**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ**
**ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО**
**ДЕРЖАВНИЙ УНІВЕРСИТЕТ "КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"**
**ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ**


# ЗБІРНИК
# ТЕЗ ДОПОВІДЕЙ

**XVI МІЖНАРОДНОЇ**
**НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

# КОМП'ЮТЕРНІ СИСТЕМИ
# ТА МЕРЕЖНІ ТЕХНОЛОГІЇ

27-28 березня 2025 року

**Київ 2025**

УДК 004.7(043.2)

Збірник тез доповідей XVI Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2025), м. Київ, 27–28 березня 2025 р., ДУ «Київський авіаційний інститут». – К.: ДУ «КАІ», 2025. – 85 с.

В процесі доповідей здійснено обмін новими ідеями, отриманими теоретичними і практичними результатами наукових досліджень в області інформаційних технологій. Обговорено сучасний стан ІТ галузі в Україні та світі, перспективні напрямки розвитку інформаційних технологій. Для науковців, викладачів, аспірантів, студентів, співробітників наукових установ та ІТ компаній. Матеріали подані мовою оригіналу (українська, англійська). Редакційна колегія зберегла авторський текст без істотних змін, звертаючись до коректування в окремих випадках.

Відповідальність за достовірність матеріалів несуть автори.



*Рекомендовано до видання вченою радою Факультету комп'ютерних наук та технологійї Державного університету «Київський авіаційний інститут» (протокол № 5 від 16 квітня 2025 р.).*

*Редакція не обов'язково поділяє думку автора. Відповідальність за достовірність фактів, цитат власних імен та іншої інформації несуть автори.*

# ЗМІСТ

УДК 004.7

**В.В. Алькема,**
**А.Л. Столяр**
*Державний Університет «Київський авіаційний інститут», Київ*

# ПРОТОКОЛИ AODV ТА E-AODV З ІНТЕГРАЦІЄЮ МЕХАНІЗМІВ ВИЯВЛЕННЯ АТАК У MANET-МЕРЕЖАХ

У світі стрімкого розвитку бездротових комунікацій мобільні адгок-мережі (*Mobile Ad-hoc Networks, MANET*) займають важливе місце, особливо у сферах, де інфраструктурне підключення є недоступним або нестабільним – зокрема у військових операціях, аварійно-рятувальних службах, тактичних мережах та розподілених *IoT*-системах. *MANET* характеризуються високою динамічністю, самоорганізацією та відсутністю фіксованої інфраструктури. Ці особливості, хоч і забезпечують гнучкість, одночасно роблять такі мережі особливо вразливими до різноманітних атак, зокрема атак на рівні маршрутизації.

Один із базових і найбільш вивчених протоколів маршрутизації в *MANET* є *AODV* (*Ad hoc On-Demand Distance Vector*), який уже тривалий час вважається стандартним підходом до динамічної маршрутизації в безінфраструктурних мережах [1-4]. Цей протокол працює за принципом реактивної маршрутизації, тобто формує маршрути лише у відповідь на необхідність передачі даних між джерелом і призначенням. Завдяки цьому *AODV* уникає постійної передачі маршрутних таблиць, що дозволяє значно зменшити накладні витрати на мережевий трафік, а також ефективно адаптуватися до частих змін топології, характерних для *MANET*. Його переваги виявляються особливо корисними у середовищах з високою мобільністю вузлів, де звичайні статичні протоколи зазнають серйозних втрат продуктивності.

Проте, попри свою ефективність з точки зору маршрутизації, *AODV* має суттєвий недолік – відсутність вбудованих механізмів безпеки. Протокол був спроектований з орієнтацією на продуктивність, але не передбачав захист від зловмисних дій з боку учасників мережі. Це робить його вразливим до широкого спектру атак, які можуть бути реалізовані з мінімальними зусиллями. Наприклад, у випадку атаки типу *black hole* зловмисний вузол фальшиво повідомляє про наявність найкоротшого маршруту до пункту призначення, перехоплює трафік і може його або знищити,

або проаналізувати. Атака *rushing* дозволяє зловмиснику домінувати в процесі побудови маршруту шляхом швидкої відповіді на запити, тоді як *wormhole* використовує тунель між двома змовниками для маніпуляції топологією мережі. Крім того, атаки типу *Sybil*, коли один вузол видає себе за кілька інших, і *hello flooding*, при якій надсилається велика кількість привітальних повідомлень для перенавантаження мережі, можуть призвести до повного порушення стабільності маршрутизації.

Всі ці атаки мають спільну рису: зловмисний вузол видає себе за легітимного учасника, інтегрується в маршрутизаційний процес і починає навмисно змінювати або блокувати передавання даних. Внаслідок цього порушується не лише доступність послуг у мережі, але й її цілісність, конфіденційність та стабільність функціонування. В умовах, де надійність зв'язку критично важлива (військові застосування, рятувальні операції, передавання даних сенсорами), такі вразливості є неприйнятними. Тому *AODV*, незважаючи на його базову ефективність, вимагає вдосконалення, особливо в контексті інтеграції захисних механізмів, які б дозволяли йому протистояти сучасним кіберзагрозам.

У відповідь на ці проблеми були розроблені вдосконалені версії *AODV*, зокрема *Enhanced AODV* (*E-AODV*). Цей протокол додає шари захисту до базового механізму маршрутизації. Однією з ключових особливостей *E-AODV* є інтеграція механізмів виявлення атак. Це можуть бути модулі аналізу поведінки вузлів, системи довіри, фільтрація аномальних маршрутних запитів, перевірка відповідності топології, інтеграція простих або складних *IDS* (*Intrusion Detection Systems*). У деяких реалізаціях використовуються навіть елементи машинного навчання або евристичні алгоритми для оцінки підозрілої активності.

Порівняння *AODV* та *E-AODV*, проведене через симуляційні моделі (*NS*2, *NS*3, *OMNeT++*), показує чіткі переваги удосконаленого протоколу в умовах атак. *AODV* демонструє значне зниження продуктивності у присутності зловмисників: кількість успішно доставлених пакетів падає, збільшується затримка, знижується пропускна здатність. Натомість *E-AODV* завдяки виявленню та блокуванню зловмисних вузлів здатен підтримувати стабільні маршрути, мінімізувати втрати і запобігати атакам ще на етапі формування маршрутів. Деякі дослідження вказують, що рівень доставки пакетів в *E-AODV* може бути на 25-40% вищим у

ворожому середовищі, ніж у базовому *AODV*.

Варто також врахувати, що додаткові модулі безпеки збільшують накладні витрати, затримку та споживання енергії. Тому вибір між *AODV* та *E-AODV* залежить від пріоритетів: продуктивність у «чистому» середовищі чи захищеність у потенційно загрозливому. *E-AODV* доцільно використовувати у критичних застосуваннях, де атаки є ймовірними та можуть мати катастрофічні наслідки для передачі даних.

Підсумовуючи, інтеграція механізмів виявлення атак в *E-AODV* значно підвищує безпеку *MANET* без кардинального зниження продуктивності. Надалі можливе подальше удосконалення протоколу через адаптивні алгоритми, блокчейн-технології або гібридні механізми на базі ШІ.

## ВИКОРИСТАНІ ДЖЕРЕЛА


*1. Hai T. H., Toi N. D., Huh E. N. Performance Evaluation of AODV and AOMDV Routing Protocols Under Collaborative Blackhole and Wormhole Attacks (2021) Advances in Computer Science and Ubiquitous Computing - CSA-CUTE 2019. (Lecture Notes in Electrical Engineering; Vol. 715). pp. 273-280. DOI: doi.org/10.1007/978-981-15-9343-7_37.*

*2. Kumari A., Dutta S., Chakraborty S. A comparative study of different security issues in MANET (2032) International Journal of Experimental Research and Review. vol. 31. pp. 168–185. DOI: 10.52756/10.52756/ijerr.2023.v31spl.016.*

*3. Keerthika V., Nandagopal, Malarvizhi. Enhanced AODV protocol to secure routing in MANET with optimization techniques (2018) International Journal of Engineering and Technology(UAE). vol. 7. pp. 75-79. DOI: 10.14419/ijet.v7i2.19.15052.*

*4. Soni S. J., Nayak S. D. Enhancing security features & performance of AODV protocol under attack for MANET (2013) 2013 International Conference on Intelligent Systems and Signal Processing (ISSP). pp. 325-328. DOI: 10.1109/ISSP.2013.6526928.*

УДК 004.8(043.2)

**Є.С. Боданов,**
**К.О. Кисіль**
*Державний Університет «Київський авіаційний інститут», Київ*

## АВТОМАТИЗАЦІЯ ВИБОРУ ПАРАМЕТРІВ ОБРОБКИ ЗОБРАЖЕНЬ НА ОСНОВІ DEEP Q LEARNING

Автоматизація підбору оптимальних параметрів алгоритмів обробки зображень є актуальною проблемою для таких галузей, як комп'ютерний зір, медицина, безпека, робототехніка та автономні системи. Традиційні алгоритми мають недоліки через необхідність ручного налаштування параметрів алгоритмів оброблення зображення, а нейромережеві методи потребують значних обчислювальних ресурсів та часу на тренування.

У даній роботі запропоновано підхід автоматичного налаштування параметрів алгоритмів бібліотеки OpenCV на основі методу Deep Q Learning [1, 2]. Deep Q Learning був обраний через його здатність ефективно узагальнювати отриманий досвід та вирішувати проблему високої розмірності простору станів, що є типовою для класичного методу Q-learning.

Для навчання нейромережі було використано датасет DIV2K, який складається з високоякісних кольорових зображень. У процесі підготовки зображення були зменшені до розміру 500×500 пікселів (для зниження споживання оперативної пам'яті при тренуванні нейромережі) та штучно спотворені додаванням гаусівського шуму (середнє значення – 50, дисперсія – 150). Для кількісної оцінки результатів використовувалися метрики Peak Signal-to-Noise Ratio (PSNR) та Structural Similarity Index (SSIM) [3].

Розроблена архітектура нейромережі включає три згорткові шари CNN для вилучення просторових ознак зображення і два повнозв'язні шари Deep Q Network, які відповідають за оптимальний вибір параметрів алгоритмів. Для стабілізації процесу навчання було використано підхід experience replay. Навчання проводилося протягом 10 епох із використанням оптимізатора Adam, швидкістю навчання 0.001 та дисконт-фактором 0.99.

Запропонований нейромережевий підхід протестовано на алгоритмі шумозаглушення Non-Local Means

(fastNlMeansDenoisingColored), який показав високу ефективність і широко використовується у практичних задачах.

За результатами тестування зафіксовано суттєве покращення чисельних показників: середнє значення PSNR зросло з 10.60 дБ до 13.39 дБ, а SSIM – з 0.11 до 0.28. Розроблена модель також продемонструвала добру узагальнювальну здатність, ефективно підбираючи параметри не лише для тренувальних, а й для нових, раніше невідомих зображень.

Отримані результати демонструють ефективність та перспективність застосування методу Deep Q Learning для автоматизації налаштування параметрів алгоритмів OpenCV. Запропонований підхід може бути інтегрований у медичні інформаційні системи, системи відеоспостереження та комплекси БПЛА, що підвищить їх ефективність, особливо за умов обмежених обчислювальних ресурсів.

Подальші дослідження передбачають створення комплексного модуля автоматизованої обробки зображень, який включатиме етапи усунення ефекту туману, адаптивного підвищення контрастності та детекції країв з використанням запропонованого нейромережевого методу налаштування параметрів.

## ВИКОРИСТАНІ ДЖЕРЕЛА

1. Боданов Євгеній, Кисіль Каріна. Застосування методу Deep Q-Learning в нейромережах для обробки зображень, отриманих з БПЛА /3-я Міжн. науково-практ. конф. «Scientific Exploration: Bridging Theory and Practice» (24-26 березня 2025 р.): тези доп. – Germany, Berlin. – 2025. – Pp. 87-89.

2. Hlazok O., Bodanov Ye. Reference-based methods for image quality assessment //The 1st International Scientific and Practical Conference “Global Trends in the Development of Information Technology and Science”, January 8-10, 2025: proceedings. – Stockholm, Sweden. – 2025. – Pp. 60-62.

3. Hester T., Vecerik M., Pietquin O. et al. Deep Q-learning from Demonstrations. – ArXiv. – 2017. – URL: https://arxiv.org/abs/1704.03732 .

УДК 004.056

**А.І. Вавіленкова**
*Національна академія Служби безпеки України, Київ*

# ЕТАПИ ПРОЦЕСУ УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ

Відповідно до визначення у законі України «Про основні засади забезпечення кібербезпеки України» інцидентом кібербезпеки або кіберінцидентом вважається подія або ряд несприятливих подій ненавмисного характеру або таких, що мають ознаки можливої кібератаки та становлять загрозу безпеці систем [1].

В умовах сучасного цифрового світу кіберінциденти можуть виникати будь-коли і в будь-якій організації, тому основною проблемою під час настання кіберінцидентів є необхідність розуміння не тільки того, що робити у разі їх виникнення, але й як підготуватися до їх ймовірного настання, створивши ефективний процес управління кіберінцидентами [2]. У свою чергу процес Управління кіберінцидентами є важливою складовою кібербезпеки, оскільки допомагає організаціям швидко реагувати на загрози та мінімізувати шкоду від інцидентів, що можуть вплинути на інформаційні системи, дані, ресурси та репутацію організації.

Процес управління кіберінцидентами передбачає виявлення, аналіз, реагування та покращення наслідків деструктивних подій (рис. 1) [3].

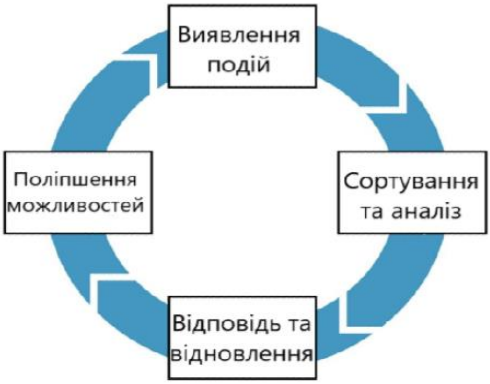



Рис.1. Схема процесу управління кіберінцидентами

Першим етапом процесу управління кіберінцидентами є виявлення подій, під якими розуміють ті чи інші ситуації, які

можуть порушити типову діяльність організації – це порушення вимог конфіденційності, цілісності та доступності.

Другим етапом в процесі управління кіберінцидентами є сортування та аналіз подій, тобто класифікація потенційних кіберінцидентів, визначення пріоритету їх усунення, зокрема, на інциденти низької важливості, серйозні інциденти та критичні інциденти. Для своєчасного реагування на кіберінциденти класифікація та пріоритизація кіберінцидентів повинна бути прописана завчасно у плані управління кіберінцидентами.

Третім етапом в процесі управління кіберінцидентами є відповідь та відновлення, тобто реагування на інцидент, обмеження впливу кіберінциденту, мінімізація шкоди від настання події. До заходів реагування на кіберінциденти відноситься проведення цифрового слідства для фіксації інциденту, вживання заходів щодо усунення вразливості, розробка та реалізація заходів реагування.

Четвертим етапом в процесі управління кіберінцидентами є поліпшення можливостей, тобто відновлення нормальної роботи системи після локалізації та знешкодження кіберінциденту.

Після інциденту важливо провести його аналіз для того, щоб визначити причини його виникнення та можливі шляхи покращення процесів безпеки в майбутньому, зокрема, проведення постінцидентного аналізу для вивчення його причин і результатів, розробка нових політик безпеки на основі уроків, отриманих під час інциденту, проведення навчань і тренувань для співробітників для підвищення їхньої обізнаності щодо кібербезпеки.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017р. №2163-VIII: станом на 30 серпня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення 23.03.2025).*

*2. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології): практичний посібник / Ю.І. Когут. – Київ: Консалтингова компанія «СІДКОН»; ВД «Дакор». 2024 – 284 с.*

*3. Посібник з додаткових ресурсів CRR. Том 5. Управління кіберінцидентами. Copyright. Університет Карнегі-Меллона. 2016. – 54 с.*

УДК 004.056.53

**Д.В. Воронков**
*Державний Університет «Київський авіаційний інститут», Київ*

# АНАЛІЗ СУЧАСНИХ МЕТОДІВ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У КОМП'ЮТЕРНИХ КЛАСТЕРАХ

У сучасних комп’ютерних системах ефективне балансування навантаження відіграє ключову роль у забезпеченні високої продуктивності, стійкості та надійності роботи. З розвитком розподілених обчислень, хмарних технологій і багатоядерних процесорів зростає необхідність у використанні методів оптимального розподілу обчислювальних ресурсів. Балансування навантаження – це процес рівномірного розподілу задач між обчислювальними вузлами або потоками, щоб мінімізувати час очікування, покращити використання ресурсів і запобігти перевантаженню окремих компонентів системи. Він дозволяє уникнути неефективного використання ресурсів комп’ютерної мережі.

До цілей, які має вирішувати балансування навантаження, можна відвести наступні:

- справедливість: необхідно досягти стану, коли на обробку кожного запиту виділялися системні ресурси і уникати ситуацій, коли один запит оброблюється, а інші очікують своєї черги
- ефективність: кожен сервер, який відповідає на запити, має бути навантажений на 100%; потрібно уникати ситуацій, коли один із серверів очікує на запити, в той час, як інші працюють.
- зменшення часу відповіді на запит: потрібно мінімізувати час між початком обробки запиту і його завершенням

Сучасні методи можуть балансувати навантаження на 3 рівнях OSI:

- Мережевий рівень (Балансування трафіку між кількома серверами або вузлами на основі IP-адрес)
- Транспортний рівень (Розподіл трафіку на основі інформації TCP/UDP, таких як порти або сесії)
- Рівень додатків (Використання HTTP/HTTPS заголовків, cookies, API-запитів для інтелектуального розподілу навантаження)

Балансування навантаження на кожному рівні має свої переваги та недоліки.

