляція: зловмисник починає витончено зсувати часові затримки у своїх сигналах. Дрон «думає», що він зміщується, наприклад, на північ, і його автопілот починає виконувати коригувальні дії, щоб повернутися на курс. Насправді ж БпЛА зміщується вбік у фізичному просторі. Таким чином, атакуючий отримує повний контроль над просторовим рухом КФС.

Вессон і Гамфріс попереджають, що наслідки спуфінгу цивільних БпЛА можуть бути катастрофічними: від викрадення цінних вантажів та дронів-носіїв до використання безпілотників як «керованих снарядів» для таранних атак на критичну інфраструктуру (аЕС, стадіони, урядові будівлі).

Головний висновок статті – цивільна інфраструктура БпЛА терміново потребує впровадження криптографічної автентифікації навігаційних повідомлень (як-от шифрування метаданих сигналів або використання багаточастотних приймачів) та комплексування GPS з іншими сенсорами (оптичний потік, радар).

Стаття «On the Requirements for Successful GPS Spoofing Attacks» (автори: Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, Srdjan Čapkun), [3] опублікована в межах престижної конференції з кібербезпеки ACM CCS, є однією з найбільш цитованих математичних та архітектурних праць у галузі дослідження GNSS-супутникових атак.

Якщо робота Гамфріса (2013) носила більш експериментальний та демонстраційний характер, то праця команди Тіппенгауера з ETH Zürich – це фундаментальне теоретичне дослідження. Автори вперше формалізували математичні та топологічні умови, за яких атака GPS-спуфінгу гарантовано залишиться непоміченою для сучасних кіберфізичних систем, зокрема БпЛА.

Головна цінність статті полягає в тому, що автори відійшли від спрощеного розуміння спуфінгу як «просто трансляції сильнішого сигналу». Вони висунули тезу: для успішної підміни координат КФС, атакуючий повинен подолати не лише радіочастотний приймач, а й просторово-геометричні обмеження системи.

Автори аналізують два типи приймачів:

1. Одиночний приймач (Single-Receiver): сценарій, коли БпЛА має одну GPS-антену (класичний випадок для більшості цивільних дронів);

2. Мережа приймачів або багатоантенні системи (Multi-Receiver): коли об'єкт (або група об'єктів) використовує кілька антен для захисту від перешкод та вимірювання кутів орієнтації (attitude детектування).

Ключові вимоги до успішного спуфінгу (Аналіз «вакууму безпеки»)

Автори математично довели, що успішність атаки критично залежить від кількості та взаємного розташування локальних антен БпЛА, а також від кількості джерел шкідливого сигналу (спуферів). Вони виділили такі фундаментальні обмеження та вимоги:

А. Синхронізація у часі та просторі. Щоб бортовий комп'ютер не зафіксував стрибок фази або аномальну затримку сигналу (що відразу викликало б підозру в системі Fail-Safe), зловмисник повинен знати точне тривимірне розташування антени БпЛА в реальному часі.

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613

Спуфер має випромінювати сигнал, який прибуває в точку розташування антени дрона з мікросекундною точністю, ідеально накладаючись на легітимні супутникові коди;

Б. Обмеження одного джерела (The Single-Spoofer Limitation). Тіппенгауер та співавтори виявили ключову геометричну ваду спуфінгу з однієї точки (одного передавача):

- якщо зловмисник використовує лише один сурогатний генератор сигналів (SDR) для імітації всього сузір'я супутників (наприклад, 4 або більше віртуальних супутників), то всі ці сигнали фізично надходять до БпЛА з одного і того самого напрямку (вектора);

- якщо у БпЛА встановлено лише одну антену (навігаційний рівень більшості комерційних КФС), дрон не здатний визначити кут приходу сигналу (AoA – Angle of Arrival). Для нього всі сигнали «просто падають з неба». Це і створює ідеальний «вакуум безпеки»;

В. Атаки на багатоантенні системи (Multi-Antenna Systems).

