УДК 004.056.5:[004.62:623.746-519 DOI: 10.31673/2412-9070.2026.318111

Ю. М. ТКАЧ, д-р пед. наук, професор;
ORCID: 0000-0002-8565-0525
І. М. ДЮБА, аспірант,
ORCID: 0009-0007-3669-6424
Національний університет "Чернігівська політехніка", Чернігів

ВИКОРИСТАННЯ МОДЕЛІ БАГАТОРІВНЕВОГО ДОСТУПУ ДЛЯ ОБРОБКИ ДАНИХ ПРИ КЕРУВАННІ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

При швидкому розвитку засобів збору та генерації інформації необхідно враховувати як прогресивні аспекти так і нові небезпеки що генеруються за рахунок побічних властивостей технологічних процесів. В умовах прямої військової протидії це може привести до трагічних наслідків. Не враховуючі випадки, коли розголошення інформації відбувається за рахунок прямої недбалості є варіанти, коли це відбувається за рахунок цивільної спрямованості деяких технологій. Наприклад, перехоплення безпілотного літального апарату (БПЛА) з записаним на флешку маршрутом польоту призводить до розголошення координат точки старту та потенціально розкриває позицію дроновода. Метою дослідження є аналіз обмежень, які викають при застосуванні засобів з відкритим каналом обміну відеоінформацією та розробка методів, які можуть покращити безпеку обробки інформації в цих випадках. Це дослідження аналізує обмеження та пропонує багатогранний підхід до підвищення захисту даних у керуванні пристроями з відкритими інформаційними каналами. Крім того, у роботі пропонується застосування моделі системи багаторівневого доступу для планування місій БПЛА.

Ця модель використовує секретні дані з державної інформаційної системи для побудови маршрутів польоту, які за своєю суттю зменшують ризик розкриття тактичної інформації, надаючи дозвіл на основі рівня чутливості завдання, а не виключно прав доступу користувача. Моделювання демонструє здійсненність цього підходу для прийняття рішень щодо маршрутів, ефективно зменшуючи ймовірність розкриття обмежених оперативних деталей неуповноваженим користувачам.

Проведені експерименти показали, що використання запропонованого підходу дозволяє скоротити час проходження маршруту БПЛА порівняно з класичним методом повного обходу зони обмеженого доступу. За результатами моделювання при проведенні 10000 експериментів середній виграш за часом становив близько 19% від максимальної довжини обхідного маршруту. Отримані результати підтверджують ефективність і практичну застосовність моделей багаторівневого доступу для задач безпечного планування маршрутів БПЛА в умовах підвищених вимог до конфіденційності інформації.

Ключові слова: моделі системи багаторівневого доступу, безпілотні літальні апарати (БПЛА), інформаційна безпека, обробка сигналів.

Вступ

У контексті швидкого розвитку засобів збору та генерування інформації необхідно враховувати як прогресивні аспекти, так і нові небезпеки, що виникають внаслідок побічних ефектів технологічних процесів. У випадках, коли розкриття інформації відбувається через пряме недбальство, існують також випадки, коли це відбувається через цивільно-орієнтований характер деяких технологій. Наприклад, перехоплення дрону з маршрутом польоту, записаним на флеш-накопичувач, може призвести до розкриття координат точки запуску та потенційно вия-

вити місце розташування оператора дрону. Тому, доцільне використання методів обмеження доступу до інформації з використанням принципу мінімально необхідного рівня ознайомлення з інформацією. Мета цього дослідження полягає в аналізі обмежень, що виникають при використанні інструментів з відкритими каналами обміну відеоінформацією, та розробці методів, які можуть підвищити безпеку обробки інформації в таких випадках.

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.

Аналіз останніх досліджень і публікацій

Кількість наукових публікацій про застосування БПЛА (дронів) демонструє експоненційне зростання. Це зростання найбільш помітне після 2015 року, коли технологія стала широко поширеною та доступною.

