DOI: https://doi.org/10.25140/2411-5363-2026-2(44)-278-287
УДК 623.746:004.056:519.85

Ігор Миколайович Дюба[1], Юлія Миколаївна Ткач[2]

[1]аспірант
Національного університету «Чернігівська політехніка» (Чернігів, Україна)
E-mail: idyuba@gmail.com. **ORCID:** https://orcid.org/0009-0007-3669-6424

[2]доктор педагогічних наук, кандидат технічних наук,
професор, завідувач кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: tkachym79@gmail.com. **ORCID:** https://orcid.org/0000-0002-8565-0525

МОДЕЛЬ МАРШРУТИЗАЦІЇ БПЛА З ОБМЕЖЕННЯМ НА РОЗГОЛОШЕННЯ ІНФОРМАЦІЇ

У статті розглядається актуальна проблема забезпечення конфіденційності даних при експлуатації БПЛА в умовах бойових дій, де використання відкритих каналів передавання інформації створює високі ризики розголошення координат базування оператора, тактичної обстановки та пріоритетів розвідки. Автором запропоновано перехід від жорстких організаційних обмежень (повний обхід критичних зон) до інтелектуального планування маршруту на основі багаторівневої системи надання повноважень (SNP).

Математична модель SNP базується на відокремленні прав користувача (оператора) від повноважень конкретної задачі, що дозволяє системі автоматично обробляти таємну інформацію про розташування дружніх об'єктів без її безпосередньої візуалізації на терміналі оператора. В основу алгоритму траєкторного планування покладено принцип адаптивного маневрування: БПЛА прокладає маршрут через зону обмеженого доступу, підтримуючи критичну дистанцію D до об'єктів, координати яких оператору невідомі.

Експериментальна перевірка моделі продемонструвала суттєву перевагу над класичними підходами. Результати показали скорочення довжини маршруту та часу виконання місії на 17,78 % порівняно з методом повного обходу критичних областей. Такий підхід не лише забезпечує високу стійкість до витоку даних про розташування стратегічних об'єктів, але й оптимізує енерговитрати БПЛА, що є вирішальним фактором в умовах обмеженого ресурсу. Запропонована модель є перспективною для впровадження в сучасні інтелектуальні системи управління автономними апаратами та засобами радіоелектронної розвідки.

Ключові слова: *БПЛА; відкриті канали зв'язку; багаторівневий доступ; система надання повноважень (SNP); траєкторне планування; конфіденційність інформації; оптимізація маршруту.*

Рис.: 6. Бібл.: 6.

Актуальність теми дослідження. Завдяки стрімкому розвитку технологій безпілотних летальних апаратів (БПЛА) виникає багато аспектів їх застосування які раніше не досліджувалися людством. Крим прямих загроз пов'язаних з перехопленням або блокування виконання прямої задачі яку виконує БПЛА, існують непрямі загрози. До непрямих загроз можна віднести як фізичні загрози, так і інформаційні. Сфокусуємо нашу увагу саме на останніх. Задача маршрутизації БПЛА з обмеженням на розголошення інформації (UAV Routing with Information Disclosure Constraints) є частиною ширшої дисципліни — Cyber-Physical Security (CPS). Основним в цьому випадку є ризик компрометації місії через витік даних про місцезнаходження та наміри. Витік даних може бути більш значущим чім сама місія особливо при попаданні в зір маршрутної камери критичної інформації. Через названі фактори дослідження впливу маршруту БПЛА на розголошення критичної інформації у цілому на даний час є надзвичайно актуальним.

Постановка проблеми. Сучасне застосування БПЛА для моніторингу та розвідки територій із критичною інфраструктурою вимагає розв'язання гострої суперечності між операційною ефективністю та інформаційною безпекою.

Традиційні підходи до планування маршрутів у зонах із конфіденційними об'єктами базуються на принципі «зон заборони польотів» (No-Fly Zones), що передбачає повний обхід території обмеженого доступу. Такий метод гарантує нерозголошення інформації про розташування критичних об'єктів, проте призводить до значного збільшення довжини маршруту, витрат палива та часу виконання польотного завдання. В умовах обмеженого енергоресурсу БПЛА та необхідності оперативного реагування, класичні моделі обходу стають малоефективними.