Наприклад, балансування на нижчих рівнях OSI (3-4) має більшу швидкість, і зазвичай підтримується більшою кількістю додатків, але балансування на рівні додатків дозволяє враховувати вміст пакетів та виконувати більш гнучке розподілення наватаження.

Існує велика кількість сучасних технологій, які дозволяють ефективно виконувати функцію балансуванн навантаження. Наприклад, Nginx – це веб-сервер, який може виконувати функцію балансування навантаження. Він підтримує велику кількість алгоритмів, таких як Round Robin, Least Connections, IP Hash та інші. Завдяки легкості і простості налаштування він є одним з найпопулярнішим рішенням у віртуальних комп'ютерних кластерах

Великі дата-центри пропонують власні технології для балансування навантаження. AWS (Amazon Web Services) – один з найбільших хмарних сервісів – пропонує для свої клієнтів технології AWS Elastic Load Balancer та AWS Auto Scaler. Основною особливістю цих технологій в тому, що вони керують не тільки розподіленням трафіку по елементам комп'ютерної системи, а також можуть виділяти додаткові ресурси за необхідністю.

Ефективне балансування навантаження є ключовим фактором для забезпечення продуктивності та надійності сучасних комп'ютерних систем, дозволяючи рівномірно розподіляти ресурси та мінімізувати затримки. Завдяки використанню різних рівнів балансування, алгоритмів і технологій, можна досягти оптимального управління навантаженням у розподілених обчислювальних середовищах.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Ремесник А. С. Балансування навантаження мережі / А. С. Ремесник // Радіоелектроніка та молодь у XXI столітті: матеріали 24-го Міжнародного молодіжного форуму, 7–9 квітня 2020 р. – Харків: ХНУРЕ, 2020. – Т. 5. – С. 63–64.*

УДК 004.056.53

**О.С. Вязнікова**
*Державний Університет «Київський авіаційний інститут», Київ*

# ІНТЕЛЕКТУАЛЬНИЙ ЗАСІБ КЕРУВАННЯ РУХОМ БПЛА В УРБАНІСТИЧНИХ УМОВАХ З ПЕРЕШКОДАМИ

Штучний інтелект – одна з ключових технологій сучасності, що активно впроваджується в усіх галузях. Розвиток методів машинного навчання відкрив широкі можливості для вирішення різноманітних завдань, зокрема в інженерії. Сучасний ринок технологій демонструє зростаючий інтерес до безпілотних літальних апаратів (БПЛА), оснащених інтелектуальними системами керування. Така інтеграція є критично важливою в умовах, що вимагають високої ефективності та безпеки, дозволяючи оптимізувати використання людських ресурсів, скоротити часові витрати та мінімізувати ризики для життя.

Авторкою було здійснено огляд існуючих архітектур комп'ютерного зору, включаючи CNN, YOLO, R-CNN та SSD, з метою вибору оптимальної моделі для детекції об'єктів у міській забудові. На основі проведеного аналізу було обрано YOLOv5, оскільки ця модель демонструє високу швидкість обробки кадрів у реальному часі, що є критичним для роботи БПЛА. Крім того, YOLOv5 має ефективний механізм детекції об'єктів, що дозволяє точно розпізнавати дорожні знаки, будівлі, дерева та інші міські перешкоди навіть в умовах змінного освітлення.

Також під час дослідження наявних алгоритмів пошуку шляху (для уникання перешкод) було розглянуто A*, D* та RRT для автономної навігації БПЛА в міських умовах. Критеріями оцінки були швидкість роботи, адаптивність до змінного середовища та ефективність обходу перешкод. На основі аналізу було обрано алгоритм D*-Lite, який забезпечує динамічне оновлення маршруту під час польоту, що критично важливо для роботи в міських умовах, де можливі несподівані перешкоди, такі як рухомі об'єкти або зміна оточення.

Авторкою було проведено дослідження із застосуванням нейромережевої моделі YOLOv5 для розпізнавання міських об'єктів (дерева, ліхтарі, будинки, дорожні знаки, світлофори) на основі Open Images Dataset v7. Процес підготовки даних включав конвертацію анотацій у формат YOLOv5 за допомогою

інструменту Roboflow, що дозволило оптимізувати і автоматизувати підготовку даних для навчання нейромережі. Навчання моделі було виконано в хмарному середовищі Google Colaboratory, що забезпечило високу продуктивність та доступність обчислювальних ресурсів для обробки великих обсягів даних.

Для обльоту перешкод використано алгоритм D*-Lite, інтегрований у систему управління БПЛА PX4, що забезпечило автономне ухилення від перешкод в міському середовищі. Моделювання польоту та перевірка ефективності алгоритму проводяться у симуляторі Gazebo, що відтворює умови міської забудови. Дослідження показало точність розпізнавання об’єктів та ефективність ухилення від перешкод, підтверджуючи перспективність нейромережевих моделей та алгоритмів планування для автономних БПЛА.

У дослідженні встановлено, що використання нейромережевих моделей для розпізнавання перешкод разом з алгоритмами пошуку оптимальних маршрутів значно підвищує ефективність автономного керування БПЛА в міських умовах. Аналіз Open Images Dataset v7 показав, що якість навчання YOLOv5 залежить від точності анотацій, що підвищує точність розпізнавання міських об’єктів.

Результати тестування підтвердили ефективність хмарного середовища Google Colaboratory для навчання моделей, а алгоритм D*-Lite показав високу адаптивність у побудові маршруту обльоту перешкод. Виявлено, що ефективність уникнення перешкод залежить від інтеграції алгоритму в програмне забезпечення БПЛА, зокрема PX4. Поєднання машинного навчання та планування маршруту підвищує автономність БПЛА в урбаністичних умовах.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. A Comprehensive Review of AI-enabled Unmanned Aerial Vehicle: Trends, Vision, and Challenges. /Arxiv. URL: https://arxiv.org/pdf/2310.16360*

*2. Вернадський, Т. М. Методи керування БПЛА із застосуванням комп'ютерного зору. DOI 10.32782/2663-5941/2024.5.1/32. URL: https://www.tech.vernadskyjournals.in.ua/ journals/2024/5_2024/part_1/34.pdf*

УДК 004.77:004.738.5:613.9:615.47:004.056

**О.О. Гетьман**
*Державний Університет «Київський авіаційний інститут», Київ*

# МОБІЛЬНИЙ ЗАСТОСУНОК ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОЇ ПРОФІЛАКТИЧНОЇ МЕДИЦИНИ НА БАЗІ IoT ТА BIG DATA

Сучасний етап розвитку медицини потребує нових технологій, що виникають на стику комп'ютерних наук, практичних медичних методів, обробки (аналізу) даних та мікроелектронних пристроїв, зокрема це Інтернет Речей (IoT) та Великі Масиви Даних (Big Data). Пристрої IoT збирають контекстно-залежні дані про фізичне, поведінкове та психологічне здоров'я пацієнтів, тоді як обробка та аналіз Big Data дозволяє отримувати цінну інформацію та виконувати прогнози для забезпечення медичних працівників здатністю приймати ефективні рішення [1].

Основне завдання IoT в області профілактичної медицини полягає в забезпеченні моніторингу стану здоров'я пацієнтів, що полегшує прийняття рішення лікуючими лікарями. Це включає в себе віддалений моніторинг стану здоров'я пацієнта, відстеження особливостей його лікування та призначення ліків. IoT має великий потенціал для покращення якості медичних послуг і зниження витрат на основі раннього виявлення та профілактики захворювань.

IoT на базі відповідних сенсорів збирає та передає важливі дані про стан здоров'я пацієнтів, за рахунок безперервного моніторингу, серверній частині з алгоритмами інтелектуального аналізу даних. Сенсори включають в себе датчики артеріального тиску, пульсу, рівня кисню, положення пацієнта в просторі, активності його м'язів та серця, рівня глюкози в крові.

IoT та Big Data значно розширюють можливості профілактичної медицини підносячи її на вищий рівень віддаленої медицини (телемедицини) в рамках концепції інтелектуального здоров'я (iHealth), де активно використовуються мобільні пристрої [2].

Використання мобільного додатку на базі IoT та Big Data надає можливість для подальшого поглиблення цифровізації в області профілактичної медицини та автоматизації обміну даними в системах охорони здоров'я в цілому, шляхом інтеграції застосунку в існуючі інформаційні та комунікаційні системи охорони здоров'я, зокрема електронних медичних записів, надаючи численні

переваги, включаючи підвищену конфіденційність, точність, покращену сумісність, можливість повторного використання даних та забезпечення ефективного прийняття рішень.

Така технологія дозволить надавати медичну допомогу пацієнтам амбулаторно, за межами лікарень та клінік, забезпечуючи при цьому збір даних, необхідних для ефективної діагностики та лікування (Рис.1).

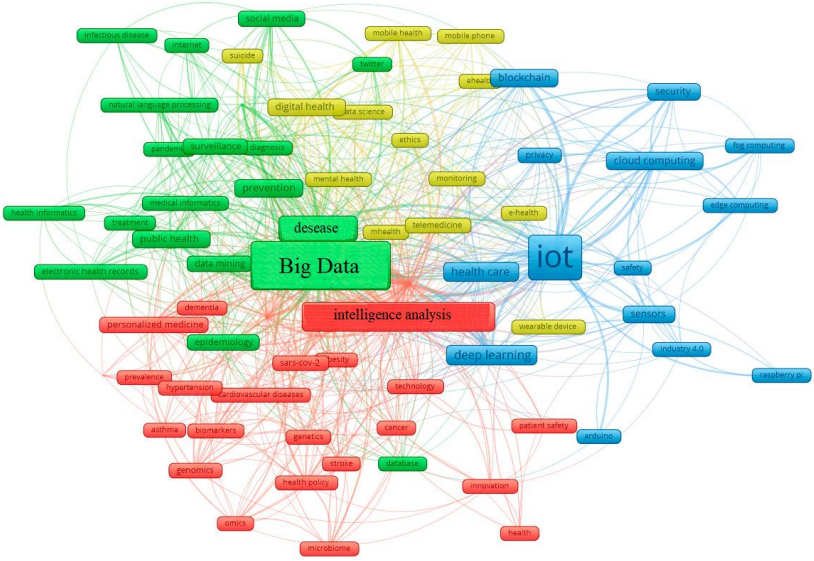



Рис.1. Забезпечення ефективної профілактичної медицини на базі IoT та Big Data.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Pulimamidi, R. To Enhance Customer (or Patient) Experience Based on IoT Analytical Study through Technology (IT) Transformation for E-Healthcare. Meas. Sens. 2024, 33, 101087.*

*2. Kaur, K.; Verma, S.; Bansal, A. IOT Big Data Analytics in Healthcare: Benefits and Challenges. In Proceedings of the 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021; pp. 176–181.*

УДК 004.274:004.056

**С.Я. Гільгурт**
*Державний Університет «Київський авіаційний інститут», Київ*

# РЕКОНФІГУРОВНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА БАЗІ РЕГУЛЯРНИХ ВИРАЗІВ

Сигнатурні мережеві систем виявлення вторгнень (NIDS), як один з найважливіших засобів захисту інформації, незважаючи на їх вагомий недолік – нездатність розпізнавати нові, ще невідомі атаки, для яких не розроблено сигнатур, досі широко розповсюджені завдяки високої надійності та низькому рівню хибних спрацювань.

Суттєво пом'якшити цей недолік дозволяє гнучке розпізнавання з використанням апарату так званих регулярних виразів – RegEx, які на відміну від патернів (фіксованих рядків символів) сигнатурних систем, дозволяють розпізнавати широко коло варіацій та комбінацій символів. Механізми RegEx дозволяють за допомогою так званих символів-джокерів (таких як "*", "?", "+", "$", "^","|" та ін.) формувати шаблони, які припускають наявність будь-якого символу (або довільної кількості символів) у певній позиції, варіанти підрядків, відстань між фіксованими патернами у довільну кількість знаків та багато інших різновидів варіацій, що можуть складатися з фрагментів рядків та окремих символів. Бази даних сигнатур майже всіх сучасних NIDS містять велику кількість регулярних виразів. За деякими спостереженнями частка таких сигнатур складає до 40% від їх загальної кількості.

Гнучке розпізнавання надає багато можливостей для виявлення найбільш складних та витончених атак на комп'ютерні системи та мережі. Головний недолік апарату регулярних виразів – відносно висока ресурсоємність, усувається зазвичай за рахунок апаратної реалізації з використанням реконфігуровних засобів, тобто пристроїв на базі програмованих мікросхем ПЛІС типу FPGA для максимального розпаралелювання процедури розпізнавання шляхом одночасної обробки багатьох RegEx-шаблонів.

Даний підхід відомий вже багато років [1, 2]. Але одним з основних факторів стримування його більш швидкого розповсюджування є неможливість стандартних реконфігуровних засобів динамічно оновлювати шаблони регулярних виразів під час функціонування. Це суттєво обмежує ключову функціональністю

таких систем в зв’язку з частою зміною сигнатур для нещодавно виявлених уразливостей.

Одним з можливих напрямів вирішення проблеми реалізації підвищення гнучкості реконфігуровних систем захисту інформації сигнатурного типу, базується на використанні так званої процедури оперативного оновлення (ПОО) [3]. Сутність підходу полягає в організації обчислювального процесу під час функціонування реконфігуровної системи таким чином, щоб забезпечити можливість здійснити ПОО в будь який момент часу. Ініціювати ПОО може, наприклад, поява нових класів атак, для протидії яким в склад NIDS потрібно додати нові апаратні схеми розпізнавання, або зміна умов роботи інформаційної системи, що захищається (модифікація локальної мережі, оновлення її складу або структури, модифікація програмного забезпечення тощо). Нарешті, здійснення спроби гібридної багатопланової атаки призводить до необхідності суттєво міняти алгоритми функціонування всіх компонентів систем об’єкта захисту. Але для запропонованого підходу ці зміни зводяться лише до штатного виконання ПОО.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Sidhu R., Prasanna V.K. Fast Regular Expression Matching Using FPGAs. 9th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2001). — 2001, Institute of Electrical and Electronics Engineers Inc. — P. 227-238.*

*2. Kim J., Park J. FPGA-based memory efficient shift-and algorithm for regular expression matching. Lecture Notes in Computer Science*. 14th International Symposium on Applied Reconfigurable Computing, *Vol. 10824. — 2018, P. 132-141.*

*3. Гільгурт С.Я., Жуков І.А. Підхід до реалізації адаптивних можливостей реконфігуровних систем захисту інформації сигнатурного типу. XV Міжнародна науково-технічна конференція «Комп’ютерні системи та мережні технології». Тези доп., 25 – 26 квітня 2024. – К.: НАУ, 2024. – С. 31-34.*

УДК 681.52

**О.М. Глазок, С.Р. Білокур**
*Державний Університет «Київський авіаційний інститут», Київ*

# ЗАСТОСУВАННЯ МЕТОДУ ВЕКТОРНОЇ ПОЛЬОВОЇ ГІСТОГРАМИ ДЛЯ КЕРУВАННЯ РУХОМ ГРУПИ БПЛА В УМОВАХ НАЯВНОСТІ ПЕРЕШКОД

Серед методів керування БПЛА в присутності перешкод особливе місце займають методи потенційних або непотенційних силових полів. Методи потенційних або непотенційних силових полів дозволяють БПЛА ефективно уникати перешкод, створюючи віртуальні «силові поля» навколо них. Ці поля відштовхують БПЛА від перешкод, дозволяючи йому знаходити безпечний шлях. Методи потенційних полів зазвичай використовують математичні функції для створення притягуючих і відштовхуючих сил. Методи непотенційних полів [1] можуть використовувати інші підходи, такі як вектори швидкості або динамічні моделі. Ці методи особливо корисні в динамічних середовищах, де перешкоди можуть рухатися або змінюватися з часом. Алгоритм розраховує ці сили для кожної точки простору та на основі отриманих значень адаптує рух апарата, щоб уникнути зіткнень і забезпечити досягнення цілі. Віртуальне силове поле дозволяє отримати точні траєкторії апарату з обмеженими обчислювальними ресурсами. З іншого боку, цей метод має свої недоліки, зокрема суттєве ускладнення математичних розрахунків і можлива втрата контролю над апаратом у складних умовах.

Метод векторної польової гістограми є іншим поглядом на метод силових полів. Цей метод був початково запропонований для керування мобільними роботами на двовимірній площині. Метод використовує двовимірну гістограмну сітку, яка дозволяє врахувати всі координати, отримані від сенсорів дальності. На основі цієї сітки формується одновимірна полярна гістограма, що дозволяє зручно оцінювати, в якому напрямку є безпечний шлях для робота [2]. Надалі метод адаптований і для безпілотних літальних апаратів [3, 4]. В цій модифікації метода будується векторне поле, яке за допомогою гістограмної карти дозволяє оцінити довкілля та визначити найбільш придатний напрямок для руху.