Найбільш важливий теоретичний висновок статті стосується складніших КФС. Якщо БпЛА обладнаний двома або більше антенами, він може вимірювати різницю фаз сигналів між ними. Якщо спуфер один, антени зафіксують, що сигнали від усіх «супутників» прийшли з однієї точки на землі, і система заблокує атаку. Проте автори довели, що цей захист можна обійти. Для успішної атаки на багатоантенну КФС зловмиснику потрібен синхронізований масив спуферів (Multiple Spoofers). Автори вивели математичні матриці та алгоритми, які розраховують, скільки саме наземних передавачів і в яких точках потрібно розмістити, щоб повністю обдурити навіть складну просторову систему захисту.

Праця Тіппенгауера є ідеальним математичним фундаментом для підтвердження тези про Навігаційний вакуум безпеки:

1. Обґрунтування системної слабкості: стаття доводить, що архітектурна вразливість цивільних БпЛА є подвійною: по-перше, інформаційне наповнення сигналу не має автентифікації (цифрового підпису), а по-друге, апаратна архітектура (Single-Receiver) не здатна аналізувати просторові характеристики радіохвилі;

2. Неможливість легкого виправлення: автори математично демонструють, що проста заміна програмного забезпечення (софтверний патч) на борту дрона не здатна вирішити проблему спуфінгу, оскільки уразливість лежить на стику фізики поширення хвиль та геометрії.

Вразливість безпілотних комплексів не є локальною IT-проблемою, а має багатошаровий, системно-структурний характер, який реалізується на трьох взаємопов'язаних рівнях:

1. Навігаційний рівень репрезентує найбільш критичну та апаратно обумовлену вразливість КФС. Відсутність криптографічного підпису в цивільних сигналах GNSS (частота L1) у поєднанні з простотовою архітектурою бортових приймачів з однією антеною (Single-Receiver) створює умови для реалізації прихованих атак типу False Data Injection (FDI). Як доведено у [3], через нездатність поодинокої антени визначати кут приходу радіохвилі (Angle of Arrival), бортові алгоритми детектування аномалій залишаються інваріантними до інтелектуального спуфінгу. Зловмисник, маніпулюючи часовими затримками з урахуванням фізичної моделі динаміки апарату, отримує повний і непомітний для автопілота контроль над просторовим рухом КФС, що веде до ризиків катастрофічного характеру [2];

2. Мережевий рівень, що базується на відкритих протоколах обміну телеметрією (зокрема MAVLink), виступає головним джерелом компрометації каналів керування актюаторами. Доступність повних ресурсів моніторингу (Disclosure Resources) дає змогу реалізувати високодеструктивні атаки повтору (Replay Attacks). За такої архітектурної прогалини фізичне відчуження безпілотника від легітимного оператора відбувається на тлі повної інформаційної асиметрії, коли наземна станція керування отримує сфальсифіковані пакети про «стабільний політ», у той час як борт виконує шкідливі команди ін'єкції;

3. Інформаційний рівень демонструє межі класичної криптографії (тріади CIA). Навіть за умов застосування стійких алгоритмів шифрування вмісту пакетів, КФС залишається

вразливою до атак на розкриття структури через сторонні канали. Аналіз непрямих метрик радіообміну – профілю зашифрованого трафіку, флуктуації бітрейту та часових патернів — дозволяє зловмиснику з високою точністю реконструювати матрицю стану системи, деанонімізувати тактичну стратегію місії та локалізувати географічні координати об’єктів особливого інтересу.

Підсумовуючи, можна стверджувати, що захищеність сучасних БпЛА підпорядковується закону мультиплікативності ризиків. Наявність архітектурного «вакууму безпеки» хоча б на одному з рівнів прямує загальну стійкість кіберфізичної системи до нуля. Усунення цих загроз неможливе за допомогою локальних програмних латок (софтверних патчів), оскільки проблема лежить на стику геометрії, фізики поширення радіохвиль та теорії автоматичного керування. Відтак, проектування майбутніх КФС потребує переходу до парадигми «Захист за замовчуванням» (Security by Design), що передбачає обов'язкове комплексування GNSS з альтернативними сенсорами (оптичний потік, інерціальні системи), впровадження криптографічної автентифікації повідомлень (на кшталт Galileo OSNMA) та обфускацію профілів мережевого трафіку.