Додатковою складністю є умова апріорної невизначеності: для підтримки високого рівня конфіденційності алгоритм керування БПЛА часто не повинен мати точних координат критичних об’єктів, щоб уникнути компрометації цих даних у разі перехоплення апарата.

Таким чином, виникає науково-практична задача, яка полягає у необхідності розробки методу траєкторного планування, що забезпечував би мінімізацію часу проходження маршруту через транзитні зони при суворому дотриманні критерію нерозголошення конфіденційної інформації (дотримання безпечної дистанції) в умовах відсутності повної інформації про точне розташування об’єктів захисту.

Ключові аспекти проблеми, які вирішує дослідження:

- геометричне обмеження: Шлях з точки А в точку С обов’язково пролягає через область В, де розташовані секретні об’єкти.
- інформаційне обмеження: Система планування працює «вслід», не отримуючи точних координат об’єктів в області В для запобігання витоку даних.

Оптимізаційне завдання: скорочення часу проходження маршруту порівняно з контурним обходом межі області В.

Комплексний реверс-інжиніринг пропрієтарного протоколу DJI DroneID, який був розроблений компанією для ідентифікації дронів правоохоронними органами [6] показав, що цей протокол транслюється у відкритому ефірі через систему радіозв'язку OcuSync і містить критично важливі дані без належного шифрування. Використовуючи недороге обладнання на базі програмно визначеного радіо (SDR), дослідники змогли перехопити та розшифрувати пакети, що містять унікальний серійний номер дрона, його точні координати, висоту, швидкість, а головне – координати точки зльоту (Home point), що фактично розкриває місцезнаходження пілота в реальному часі.

Результати роботи демонструють серйозну загрозу безпеці та приватності операторів, оскільки будь-яка третя сторона в радіусі дії сигналу (до декількох кілометрів) може здійснювати пасивне спостереження за польотами без ризику бути виявленою. Дослідники підкреслюють, що архітектура DroneID ігнорує базові принципи конфіденційності, перетворюючи дрон на «маячок», який видає свого власника. Ця праця стала фундаментальною для розуміння ризиків використання комерційних БПЛА в зонах конфліктів та на режимних об'єктах, де анонімність пілота є питанням фізичної безпеки.

У дослідженні [5] представлено результати експериментального аналізу вразливостей каналів зв'язку БПЛА, що використовують стандартні протоколи передачі даних на базі IEEE 802.11 (Wi-Fi). Автори зосереджуються на пасивному прослуховуванні (eavesdropping) мережевого трафіку між дроном та станцією керування. У процесі експериментів було доведено, що попри використання прикладних рівнів шифрування, структура передачі пакетів UDP/RTP дозволяє зловмиснику не лише виявити присутність відеотрансляції в ефірі, а і провести глибокий аналіз трафіку. Дослідники успішно реконструювали окремі аспекти відеопотоку, використовуючи відкриті інструменти для аналізу мережевих пакетів, що підтвердило критичну вразливість комерційних дронів (зокрема моделей Parrot та DJI) до перехоплення візуальної інформації.

Особлива увага в роботі приділяється аналізу метаданих та телеметрії, що передаються разом із відеосигналом. Автори демонструють, що перехоплювач може отримати доступ до критичних параметрів польоту (висота, швидкість, стан батареї та GPS-координати), які часто вбудовуються безпосередньо в транспортні протоколи або накладаються як On-Screen Display (OSD) дані. Наукова новизна праці полягає в систематизації методів класифікації трафіку в реальному часі, що дозволяє автоматизувати процес виявлення шпигунських БПЛА. Стаття завершується пропозиціями щодо посилення безпеки, зокрема через впровадження динамічного шифрування на рівні каналу передачі та використання методів обфускації трафіку для приховування характерних патернів відеопотоку.