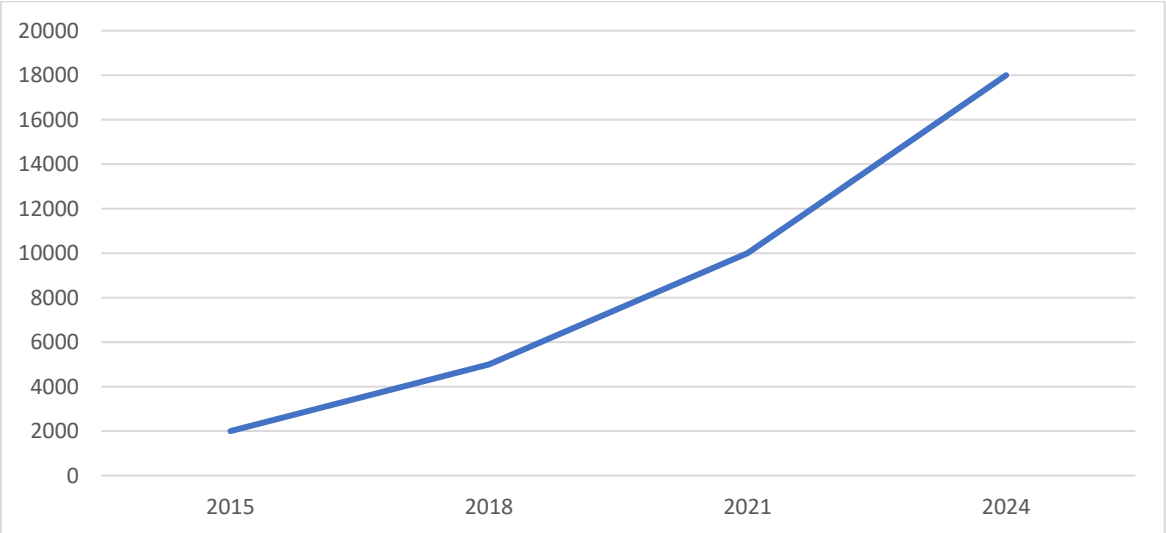

Рис. 1. Кількість наукових публікацій про застосування БПЛА (дронів)

В [1] розглянуто практичну задачу захисту даних. Сучасне збереження дикої природи все частіше покладається на дрони для неінвазивного моніторингу популяцій тварин та їхніх середовищ існування. Однак чутливі дані, зібрані дронами, включаючи зображення та відео, потребують надійного шифрування, щоб запобігти несанкціонованому доступу та експлуатації. Ці дані можуть містити інформацію про місцезнаходження рідкісних видів, їхню поведінку або вразливі місця, що може бути використано браконьєрами або іншими зловмисниками. Існуючі методи шифрування не завжди оптимально підходять для візуальних даних, особливо з урахуванням ресурсних обмежень на БПЛА. Нас це цікавить як підтвердження факту практичної вразливості обміну відео даними.

У [2] запропоновано модель багаторівневої системи доступу для визначення параметрів прикладних задач та методи їх оцінок, які за рахунок використання таємних даних з державної інформаційної системи не залежно від користувача, який представив відповідну задачу, дозволяють здійснювати прийняття рішень системою надання повноважень, уникаючи небезпек, які можуть з’явиться під впливом дій користувача.

У контексті забезпечення інформаційної безпеки критично важливих систем, традиційні моделі керування доступом на основі ролей (RBAC) поступово вичерпують свій потенціал через надмірну статичність. У дослідженні Y. Zhou, L. Ma та M. Wen [4] запропоновано модифіковану модель Task-Constrained RBAC, яка впроваджує обмеження на рівні конкретних завдань. Автори акцентують увагу на проблемі надмірності привілеїв, що є критичним фактором ризику при реалізації внутрішніх загроз. Впровадження механізму аналізу надмірності дозволяє реалізувати принцип мінімальних привілеїв шляхом динамічного надання прав лише на час виконання визначеної технологічної операції. Це забезпечує вищу гнучкість системи порівняно з класичними моделями, де права закріплені за роллю на постійній основі.