Мета і задачі дослідження

Метою є розроблення та дослідження математичної моделі процесу передавання даних по відкритому каналу при застосуванні БПЛА в умовах ведення бойових дії.

Тому актуальною є задача використання моделі багаторівневого доступу для захисту даних при плануванні маршрутів БПЛА, що саме і пропонується в цієї роботи.

Математичне формулювання постановки проблеми

Багаторівневі системи доступу до інформаційних засобів забезпечують можливість реалізації оптимальних процедур здійснення доступу до даних та інших засобів інформаційної системи [4]. При побудові систем надання повноважень SNP , розв’язується задача надання повноважень не користувачеві, який отримав статус санкціонованого користувача SK системи захисту доступу до інформаційної системи DIS , а надається повноваження задачі, що представляється SK і потребує тих, чи інших даних, включаючи дані, що відносяться до категорії таємних.

Кількість рівнів, що реалізуються в системі SNP, може визначатися в залежності від вимог до захисту даних. По перше існують власні ідентифікаційні дані та інші дані, які потрібні для того, щоб користувач h який ініціює відповідний запит, мав його отримати. Відповідний користувач h повинен сформувати дані про задачу, яку йому необхідно розв’язати, використовуючи дані з системи DIS . Далі на основі цих даних аналізується рівень секретності даних які йому потрібні.

Якщо для розв’язку задачі не потребується таємних даних певного рівня, то він може отримати дані від системи DIS . При цьому, сама задача може розв’язуватися засобами, що не належать DIS . Такий рівень доступу позначається нульовим рівнем. Як що для розв’язку задачі потребується таємних даних певного рівня, то він не може отримати дані від системи DIS . В цьому випадку потрібно визначиться с кількістю рівнів доступу. Кількість етапів побудови багаторівневої системи доступу залежить від вибраної кількості рівнів, які будуть використовуватися в системі надання повноважень на використання таємних даних. Кількість визначених рівнів таємності даних та міри їх таємності встановлюється на основі аналізу предметної області до якої відносяться ці дані. В якості прикладу розглянемо побудову системи надання повноважень, що складається з трьох рівнів. В цьому випадку система DIS буде мати двох блокову структуру.

Перший рівень доступу – користувач h, що представляє задачу Za, яка потребує для розв’язку дані, що характеризуються таємністю, наприклад, першого рівня, реєструється в

системі доступу, а задача реєструється в системі наданням повноважень. Якщо система доступу автентифікувала користувача, то у випадку, коли задача, для розв’язку якої потрібні дані, що мають перший рівень таємності, повинна системі SNP надати певні дані про задачу

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613

Za. Користувач вводить в систему задачу Za може не знати, який рівень таємності мають дані, що потрібні для задачі. Тому інформація про задачу може вводитися в повному обсязі. Після надання задачі повноважень, фрагменти алгоритмів SNP , що визначають допустимі способи використання даних першого рівня , реалізують відповідні перетворення і тільки результат цих перетворень, який уже не має рівня таємності передається задачі і задача активізується з місця, для якого дані з SNP є вхідними.

В нашому випадку це можна інтерпретувати наступним чином: картографічна інформація маршруту доступна користувачеві а оперативна інформація з обмеженим доступом має бути оброблена з урахуванням властивостей БПЛА та спеціальної підпрограмою що належить системі DIS та на її основі побудовано маршрут руху БПЛА використання якого зніжує вірогідність розголошення інформації.

Побудова маршруту руху БПЛА з мінімізацією рівня розголошення інформації при нормальному розподіли критичних об’єктів. Розглянемо прикладну задачу побудові маршруту руху БПЛА з мінімізацією рівня розголошення інформації при нормальному розподіли критичних об’єктів, не розкриваючи повністю предметну область інтерпретації, а обмежившись лише критичними умовами її реалізації. Задано три суміжні області A, B, C.