У роботі [3] автори досліджують фундаментальну вразливість зашифрованих відеопотоків БПЛА, пов'язану з використанням змінного бітрейту (**VBR**). Дослідники розробили інноваційну атаку по сторонніх каналах (side-channel attack), яка дозволяє визначити, чи веде дрон спостереження за конкретним об'єктом, навіть якщо весь трафік захищений стійким шифруванням (наприклад, AES). Суть методу полягає у використанні фізичного стимулу – керованого мерехтіння світла (модуляції) на цілі або використання «розумної плівки» на вікні, що змінює свою прозорість. Оскільки відеокодеки (H.264/H.265) реагують на зміну пікселів у кадрі збільшенням обсягу даних, ці візуальні зміни відображаються на розмірі зашифрованих пакетів. Аналізуючи кореляцію між шаблоном мерехтіння та коливаннями бітрейту в ефірі, зловмисник може з високою точністю підтвердити факт стеження за об'єктом.

Наукова значущість дослідження полягає в руйнуванні міфу про те, що шифрування повністю забезпечує конфіденційність місії БПЛА. Автори продемонстрували успішну реалізацію атаки на популярних дронах (зокрема **DJI Mavic Air**) за допомогою звичайного ноутбука та антени, не маючи доступу до ключів дешифрування. Робота доводить, що інформація про зміст відео «протікає» через метадані трафіку, що дозволяє ідентифікувати ціль спостереження у реальному часі. Як засіб протидії, дослідники пропонують використання постійного бітрейту (**CBR**) або додавання «шумового» трафіку (traffic padding), проте зазначають, що це значно збільшує навантаження на канали зв'язку та акумулятор БПЛА, створюючи складний компроміс між безпекою та автономністю.

Наведені приклади потверджують актуальність поставленої наукової задачі.

Аналіз останніх досліджень та публікацій. Упродовж останнього десятиріччя спостерігається значна зацікавленість наукової спільноти у дослідженні та аналізу розголошення візуальної інформації, що передається з борта апарата на станцію керування. Зі зростанням інтенсивності використання цивільних та військових БПЛА, питання захищеності каналів зв'язку набуло критичного значення. Фундаментальні проблеми безпеки БПЛА були окреслені у доповіді Humphreys (2016) [1], де автор наголосив на вразливості навігаційних та комунікаційних систем перед недорогими засобами радіоелектронного впливу. Одним із найбільш критичних аспектів є несанкціоноване розголошення візуальної інформації, що передається з борта апарата на станцію керування.

Атаки через пряме перехоплення та вразливості протоколів. Найбільш вразливими є системи, що використовують аналогову передачу сигналу або незашифровані цифрові протоколи.

Аналогові системи: У дослідженні Birnbach (2017) [2] підкреслюється, що аналогові FPV-сигнали (5.8 GHz) за своєю природою є широкомовними та позбавленими будь-яких засобів аутентифікації. Це дозволяє здійснювати пасивне перехоплення відео на відстанях до декількох кілометрів без ризику виявлення зловмисника.

Wi-Fi протоколи: Дослідження Girma, A., Brown, K. (2024) [3] демонструють вразливість цивільних дронів, що використовують стандарти 802.11. Автори доводять можливість перехоплення відеопотоку (UDP/RTSP) через атаки типу «людина посередині» (MITM) та сніффінг пакетів через відсутність надійної криптографії в ранніх моделях комерційних БПЛА.

Атаки по сторонніх каналах (Side-Channel Attacks)

Сучасні цифрові системи (наприклад, DJI OcuSync) використовують шифрування AES, що робить пряме дешифрування відео майже неможливим. Проте наукові роботи останніх років доводять можливість компрометації даних навіть за умови шифрування.

Найбільш значущою у цьому напрямку є праця Nassi et al. (2019) [4] «Game of Drones». Автори розробили метод ідентифікації об'єкта, за яким стежить дрон, аналізу-

ючи лише коливання бітрейту зашифрованого трафіку. Використовуючи модульоване світлове випромінювання на цілі, дослідники змогли підтвердити факт спостереження за об'єктом, не розшифровуючи жодного кадру відео.

Розголошення метаданих та телеметрії. Часто критичною інформацією є не саме зображення, а дані про місцезнаходження дрона та його пілота.

Протокол DroneID: Робота Scharnowski (2022) [6] виявила критичні недоліки в системі ідентифікації DJI. Дослідники довели, що дрони транслюють у відкритому ефірі GPS-координати оператора та унікальні серійні номери. Це дозволяє третім особам не лише відстежувати маршрут місії, а й фізично локалізувати пілота.