Для застосування методу необхідно побудувати цільову функцію прийняття рішення щодо уникнення перешкод, яка враховує розмір і рух перешкоди. Для кожного потенційного напрямку руху обчислюється оцінка доцільності або загрози за допомогою цієї функції прийняття рішення. Додатково може бути введений механізм динамічної пам'яті, яка використовується при оновленні гістограм загрози на поточний момент, з урахуванням даних з минулих моментів часу. Механізм динамічної пам'яті дозволяє підвищити ефективніть дій БПЛА за рахунок обходу локальних мінімумів цільової функції. Далі необхідно розрахувати скориговані ступені безпеки з урахуванням динамічних обмежень БПЛА та визначити оптимальний напрямок обходу перешкоди. Перспективним напрямком досліджень може бути напрацювання алгоритму регулювання швидкості на основі консенсусу у хмарній моделі, щоб забезпечити колективність реакції групи в цілому при наближенні до перешкод, а також врахування позитивного «досвіду» окремих членів групи, які першими змогли здолати або обійти перешкоду.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Olexiy M. Glazok. A non-potential Target Function for Controlling the UAVs Group Flight in Presence of Concave Obstacles /2019 IEEE 5th Int. Conf. "Actual Problems of Unmanned Aerial Vehicles Developments" (APUAVD), October 22-24, 2019: proceedings. – IEEE, 2019. – Pp. 238-241. DOI:10.1109/APUAVD47061.2019.8943870.*

2. *Alagic E., Velagic J., Osmanovic A. Design of Mobile Robot Motion Framework based on Modified Vector Field Histogram /2019 Int. Symposium ELMAR: Proceedings. – 2019. – Pp. 135-138. DOI: 10.1109/ ELMAR.2019.8918891.*

3. *Mohamed K., Aliedani A., Al-Ibadi A. Adaptive Vector Field Histogram Plus (VFH+) Algorithm using Fuzzy Logic in Motion Planning for Quadcopter //Journal of Robotics and Control (JRC). – 2024. – Vol. 5. – Pp. 582-596. DOI: 10.18196/jrc.v5i2.21540.*

4 *A fish evasion behavior-based vector field histogram method for obstacle avoidance of multi-UAVs /Li M., Huang Z., Wenhao B., Hou T., Yang P., Zhang A. //Aerospace Science and Technology. – 2025. – Vol. 159. – P. 109974. DOI: 10.1016/j.ast.2025.109974*

УДК 004.056

**Ю.О. Глущук**,
**А.О. Фесенко**
*Державний Університет «Київський авіаційний інститут», Київ*

# ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ОБРОБКИ ПРИРОДНОЇ МОВИ ТА МОДЕЛЮВАННЯ ПОВЕДІНКИ КОРИСТУВАЧА В АВТОМАТИЗАЦІЇ ТЕСТУВАННЯ

У сучасних умовах стрімкого розвитку інформаційних технологій автоматизація тестування програмного забезпечення (ПЗ) стає ключовим фактором підвищення його якості та надійності. Одним із найбільш перспективних напрямів у цій сфері є застосування інтелектуальних методів, зокрема обробки природної мови (Natural Language Processing, NLP) та моделювання поведінки користувача (User Behavior Modeling).

**Обробка природної мови (NLP)** — це підгалузь комп'ютерних наук і штучного інтелекту, що займається взаємодією між комп'ютерами і людськими (природними) мовами. Простіше кажучи, мета полягає в тому, щоб дозволити комп'ютерам розуміти, інтерпретувати і навіть генерувати людську мову [1].

**Моделювання поведінки користувача (User Behavior Modeling) –** метод, в основі якого лежить застосування штучного інтелекту (ШІ) для аналізу даних про поведінку користувачів та автоматичне генерування тестів, що імітують реальні сценарії взаємодії з продуктом.

На ілюстрації нижче (Рис.1) зображено весь пайплайн діалогового менеджера, і розуміння роботи з кожним модулем – ключ до налагодженої роботи NLP-інженера. Як бачимо, сама схема проста: модуль ASR перетворює людське мовлення на текст, після чого NLP-алгоритм структурує і маркує його, а діалоговий менеджер інтерпретує його в команди та диригує усією системою. На виході користувач отримує очікуваний результат, що супроводжується згенерованим текстом, аудіо повідомленням, посиланням чи зображенням [2].

Моделювання поведінки користувача, у свою чергу, дає можливість прогнозувати можливі сценарії взаємодії з ПЗ, що дозволяє ідентифікувати потенційні проблеми ще на ранніх етапах розробки.

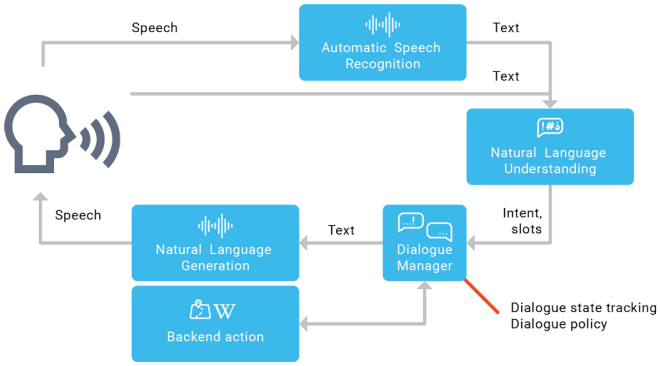



Рис.1. Пайплайн діалогового менеджера

Інтелектуальні алгоритми аналізу поведінкових патернів можуть допомагати створювати реалістичні тестові сценарії, що забезпечують глибше покриття тестуванням та виявлення прихованих помилок, які можуть виникати у реальних умовах експлуатації [3].

Попри значні переваги застосування інтелектуальних методів у тестуванні, існує низка проблем, які ускладнюють їх ефективне впровадження:

- **Якість та повнота даних** – алгоритми NLP та моделювання поведінки користувачів залежать від обсягу та якості наявних даних.
- **Складність реалізації та обчислювальні витрати** – використання методів ШІ вимагає значних обчислювальних ресурсів та висококваліфікованих спеціалістів, що може ускладнити інтеграцію в існуючі процеси тестування.
- **Гнучкість та адаптивність** – поведінка користувачів змінюється з часом, що потребує постійного оновлення та навчання моделей, щоб підтримувати їхню актуальність.
- **Інтеграція з існуючими системами** – забезпечення сумісності нових інтелектуальних методів із наявними інструментами.

Для подолання вищезазначених проблемних аспектів необхідно впроваджувати комплексні підходи та інноваційні рішення:

- **Покращення якості даних** – застосування методів очищення, аугментації та синтетичної генерації даних для

покращення навчального набору, що використовують алгоритми NLP та поведінкові моделі.

- **Оптимізація обчислювальних витрат** – використання хмарних технологій та спеціалізованого апаратного забезпечення (GPU, TPU) для прискорення обчислень і зменшення навантаження на локальні ресурси.
- **Динамічне оновлення моделей** – автоматичне навчання моделей у реальному часі на основі нових даних та адаптація алгоритмів до змін у поведінці користувачів.
- **Глибока інтеграція з існуючими системами** – розробка гібридних рішень, які поєднують традиційні методи тестування з інтелектуальними моделями, що дозволяє забезпечити їхню ефективну взаємодію.

Інтелектуальні методи обробки природної мови та моделювання поведінки користувачів мають значний потенціал у сфері автоматизованого тестування ПЗ. Вони дозволяють підвищити ефективність тестування, скоротити витрати на розробку тестових сценаріїв та підвищити якість кінцевого продукту. Однак для успішного впровадження цих методів необхідно враховувати проблеми, пов'язані з якістю даних, обчислювальними витратами, інтерпретованістю результатів та адаптивністю алгоритмів.

## ВИКОРИСТАНІ ДЖЕРЕЛА


*1. Що таке обробка природної мови (Natural Language Processing, NLP)? [Електронний ресурс] // thetransmitted – 2024. – Режим доступу до ресурсу: https://thetransmitted.com/adlucem/shho-take-obrobka-pryrodnoyi-movy-natural-language-processing-nlp/.*

*2. Ян Б. Вступ до NLP. Як розробити діалогову систему [Електронний ресурс] / Ян Бутельський // dou – 2021. – Режим доступу до ресурсу: https://dou.ua/lenta/columns/introduction-to-nlp/.*

*3. Sumit K. A Guide to User Behavior Modeling [Електронний ресурс] / Sumit Kumar // blog.reachsumit – 2024. – Режим доступу до ресурсу: https://blog.reachsumit.com/posts/2024/01/user-behavior-modeling-recsys/.*

УДК 004.75:621.39

**В.О. Гнатюк[1,2],**
**І.О. Горбачов[1]**
*[1]Державний Університет «Київський авіаційний інститут», Київ*
*[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ*

# МЕТОД УПРАВЛІННЯ SLICE-МЕРЕЖАМИ 5G ДЛЯ QOS У VOIP

Сучасні мережі IP-телефонії стикаються з проблемами гарантування QoS для голосового трафіку через динамічні зміни навантаження, затримку, джитер і втрати пакетів. Традиційні механізми QoS (DiffServ, MPLS) обмежено адаптуються до швидких змін у мережах, що знижує продуктивність VoIP, особливо у 5G із використанням Network Slicing.

Для вирішення цієї проблеми запропоновано метод на основі ML: LSTM-мережі прогнозують QoS-параметри, а Reinforcement Learning оптимізує вибір slice. Це дозволяє мінімізувати затримку, зменшити джитер і втрати пакетів, а також автоматизувати управління мережею.

Розробка інтелектуальних механізмів прогнозування QoS є ключовою для покращення VoIP-сервісів та ефективності 5G-мереж. Метою роботи є розробка методу динамічного управління slice-мережами у 5G для підвищення QoS у VoIP.

У сучасних дослідженнях [1-3] значна увага приділяється підвищенню якості обслуговування (QoS) в системах IP-телефонії шляхом впровадження методів машинного навчання (ML) та динамічного управління ресурсами. Ці підходи спрямовані на адаптацію мережевих параметрів в реальному часі для забезпечення стабільної та якісної передачі голосових даних. Серед сучасних підходів виділяють наступні: використання машинного навчання для прогнозування та оптимізації QoS, адаптивні алгоритми управління трафіком, інтеграція методів оптимізації та машинного навчання тощо.

Метод складається з трьох основних модулів:

Модуль 1. Моніторинг QoS у slice-мережах:

- вимірювання затримки (latency), джитера (jitter), втрат пакетів (packet loss) та пропускної здатності;
- отримання даних із 5G Core (AMF, SMF) та MEC-серверів;

- використання технології Software-Defined Networking (SDN) для централізованого управління мережею.

Модуль 2. Прогнозування QoS за допомогою AI/ML:

- алгоритм LSTM (Long Short-Term Memory) прогнозує, коли QoS погіршиться;
- аналіз історичних даних трафіку для оцінки ймовірності деградації QoS;
- врахування завантаження slice та загального стану 5G-мережі.

Модуль 3. Динамічне перемикання slice-мереж:

- при прогнозованому погіршенні QoS → VoIP-трафік перемикається на slice із кращими параметрами;
- використання Network Function Virtualization (NFV) для адаптивного виділення ресурсів;
- Reinforcement Learning (RL) оптимізує алгоритм вибору slice залежно від QoS.

У роботі було розглянуто підхід до підвищення QoS в системах VoIP шляхом використання машинного навчання для прогнозування мережевих параметрів та динамічного управління ресурсами.

Запропоновано метод прогнозування ключових показників QoS на основі алгоритмів машинного навчання, що дозволяє виявляти потенційні проблеми ще до їх виникнення.

Отримані результати можуть бути використані для подальшої оптимізації мереж IP-телефонії, а також у майбутніх дослідженнях, пов'язаних із підвищенням ефективності управління ресурсами в реальному часі.

ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Sun, W., Peng, M., Mao, S., Wang, Y., & Huang, C. (2019). Edge computing and caching for 5G and beyond networks. IEEE Communications Magazine, 57(1), 22–27.*

*2. Li, W., & Wang, H. (2019). User association for load balancing in vehicular networks: An online reinforcement learning approach. IEEE Transactions on Intelligent Transportation Systems, 20(12), 4313–4323.*

*3. Huang, T., Yang, R., Zhang, H., & Wu, G. (2020). Deep reinforcement learning for multimedia traffic control in software defined networking. IEEE Network, 34(3), 70–75.*

УДК 004.91

**А.Ю. Динько**
*Державний Університет «Київський авіаційний інститут», Київ*

# АЛГОРИТМ ФОРМУВАННЯ СИНОНІМІЧНИХ РЯДІВ ДЛЯ ЕЛЕМЕНТІВ ЛОГІКО-ЛІНГВІСТИЧНОЇ МОДЕЛІ

В епоху домінування інформаційних технологій, електронні тексти стали основою для обміну та збереження текстової інформації. Зокрема у сфері наукових досліджень, праці вчених все частіше публікуються в електронному вигляді ніж у друкованому, а роботи попередників оцифровуються. Проте в обох випадках першочергово текст перебуває в електронному форматі та підлягає перевірці на доброчесність, адже з розвитком технологій зростає ймовірність використання чужих напрацювань, плагіату, через легкодоступність других у мережі Інтернет.

Одним із найпопулярніших способів використання чужої інтелектуальної власності є перефразування тексту з використанням синонімів, котре замінюючи порядок слів у реченнях і використовуючи словозаміни, є перешкодою для сучасних систем виявлення збігів за змістом.

Для спрощення аналізу тексту за змістом використовують представлення речень у формалізованому вигляді, більш зрозумілому для електронно обчислювальних систем, а саме за допомогою логіко-лінгвістичних моделей. В [1] речення природньої мови подається у вигляді простого предикату, що описує частину цього речення, яке має закінчений зміст та відображає у реченні S p-е відношення з h-ю характеристикою між суб'єктом x з характеристикою g і об'єктом y з характеристикою q, предмет якого z володіє характеристикою r:

$$L\_p\text{^}S\ (x,g,y,q,z,r,h) \qquad (1)$$

У [2] було запропоновано сформувати синонімічні ряди, масиви синонімів, для кожного з елементів логіко-лінгвістичної моделі речення, котрі в майбутньому при співставленні з аналогічними предикатами з інших текстів зможуть показати чи була використана словозаміна.

Процес формування масивів синонімів відбувається наступним чином:

формування логіко-лінгвістичних моделей речень тексту, як описано в [3];

надсилання елементів сформованих моделей в базу даних синонімів слів української мови, як запит для пошуку, і отримання масиву синонімів за даним запитом;

формування і збереження масивів синонімів для кожного елемента моделі.

Блок-схема, що описує даний процес подана на рис. 1.

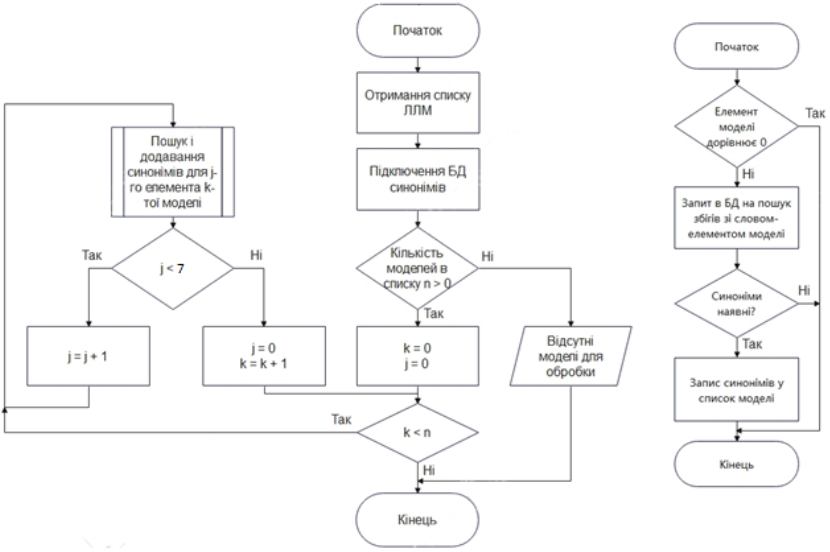



Рис. 1. Блок-схема формування синонімічних рядів для елементів логіко-лінгвістичної моделі

ВИКОРИСТАНІ ДЖЕРЕЛА


*1. Вавіленкова А.І. Аналіз і синтез логіко-лінгвістичних моделей речень природної мови: монографія. – К.: ТОВ "СІК ГРУП УКРАЇНА", 2017. – 152 с.*

*2. Динько А.Ю. "Автоматизоване формування синонімічних рядів для елементів логіко-лінгвістичної моделі речення природньої мови." International Science Journal of Engineering & Agriculture 3.5 (2024): 87-92.*

*3. Динько, А. Ю. (2020). Технологія автоматизованої побудови логіко-лінгвістичних моделей.*

УДК 004.056

**Д.М. Загорулько**
*Державний Університет «Київський авіаційний інститут», Київ*

# ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ АВТОМАТИЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ ЧЕРЕЗ API: КОНЦЕПТУАЛЬНІ ЗАСАДИ БЕЗПЕКОВОГО ЗАБЕЗПЕЧЕННЯ

Вступ. У контексті трансформації цифрового бізнес-середовища спостерігається стійка тенденція до переходу від ізольованих інформаційних систем до відкритих, взаємопов'язаних цифрових екосистем. В основі цієї трансформації лежить застосування API як основного засобу інтеграції та автоматизації бізнес-процесів. Проте зростання відкритості систем призводить до суттєвого ускладнення загальної парадигми інформаційної безпеки, що вимагає переосмислення архітектурних рішень і процедур захисту.

Мета дослідження. Розробка та теоретичне обґрунтування інформаційної технології автоматизації бізнес-процесів на основі API з вбудованим механізмом безпекового захисту на концептуальному, архітектурному та прикладному рівнях.

1. Методологічні основи інтеграції на базі API

У сучасних інформаційних системах API виступає посередником між суб'єктами цифрової взаємодії, забезпечуючи стандартизований доступ до функціональності зовнішніх або внутрішніх сервісів. Це дозволяє реалізувати динамічну оркестрацію бізнес-процесів, зменшити рівень ручного втручання та досягти високого ступеня адаптивності інформаційного середовища підприємства.