Причому області A і C не мають спільних кордонів і шлях з A в C пролягає через B. У області B розташовано деякі критічні об’єкти, інформація про які є конфіденційною. Нам необхідно прокласти шлях суб’єкту з області A в область C. При цьому суб’єкт не повинен наближатися до об’єкту на відстань D для попередження розголошення конфіденційної інформації про об’єкт з області B. Класична модель доступу вирішує цю проблему за рахунок обходу області B межею.

Використовуючи дворівневу модель доступу до даних, можна побудувати критерій нерозголошення конфіденційної інформації. Наприклад, дозволити рух об’єкта в області B та аналізуючи траєкторію його руху, з метою не допущення його попадання в деяку область контакту об’єктів із області B. За рахунок цього буде відбуватися скорочення часу проходження маршруту БПЛА. Слід зауважити, що існує деяка мінімальна відстань, менше якої скоротити шлях неможливо. Проведемо серії експериментів: генеруючи в області B чотири об’єкти, випадковим чином дотримуючись рівномірного розподілу (завдання контролю об’єкта, забороненої території і території обмеженого доступу), для об’єкта з області A будується гарантований обхідний маршрут і будується маршрут проходження через область B з деякою точністю H. Критерієм нерозголошення встановимо не допущення наближення об’єкта з області A до об’єктів з області B на відстань D. Алгоритм пошуку шляху у таких умовах працює не отримуючи інформації про розташування об’єктів області B, що відповідає нашим вимогам з конфіденційності. Результатом експерименту буде розрахунок часу скорочення шляху у частках від максимального (обхідного) шляху.

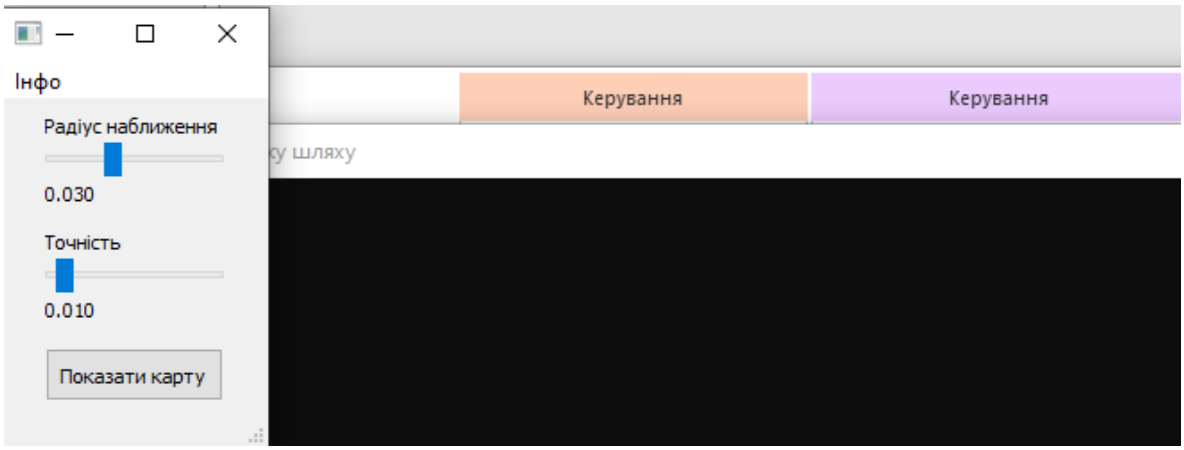

Рис. 1. Попереднє налаштування параметрів моделі.