Телеметрія OSD: Pecori (2020) [5] зазначають, що навіть при частковому перехопленні сигналу, накладені на відео дані (On-Screen Display) можуть розкрити параметри польоту, стан батареї та навігаційні точки, що є розголошенням конфіденційних оперативних даних.

Аналіз наукової літератури свідчить, що безпека відеоданих БПЛА еволюціонувала від захисту від простого прослуховування до необхідності протидії складним методам аналізу трафіку. Основними загрозами залишаються:

Витік метаданих через незахищені ідентифікаційні протоколи.

Можливість непрямого аналізу вмісту відео через коливання бітрейту.

Низька захищеність бюджетних FPV-систем.

Мета і задачі дослідження. Метою є розроблення та дослідження математичної моделі процесу передавання даних по відкритому каналу при застосуванні БПЛА в умовах ведення бойових дій. Передавання даних по відкритому каналу при застосуванні БПЛА в умовах ведення бойових дій породжує задачі:

- не розголошення координат базування дроновода;
- не розголошення поточної тактичної інформації про дружні підрозділи по маршруту польоту БПЛА;
- не розголошення інформації про фокус уваги дроновода.

Перша задача може бути вирішена організаційно зміною точки дислокації після запуску дрона. Третя задача не може бути вирішена в межах початкових умов і потребує переходу до захищеного каналу зв’язку, що не завжди можливо, або передачі спостереження іншому засобу розвідки. Друга задача може бути вирішена за рахунок попереднього планування, але це потребує додаткової інформації яка може бути недоступна із за недостатнього рівня доступу оператора. 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 [2]. 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 належать до категорії таємних.

Кількість рівнів, що реалізуються в системі SNP, може визначатися залежно 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 необхідні таємні дані певного рівня, то він не може отримати дані від системи DIS. У 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. Як приклад розглянемо побудову системи надання повноважень, що складається з трьох рівнів. У 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 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, й задача активізується з місця, для якого дані з SNP є вхідними.

Експериментальна частина. У 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 спеціальною 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 критичні 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'єкта на відстань D для запобігання розголошенню 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.

Для проведення експериментів було розроблено дві моделі: модель доступу та модель пошуку.

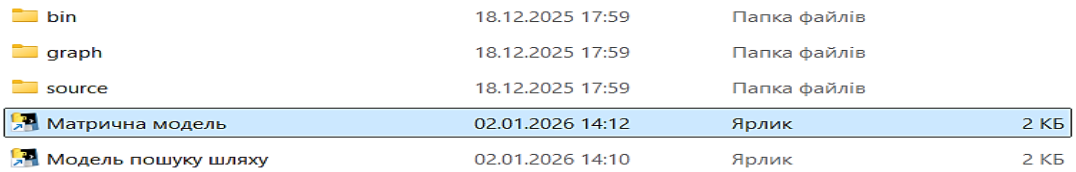
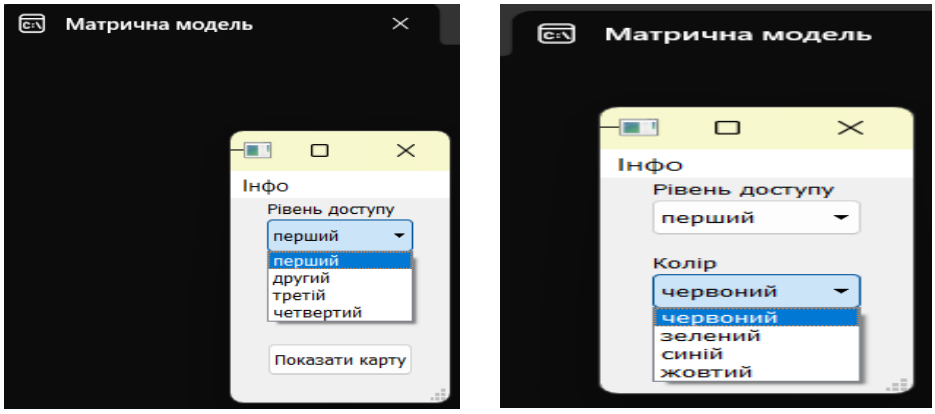


Рис. 1. Інформаційна структура програмного забезпечення

Матрична модель доступу та модель пошуку шляху за нашими умовами. На рис. 1, 2 наведена інформаційна структура програмного забезпечення для проведення експерименту. Директорія bin містить необхідні бібліотечні файли із загальними функціями, graph – графічними, sourse вихідні файли проєкту.