Розвиток безпілотних технологій зумовлює появу нових стратегій ведення міждоменних операцій. M. Ren, B. Wang та J. Liu [5] розглядають концепцію застосування іноземних гетерогенних безпілотних апаратів у межах спільної радіоелектронної боротьби. Особливістю даного підходу є використання різнорідних за своїми характеристиками БПЛА, що інтегровані в єдину інформаційну мережу. Дослідження підкреслює, що ефективність таких систем залежить від здатності до крос-доменної взаємодії (повітря-земля-море), що дозволяє створювати складні адаптивні структури для подавлення систем протиповітряної оборони та управління військами противника.

Технічна реалізація групового застосування безпілотних засобів потребує детального математичного моделювання фізичних процесів. У праці Yang Zhang та співавт. [6] представлено результати моделювання та симуляції електромагнітних операцій рою БПЛА. Авторами доведено, що розподілена конфігурація випромінювачів у межах рою дозволяє досягти ефекту просторової селекції завад. Використання алгоритмів координації дозволяє малим апаратам з низькою потужністю випромінювання формувати сумарний електромагнітний сигнал високої інтенсивності в заданій точці простору. Симуляційні експерименти підтверджують, що така архітектура є більш стійкою до засобів протидії РЕБ противника порівняно з поодинокими потужними джерелами випромінювання.

Дослідження M. Ren, B. Wang та J. Liu [7] присвячене аналізу перспективних концепцій застосування різнорідних (гетерогенних) безпілотних систем у межах сучасних мережецентричних воєн. Автори фокусуються на досвіді провідних іноземних держав щодо впровадження «міждоменних» операцій.

Стратегічний контекст: Робота обґрунтовує необхідність переходу від однорідних груп БПЛА до складних систем, що включають апарати з різними технічними характеристиками та функціональним призначенням. Це дозволяє одночасно вирішувати завдання розвідки, ретрансляції та активного радіоелектронного подавлення.

Крос-доменна взаємодія: Ключовим елементом концепції є здатність БПЛА взаємодіяти не лише всередині своєї групи, а й з іншими платформами в різних доменах (повітряному, наземному, морському). Такий підхід забезпечує створення адаптивного «завадового середовища», яке здатне протидіяти багатошаровим системам ППО.

Операційні переваги: У статті підкреслюється, що гетерогенність систем значно ускладнює роботу алгоритмів розпізнавання цілей противником, оскільки різноманітність сигнатур та траєкторій руху засобів РЕБ створює ефект невизначеності.

У праці Yang Zhang та співавторів [8] розглядається технічна реалізація групового застосування БПЛА через призму математичного моделювання електромагнітної взаємодії. Дослідження спрямоване на визначення оптимальних параметрів функціонування рою як цілісної випромінювальної системи.

Моделювання електромагнітного впливу: Автори пропонують математичну модель, яка дозволяє розрахувати сумарний завадовий ефект, що створюється розподіленою групою малопотужних передавачів. Основна увага приділяється принципу когерентного та некогерентного додавання сигналів у заданій точці простору.

Симуляція сценаріїв: За допомогою серії комп'ютерних симуляцій було проаналізовано залежність ефективності придушення радарів противника від геометрії розташування дронів у рої. Результати підтверджують, що використання алгоритмів самоорганізації рою дозволяє досягати високої щільності завад навіть при значному віддаленні від об'єкта впливу.

Оцінка живучості: Важливим аспектом роботи є доведення того, що розподілена природа рою забезпечує високу стійкість до фізичного знищення окремих одиниць. Модель показує, що функціональність системи зберігається за умови дотримання мінімально необхідної кількості активних вузлів випромінювання.

Аналіз представлених робіт свідчить про наявність чіткої тенденції до інтелектуалізації та децентралізації систем управління. Якщо в сегменті кібербезпеки це проявляється у переході до атомарного керування доступом через завдання [4], то у військовій сфері — у переході до кооперативних міждоменних операцій гетерогенних роїв [5], [6]. Концептуальні розробки [7] визначають стратегію використання гетерогенних структур у різних середовищах, математичні моделі [8] надають необхідний інструментарій для точного розрахунку фізичних параметрів електромагнітного впливу таких груп.