2. Безпекові ризики API-інтеграцій

Уразливість до атак типу Injection, Broken Authentication, Excessive Data Exposure та Insecure Direct Object References (IDOR) становить загрозу як для даних, так і для інфраструктури. Також критичним є питання керування сесіями, захисту від Replay-атак та впровадження принципів Zero Trust.

3. Засоби протидії та захисні механізми

Пропонується імплементація багаторівневої безпекової моделі, що передбачає: – криптографічний захист транспортного каналу (TLS ≥ 1.2); – автентифікацію та авторизацію користувачів за протоколом OAuth 2.0 із застосуванням JWT; – логування і моніторинг усіх API-викликів з інтеграцією в SIEM-системи;

– впровадження API Gateway з політиками rate-limiting, IP-фільтрацією та аналізом аномальної активності.

4. Пропонована архітектура інформаційної технології

На рівні архітектури обґрунтовується доцільність використання моделі, що поєднує адаптивне API-орієнтоване ядро, сервіс керування безпековими політиками та модуль аудиту взаємодій. Така структура забезпечує цілісне управління безпекою в динамічному середовищі цифрових сервісів.

Висновки

Запропонована концепція інформаційної технології автоматизації бізнес-процесів через API враховує актуальні виклики інформаційної безпеки та базується на принципах гнучкої масштабованості, захисту даних та відповідності стандартам безпеки. Запропонований підхід сприяє підвищенню довіри до інтеграційних рішень та забезпечує сталість функціонування бізнес-процесів в умовах кіберризиків.

ВИКОРИСТАНІ ДЖЕРЕЛА


1. *OWASP Foundation. API Security Top 10 – 2023.*
2. *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection.*
3. *Fielding R.T. Architectural Styles and the Design of Network-based Software Architectures. – University of California, Irvine, 2000.*
4. *NIST SP 800-207. Zero Trust Architecture. – National Institute of Standards and Technology, 2020.*
5. *Klyuev V. API Security Fundamentals. – Springer, 2021.*

УДК 004.71:656.073

**М.Р. Зайцев[1],**
**М.М. Гузій[1]**
**Є.І. Безвершенко[2]**
*[1]Державний Університет «Київський авіаційний інститут», Київ*
*[2]Ужгородський національний університет, Ужгород*

## СИСТЕМА ЗВ'ЯЗКУ БПЛА НА БАЗІ ТЕХНОЛОГІЇ STARLINK

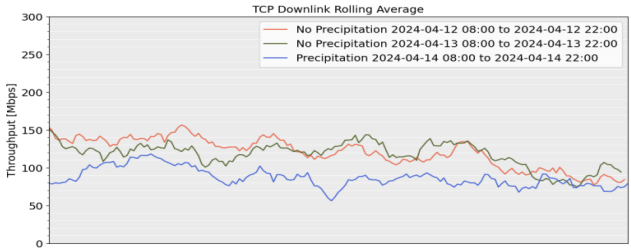
Сучасні безпілотні літальні апарати (БПЛА) вимагають стабільного зв'язку для виконання широкого спектру завдань, від військових операцій до цивільних рятувальних місій. Однією з основних задач для успішного застосування БПЛА в екстремальних умовах є забезпечення надійного зв'язку.

Технологія *Starlink*, розроблена компанією SpaceX, пропонує нові можливості для вирішення поставленої задачі. Завдяки мережі низькоорбітальних супутників Землі, *Starlink* забезпечує високошвидкісний Інтернет-зв'язок з незначними затримками. Дослідження можливостей та обмежень використання технології *Starlink* для забезпечення надійного зв'язку БПЛА в екстремальних умовах є актуальною прикладною проблемою.

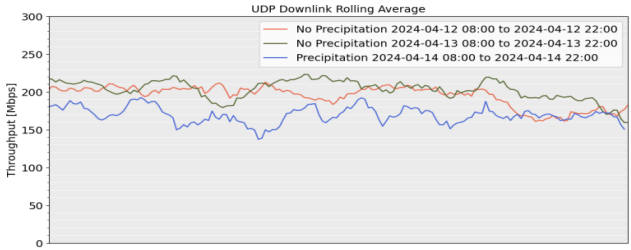
Мережева комунікація виступає базовою технологією для вирішення задач навігації, контролю повітряного простору та управління БПЛА. Однією з важливих проблем є вплив зовнішніх факторів на *QoS* інфокомунікаційних мереж. Якість зв'язку між супутниками *LEO* та наземним сегментом мережі залежить атмосферних впливів (зокрема дощу). Для оцінки впливу опадів на продуктивність *Starlink* використовується модель *ITU-R P.838-3*, яка враховує згасання сигналу при інтенсивних опадах.

Пропускна здатність мережі *Starlink* також залежить від використовуваного частотного діапазону, оскільки високочастотні діапазони піддаються значному впливу опадів: для *Ka*-діапазону (26-40 ГГц) згасання сигналу більш виражено порівняно з *Ku*-діапазоном (12-18 ГГц). Тести на пропускну здатність мережі *Starlink* в умовах наявності та відсутності опадів проводились для транспортних протоколів *TCP* та *UDP*. Результати тестування показують вищу пропускну здатність для протоколу *UDP*, порівняно з протоколом *TCP* (рис.1). Середнє значення бітрейту

протоколу *TCP* вище порівняно з вимірюваннями для протоколу *UDP* (рис.2).



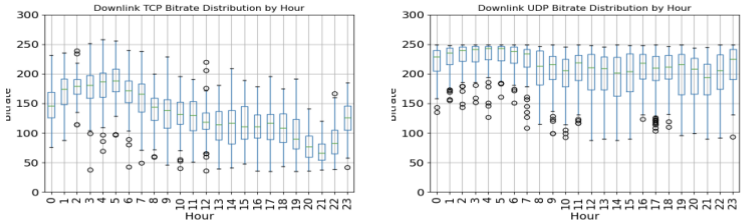

(a) TCP




(b) UDP

Рис .1 Пропускна здатність мережі *Starlink* для *TCP* та *UDP*

Добове коливання бітрейду для протоколу *UDP* складає ±10%, а для протоколу *TCP* близько ±30% (рис.2).




(a) TCP (b) UDP

Рис. 2 Добовий розподіл бітрейту мережі *Starlink*

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Zhukov I., Dolintse B., Balakin S. Improving the Accuracy of Air Navigation Systems for Unmanned Aerial Vehicles. Dependable Systems, Services and Technologies – 2023. – IEEE Xplore, Athens. – P. 1-7.*

УДК 004.056.53(043.2)

**А.В. Ільєнко,**
**О.В. Дубчак**
*Державний Університет «Київський авіаційний інститут», Київ*

# АНАЛІЗ АТАК І ЗАСОБІВ УБЕЗПЕЧЕННЯ DATA LINK LAYER

Згідно з даними дослідницької компанії DataReportal, опублікованими у звіті Digital 2025, кількість користувачів всесвітньої мережі станом на грудень 2024 р. у світі перевищила 5,5 млрд осіб, а в Україні цей показник склав 31,5 млн осіб, при цьому рівень проникнення Інтернет становив 82,4%. [1]

Разом з кількістю санкціонованих користувачів в мережах зростає і кількість кіберзловмисників. Так, відповідно до звіту Держспецзв'язку, у 2024 р. кількість кібератак на Україну зросла на 69,8% та досягла 4315 інцидентів, тоді як в попередньому році було зафіксовано 2541 інцидент. Крім того, спостерігається тенденція до здійснення кібератак на об'єкти критичної інфраструктури, а метою зловмисників стає не тільки викрадення чутливої інформації, але й знищення даних та інформаційних систем. [2]

Зовнішні загрози, такі як DDoS-атаки, залишаються найбільш поширеними. [3] Але захист внутрішньої локальної мережі (Local Area Network, LAN) так само важливий, як і захист периметра мережі. Без безпеки LAN користувачі в організації можуть не мати доступу до мережі, що може значно знизити продуктивність.

Мережева інфраструктура - один з напрямків забезпечення безпеки LAN. Потужність безпеки мережевої інфраструктури часто визначається Data Link Layer - рівнем 2 (канальний рівень) моделі OSI (Open System Interconnection), незалежність якого забезпечує функціональну сумісність та взаємопов'язаність, а частиною його захисту є пом'якшення наслідків атак, таких як: спуфінг MAC-адрес (Media Access Control); маніпулювання STP (Spanning Tree Protocol); переповнення таблиці MAC-адрес; LAN Storm-атаки; атаки VLAN (Virtual LAN). [4-7]

Обидві атаки - підробки MAC-адрес та атаки переповнення таблиці MAC-адрес - можуть бути пом'якшені шляхом налаштування захисту порту на комутаторі.

Атака маніпулювання STP може бути використана для ураження всіх трьох цілей безпеки: конфіденційності, цілісності та доступності. Методи пом'якшення для атаки маніпулювання STP містять включення PortFast, а також Root Guard і BPDU.

LAN Storm-атаки відбуваються, коли пакети заповнюють LAN, створюючи надмірний трафік та знижуючи продуктивність мережі. Їх можна придушити за допомогою Storm control, що запобігає перериванню трафіку в LAN внаслідок широкомовного, багатоадресного або одноадресного Storm на одному з фізичних інтерфейсів

Для пом'якшення VLAN – атаки, зокрема, VLAN hopping attack, - необхідно переконатися, що транкінг включений лише на портах, для яких він потрібний. Крім того, обов'язково відключити узгодження DTP (Dynamic Trunking Protocol) та увімкнути його вручну. Також, мережевий трафік, що проходить через порти або VLAN, можна аналізувати за допомогою аналізатора комутованих портів (Switched Port Analyzer, SPAN). [8]

SPAN зазвичай розгортається при додаванні IDS (Intrusion Detection System) до мережі. Пристрої IDS повинні зчитувати всі пакети в одній або декількох VLAN, а SPAN можна використовувати для отримання пакетів на пристрої IDS. [9]

Висновки. Проведений аналіз атак на Data Link Layer та засобів їх пом’якшення демонструє важливість забезпечення захисту та надійності функціонування мережевої інфраструктури. Як комплексне рішення проблеми захисту Data Link Layer пропонується використання Cisco Meraki MS150 – доповнення до комутаторів Cisco, що керуються Cisco Security Cloud. Дане рішення гарантує засоби безпеки, зокрема, такі, як: інтегрована багатофакторна автентифікація для керування Dashboard; керування доступом на основі ролей (Role-Based Access Control, RBAC); безпека портів (Sticky MAC, MAC Whitelisting); DHCP Snooping, виявлення та блокування, Dynamic ARP Inspection; списки контролю доступу (IPv4 та IPv6 ACLs).[10]

Для цих комутаторів характерна гнучкість сучасного обладнання та потужність Meraki Dashboard, що дозволяє ефективно керувати мережевою інфраструктурою з високим рівнем безпеки.

# ВИКОРИСТАНІ ДЖЕРЕЛА


1. *DataReportal. Digital 2025. [Електронний ресурс] – Режим доступу: https://datareportal.com/reports/digital-2025-local-country-headlines*

2. *Дячук К. У 2024 р. кількість кібератак на Україну зросла. [Електронний ресурс] – Режим доступу: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931#*

3. *Microsoft. Звіт про цифровий захист Microsoft 2024. [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024*

4. *ARP Spoofing: перехоплення даних мережі. [Електронний ресурс] - Режим доступу: https://cyberset.com.ua/network/arp-spoofing-percept-data-mergesecurity/*

5. *Трокоз Є.М. Атаки STP-маніпуляції . [Електронний ресурс] – Режим доступу: http://ten.ztu.edu.ua › article › view*

6. *Marcin Bialy. LAN Security and how it is hacked. [Електронний ресурс] - Режим доступу: https://www.grandmetric.com/lan-security-attacks/*

7. *Andrew Zola. Virtual Local Area Network Hopping. [Електронний ресурс] - Режим доступу: https://www.techtarget.com/searchsecurity/definition/VLAN-hopping*

8. *Cisco Networking Academy. Network Security [Електронний ресурс] - Режим доступу: https://www.netacad.com/*

9. *Дубчак О.В. Використання технології штучного інтелекту для убезпечення комунікаційних мереж/ О.В. Дубчак, Н.К. Гулак// CSNT-2024: XV міжнародна науково-практична конференція, 25-26 квітня 2024:тези доп. - К., 2024 .- С.53-54. [Електронний ресурс] - Режим доступу: https://csnt.nau.edu.ua/files/2024/sbirnyk2024.pdf*

*Stratus. Cisco Meraki Overviewко [Електронний ресурс] - Режим доступу: https://www.stratusinfosystems.com/news/cisco-meraki-ms150-overview/*

УДК 004.056.53

**М.О. Калашник**
*Державний Університет «Київський авіаційний інститут», Київ*

# АДАПТИВНІ ГІБРИДНІ МОДЕЛІ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ДИНАМІЧНИХ IOT МЕРЕЖАХ

Інтернет речей (IoT) охоплює широкий спектр застосувань, створюючи інфраструктуру, вразливу до кіберзагроз. Виявлення аномалій у таких мережах ускладнюється мінливістю трафіку, обмеженими ресурсами пристроїв і браком маркованих даних. Традиційні методи машинного навчання та глибокого навчання часто не справляються з цими викликами, що потребує застосування гібридних адаптивних моделей для підвищення ефективності аналізу IoT-мереж [1].

Основні труднощі виявлення аномалій у IoT включають гетерогенність трафіку, обмежені ресурси пристроїв і відсутність маркованих даних. Використання складних DL-моделей часто ускладнене, а статичні методи неефективні перед динамічними загрозами. Адаптивні гібридні підходи поєднують ML і DL, дозволяючи моделям самонавчатися та швидко адаптуватися до змін у реальному часі [2].

Гібридні моделі інтегрують методи машинного навчання, наприклад, метод опорних векторів (SVM), випадкові ліси, ізоляційні ліси із глибокими нейронними мережами [3], такими як автоенкодери, рекурентні нейронні мережі (RNN), трансформери. Такий підхід дозволяє використовувати автоенкодери для попередньої фільтрації трафіку та визначення відхилень без необхідності маркування даних. Також можна поєднувати CNN для аналізу структурованого мережевого трафіку та LSTM/GRU для виявлення змін у часі. Напівконтрольоване навчання дозволяє обробляти нові типи атак без явних аномалій у вихідних наборах даних.

Адаптивні гібридні моделі можуть бути ефективно застосовані для виявлення аномалій у різних сферах IoT. Вони дають змогу аналізувати поведінку сенсорних пристроїв, оцінювати відхилення від норми та швидко адаптуватися до змін у структурі трафіку. Такі підходи сприяють підвищенню ефективності систем кібербезпеки та зменшенню кількості хибнопозитивних спрацювань.

Впровадження адаптивних гібридних моделей у реальних IoT-

системах потребує оптимізації обчислювальних ресурсів, зокрема використання квантованих моделей та FPGA-прискорення для виконання складних обчислень на пристроях IoT. Реалізація розподіленої обробки через інтеграцію моделей у хмарні сервіси та edge computing сприяє балансуванню навантаження. Інтеграція в існуючі IoT-платформи потребує використання відкритих стандартів для сумісності з комерційними рішеннями.

Адаптивні гібридні моделі демонструють високу ефективність для виявлення аномалій у динамічних IoT-мережах. Їхня здатність до самонавчання, комбінування методів машинного та глибокого навчання дозволяє підвищити точність і швидкість виявлення загроз. Такі підходи сприяють покращенню кібербезпеки в умовах змінних мережевих середовищ, забезпечуючи адаптацію моделей до нових типів атак і змін у поведінці IoT-пристроїв. Подальший розвиток цієї сфери має бути зосереджений на розробці ефективних механізмів оновлення моделей у реальному часі, інтеграції гібридних підходів у розподілені обчислювальні системи, а також на оптимізації їх продуктивності для використання в IoT-інфраструктурі з обмеженими ресурсами. Крім того, важливим напрямом є вдосконалення механізмів виявлення нових типів аномалій у реальному часі, підвищення стійкості моделей до змін у структурі трафіку та забезпечення ефективної обробки великих обсягів даних у децентралізованих IoT-мережах.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. König R., Nikolic J., Wenzel S., Kirchner F. Hybrid learning approaches for anomaly detection in cyber-physical systems. // Journal of Machine Learning Research. — 2019. — Vol. 20(125). — P. 1-29. DOI: https://doi.org/10.5555/3322706.3322723.*

*2. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection. // IEEE Symposium on Security and Privacy. — 2010. — P. 305–316. DOI: https://doi.org/10.1109/SP.2010.25.*

*3. Bridges R. A., Glass K., Cannon A. S. Multi-level anomaly detection on IoT networks using deep learning. // Journal of Cybersecurity. — 2022. — Vol. 8(1). — P. 1-17. DOI: https://doi.org/10.1093/cybsec/tyac009.*

УДК 656.71-047.36(045)

**Є.Є. Карпов**
Державний Університет «Київський авіаційний інститут», Київ

# АЛЬТЕРНАТИВНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ КООРДИНАТ АВТОТРАНСПОРТУ АЕРОПОРТУ БЕЗ GPS

Управління спецавтотранспортом в аеропортах вимагає високої точності навігації та стабільного визначення місцеположення. Однак у складних умовах, таких як радіоелектронна боротьба (РЕБ) [1][2], сильні атмосферні перешкоди або вплив масивних металевих конструкцій, *GPS*-приймачі можуть втрачати зв'язок із супутниками. Це створює ризики для ефективності та безпеки роботи наземних служб. Одним із альтернативних методів визначення координат є використання радіомодуля *SX1280*, який дозволяє вимірювати відстань між об’єктами на основі технології *LoRa* та сигналів із фіксованих наземних станцій [3].

Метою дослідження є аналіз можливості використання радіомодуля *SX1280* для визначення координат спецавтотранспорту в аеропортах у випадках втрати *GPS*-сигналу.