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613

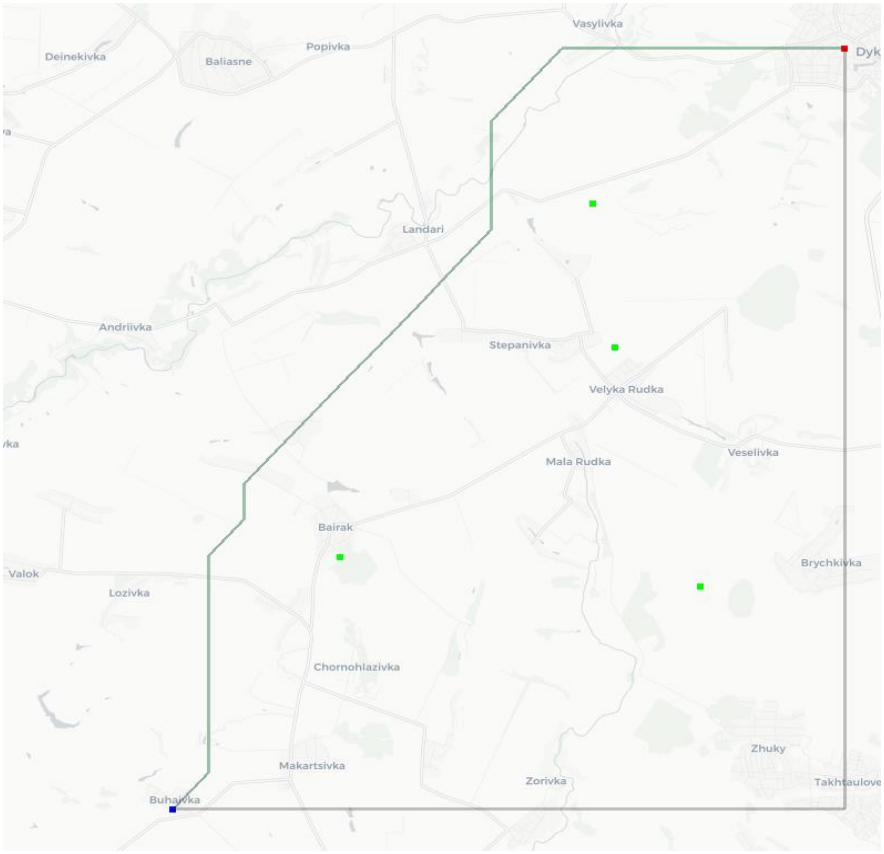

Рис. 2. Картографічне представлення результату (скорочення шляху менш 50%)

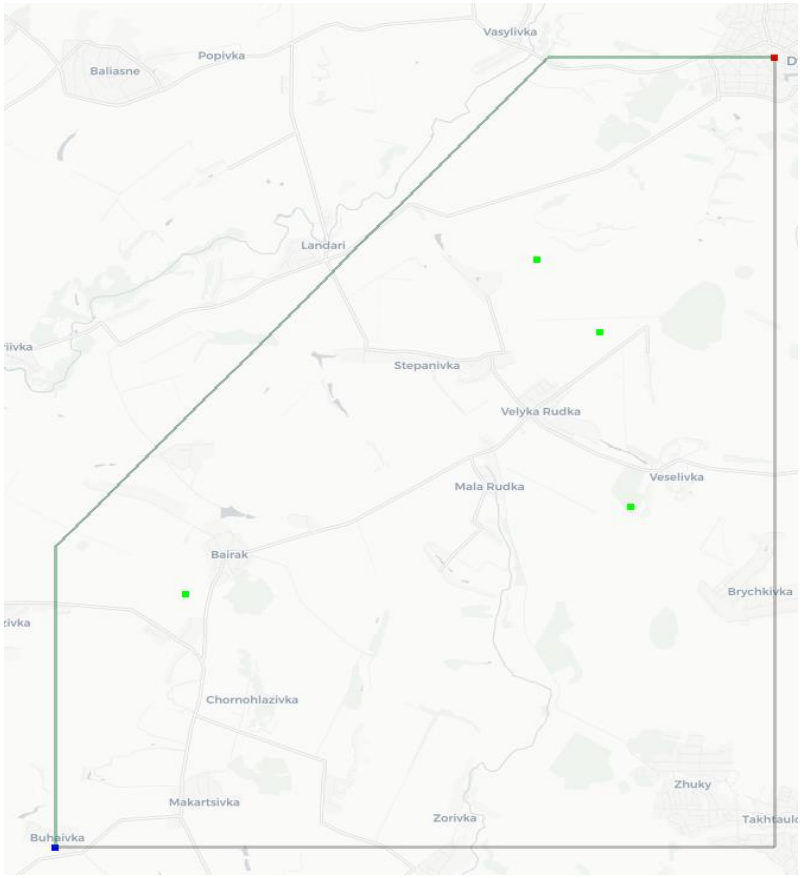

Рис. 3. Картографічне представлення результату (скорочення шляху біля 20%)