Подальші дослідження в цих напрямках є критично важливими для створення комплексних систем захисту та ефективних засобів радіоелектронного впливу.

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. Передавання даних по відкритому каналу при застосуванні БПЛА в умовах ведення бойових дії породжує задачі:

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

Перша задача може бути вирішена організаційно зміною точки дислокації після запуску дрону. Третя задача не може бути вирішена в рамках начальних умов та потребує переходу до захищеного каналу зв'язку, що не завжди можливо або передавання 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 у даній 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 або 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.

Якщо для розв'язку задачі необхідні таємні дані певного рівня, то він не може отримати дані від системи DIS. У цьому випадку потрібно визначиться з 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 встановлюються 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 двоблокову структуру.

Перший рівень доступу - Користувач h, що представляє задачу Za, яка потребує для роз-в'язку дані, що характеризуються таємністю, наприклад, першого рівня, реєструється в сис-темі доступу, а задача реєструється в системі наданням повноважень. Якщо система доступу аутентифікувала 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. Ко-ристувач вводить в систему задачу Za й може не знати, який рівень таємності мають дані, що потрібні для задачі. Тому, інформація про задачу може вводитися в повному обсязі. Після на-дання задачі повноважень, фрагменти алгоритмів SNP, що визначають допустимі способи ви-користання даних першого рівня, реалізують відповідні перетворення і тільки результат цих перетворень, який уже не має рівнів таємності, передається і задача активізується з місця, для якого дані з SNP є вхідними.

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 спеціальної підпрограми, 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 розподілу критичних об'єктів. Розглянемо прикладну задачу побудови маршруту руху БПЛА з мінімізацією рівня розголошення інформації при нормальному розподілу 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'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 А будується гарантований обхідний маршрут і будується маршрут проходження через область В з деякою точністю Н. Критерієм нерозголошення встановимо не допущення наближення об'єкта з області А до об'єктів з області В на відстань D. Алгоритм пошуку шляху у таких умовах працює, не отримуючи інформації про розташування об'єктів області В, що відповідає нашим вимогам з конфіденційності. Результатом експерименту буде розрахунок часу скорочення шляху у частках від максимального (обхідного) шляху.

На рис. 2 приведено графічні результати проведених експериментів при зростанні їх числа. Аналізуючи отриману поверхню видно, що із збільшенням кількості проведених експериментів форма кривої наближається до класичної для нормального розподілу. Математичне сподівання частки шляху становить 0,8113, тобто середній виграш від застосування дворівневої моделі при 10000 експериментах становить майже 19% від максимального часу проводки БПЛА.