Предметом дослідження є методи альтернативного визначення місцеположення спецавтотранспорту на основі *SX1280*, принципи вимірювання відстані та алгоритми позиціонування.

Проблеми втрати *GPS*-сигналу в аеропортах є:

1. Атмосферні умови – щільна хмарність, грози, снігопади можуть впливати на якість супутникового сигналу.
2. Металеві конструкції – багатопроменеві ефекти та екранування сигналу будівлями, літаками або транспортом.
3. Підземні та закриті приміщення – відсутність прямої видимості супутників у закритих ангарах та тунелях.
4. РЕБ (засоби радіоелектронної боротьби) – навмисне заглушення *GPS*-сигналів або перешкоди від військових засобів зв’язку.

*SX1280* – це радіомодуль з підтримкою зв’язку на частоті 2,4ГГц, який дозволяє вимірювати відстань до інших модулів *SX1280* на основі часу проходження сигналу (*ToF – Time of Flight*). Використання декількох наземних станцій (три та більше) з фіксованими координатами дозволяє розраховувати місцеположення рухомого об'єкта за допомогою трилатерації.

Радіомодуль *SX1280* використовує метод *ToF* [3], який полягає у вимірюванні часу, за який радіосигнал проходить від передавача до приймача і назад. Оскільки швидкість поширення сигналу у повітрі відома (приблизно $3\times10^8$ м/с), можна розрахувати відстань за формулою:

$d=ct/2$, де: $d$ – відстань між двома модулями, *м*; $c$ – швидкість світла, *м/с*; $t$ – час проходження сигналу, *с*.

Основні джерела похибок при вимірюванні *ToF* [3]:

- Багатопроменеве поширення сигналу – відбиття сигналу від перешкод може змінювати виміряний час проходження [4].
- Частотні нестабільності – незначні варіації в тактовій частоті приймача можуть впливати на точність вимірювань [5].
- Атмосферні фактори – зміни температури та вологості можуть впливати на швидкість поширення сигналу [6].

Для мінімізації похибок можна використовувати фільтр Калмана [5], що дозволяє згладжувати шум у вимірюваннях.

Для підвищення ефективності розрахунків координат на сервері можна застосувати такі методи:

- Фільтрація шумів та згладжування сигналів – використання фільтра Калмана [5] або інших адаптивних алгоритмів для попередньої обробки вхідних даних перед розрахунками.
- Розпаралелення обчислень – якщо обробляється велика кількість точок одночасно, можна використовувати багатопотокову обробку або *GPU*-прискорення для матричних операцій.
- Кешування статичних даних – зберігання координат стаціонарних наземних станцій у пам’яті сервера, що зменшує кількість повторних розрахунків і пришвидшує обробку запитів.

Щоб визначити точне положення транспортного засобу, використовується метод трилатерації [1], що передбачає наявність трьох або більше наземних передавачів (маяків) із відомими координатами $(x_1,y_1)$, $(x_2,y_2)$, $(x_3,y_3)$. Якщо відстані до цих маяків позначити як $d_1$, $d_2$, $d_3$, то координати рухомого об'єкта $(x,y)$ можуть бути знайдені шляхом розв’язання системи рівнянь:

$(x-x_1)^2+(y-y_1)^2=d_1^2$

$(x-x_2)^2+(y-y_2)^2=d_2^2$

$(x-x_3)^2+(y-y_3)^2=d_3^2$

*SX1280* компенсує втрату *GPS* у складних умовах аеропортів завдяки технології *ToF*, що забезпечує стабільний моніторинг спецавтотранспорту. Крім того, метод оцінки технічних

характеристик спеціалізованих ієрархічних систем з використанням штучного інтелекту можна застосовувати для аналізу похибок вимірювань, оптимізації алгоритмів фільтрації сигналів і прогнозування роботи системи позиціонування. Використання алгоритмів машинного навчання дозволяє аналізувати похибки вимірювань, оптимізувати роботу фільтрів і покращувати прогнозування роботи системи. Враховуючи можливі похибки, застосування фільтра Калмана дозволить покращити точність розрахунків. Використання наземних станцій та методів трилатерації дає змогу створити ефективну систему позиціонування навіть у складних умовах експлуатації.

ВИКОРИСТАНІ ДЖЕРЕЛА


*1. Літаки у Фінляндії стикалися з масштабними збоями в роботі GPS, в Савонлінні літак не зміг приземлитися – за цим може стояти Росія // Yle News. – 2024. – URL: https://yle.fi/a/74-20015672 (дата звернення: 23.03.2025).*

*2. Світ: літак Finnair не зміг приземлитися в Естонії через перешкоди GPS з боку РФ // Espreso. URL : https://espreso.tv/svit-litak-finnair-ne-zmig-prizemlitisya-v-estonii-cherez-pereshkodi-gps-z-boku-rf (дата звернення: 23.03.2025).*

*3. Design of the SX1280 Ranging Protocol and Result Processing AN1200.50. – Semtech. – URL : https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/2R000000UypY/5mprGH6TIzeLnfosUgj1xK5ftoqDpoCnRk_dzY_jAx4 (дата звернення: 23.03.2025)*

*4. Patwari N., Hero A. O. Using proximity and quantized RSS for sensor localization in wireless networks // IEEE Transactions on Wireless Communications. – 2003. – Т. 2, №3. – С. 374-383.*

*5. Mao G., Anderson B. D., Fidan B. Path loss exponent estimation for wireless sensor network localization // Computer Networks. – 2007. – Т. 51, №10. – С. 2467-2483.*

*6. Dardari D., Conti A., Ferner U., D'Amico A., Win M. Z. Ranging with ultrawide bandwidth signals in multipath environments // Proceedings of the IEEE. – 2009. – Т. 97, №2. – С. 404-426.*

УДК 004.056.53

**С.О. Кашкевич,**
**Є.В. Тупота,**
**С.В. Подельський**
*Державний Університет «Київський авіаційний інститут», Київ*

# БЕЗПРОВІДНІ AD-HOC МЕРЕЖІ: ПРИНЦИПИ САМООРГАНІЗАЦІЇ, ФУНКЦІОНУВАННЯ ТА СФЕРИ ЗАСТОСУВАННЯ

Основним завданням мереж з можливістю самоорганізації передачі даних є: побудова стійкої до відмов мережної інфраструктури; підвищення використання радіо та радіочастотного ресурсу; забезпечення адаптації мереж до дії зовнішніх факторів; зменшення вартості розгортання та функціонування мережі в порівнянні з класичними принципами побудови.

Децентралізована мережа з можливістю самоорганізації складається з маршрутизаторів та мобільних пристроїв, що зв'язані між собою і одночасно виконують функції як клієнта, так і маршрутизатора. На відміну від класичного варіанта побудови безпровідних мереж, де всі клієнти зв'язуються з маршрутизатором та передача даних відбувається лише через нього, у децентралізованій мережі кожен з цих пристроїв може переміщуватися в різних напрямках, при цьому в результаті переміщення розривати та встановлювати нові з'єднання із сусідніми пристроями.

Безпровідні *Ad-hoc* мережі належать до безпровідних мереж, що використовують множину хопів *(MultiHop)* для ретрансляції та здатні працювати без підтримки будь-якої фіксованої інфраструктури.

*Ad-hoc* безпровідні мережі завдяки швидкому та дешевшому розгортанню знаходять застосування в кількох сферах діяльності: військові операції, спільні та розподілені обчислення, пошуково-рятувальні операції під час надзвичайних ситуацій, безпровідні *mesh* мережі, безпровідні сенсорні мережі та безпровідні мережі з гібридною архітектурою.

Спеціальні безпровідні мережі використовуються для встановлення зв'язку між групою солдатів під час тактичних операцій, де неможливо організувати фіксовану інфраструктуру.

У таких середовищах спеціальні безпровідні мережі швидко забезпечують необхідний механізм зв'язку. Іншим прикладом застосування може бути координація руху військових об'єктів на високій швидкості, таких як літаки або військові кораблі.

Також однією галуззю, де можуть використовуватися *Ad-hoc* мережі є мережі спільного та розподіленого обчислення, де вимагається швидка побудова комунікаційної інфраструктури для з'єднання вузлів з мінімальними налаштуваннями. Цей вид комунікацій, на відміну від військових мереж спеціального призначення, не має таких вимог до забезпечення захисту з'єднання але потребує багатоадресної передачі даних та гарантованої доставки даних, а передача потокових мультимедійних даних також вимагає підтримки безперервного зв'язку в режимі реального часу.

Оскільки спеціальні безпровідні мережі вимагають мінімальної початкової конфігурації для їх функціонування, то час на побудову мережі дуже малий або взагалі не потрібен на побудову мережі для її функціонування.

Іншим видом безпровідних мереж з можливістю до самоорганізації є *mesh* мережі. *Mesh* мережі є спеціальними безпровідними мережами, що використовуються для забезпечення надлишкової інфраструктури зв'язку як для мобільних, так і для фіксованих вузлів, без обмежень повторного використання спектру і вимог мережного планування стільникових мереж.

Топологія *mesh* мережі забезпечує багато альтернативних шляхів для передачі даних між джерелом і адресом призначення, призводячи до швидкої реконфігурації шляху, коли існуючим шляхом неможливо передати повідомлення.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Шишацький А.В., Кашкевич С.О., Вакуленко Ю.В., Протас Н. М., Воропай В.В. Аналіз характеристик протоколів адаптивної маршрутизації в телекомунікаційних мережах, що самоорганізовуються. The main directions of the development of scientific research: proceedings of the XV International Scientific and Practical Conference (Helsinki, Finland, April 18-21, 2023). 2023. P. 390-399.*

УДК 004.22

**Р.Є. Корчемний**
*Державний Університет «Київський авіаційний інститут», Київ*

# ІНФОРМАЦІЙНИЙ МОДУЛЬ ПАСИВНОЇ СИСТЕМИ НАВЕДЕННЯ: РЕАЛІЗАЦІЯ АЛГОРИТМУ MUSIC

Алгоритм MUSIC забезпечує всі необхідні характеристики для створення інформаційного модуля пасивної системи наведення на радіоелектронне випромінювання. Його висока точність, стійкість до завад, здатність обробляти сигнали від кількох джерел одночасно та сумісність із реальними обчислювальними системами роблять його оптимальним вибором для побудови надійних і високопродуктивних систем. Розроблена архітектура модуля включає приймач сигналу, блок обробки, модуль визначення напрямку та інтерфейс управління, що забезпечує точне визначення координат джерел випромінювання навіть в умовах високого рівня шуму.

Завдяки реалізації алгоритму MUSIC та використанню ефективних методів обробки сигналів у реальному часі, модуль здатний працювати у складних середовищах, зберігаючи високу точність і продуктивність. Процес обробки сигналів дозволяє не лише визначати напрямки на джерела радіоелектронного випромінювання, але й відокремлювати кілька джерел одночасно, що робить цей модуль універсальним інструментом для навігаційних, тактичних та розвідувальних завдань.

Обчислювальні та апаратні аспекти реалізації інформаційного модуля забезпечують його ефективну роботу, швидку адаптацію до змін навколишнього середовища та точне визначення параметрів сигналу. Використання високопродуктивних графічних процесорів (GPU) і цифрових сигнальних процесорів (DSP) дозволяє суттєво збільшити швидкість обробки, а застосування нейронних мереж для адаптивної фільтрації та когерентної інтеграції підвищує надійність та точність отриманих даних.

Додатково, інтеграція алгоритму MUSIC із методами синтетичної апертури (SAR) та технологіями глибокого навчання дозволяє підвищити просторову роздільну здатність і забезпечити автоматичне розпізнавання та класифікацію сигналів. Це особливо важливо для моніторингових систем, які працюють у режимі реального часу, зокрема в безпілотних авіаційних системах та

автономних навігаційних комплексах.

Окрім цього, перспективним напрямком розвитку пасивних систем наведення є впровадження технологій квантової обробки сигналів та використання розподілених мереж датчиків, що значно покращить можливості виявлення слабких і малопомітних джерел випромінювання. У поєднанні з алгоритмом MUSIC, ці методи дозволять зменшити рівень помилкових спрацьовувань та підвищити стійкість системи до навмисних перешкод.

Таким чином, вдосконалення інформаційного модуля за рахунок алгоритму MUSIC, сучасних обчислювальних технологій та штучного інтелекту відкриває широкі можливості для створення ефективних пасивних систем наведення, здатних працювати в умовах складного електромагнітного середовища та забезпечувати точне визначення місцеположення джерел випромінювання.

## ВИКОРИСТАНІ ДЖЕРЕЛА


1. *URL: https://ieeexplore.ieee.org/document/6631538.*
2. *URL: https://www.mathworks.com/help/phased/ug/direction-of-arrival-estimation.html.*
3. *URL: https://www.researchgate.net/publication/270594303_Overview_of_Passive_Radar_Systems_and_Applications.*
4. *URL: https://www.researchgate.net/publication/331882259_Performance_comparison_of_MUSIC_and_ESPRIT_algorithms_in_DOA_estimation.*

УДК 004.775:004.65:004.67:005.32:005.92

**А.М. Леперт**
*Державний Університет «Київський авіаційний інститут», Київ*

# ІНТЕРАКТИВНИЙ ВЕБЗАСТОСУНОК ДЛЯ КЕРУВАННЯ ЗАВДАННЯМИ

Сучасний ритм життя вимагає ефективного управління завданнями та часом, що сприяє продуктивності як у професійній, так і в особистій діяльності. Односторінкові вебзастосунки (SPA) стали популярними завдяки швидкому відгуку на дії користувачів та зручному інтерфейсу, що робить їх ідеальним рішенням для планування завдань [1,2].

Метою розробки інтерактивного вебзастосунку є забезпечення користувачів ефективним інструментом для створення, редагування, видалення та управління завданнями. Для реалізації проєкту використано HTML5 для структурування контенту, CSS3 для оформлення та JavaScript для інтерактивності. Фреймворк React обрано завдяки його компонентному підходу та ефективному управлінню станом. Firebase використовується для збереження даних і їх синхронізації в реальному часі.

Функціонал вебзастосунку включає можливість встановлення пріоритетів, дедлайнів і фільтрації завдань за різними критеріями. Інтуїтивний інтерфейс та швидка взаємодія без перезавантаження сторінки забезпечують зручність використання. Завдяки інтеграції з Firebase дані залишаються доступними з будь-якого пристрою, що робить цей вебзастосунок надійним і практичним інструментом для керування завданнями.

На рис. 1 наведено блок-схему роботи застосунку. Опис блок-схеми:

1. Початок. Користувач розпочинає роботу з вебаплікацією.
2. Додавання задач. Користувач має можливість додати задачу:

- якщо так, відбувається зміна статусу задачі, і далі — стоп (тобто завершення поточної операції).
- якщо ні, переходимо до наступного етапу.

3. Групування задач. Якщо задачі групуються:

- якщо так, відбувається початок роботи, і потім — стоп.
- якщо ні, переходимо до наступного кроку.

4. Видалення. Якщо задачі не додано й не згруповано — вони

видаляються.

5. Повернення до початку. Після завершення будь-якої дії (зміни статусу, початку роботи або видалення), цикл повертається до початку, що вказує на інтерактивність та повторюваність процесу.

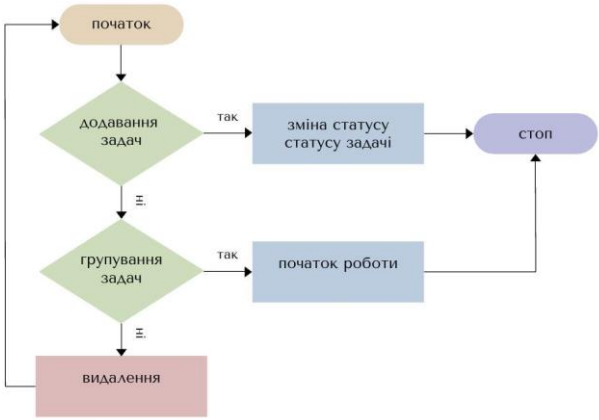



Рис.1 Блок-схема роботи

Ця схема демонструє основну логіку інтерфейсу вебаплікації, де користувачі можуть додавати задачі, групувати їх, змінювати статус, розпочинати виконання, або видаляти задачі.

Блок-схема добре ілюструє гнучкий підхід до взаємодії з системою в реальному часі.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Архітектура вебзастосунків 2024.*
*URL: https://robotdreams.cc/uk/blog/567-arhitektura-vebzastosunkiv?utm*
*2. Створення інтерактивних веб-сторінок за допомогою обробників подій JavaScript.*
*URL: https://webcraftingcode.com/uk/osnovy-javascript/stvorennia-interaktyvnykh-veb-storinok-za-dopomohoiu-obrobnykiv-podiy-javascript .*

УДК 004.056.53

**М.В.Лінник**
*Державний Університет «Київський авіаційний інститут», Київ*

# ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ НА ЗОБРАЖЕННІ

Штучний інтелект (ШІ) стає невід’ємною частиною сучасних технологій, особливо в авіаційній галузі, де точність, оперативність та ефективність є ключовими факторами успіху. Одним із найперспективніших напрямків застосування ШІ є розпізнавання об’єктів на зображеннях. Ця технологія має величезний потенціал для покращення безпеки, оптимізації процесів та підвищення якості послуг у авіаційній індустрії.

Автоматизація перевірки багажу та виявлення небезпечних предметів є одним із найбільш актуальних завдань у сфері авіаційної безпеки. ШІ може аналізувати рентгенівські знімки багажу пасажирів у реальному часі, автоматично виявляючи потенційно небезпечні предмети, такі як зброю, вибухові речовини або заборонені матеріали. Це не лише прискорює процес перевірки, але й зменшує ймовірність помилок через людський фактор.