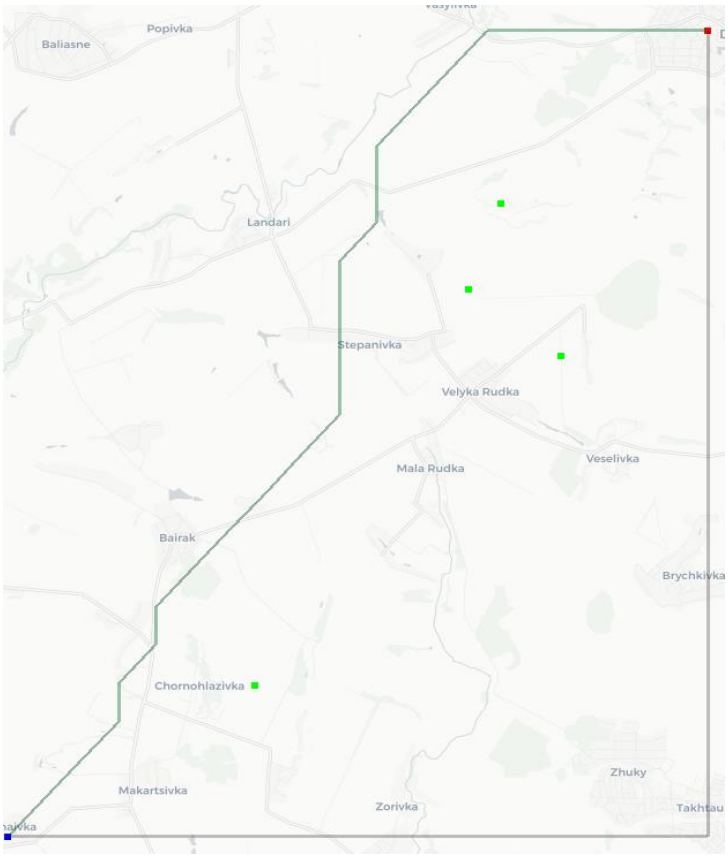

Рис. 4. Картографічне представлення результату (скорочення шляху біля 70%)

На рис. 2-4 приведено графічні результати проведених експериментів. Аналізуючи отримані криві видно, що результати досі різні та потребують набору більшого числа експериментів.

Проведене дослідження підтверджує ефективність застосування дворівневої моделі доступу при розв'язанні прикладних задач траєкторного планування БПЛА в умовах жорстких обмежень на розголошення конфіденційної інформації. Порівняльний аналіз класичного підходу (повний обхід критичної області B) та запропонованого методу дозволяє сформулювати наступні положення:

- практична цінність: запропонована методика дозволяє знайти раціональний компроміс між безпекою (мінімізація рівня розголошення) та ефективністю (мінімізація часу польоту);

- такий підхід є критично важливим для оперативного планування місій у зонах із великою кількістю об'єктів обмеженого доступу, де кожен відсоток збереженого часу може мати вирішальне значення для успіху операції;

- резюмуючи перехід від жорстких кордонів зон заборони до адаптивного аналізу траєкторії в межах дворівневої моделі є перспективним напрямком для інтелектуальних систем управління БПЛА, особливо в задачах радіоелектронної розвідки та моніторингу територій із критичною інфраструктурою.