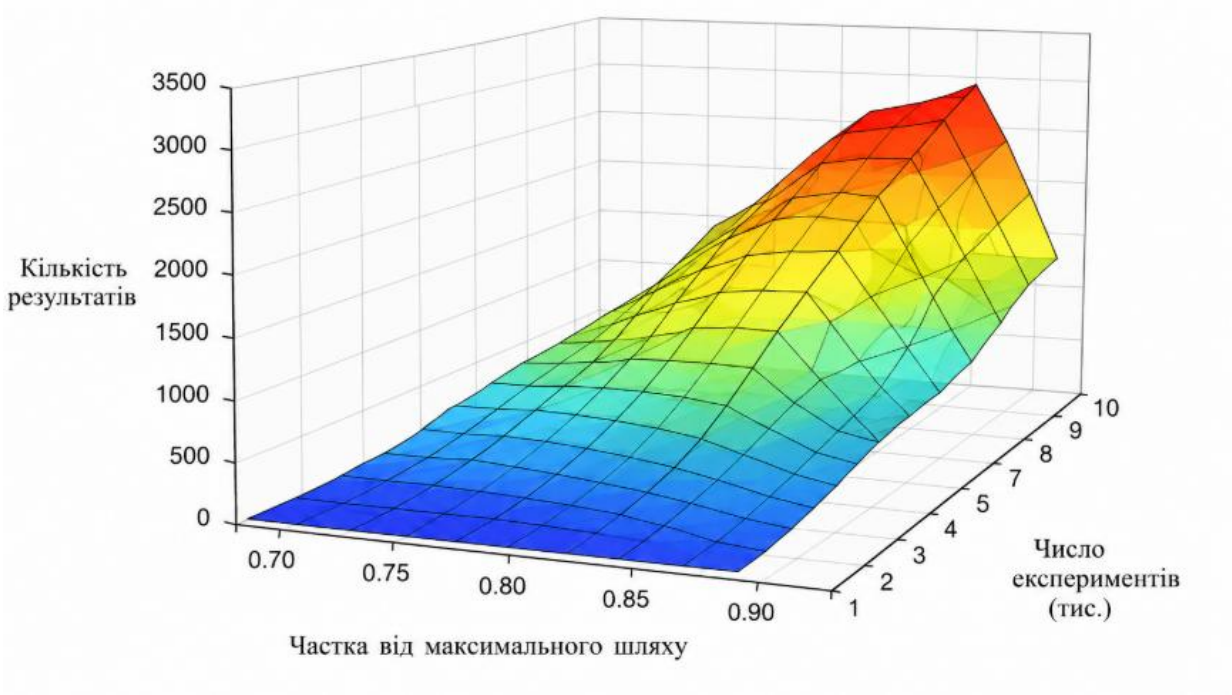

Рис. 2. Скорочення часу проходження маршруту при рівномірному розподілі

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 В) та запропонованого методу дозволяє сформулювати наступні положення:

Оптимізація часових ресурсів: Експериментально доведено, що дозвіл на проходження суб'єкта через область В із дотриманням безпекової дистанції D до критичних об'єктів забезпечує суттєве скорочення маршруту. При проведенні серії з 10,000 експериментів математичне сподівання частки шляху склало 0.8113, що еквівалентно середньому виграшу в часі на рівні 19% відносно максимальної траєкторії обходу.

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 В. Це дозволяє підтримувати необхідний рівень секретності, не жертвуючи при цьому оперативністю виконання польотного завдання.

Закономірність розподілу: Статистичний аналіз отриманих результатів (зокрема форма кривої на рис. 2) демонструє конвергенцію до класичного нормального розподілу при збільшенні кількості ітерацій. Це свідчить про стабільність запропонованої моделі та її передбачувані-

сть у реальних умовах експлуатації, де розташування критичних об'єктів може мати випадковий характер.

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.

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 наступні 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. При проведенні серії з 10,000 експериментів математичне сподівання частки шляху склало 0.8113, що еквівалентно середньому виграшу в часі на рівні 19% відносно максимальної траєкторії обходу.

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.

Закономірність розподілу: Статистичний аналіз отриманих результатів (зокрема форма кривої на рис. 2) демонструє конвергенцію до класичного нормального розподілу при збільшенні кількості ітерацій. Це свідчить про стабільність запропонованої моделі та її передбачуваність у реальних умовах експлуатації, де розташування критичних об'єктів може мати випадковий характер.

Практична цінність: Запропонована методика дозволяє знайти раціональний компроміс між безпекою (мінімізація рівня розголошення) та ефективністю (мінімізація часу польоту).

Перехід від жорстких кордонів зон заборони до адаптивного аналізу траєкторії в межах дворівневої моделі є перспективним напрямком для інтелектуальних систем управління БПЛА.

Внесок авторів

Юлія ТКАЧ – аналіз сучасних підходів до забезпечення інформаційної безпеки при керуванні безпілотними літальними апаратами, дослідження обмежень застосування засобів з відкритими каналами передавання інформації; Ігор ДЮБА – формування концепції та методології дослідження, постановка наукової задачі, аналіз та інтерпретація результатів моделювання, перевірка коректності запропонованих підходів.

Декларація про штучний інтелект

Автори не використовували штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтер-

претацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Akram Belazi, Héctor Migallón "Drone-Captured Wildlife Data Encryption: A Hybrid 1D–2D Memory Cellular Automata Scheme with Chaotic Mapping and SHA-256".,"Mathematics", MDPI, Vol. 12(22), 2024.