Моніторинг технічного стану літаків також є важливим застосуванням ШІ. За допомогою аналізу зображень деталей літаків, отриманих за допомогою дронів, камер або спеціального обладнання, ШІ може виявляти тріщини, корозію або інші пошкодження на ранніх стадіях. Це дозволяє проводити профілактичний ремонт та запобігати серйозним поломкам, що є критичним для забезпечення безпеки польотів.

Контроль повітряного простору та виявлення загроз також можуть бути покращені завдяки ШІ. Системи, що аналізують супутникові знімки та радарні дані, допомагають виявляти несанкціоновані об’єкти, такі як дрони або малі літаки, які можуть становити загрозу для регулярних рейсів. Також ШІ може допомогти виявляти непередбачувані метеорологічні умови, що впливають на безпеку польотів.

Покращення системи навігації та приземлення також можливе завдяки ШІ. Аналіз зображень з камер літаків під час польоту або приземлення дозволяє виявляти перешкоди на смузі приземлення або погодні умови, які можуть вплинути на безпеку польоту. Це

допомагає пілотам приймати більш обґрунтовані рішення та запобігати можливим інцидентам.

Виявлення порушень правил безпеки є ще одним важливим застосуванням ШІ. Системи, що аналізують відеозаписи з камер спостереження, можуть автоматично виявляти підозрілу поведінку пасажирів або персоналу на території аеропорту. Це допомагає запобігти можливим інцидентам та покращити загальну безпеку.

Покращення якості обслуговування пасажирів також можливе завдяки ШІ. Аналіз зображень черг на пунктах контролю та пропозиція оптимальних маршрутів для пасажирів дозволяє зменшити час очікування та покращити їхній досвід. Це особливо важливо в умовах великих аеропортів, де рух пасажирів може бути складним та хаотичним.

Оптимізація управління аеропортами є ще одним важливим напрямком застосування ШІ. Аналіз відеозаписів з камер спостереження дозволяє контролювати рух пасажирів, багажу та наземного обладнання. Це допомагає оптимізувати логістику, скорочувати час простою літаків та покращувати загальну ефективність роботи аеропорту.

Впровадження штучного інтелекту для розпізнавання об’єктів на зображеннях має величезний потенціал у авіаційній галузі. Воно дозволяє покращити безпеку, оптимізувати процеси та підвищити конкурентоспроможність компаній. Автоматизація та точність, які забезпечує ШІ, роблять його незамінним інструментом для сучасної авіації.

## ВИКОРИСТАНІ ДЖЕРЕЛА


1. *Automating Prohibited Items Detection with AI* - *https://mpost.io/singapore-changi-airport-trials-ai-driven-luggage-screening-system-to-enhance-security/*

2. *Штучний інтелект та авіація* *https://utc-aviator.com/iskusstvennyj-intellekt-i-aviatsiya*

УДК 004.93’1:629.735

**Ю.В. Лукаш**
*Державний університет "Київський авіаційний інститут", Київ*

# ІНТЕГРАЦІЯ ФУНКЦІЇ СЛІДУВАННЯ ЗА ОБ’ЄКТОМ НА СИМУЛЯТОРІ БПЛА SITL З ВИКОРИСТАННЯМ ПРОТОКОЛУ MAVLINK

За останні роки активного розвитку, поширення та використання набувають різні алгоритми розпізнавання об’єктів, комп’ютерного зору та нейронних мереж на базі відео потоку для використання різноманітних цільових задач на БпЛА.

Один з напрямів таких досліджень та розробок є реалізація автономного слідування за об’єктом БпЛА літакового або роторного типу.

Для реалізації та подальшого удосконалення такого методу в роботі [1] запропонована архітектура комплексу БпЛА з комп’ютером-компаньйоном на борту. Основні елементи такої архітектури можна – це польотний контролер безпосередньо на БпЛА, камера для захоплення зображення, та додатковий одноплатний комп’ютер на борті БпЛА, котрий має забезпечувати автономне керування коптером.

На попередньому етапі дослідження було реалізовано програмну частину, яка успішно запускається на Raspberry Pi 4, читає відео з під’єднаної камери та аналізує це відео і на виході формує вектор зміщення від центру шуканого об’єкту. Цей вектор в подальшому повинен перетворюватися у напрям рух літального апарату та формувати керуючі команди, щоб направити БпЛА в бажану точку.

Порівнявши різні вбудовані в бібліотеку OpenCV алгоритми трекінгу – обрано як найбільш підходящий по стабільності та швидкодії алгоритм CSRT. Робота алгоритму трекінгу покращена додатковими перевірками для фільтрування нетипових спрацювань. Також додано функціонал, котрий реалізує повторне захопленню цілі у разі її втрати алгоритмом.

Наступним кроком дослідження стало інтеграція програмної частини з командами управління польотним контролером та передача команд з використання протоколу MAVLink. Реалізовано на мові програмування Python.

MAVLink (Micro Air Vehicle Link) є сучасним легковаговим

протоколом обміну телеметрією між БпЛА та зовнішніми модулями. Він підтримується більшістю популярних автопілотів, включаючи ArduPilot та PX4. У межах проекту реалізовано надсилання керуючих команд з трекера до польотного контролера через MAVLink, використовуючи Python-бібліотеку MAVSDK.

Для перевірки коректності роботи команд керування програмна частина трекінгу та формування команд була інтегрована з симулятором БпЛА SITL, та проведено тестові запуск, які візуально підтвердили, що на базі вхідного відео програма приймає рішення та віддає команди керування дрону, а він змінює напрям свого руху.

Передача даних може здійснюватися через UART-з'єднання або TCP/UDP-порт, в залежності від типу платформи. В межах інтеграції були успішно випробувані обидва типи з'єднання. З симулятором – UDP з'єднання. А тестове підключення до польотного контролера для зчитування телеметрії, без команд керування та зльоту – UART.

Подальшим кроком інтеграції проекту планується встановлення Raspberry Pi безпосередньо на БпЛА з польотним контролером Pixhawk та проведення експериментів і оцінці стабільності тримання цілі та слідування за об'єктом в автономному режимі без стороннього втручання оператору.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Жуков І.А., Лукаш Ю.В. Використання алгоритму трекінгу об'єкту по відеозображенню для реалізації автономної функції слідування за ціллю для БпЛА – 2024 – Проблеми інформатизації та управління, №2 (78), с.14-17 - DOI: 10.18372/2073-4751.78.18956*

*2. Khan, N.A. et al. Emerging use of UAV's: secure communication protocol issues and challenges. Drones in Smart-Cities: Security and Performance. 2020. pp. 37-55. DOI: 10.1016/B978-0-12-819972-5.00003-3*

*3. Alzubaidi, L., Bai, J., Al-Sabaawi, A., etal. A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. – 2023 – Journal of Big Data, 10 (1), art. no. 46 - doi: 10.1186/s40537-023-00727-2*

УДК 004.056.53

**Д.М. Маршалок**
*Державний Університет «Київський авіаційний інститут», Київ*

## SOFTWARE FOR CAPTURING AERIAL TERRAIN PHOTOGRAPHY WITH A DJI QUADCOPTER

DJI is one of the most successful companies in the UAV world. The company occupies about 75% of the global UAV market for private consumers [1]. DJI is also a leading company in the corporate UAV sector. Notably, DJI products have been widely adopted by the military for reconnaissance and combat operations against adversaries. Internet sources indicate that about 95% of all drones used by the Ukrainian military are DJI and Autel models. [2].

All the programs used with DJI drones share a major drawback – the lack of pre-programmed routes. Even if a terrain mapping feature is available, it cannot be utilized without a stable GPS signal.

Another significant issue is the imposed safety restrictions on UAV flights, such as limitations on drone altitude and the inability to fly in certain areas.

To address this, a new application was proposed to enable the creation of static routes for terrain photography using a DJI quadcopter. These routes would function independently of the GPS signal. Additionally, the application would allow for the merging of captured images into a unified map.

The OpenCV (Open Source Computer Vision) library was utilized for image processing.

The DJITelloPy library was selected for creating flight scripts for DJI drones. Originally designed for controlling the Tello drone via Python, it is relatively easy to use, even for beginners, while providing a robust set of features for drone control and interaction. The library operates using the DJI Onboard SDK protocol, which is compatible with most DJI drones.

This library greatly simplifies programming by providing simple one-line functions to control the drone in various ways, such as: take off, land, move forward, backward, right, left, up, down, and rotate clockwise and counterclockwise [3].

The application has two main windows. The first window is responsible for creating a drone flight script; the second window provides access to the means of combining photos obtained from the

drone.

Elements of the first window:

1. Selection of the drone flight model.
2. Choosing a drone model.
3. Selection of the shooting area.
4. The possibility of departure from the starting point.
5. Demonstration of the drone flight model.
6. Calculation of the shooting size.
7. Demonstration of a drone model.
8. Creating a drone flight script.
9. Switching to another window that is responsible for working with images.

Elements of the second window:

1. Selection of the drone flight model.
2. Demonstration of a drone flight model.
3. Creating a map from images obtained from a drone.
4. Creating a map from third-party images.
5. Print the received images.

Thus, the developed software enables users to create flight scripts for various DJI drones and merge the captured images into a unified map.

## REFERENCES LIST

*1. Підгайна Є. Галузі майбутнього: як безпілотники підкорюють Україну [Електронний ресурс] / Євгенія Підгайна // Mind. – 2018. – Access mode: https://mind.ua/publications/20187343-galuzi-majbutnogo-yak-bezpilotniki-pidkoryuyut-ukrayinu.*

*2. Перша у світі війна дронів іде в Україні: як БПЛА змінили бойові дії у 2022-2024 роках [Електронний ресурс] / Злата Олександр // Фокус. – 2024. – Access mode: https://focus.ua/uk/digital/626579-persha-u-sviti-viyna-droniv-ide-v-ukrajini-bpla-zminili-boyovi-diji-u-2022-2024-rokah.*

*3. Sai Krishna L. Y. Enhancing path following drone using image-based sensor matrix / L. Y. Sai Krishna, T. P. Frazer. – Karlskrona, Blekinge Institute of Technology, 2023. – 36 с.*

УДК 004.056

**А.О.Мельник**
*Державний Університет «Київський авіаційний інститут», Київ*

# СУЧАСНІ ПІДХОДИ ДО АНАЛІЗУ ДАНИХ І МАШИННОГО НАВЧАННЯ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Машинне навчання відіграє ключову роль у процесі обробки та аналізу великих обсягів даних, дозволяючи виявляти закономірності, прогнозувати майбутні події та автоматизувати складні процеси. У сучасних комп'ютерних системах аналіз даних здійснюється за допомогою різних методів.

Описовий аналіз використовується для виявлення основних характеристик даних, таких як середнє значення, медіана та стандартне відхилення. Наприклад, у сфері фінансів описовий аналіз застосовується для оцінки середньої дохідності акцій або визначення рівня волатильності ринку. Діагностичний аналіз дозволяє визначати причинно-наслідкові зв’язки між змінними. Прогнозний аналіз застосовується для побудови моделей, що дають змогу передбачати подальший розвиток подій на основі історичних даних. У роздрібній торгівлі такі методи використовуються для прогнозування попиту на товари та оптимізації запасів. Приписувальний аналіз спрямований на пошук оптимальних рішень шляхом аналізу альтернативних сценаріїв. Наприклад, у сфері логістики цей метод допомагає визначити найкращі маршрути доставки для мінімізації витрат і часу.

Сучасні підходи до машинного навчання охоплюють як класичні алгоритми, так і новітні методики. До традиційних методів належать лінійна та логістична регресія, метод опорних векторів, дерева рішень і випадкові ліси. Наприклад, логістична регресія широко використовується в кредитному скорингу для прогнозування ймовірності дефолту позичальника. Глибоке навчання базується на використанні нейронних мереж, зокрема згорткових, що ефективні для обробки зображень, та рекурентних, які працюють із послідовними даними. Наприклад, згорткові нейронні мережі використовуються в системах автономного водіння для розпізнавання дорожніх знаків і пішоходів, а рекурентні мережі застосовуються в голосових асистентах, таких як Siri або Google Assistant, для обробки запитів користувачів. Методи ансамблевого навчання, такі як градієнтний бустинг

(XGBoost, LightGBM) і випадковий ліс, поєднують кілька слабких моделей для покращення точності результатів. Наприклад, XGBoost ефективно використовується в системах виявлення шахрайства з кредитними картками. Автоматизоване машинне навчання (AutoML) спрощує процес створення моделей, зокрема через автоматичний підбір гіперпараметрів та оптимізацію архітектури.

Машинне навчання та аналіз даних широко використовуються в різних сферах комп'ютерних систем. У галузі кібербезпеки алгоритми ML допомагають виявляти аномалії та загрози, наприклад, аналізуючи мережевий трафік для виявлення підозрілих активностей. В обробці природної мови вони застосовуються для аналізу тексту, розпізнавання мови та автоматичного перекладу, як у випадку Google Translate. У комп'ютерному зорі використовуються для розпізнавання об'єктів і біометричної ідентифікації, наприклад, для розпізнавання облич у смартфонах. Рекомендаційні системи базуються на ML-моделях для персоналізації контенту в стримінгових сервісах, таких як Netflix та YouTube, а також в інтернет-магазинах, як-от Amazon, для пропозиції товарів на основі історії покупок користувача.

Розвиток методів аналізу даних і машинного навчання суттєво впливає на вдосконалення комп'ютерних систем. Постійне покращення алгоритмів та впровадження нових методик відкривають можливості для підвищення ефективності в таких галузях, як медицина, фінанси, штучний інтелект та автоматизація виробництва. Наприклад, в онкології алгоритми глибокого навчання застосовуються для аналізу медичних знімків, що дозволяє раннє виявлення пухлин. У фінансовій сфері нейронні мережі використовуються для алгоритмічної торгівлі, допомагаючи прогнозувати рух ринку та знаходити прибуткові можливості. Удосконалення цих технологій сприяє глибшому розумінню даних і створенню інноваційних рішень, що змінюють світ.

УДК 004.72.5

**В.В. Нечипорук,**
**І. В. Брановицька,**
**М.Ю. Войтех**
*Державний університет «Київський авіаційний інститут», Київ*

# АНАЛІЗ МЕТОДІВ МАРШРУТИЗАЦІЇ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

Програмно-конфігурована мережа *(Software-defined Networking)* – мережа передачі даних, в якій рівень управління мережею відділений від пристроїв передачі даних і реалізується програмно, одна з форм віртуалізації обчислювальних ресурсів.

Головна мета *SDN* є відокремлення рівня додатків від рівня управління і рівня управління від рівня передачі даних. Таким чином, можна значно спростити складність фізичних пристроїв, оскільки виконування логічних функції повністю переноситься на вищий рівень. Це не тільки здешевлює фізичні пристрої, а й покращує надійність і спрощує управління мережі в цілому. Тепер, замість маршрутизаторів можна використовувати звичайні комутатори. Для адміністратора мережі буде значно легше контролювати мережу в цілому. Також, це дозволяє абстрагуватися від реалізації кожного конкретного пристрою, оскільки рівень управління зв'язується з рівнем даних через стандартний інтерфейс. А це, в свою чергу, значно спрощує взаємодію між пристроями різних виробників, і зменшує час налаштування і підготовки або ремонту всієї мережі. Окрім того, така побудова мережі значно прискорює створення нових мережевих додатків. Оскільки для взаємодії рівнів додатків і управління також використовується стандартний інтерфейс, програмісту більше не потрібно думати про те, яким саме чином можна передавати команди і запити до мережі.

Для забезпечення надійного управління в програмно-конфігурованих інформаційних мережах, важливо використовувати відповідні протоколи маршрутизації. Протоколи маршрутизації призначені для автоматичної побудови таблиць маршрутизації, які використовуються для просування пакетів даних. Алгоритми маршрутизації можна умовно розділити на дві великі групи: одношляхова маршрутизація і багатошляхова. При одношляховій маршрутизації передача інформації здійснюється по одному каналу

зв'язку, при багато шляховій – використується кілька маршрутів до одного вузла призначення. Однією з найважливіших вимог, що висуваються до протоколів маршрутизації, є надійність і відмовостійкість. Ці критерії ефективно задовольняють методи багатошляхової маршрутизації (*multipath routing*). З цієї причини розробці і дослідженню алгоритмів передачі даних одночасно по декількох маршрутах присвячено безліч наукових робіт, тому що вона забезпечує стабільність, балансування навантаженням, запобігання перевантажень і оптимальне використання ресурсів мережі.

Динамічні протоколи засновані на лавинних алгоритмах маршрутизації і алгоритмах маршрутизації від джерела і здатні динамічна реагувати на зміну топології мережі. Одним з таких протоколів є *Ad hoc On Demand Distance Vector*. Динамічні протоколи маршрутизації, що застосовуються в даний час в обчислювальних мережах, діляться на три групи, кожна з яких пов'язана з одним з наступних типів алгоритмів: дистанційно-векторні протоколи *(Distance Vector Algorithms, DVA*); протоколи стану каналу (*Link State Algorithms, LSA*); гібридні протоколи.

Отже, використання різних методів багатошляхової маршрутизації в інформаційних технологіях має великий потенціал і допомагає вирішити проблеми, що зустрічаються в класичних підходах до організації мереж, зокрема зменшити витрати на організацію мережі за рахунок використання більш простих пристроїв і спростити контроль за мережею, за рахунок чіткого відокремлення рівня даних і рівня управління.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Нечипорук В.В., Кашкевич С.О., Голего Н.М. Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж. XIX Міжнародна науково-практична конференція «Innovative approaches to solving scientific problems», 16-19 травня 2023 р., Токіо, Японія С. 454-458.*

УДК 004.93

**О.П. Нечипорук**,
**І-Ф.Ф. Кашкевич**,
**О.І. Ластівка**
*Державний університет «Київський авіаційний інститут», Київ*

# МЕТОДИКА ОЦІНКИ АДАПТИВНОСТІ АЛГОРИТМІВ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ НА ОСНОВІ НЕЧІТКИХ КОГНІТИВНИХ МОДЕЛЕЙ

Методика оцінки адаптивності алгоритмів в інформаційних технологіях складається з наступної послідовності дій:

1. Введення вихідних даних. На даному етапі вводяться вихідні дані що наявні про об'єкт, що підлягає аналізу. Проводиться ініціалізація базової моделі стану об'єкту.