Висновки

Безпека сучасних БпЛА не може розглядатися виключно через призму класичного захисту інформації (тріади CIA). Синергетична інтеграція цифрових алгоритмів із динамічними процесами у фізичному світі вимагає застосування теоретико-керівного підходу (Control-Theoretic Approach). Дослідження доводить обмеженість суто криптографічних засобів захисту. Навіть за умови використання стійкого шифрування вмісту пакетів (AES-256), інформаційний контур КФС залишається вразливим до атак по сторонніх каналах (Side-Channel Attacks). Аналіз профілю зашифрованого трафіку (частота, розмір пакетів, коливання

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613

бітрейту) дозволяє сторонньому спостерігачу з високою точністю реконструювати структуру місії, деанонімізувати тактичні алгоритми поведінки БпЛА та локалізувати координати об'єктів особливого інтересу оператора (тактичних цілей, екологічних зон). Запропонована модель багаторівневої системи доступу для визначення параметрів прикладних задач. Ця модель, використовуючи секретні дані з інформаційної системи незалежно від користувача, який подав відповідну задачу, дозволяє системі надання авторизації приймати рішення, уникаючи небезпек, які можуть виникнути під впливом дій користувача. Резюмуючи перехід від жорстких кордонів зон заборони до адаптивного аналізу траєкторії в межах дворівневої моделі є перспективним напрямком для інтелектуальних систем управління БПЛА.

Перелік посилань

1.Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for cyber-physical systems. Foundations and Trends in Systems and Control, 2(3-4), 243–410. https://doi.org/10.1561/2600000008.

2.. Wesson, T. Humphreys, Hacking drones. Sci. Am. 309(5), 54–59 (2013).

3.N. Tippenhauer, C. Pöpper, K. Rasmussen, On the Requirements for Successful GPS Spoofing Attacks (n.d.). Retrieved March 27, 2023, from https://www.cs.ox.ac.uk/files/6489/gps.pdf.

4.Sulima O. Model of multilevel access system // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 2, p. 122-129. DOI: 10.18372/2225-5036.23.11817.

Yuliia Tkach
Doctor of Pedagogical Sciences, Candidate of Technical Sciences, Professor, Head of the Department of Cybersecurity and Mathematical Modeling
National University "Chernihiv Polytechnic", Chernihiv, Ukraine
ORCID: 0000-0002-8565-0525
E-mail: tkachym79@gmail.com

Ihor Dyuba
Postgraduate student, Department of Cybersecurity and Mathematical Modeling
National University "Chernihiv Polytechnic", Chernihiv, Ukraine
ORCID: 0009-0007-3669-6424
E-mail: idyuba@gmail.com

MULTILAYER ANALYSIS OF VULNERABILITY OF CYBERPHYSICAL SYSTEMS USING THE EXAMPLE OF UNMANNED AIRCRAFT

The article examines the complex nature of vulnerabilities of modern unmanned aerial vehicles (UAVs) as a class of cyber-physical systems (CFS). The authors theoretically substantiated and detailed the concept of a "security vacuum" – the systemic insecurity of the drone architecture, which arises as a result of the rapid integration of computing algorithms and physical processes while ignoring the basic security criteria. Within the Control-Theoretic Approach, a layer-by-layer decomposition analysis of three critical levels of UAV architecture: navigation, network, and information were carried out. It is mathematically and empirically proven that the openness of civil GNSS signals in combination with the hardware architecture with one antenna (Single-Receiver) makes KFS defenseless against hidden attacks of false data injection (False Data Injection). Mechanisms of control channel compromise due to MAVLink protocol vulnerabilities using Replay Attacks were investigated. Special attention is paid to the information level, where the possibility of deanonymization of the strategy of using the system through the analysis of the encrypted traffic profile (Side-Channel Attacks) is demonstrated. Based on the analysis of the world's leading researches, the law of the multiplicity of risks of the CFS was formulated and systemic recommendations for the transition to the Security by Design paradigm were proposed.

Keywords: cyber-physical systems (CFS), unmanned aerial vehicles (UAVs), security vacuum, GPS spoofing, jamming, MAVLink protocol, replay attack, false data injection (FDI), third-party channel analysis, multiplicity of risks, Security by Design.

Надійшла до редакції (Received): 01.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Ткач Ю.М., Дюба І.М. Багатошаровий аналіз вразливостей кіберфізичних систем на прикладі безпілотних літальних апаратів. Сучасний захист інформації, 2(66), 152–161.
https://doi.org/10.31673/2409-7292.2026.028613