2. 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

3. Chen, C.; Wang, Z.; Gong, Z.; Cai, P.; Zhang, C.; Li, Y. Autonomous Navigation and Obstacle Avoidance for Small VTOL UAV in Unknown Environments. Symmetry 2022, 14, 2608. https://doi.org/10.3390/sym14122608

4. M. Bondar, "Advancing Ukrainian Unmanned Systems with Autonomy and AI," Center for Strategic and International Studies, Mar. 06, 2025. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250306_Bondar_Autonomy_AI.pdf?VersionId=E2h8uqROea77udoc_og82HWsrfgfJRTZ. [Accessed: Apr. 30, 2025].

5. Constantin-Adrian CIOLPONEA, THE INTEGRATION OF UNMANNED AIRCRAFT SYSTEM (UAS) IN CURRENT COMBAT OPERATIONS, Land Forces Academy Review Vol. XXVII, No 4(108), 2022 [Online]. Available: [https://www.researchgate.net/publication/367055350_The_Integration_of _Unmanned_Aircraft_System_UAS _in_Current_Combat_Operations]. [Accessed: Apr. 30, 2025].

6. Y. Zhou, L. Ma, M. Wen, «Task-Constrained RBAC Model and Its Privilege Redundancy Analysis», 2nd International Conference on Information Science and Control Engineering, pp. 489–492, 2015.

7. Ren, M., Wang, B., Liu, J. (2024). Conception of Foreign Heterogeneous Electronic Warfare UAV Cross Domain Cooperative Operations. In: Qu, Y., Gu, M., Niu, Y., Fu, W. (eds) Proceedings of 3rd 2023 International Conference on Autonomous Unmanned Systems (3rd ICAUS 2023). ICAUS 2023. Lecture Notes in Electrical Engineering, vol 1171. Springer, Singapore. https://doi.org/10.1007/978-981-97-1083-6_2

8. Yang ZHANG, Guangya SI, Yanzheng WANG, Wenbin HAN. (2023). Modeling and simulation of UAVs swarm electromagnetic operation. Systems Engineering and Electronics ›› 2023, Vol. 45 ›› Issue (7): 2121-2130. doi: 10.12305/j.issn.1001-506X.2023.07.23

Yu. Tkach, I. Diuba

USE OF A MULTILEVEL ACCESS MODEL FOR DATA PROCESSING IN UNMANNED AERIAL VEHICLE CONTROL

With the rapid development of information collection and generation technologies, it is necessary to consider not only their progressive advantages but also new risks arising from the side effects of technological processes. In conditions of direct military confrontation, these risks may lead to severe consequences. Beyond cases of information disclosure caused by direct negligence, there are scenarios where such disclosure occurs due to the civilian-oriented nature of certain technologies. For example, interception of an unmanned aerial vehicle (UAV) carrying a flight route stored on removable media may result in the exposure of launch coordinates and potentially reveal the operator's position. The aim of this study is to analyze the constraints that arise when using systems with open video transmission channels and to develop methods for improving the security of data processing in such environments. The research examines these limitations and proposes a comprehensive approach to enhancing data protection in the control of devices operating over open information channels. In addition, the paper proposes the application of a multilevel access control model for UAV mission planning.

This model utilizes classified data from a state information system to generate flight routes that inherently reduce the risk of tactical information disclosure. It grants authorization based on the sen-

sitivity level of the task rather than solely on user access rights. Modeling results demonstrate the feasibility of this approach for route decision-making, effectively reducing the likelihood of exposing restricted operational details to unauthorized users.

The conducted experiments demonstrated that the proposed approach makes it possible to reduce UAV route traversal time compared to the classical method of completely bypassing restricted-access areas. According to simulation results obtained from 10,000 experiments, the average time gain was approximately 19% relative to the maximum bypass route length. The obtained results confirm the effectiveness and practical applicability of multilevel access models for secure UAV route planning tasks under conditions of increased information confidentiality requirements.

Keywords: multilevel access control models, unmanned aerial vehicles (UAVs), information security, signal processing.

Надійшла до редакції: 16.02.2026
Прийнята до друку: 06.04.2026
Опубліковано: 29.06.2026