2. Виявлення факторів та зв'язків між ними.

3. Побудова НКМ (нечіткої когнітивної моделі).

НКМ полягає в завданні структурних взаємозв'язків (у вигляді відображаються часових лагів) між концептами НКМ, зважених нечіткими значеннями їх впливу один на одного. В зазначеній роботі в якості НКМ $FS_i$, що реалізують нечіткі темпоральні перетворення $F_i$, пропонуються модифіковані моделі *ANFIS*-типу *(Adaptive Neuro-Fuzzy Inference System).* НКМ забезпечують формування, зберігання і виведення прогнозованих нечітких значень відповідних компонентів багатовимірного часового ряду з необхідними для НКМ часовими затримками.

Вхідні темпоральні нечіткі змінні моделі $FS_i$ концепту $C_i$ пов'язані з вихідними темпоральними нечіткими змінними тих концептів, які надають на концепт $C_i$ безпосередній вплив. При цьому вхідні темпоральні нечіткі змінні $C_i$ попередньо "зважуються" відповідними нечіткими ступенями впливу, на підставі чого здійснюється наступне перетворення:

$$\tilde{s}_j^{\left(t-l_i^j\right)} = \left( w_{ij}^{\left(t-l_i^j\right)} \mathrm{T}\, \tilde{s}_j^{\left(t-l_i^j\right)} \right), l_i^j = 0,\ldots, L_i^j, \tag{1}$$

Вихідні ж темпоральні нечіткі змінні моделі $FS_i$ концепту $C_i$ призначені для формування, зберігання і виведення прогнозованих значень $i$-го компонента багатовимірного часового ряду, відповідних часовим лагам. Для побудови нечітких компонентних темпоральних моделей $FS_i$ можуть бути використані як апріорні

відомості про компоненти багатовимірного часового ряду, що є в базі знань, так і дані, отримані в результаті оцінювання або вимірювань.

$$\alpha_p = \min \mu_{\tilde{L}}\left(\tilde{s}_1^{'(t-1)}\right), \mu_{\tilde{L}}\left(\tilde{s}_3^{'(t-3)}\right), \mu_{\tilde{M}}\left(\tilde{s}_4^{'(t-3)}\right), \mu_{\tilde{M}}\left(\tilde{s}_5^{'(t-3)}\right), \mu_{\tilde{H}}\left(\tilde{s}_1^{'(t-3)}\right). \quad (2)$$

Далі активізують укладення відповідних правил відповідно до ступенями істинності їх передумов на основі операції імплікації (тут, імплікації Мамдані - операції *min*-активації)

$$\mu_{\tilde{M}}\left(\tilde{s}_1^{'(t)}\right) = \min\left(\alpha_p, \tilde{M}\right). \quad (3)$$

Після чого здійснюється операція *max*-диз'юнкції, акумулюючи активізовані укладення всіх правил моделі:

$$\tilde{s}_1^{(t)} = \max\left(\mu_{\tilde{M}}\left(\tilde{s}_1^{'(t)}\right), ..., \mu_{\tilde{M}}\left(\tilde{s}_1^{'(t)}\right), ..., \mu_{\tilde{H}}\left(\tilde{s}_1^{'(t)}\right)\right). \quad (4)$$

Далі відбувається нормалізація, зберігання і виведення нечітких значень вихідних змінних моделі з необхідними для НКМ часовими затримками

$$\tilde{s}_{1(norm)}^{(t)} = Z^0\left(\tilde{s}_1^{(t-1)}\right), \tilde{s}_{1(norm)}^{(t-2)} = Z^{-1}\left(\tilde{s}_1^{(t-1)}\right). \quad (5)$$

4. Навчання штучних нейронних мереж (ШНМ).

5. Прогнозування стану об'єкту аналізу.

Багатовимірний аналіз і прогнозування стану складної системи/процесу виконується на основі структурно і параметрично налаштованої НКМ.

ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Нечипорук О.П., Кашкевич С.О., Дегтяр Ю.В. Дослідження та аналіз пропускної здатності каналів передачі в телекомунікаціях. XX Міжнародна науково-практична конференція «Technologies, innovative and modern theories of scientists», 23-26 травня 2023 р., Грац, Австрія С. 495-499.*

*2. Volodymyr Koval, Olena Nechyporuk, Andrii Shyshatskyi, Oleksii Nalapko, Oleh Shknai, Yevhen Zhyvylo, Viktor Yerko, Borys Kreminskyi, Oleksandr Kovbsiuk, Anton Bychkov. (2023). Development of a method of complex analysis and multidimensional forecasting of the state of intelligence objects. Eastern-european Journal of Enterprise Technologies, 31-41. DOI: https://doi.org/10.15587/1729-4061.2023.276168.*

УДК 004.94

**N.V. Pashchenko**
*State University "Kyiv Aviation Institute", Kyiv*

## VIRTUAL REPRESENTATIONS OF PHYSICAL SYSTEMS: ANALYSIS OF DIGITAL TWINS

A digital twin is a virtual representation of a physical object or system that is dynamically updated based on real-time data received via the Internet of Things (IoT). Its functioning involves the use of machine learning methods to support the decision-making process. Integrated sensors located on a physical object collect operational data that is transferred to a virtual model. This allows you to get a holistic view of the state and operation of the physical object in real conditions.

A digital twin is a key tool for analyzing not only the current functioning of the system but also predicting its future behavior. Combining sensor data with other sources of information helps to develop analytical models that improve the accuracy of forecasts. This technology is used to model and optimize the operation of energy facilities, transportation systems, etc. In addition, digital twins are actively used to reproduce technological processes in order to collect data necessary to assess their efficiency.

One of the key advantages of digital twins is the ability to predict the behavior of products and processes by analyzing real-time data and conducting virtual simulations. To improve the accuracy of forecasts and optimize operational efficiency, digital twins integrate artificial intelligence, software analytics and the Internet of Things technologies, which is in line with the Industry 4.0 concept. The use of this technology helps to strengthen strategic technological trends, minimize the costs associated with possible failures of physical facilities, and provides the ability to test processes and services using advanced analytics, forecasting and monitoring methods.

Simulation and modeling, along with digitization and virtualization as key technologies in the context of Industry 4.0, have radically changed the implementation of engineering projects.

A digital twin of a product includes a geometric and structural model of an object, a set of design data for parts, assemblies, and products in general, mathematical models that describe all physical processes occurring in the product, information about the manufacturing and assembly processes of individual elements and the product as a whole,

and a product life cycle management system. A digital twin is used at all stages of the product life cycle, including design, production, operation, and disposal.

Classification of product twins: Digital Twin Prototypes (DTP), Digital Twin Instances (DTI), and Digital Twin Aggregates (DTA). Classification of production system twins: DT of a production system, a production line, a specific asset in a production line.

One of the main tools of digital twins is modeling. A model allows you to perform calculations, predict failures, and optimize behavior before applying it to a physical object. There are three main approaches to modeling: fundamental modeling, data-driven modeling, and hybrid modeling.

Due to the different nature and level of integration of digital twin concepts, the set of technologies required to integrate them differs significantly. Commonly mentioned technologies include, but are not limited to, modeling methods (e.g., discrete event simulation, continuous simulation, etc.), communication protocols (OPC-UA, MQTT, etc.).

The concept of a digital twin remains relatively new and dynamically developing, but has already gained wide practical application. Today, there are a significant number of successful cases of its integration that demonstrate the effectiveness of this technology. The introduction of digital twins helps to improve safety, optimize operating costs, introduce predictive maintenance, and provide a reasonable assessment of the life cycle and effectiveness of conceptual solutions.

## REFERENCES

*1. Negri E., Fumagalli L., Marco M. A Review of the Roles of Digital Twin in CPS-based Production Systems. - 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, Procedia Manufacturing. – 2021. – Vol. 11. – P. 939–948.*

*2. Digital Twins for Industrial Applications. Definition, Business Values, Design Aspects, Standards And Use Cases. An Industrial Internet Consortium White Paper. - Version 1.0. – 2020 - 19 pages.*

УДК 004.45:629.735-519(043.2)

**М.К. Печурін,**
**М.А. Сіренко**
*Державний Університет «Київський авіаційний інститут», Київ*

# ПОЧАТКОВЕ НАЛАШТУВАННЯ НЕЙРОКОМП'ЮТЕРА ЗА ПОКАЗНИКОМ ЕНЕРГОСПОЖИВАННЯ

В умовах активного фокусування великого загалу комп'ютерних інженерів вітчизняної авіаційної сфери на проблему створення телекомунікаційної інфраструктури автономних комплексів БПЛА, особлива увага приділяється системам, де обчислювальне середовище (нейрокомп'ютер) утворюється взаємодіючими елементарними обчислювальними (нейро)компонентами, розміщеними на рухомих (авіаційних) апаратах. При цьому, належна увага приділяється таким системам, в яких елементарні компоненти, що реалізують свою основну задачу, функціонують у складі автономної групи (роя). Важливо зазначити, що на ймовірність досягнення основної цілі рою (напр. відшукання та ідентифікації речей в тривимірному просторі) значно впливає рівень енергоспоживання апаратури комп'ютерно-телекомунікаційної інфраструктури рою [2,3]. Особливої актуальності це питання набуває для БПЛА надлегкого класу, де характерні суттєві обмеження щодо допустимого рівня енергоспоживання.

Основним припущення, що покладено в основу даної роботи є можливість реалізації адаптивного (не можна не згадати фундаментальні праці по системах з адаптивним управлінням проф. Костюка В.І. з Київського політехнічного інституту) керування потужністю приймально-передавального обладнання, а також можливість формалізації залежності вагового коефіцієнта $W_{ij}$ для кожної пари компонентів *i-j* від значень потужностей $P_{ij}$, тобто існування функції $W_{ij}$ ($P_{ij}$).

В роботі [1] пропонується простий, з погляду витрат інформаційно-обчислювальних ресурсів, алгоритм навчання нейрокомп'ютера для розв'язання задачі пошуку речей у тривимірному просторі, але ефективність його залежить від значень координат початкової точки.

Робота спрямована на створення методу початкового визначення параметрів нейрокомп'ютера, призначеного для адаптивного регулювання потужності передавального обладнання у складі рою безпілотних літальних апаратів із забезпечення мінімального рівня енергоспоживання.

Для розв’язання поставленої задачі було висунуто припущення щодо характеру загасання сигналу в каналі зв’язку, а також щодо наявності залежності між енергоспоживанням та потужністю приймально-передавального обладнання компонентів нейрокомп’ютерної системи. Вхідними даними є просторові координати кожного з $m$ компонентів нейромережі, розташованих на взаємодіючих БПЛА.

Суть запропонованого методу полягає у визначенні мінімального значення потужності приймально-передавального обладнання $P$ (за умови збереження достатнього ступеня інтегрованості системи), що опосередковано визначає початкові координати вектора $W$ для кожної пари вузлів, на основі аналізу синтезованої нормативної математичної моделі, яку отримано шляхом релаксації ряду обмежень, і яка класифікується як модель лінійного програмування. Використання одержаної моделі математичного програмування дозволяє застосовувати ефективні алгоритми її аналізу. Зокрема, для розв'язання відповідної задачі лінійного програмування доцільним є використання швидких алгоритмів, таких як алгоритм Данцига-Вулфа.

Основне співвідношення системи обмежень моделі:

$$P = \frac{1}{k^3} L^{\circ 3},\ P \geq 0,$$

де $P$ - матриця розмірністю (m*m), елементами якої є величини потужності передавального обладнання;

$L$ - матриця розмірності (m*m), елементи якої визначають відстані між взаємодіючими вузлами мережі;

$k$ - коефіцієнт, що характеризує властивості середовища передачі даних (затухання сигналу, завади тощо).

Форма представлення отриманих результатів для умовного прикладу наведено в таблиці 1.

Таблиця 1

Форма представлення отриманих результатів для передавальної складової прийомо-передавального обладнання

| $P_{ij}$ | 1 | 2 | 3 | 4 | ... |
|---|---|---|---|---|---|
| 1 | 72.45 | 65.26 | 51.94 | 103.76 | ... |
| 2 | 92.84 | 75.91 | 120.05 | 66.90 | ... |
| 3 | 82.42 | 42.56 | 77.94 | 76.93 | ... |
| 4 | 79.67 | 76.90 | 98.04 | 70.51 | ... |
| ... | ... | ... | ... | ... | ... |

Запропонований спосіб налаштування нейрокомп'ютерної системи, в частині визначення початкових значень потужностей прийомо-передавального обладнання, забезпечуючий необхідну інтегрованість роя, дає можливість розрахунку значень мінімальних сумарних енерговитрат на опосередковане формування вектора $W$ нейромережі.

## ВИКОРИСТАНІ ДЖЕРЕЛА


*1. PechurinM.K., BoyarinovaYu.Ye., KondratovaL.P., VoroninM.G., SirenkoM.A. (2022). Models of the topologies for the weak-emitting telecommunication system of interacting UAVs. Problems of Informatization and Management, 4(72), 48-54.*

*2. Tian, W., Liu, L., Zhang, X., Shao, J., & Ge, J. (2023). A coordinated optimization method of energy management and trajectory optimization for hybrid electric UAVs with PV/Fuel Cell/Battery. International Journal of Hydrogen Energy, 50, 1110–1121. https://doi.org/10.1016/j.ijhydene.2023.11.030*

*Zhang, J., Maimaiti, S., Gao, W., & Zhang, K. (2025). Energy Consumption Minimization for UAV-Assisted Network in Hotspot Area. Drones, 9(3), 178. https://doi.org/10.3390/drones9030178*

УДК 004.8

**О.О. Супрун[1],**
**А.А. Волик[2],**
**М.Є. Тищенко[2]**
*[1]Державний Університет «Київський авіаційний інститут», Київ*
*[2]КНУ ім. Тараса Шевченка, Київ*

# ГЕНЕРАЦІЯ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ LOW-RANK ADAPTATION

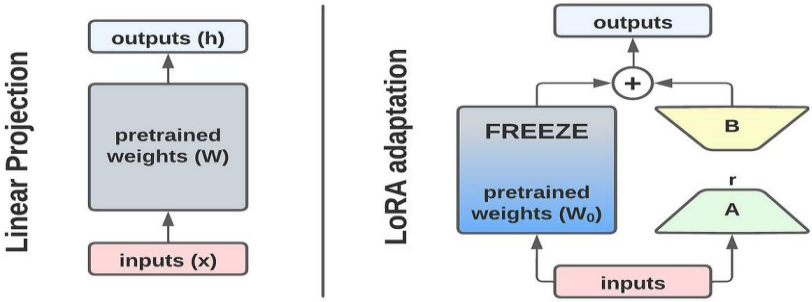
Сфера генеративних моделей для створення зображень швидко розвивається, та протягом останніх років активно використовується у багатьох сферах, витісняючи художників з корпоративного сегменту, наприклад, реклами та маркетингу [1]. Цей напрям еволюціонував від статистичних методів до складних архітектур побудованих на базі моделей глибокого навчання(Deep Learning). До створення ефективних алгоритмів глибокого навчання використовувались статистичні методи, а саме Марківські мережі, Обмежена машина Больцмана тощо. Марківські мережі використовувались для задач покращення якості зображень, а також для генерації різних текстур: трави, цегли. В свою чергу машини Больцмана могли генерувати рукописні цифри.

Архітектура **FLUX** – це серія text2image моделей, які є наступним етапом розвитку генеративних моделей після Stable Diffusion. Модель базується на гібридній архітектурі, яка поєднує в собі мультимодальні й паралельні блоки які були масштабовані до 12 мільярдів параметрів. Модель має три версії з трьома різними ліцензіями. Перша версія Flux-Schnell, що є абсолютно відкритою, є найшвидшою серед усіх варіантів Flux. Друга версія це Flux-Dev, що також є відкритою моделлю, але не може бути використана для комерційних цілей без попередніх угод. Вона є менш швидкою, але генерує більш якісні зображення. Третя версія це модель Flux-Pro, яка є повністю закритою і доступ до неї лише можливий через API.

Сімейство моделей Flux продемонструвало найкращі результати на різних бенчмарках. Перший бенчмарк базувався на Human Evaluation, де для кожної моделі обчислювався її ELO-рейтинг. Другий бенчмарк також ґрунтувався на Human Evaluation, але був більш детальним, оскільки оцінював додаткові параметри, такі як різноманітність згенерованих зображень, відповідність текстовому опису, якість тощо.

Дрібне налаштування – це процес адаптації попередньо навченої моделі до нового, специфічного завдання. Наприклад, це може бути налаштування моделі для генерації коду певної мови програмування, роботи з власним фреймворком чи бібліотекою або створення текстів і зображень у заданому стилі.

**LoRA(Low Rank Adaptation)** – техніка навчання моделей, яка навчає лише дуже обмежену кількість ваг моделей, що значно прискорює час тренування.




**QLoRA(Quantized Low-Rank Adaptation)** – це новий підхід до fine-tuning моделей, головною ідеєю цього метода є використання 4 бітної квантизації заморожених ваг. Ця техніка суттєво зменшила час навчання моделі і кількості потрібної пам'яті. NVIDIA має нову функцію уніфікованої пам'яті, яка автоматично здійснює передачу сторінок між CPU та GPU, що забезпечуючи безпомилкову обробку на GPU у випадках, коли відеопам'яті тимчасово не вистачає.