а *б*

Рис. 2. Матрична модель:
а – вибір рівня доступу; б – колір об’єкта

Матрична модель ілюструє наявність чотирьох рівнів доступу та можливості показу об’єктів відповідно до заданого рівня доступу рис. 3 – перший, рис. 4 – другий, рис. 5 – третій відповідно.

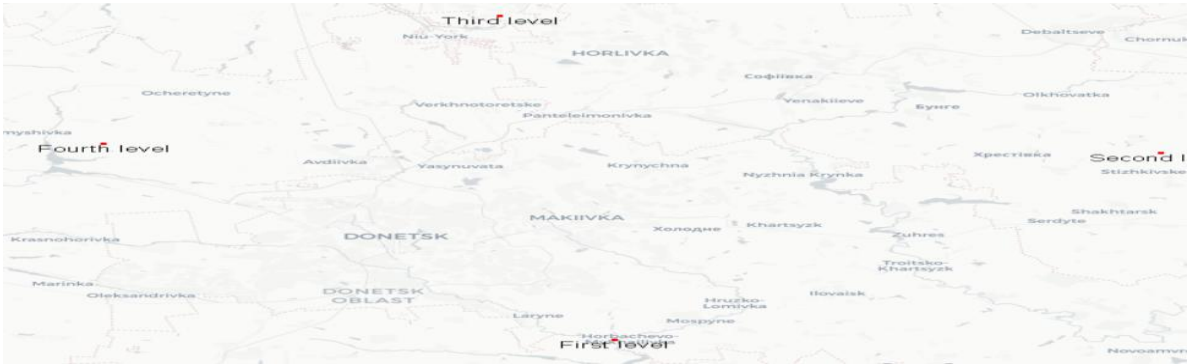


Рис. 3. Інформація про об’єкти на першому рівні доступу

Рис. 4. Інформація про об’єкти на другому рівні доступу

Рис. 5. Інформація про об’єкти на другому рівні доступу

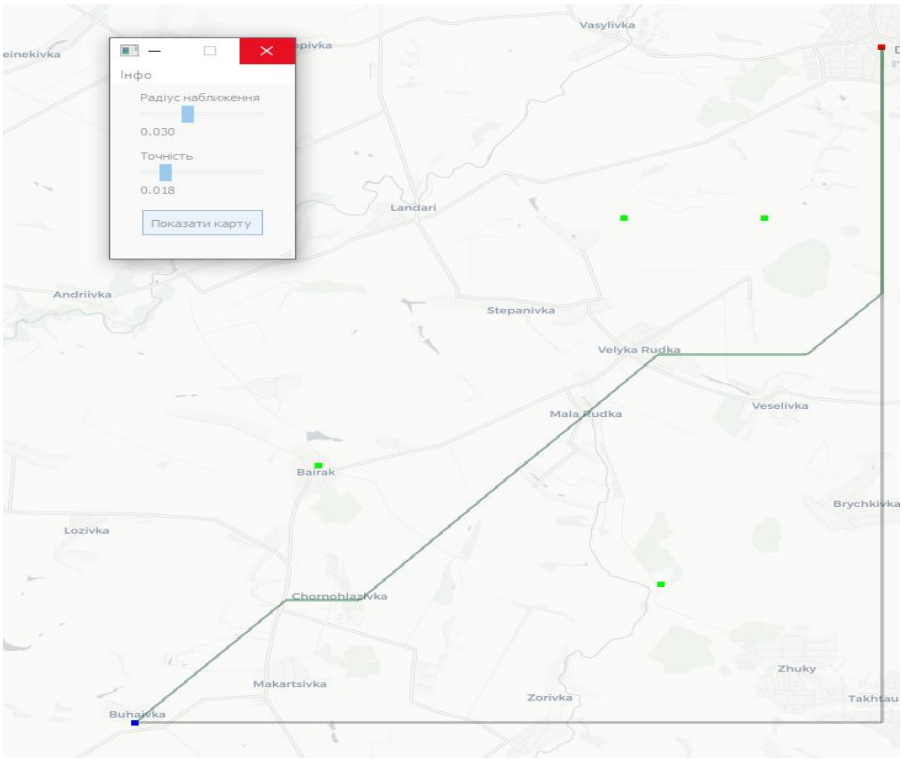


Рис. 6. Планування маршруту з дотриманням обмежень на розголошення критичної інформації

На рис. 6 приведено графічний результат проведення експерименту. Він ілюструє користь від застосування багаторівневої моделі доступу. Розглянемо це більш детально. За умовами БПЛА має рухатися від синього об'єкта до червоного, не наближаючись до критичних об'єктів (на мапі зелені) ближче заданого радіуса наближення. Підпрограма планування маршруту прокладає маршрут курсом на червоний об'єкт, але при вході в коло, у якому буде порушено заданий радіус наближення, змінює маршрут на неоптимальний, але який гарантує нерозголошення інформації про перший критичний об'єкт. Через деякий час, визначений у нашому випадку параметром точності, планувальник повертається на заданий курс. Достигаючи зоні обмежень третього об'єкта, курс знов змінюється на неоптимальний, цього разу повернутися на курс заважає четвертий об'єкт, але після проходження його курс знову змінюється. Враховуючи факт того, що противнику невідомо значення параметрів радіуса наближення та точності, які ми можемо змінювати, він не може розрахувати розташування критичних об'єктів. Маршрут не є оптимальним, але частка шляху становить 0,8822, тобто виграш від застосування дворівневої моделі при цьому експерименті становить 17,78 % від максимального часу проводки БПЛА. Що може бути критичним для успіху задачі, враховуючи енергетичні обмеження при застосуванні БПЛА.

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 такі положення.

Оптимізація часових ресурсів: Експериментально доведено, що дозвіл на проходження суб'єкта через область B із дотриманням безпекової дистанції D до критичних об'єктів забезпечує суттєве скорочення маршруту. Актуальним є проведення більшої кількості експериментів для більш точного визначення математичного очікування скорочення маршруту.

Забезпечення конфіденційності: Алгоритм пошуку шляху демонструє високу стійкість до витоку даних, оскільки він функціонує в умовах відсутності апріорної інформації про точне розташування об'єктів в області B. Це дозволяє підтримувати необхідний рівень секретності, не жертвуючи при цьому оперативністю виконання польотного завдання. Доцільним є побудова методики оцінки ризиків розголошення в кількісному вигляди.

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. 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.

Порівняльний аналіз класичного підходу (повний обхід критичної області B) та запропонованого методу дозволяє сформулювати такі положення.

Забезпечення конфіденційності. Алгоритм пошуку шляху демонструє високу стійкість до витоку даних, це дозволяє підтримувати необхідний рівень секретності, не жертвуючи при цьому оперативністю виконання польотного завдання.

Практична цінність. Запропонований підхід дозволяє знайти раціональний компроміс між безпекою (мінімізація рівня розголошення) та ефективністю (мінімізація часу польоту).

Резюмуючи, перехід від жорстких кордонів зон заборони до адаптивного аналізу траєкторії в межах дворівневої моделі є перспективним напрямком для інтелектуальних систем управління БПЛА. Модель може бути використана для передбачення того, як швидко інформація поширюватиметься в мережі.

Список використаних джерел

1. Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, *104*(6), 1258–1270. https://doi.org/10.1109/jproc.2016.2526658.

2. Birnbach, S., Baker, R., & Martinovic, I. (2017). *Privacy-preserving drone surveillance*. University of Oxford.

3. Girma, A., & Brown, K. (2024). Security analysis of drone communication methods. In S. Latifi (Ed.), *ITNG 2024: 21st International Conference on Information Technology-New Generations* (Vol. 1456, Advances in Intelligent Systems and Computing). Springer. https://doi.org/10.1007/978-3-031-56599-1_18.

4. Nassi, B., et al. (2019). Game of drones: Detecting captured images from an encrypted video stream. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1629–1642). https://arxiv.org/pdf/1801.03074.

5. Pecori, P., et al. (2020). Eavesdropping on UAV Video Links: An Experimental Study. *Sensors, 20(19),* 5502. https://doi.org/10.3390/s20195502.

6. Scharnowski, T., Bars, N., Schloegel, M., Gustafson, E., Muench, M., Vigna, G., Kruegel, C., Holz, T., & Abbasi, A. (2022). *Fuzzware: Using precise MMIO modeling for effective firmware fuzzing*. In *Proceedings of the USENIX Security Symposium*.

References

1. Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, *104*(6), 1258–1270. https://doi.org/10.1109/jproc.2016.2526658.

2. Birnbach, S., Baker, R., & Martinovic, I. (2017). *Privacy-preserving drone surveillance*. University of Oxford.

3. Girma, A., & Brown, K. (2024). Security analysis of drone communication methods. In S. Latifi (Ed.), *ITNG 2024: 21st International Conference on Information Technology-New Generations* (Vol. 1456, Advances in Intelligent Systems and Computing). Springer. https://doi.org/10.1007/978-3-031-56599-1_18.

4. Nassi, B., et al. (2019). Game of drones: Detecting captured images from an encrypted video stream. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1629–1642). https://arxiv.org/pdf/1801.03074.

5. Pecori, P., et al. (2020). Eavesdropping on UAV Video Links: An Experimental Study. *Sensors, 20(19),* 5502. https://doi.org/10.3390/s20195502.

6. Scharnowski, T., Bars, N., Schloegel, M., Gustafson, E., Muench, M., Vigna, G., Kruegel, C., Holz, T., & Abbasi, A. (2022). *Fuzzware: Using precise MMIO modeling for effective firmware fuzzing*. In *Proceedings of the USENIX Security Symposium*.

Дата першого надходження статті до видання: 02.03.2026
Дата прийняття статті до друку після рецензування: 12.03.2026

UDC 623.746:004.056:519.85

Ihor Diuba[1], Yuliia Tkach[2]

[1] PhD student of Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: idyuba@gmail.com **ORCHID:** https://orcid.org/0009-0007-3669-6424

[2] Doctor of Pedagogical Sciences, PhD of Technical Sciences, Professor, Head of the Department of Cybersecurity and Mathematical Simulation
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: tkachym79@gmail.com **ORCHID:** https://orcid.org/0000-0002-8565-0525

UAV ROUTING MODEL WITH INFORMATION DISCLOSURE CONSTRAINT

This paper addresses the critical issue of ensuring data confidentiality during UAV operations in combat environments, where the use of open communication channels poses high risks of disclosing operator base coordinates, tactical situations, and reconnaissance priorities. The author proposes a transition from rigid organizational constraints (total bypass of critical zones) to intelligent route planning based on a Multi-level System for Nominating Powers (SNP).

The mathematical SNP model is based on the decoupling of user (operator) rights from the privileges of a specific task. This allows the system to automatically process classified information regarding the location of friendly assets without direct visualization on the operator's terminal. The trajectory-planning algorithm is built on the principle of adaptive maneuvering: the UAV plans a route through a restricted area while maintaining a critical distance D from objects whose exact coordinates remain unknown to the operator.

Experimental validation of the model demonstrated significant advantages over classical approaches. The results showed a reduction in route length and mission execution time by 17.78% compared to the total bypass method of critical areas. This approach not only provides high resilience against data leakage regarding strategic asset locations but also optimizes the UAV's energy consumption—a decisive factor in resource-constrained environments. The proposed model is promising for integration into modern intelligent control systems for autonomous vehicles and electronic reconnaissance assets.

Keywords: *UAV, open communication channels, multi-level access, System for Nominating Powers (SNP), trajectory planning, information confidentiality, route optimization.*

Fig.: 6. References: 6.

Дюба І. М., Ткач Ю. М. Модель маршрутизації БПЛА з обмеженням на розголошення інформації. *Технічні науки та технології*, 2026. № 2(44). С. 278-287. DOI: https://doi.org/10.25140/2411-5363-2026-2(44)-278-287.