Модель може легко стати перенавченою якщо оновлювати усі її параметри на невеликому або не різноманітному наборі даних. Запропоновано тренувати не усі ваги цієї моделі, а тільки їх обмежену кількість, назвемо цей підхід PEFT(parameter efficient fine tuning).

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. K. Kurin, O. Yudin, O. Suprun, O. Provotar, V. Kotetunov and D. Barannik, "Video Data Compression Coder Based on the Method of Structural Digital Image Representation," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 285-289, doi: 10.1109/ATIT58178.2022.1002424.*

УДК ***004.738.5.055.7***

**І.В. Телешко**

*Державний Університет «Київський авіаційний інститут», Київ*

# ПАКУНКОВЕ КОДУВАННЯ В МЕРЕЖАХ З ВТРАТОЮ ПАКЕТІВ

Мережі з втратою пакетів (Lossy network) – це тип мереж, в яких частина переданих даних втрачається або пошкоджується під час передачі. Це може статися через різні фактори, такі як перешкоди в сигналі, обмеження пропускної здатності каналу, перевантаження мережі або несправності обладнання.

У таких мережах не завжди можливе відновлення втрачених даних через що вони зазвичай застосовуються там, де втрата пакетів не є критично важливою, наприклад, у потоковому відео або аудіо. Але втрата даних може бути компенсована техніками такими, як стиснення або використання алгоритмів корекції помилок.

В цьому світлі надзвичайно цікавою є проблема встановлення ефективних одноадресних з'єднань через бездротові пакетні мережі. В такому випадку мережеве пакункове кодування в поєднанні з оптимізацією розподіленого потоку може дати практичний результат, що обіцяє значно перевершити показники для відомих підходів наскрізної передачі або повторної передачі за посиланнями з точки зору споживання енергії, заторів або будь-яких інших витрат, які зростають разом із кількістю передач, здійснених кожним вузлом.

Для передачі пакетів в мережах із втратою пакетів кількома стрибками може бути застосоване пакункове мережеве кодування або Branch Network Coding (BNC) [1]. Для досягнення сумісності з існуючою інфраструктурою BNC зазвичай реалізовуються через спрощену версію протоколу UDP. Спрощений UDP — це варіант UDP, який підтримує часткові контрольні суми. BNC - це клас лінійного мережевого кодування [2], [3], призначений для практичної реалізації в мережах з кількома стрибками з втратою пакетів. Замість простого пересилання пакетів на проміжних вузлах виконується їх лінійне перекодування [4] для генерації більшої кількості пакетів. Існує версія BNC, яка може реалізовувати швидкості, наближену до оптимальної, наприклад, кодування BATS [1].

Дані, які потрібно передати, розбиваються на набір вхідних пакетів, кожен з яких розглядається як вектор з K символів над

фіксованим кінцевим полем. Розмір поля має бути досить великим для припущення про те, що два випадкові вектори над цим полем є лінійно незалежними один від одного з високою ймовірністю.

Кожний пакунок складається з M кодованих пакетів. M - це ціле число більше за нуль відоме як розмір пакунку. Для створення пакунку вибирається підмножина вхідних пакетів. Спосіб вибору підмножини залежить від програми та конструкції коду. Кожен кодований пакет у пакунку є випадковою лінійною комбінацією на вибраній підмножині вхідних пакетів. До кожного пакету також додається вектор коефіцієнтів. Призначення векторів коефіцієнтів - перекодування на проміжних вузлах. Два кодованих пакети в пакунку називаються лінійно незалежними один від одного, якщо і тільки якщо їхні вектори коефіцієнтів лінійно незалежні один від одного.

Заголовок BNC разом із корисним навантаженням називається пакетом BNC. В нашому випадку мова іде про просту стратегію планування, згідно з якою пакети надсилаються послідовно. Кількість лінійно незалежних пакетів у пакунку, іменується рангом пакунку, і є мірою інформації, що передається пакунком. Таким чином, продуктивність BNC зазвичай вимірюється очікуваним рейтингом серед усіх пакетів, що надходять до вузла приймача.

Таким чином, реалізація пакункового кодування в мережах із втратами пакетів не тільки можлива, але й корисна для підвищення надійності та ефективності передачі даних. Методи пакетного кодування, такі як пакетні розріджені коди (BATS), спеціально розроблені для вирішення проблем, пов'язаних із мережами з втратами даних.

## ВИКОРИСТАНІ ДЖЕРЕЛА


1. *S. Yang and R. W. Yeung*, "Batched sparse codes," IEEE Trans. Inf.*Theory, vol. 60, no. 9, pp. 5322–5346, Sep. 2014.*
2. *R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung,* "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
3. *S.-Y. R. Li, R. W. Yeung, and N. Cai*, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.
4. *T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong*, "A random linear network coding approach to multicast", *IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4413–4430, Oct. 2006*

УДК 629.735.064 5:621.39 (075.8)

**О.В. Толстікова**,
**С.В. Водоп'янов**,
**О.В. Андреєв**,
**В.І. Дрововозов**
*Державний Університет «Київський авіаційний інститут», Київ*

# ВИЯВЛЕННЯ ЛОГІЧНИХ ЗВ'ЯЗКІВ МАТЕМАТИЧНОЇ МОДЕЛІ ТАБЛИЦІ МАРШРУТИЗАЦІЇ ТА ПСИХОФІЗІОЛОГІЧНИХ РЕАКЦІЙ ОПЕРАТОРА КОМП'ЮТЕРНОЇ МЕРЕЖІ

Щоб за адресою мережі призначення можна було б вибрати раціональний маршрут подальшого проходження пакету, Кожен мережний вузол (маршрутизатор) створює таблицю маршрутизації (ТМ). Структура ТМ залежить від типу використовуваної операційної системи, стека протоколів передачі даних, способу реалізації (апаратна або програмна) маршрутизатора і інших чинників, в тому числі людського чинника [1, 2].

Як експерти у розглянутій задачі можуть виступати адміністратор мережі; користувачі – замовники послуг; експертна система, в якій накопичується та обробляється інформація про поточний стан мережі та комутаційних вузлів.

Походження записів у рядку:

- із програмного забезпечення стека комунікаційних протоколів (створення мінімальних ТМ, записів про адреси особливого призначення типу адрес локального тестування, групових або широкомовних адрес);
- від адміністратора мережі (статичні записи без обмеження терміну життя, що зберігаються при перезавантаженні, а іноді – після вимкнення та повторного включення маршрутизатора);
- від стандартних протоколів маршрутизації (динамічні записи з обмеженим терміном життя).

Найпоширенішими є алгоритми адаптивної (або динамічної) маршрутизації. Ці алгоритми забезпечують автоматичне оновлення таблиць маршрутизації після зміни конфігурації мережі

Адаптивні алгоритми маршрутизації звичайно мають розподілений характер і мають відповідати декільком важливим вимогам. По-перше, вони повинні забезпечувати, якщо не оптимальність, то хоча б раціональність маршруту. По-друге,

алгоритми повинні бути достатньо простими, щоб при їх реалізації не витрачалися дуже багато мережних ресурсів, зокрема, вони не повинні вимагати дуже великого об'єму обчислень або породжувати інтенсивний службовий трафік. І, нарешті, алгоритми маршрутизації повинні володіти властивістю збіжності, тобто завжди приводити до однозначного результату за прийнятний час.

Для якнайповнішої порівняльної оцінки ефективності того або іншого маршруту, крім метрики, треба враховувати так звану адміністративну відстань (АВ) – параметр (метрика) маршруту, за допомогою якого визначається ступінь довіри до інформації, одержаної від сусідніх пристроїв. АВ виражається цілим числом від 0 до 255, де нуль означає найбільшу довіру, а 255 – заборону передачі трафіку по даному маршруту.

Стандартні значення АВ визначені для джерел, починаючи від приєднаного інтерфейсу (0), статичного маршруту (1), внутрішніх і зовнішніх маршрутів стандартних протоколів маршрутизації (від 5 до 200) і аж до невідомого джерела (255) (див. табл. 1).

Таблиця 1. Стандартні адміністративні відстані

| Параметр (метрика) маршруту | Адміністративна відстань |
|---|---|
| Безпосередньо підключений маршрут | 0 |
| Статичний маршрут | 1 |
| Сумарний маршрут, оголошений протоколом EIGRP | 5 |
| Зовнішній маршрут, оголошений протоколом BGP | 20 |
| Внутрішній маршрут, оголошений протоколом EIGRP | 90 |
| Маршрут, оголошений протоколом IGRP | 100 |
| Маршрут, оголошений протоколом OSPF | 110 |
| Маршрут, оголошений протоколом IS-IS | 115 |
| Маршрут, оголошений протоколом RIP | 120 |
| Маршрут, оголошений протоколом EGP | 140 |
| Зовнішній маршрут, оголошений протоколом EIGRP | 170 |
| Внутрішній маршрут, оголошений протоколом BGP | 200 |
| Невідомий маршрут | 255 |

Як наголошувалося раніше, одним з компонентів метрики $V_{ki}$ є адміністративна відстань, величина якого призначається, виходячи з практичних міркувань, в межах від 0 до 255. Для виконання умов нормування введемо функцію адміністративної відстані

$$\psi(A_d) = 1 + log_2(1 + A_d) = \frac{1}{m_j},$$

де $m_j$ – компонент метрики маршруту, пов'язаний з адміністративною відстанню; індекс $j$ може мати значення від 1 до $N_c$. Оскільки адміністративна відстань $A_d$ лежить в межах від 0 до 255, то значення, відповідно, змінюватимуться від 1 до 9. Інформаційна цінність параметра $A_d$ залежить від його величини: при $A_d = 0$ інформація про стан маршруту вважається абсолютно достовірною; при $A_d = 255$ інформація про стан маршруту вважається абсолютно недостовірною і відкидається. Тому у якості кількісної оцінки достовірності інформації про адміністративну відстань можна вибрати ентропійну міру Шеннона [3] або зіставити з достовірністю значення (у загальному випадку – вибрану деяким чином функцію) вагового коефіцієнта $\nu_j$. У якості функції $\nu_j$ можна узяти функцію вигляду

$$\phi(\nu_j) = c_j \left\{\frac{1-[\Psi(A_d)-1]}{8}\right\}, \quad n = 2k, \quad k \geq 1,$$

де $c_j$ – коефіцієнт нормування.

Вибір функції адміністративної відстані $\psi(A_d)$ у вигляді (6) продиктований наступними міркуваннями.

По-перше, в методі аналізу ієрархій вибрана верхня межа шкали, рівна 9. Приводяться наступні обґрунтування такого вибору [5].

1. Використовування шкали парних порівнянь в діапазоні від 0 до ∞ може виявитися даремним, оскільки при цьому передбачається, що людська думка якимсь чином здатна оцінити відносну перевагу будь-яких двох об'єктів, що зовсім не так. Як добре відомо з досвіду, наша здатність розрізняти знаходиться у вельми обмеженому діапазоні, і коли є значна невідповідність між порівнюваними об'єктами або діями, наші припущення тяжіють до свавілля, і звичайно виявляються далекими від дійсності. Це підтверджує думку про те, що наші шкали повинні мати кінцевий діапазон.

2. Якісні відмінності значущі на практиці і володіють елементом точності, коли величина порівнюваних предметів одного порядку або предмети близькі щодо властивості, використаної для порівняння. Психологічна межа 7 ± 2 градацій при одночасному порівнянні пояснюється тим фактом, що якщо узяти 7±2 окремих об'єктів з близькими властивостями, то знадобиться не більш 9 точок, щоб розрізнити їх.

3. Здатність людини виробляти якісні порівняння об'єктів або явищ обмежується наступними рамками: рівність, слабка, сильна, дуже сильна і абсолютна перевага. Можна прийняти компромісні визначення між сусідніми визначеннями, коли потрібна більша точність. В цілому потрібно дев'ять значень, і вони можуть бути добре узгоджені; одержувана в результаті шкала підтверджується практикою.

Практичний метод, часто використовуваний для оцінки окремих предметів, полягає в класифікації стимулів в трихотомію зон: неприйняття, байдужості, ухвалення. Для тоншої класифікації в кожну з цих зон також закладений принцип трихотомії – розподіл на низький, помірний і високий ступені. Таким чином, виходить дев'ять відтінків значущих особливостей.

По-друге, відповідно до закону Вебера-Фехнера [3] реакції $R$ людини на зовнішні подразники $S_e$ описуються лінійною функцією логарифма інтенсивності подразника:

$$R = a\,log\,s_e + b, \quad a \neq 0,$$

де $a$ і $b$ – константи, вибирані з практичних міркувань. Решта компонентів $m_i$, $i = \overline{1, N_c}$, $i \neq j$ метрик $V_{ki}$ вибирається, виходячи з порівняльних експертних оцінок переваг кожного з можливих маршрутів.

На рис. 1 зображено графік залежності затримки $\tau_R(x, N_P)$ інтуїтивної реакції оператора на відносну величину *x* подразника та на логарифм метрики $N_P$ адміністративної відстані (АВ). Чим більше зростає шкала АВ, тим важче оператору вчасно реагувати на зовнішні подразники.

Завдяки оптимізації топологічної структури мережі з поточним вибором найкращого маршруту кількісні характеристики функціонала якості покращуються не менш, чим на 5% - 7% (у порівнянні з вибором фіксованої топології мережі).

Легко помітити очевидну відповідність вибраної апроксимації психофізичному закону Вебера-Фехнера. Крім того, при застосуванні закону Вебера-Фехнера спостерігається 10...15-відсоткове прискорення інтуїтивних реакцій адміністратора мережі на раптові збудження, що дає додатковий виграш у зниженні затримок адаптації до змін маршрутів приблизно на 2% - 3%.

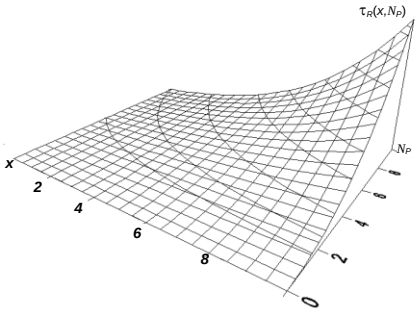



*Рис. 1. Залежність затримки $\tau_R(x, N_P)$ інтуїтивної реакції оператора на відносну величину* x *подразника та на логарифм метрики $N_P$ адміністративної відстані*

Зменшення масштабу функції адміністративної відстані веде до прискорення інтуїтивних реакцій оператора на раптові збудження, отже, на досягнення можливостей роботи у реальному часі.

Завдяки оптимізації топологічної структури мережі з поточним вибором найкращого маршруту та застосуванням закону Вебера-Фехнера кількісні характеристики функціонала якості покращуються не менш, ніж на 5% - 7% (у порівнянні з фіксованою топологією мережі).

ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Sheridan T.B. Man-Machine Systems: Information, Control, and Decision Models of Human Performance / Thomas B. Sheridan, William R. Ferrell – MIT Press (April 8, 1981) – 472 pp.*

*2. Gebru B., Zeleke L., Blankson D., Nabil M., Nateghi S., Abdollah Homaifar A., Tunstel E. A Review on Human–Machine Trust Evaluation: Human-Centric and Machine-Centric Perspectives // IEEE Transactions on Human-Machine Systems (Volume: 52, Issue: 5), 2022. – p. 952 - 962.*

*3. Soret, B., Mogensen, P., Pedersen, K. I., & Aguayo-Torres, M. C. (2014). Fundamental tradeoffs among reliability, latency and throughput in cellular networks. 2014 IEEE Globecom Workshops (GC Wkshps). – pp.1391 - 1396. https://doi:10.1109/glocomw.2014.7063628*

*4. Resende M.G.C. Handbook of Optimization in Telecommunications / Mauricio G.C. Resende, Panos M. Pardalos. (Eds.) - Springer Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, USA, 2006. – 1134 pp.*

УДК 004.77:004.8:371.3

**А.Т. Торський**
*Державний Університет «Київський авіаційний інститут», Київ*

# ПРОГРАМНИЙ ЗАСІБ ДЛЯ АНАЛІЗУ НАВЧАЛЬНОЇ АКТИВНОСТІ

У сучасних умовах цифрової трансформації освітнього середовища все більшої актуальності набуває необхідність впровадження програмних засобів, що дозволяють здійснювати якісний моніторинг та аналіз навчальної активності учнів і студентів. Цей напрям є важливим не лише з точки зору контролю успішності, а й як інструмент підвищення ефективності навчального процесу загалом.

Навчальні заклади все частіше використовують електронні платформи (наприклад, Google Classroom, Moodle, Edmodo), однак більшість із них мають обмежену функціональність у частині аналізу поведінки учнів та прогнозування результатів. Існуючі рішення не завжди відповідають специфічним потребам конкретних навчальних закладів через обмежену гнучкість, недостатню інтеграцію з локальними системами управління освітою, а також відсутність можливості налаштовувати критерії оцінювання відповідно до методик викладачів. Це підкреслює необхідність розробки адаптивного, настроюваного програмного забезпечення для аналітики навчальної активності [1, 2].

Метою даної розробки є створення програмного засобу, який автоматизує збір, обробку та аналіз даних про залученість учнів у навчальний процес. Основними джерелами даних є: активність користувача в системі (частота входу, тривалість сесій), виконання домашніх завдань, участь у форумах чи чатах, перегляд навчальних матеріалів (презентацій, відеолекцій), результати тестувань тощо.

Для аналітики використовуються такі методи:

- кореляційний аналіз для виявлення взаємозв’язку між активністю та успішністю;
- кластеризація (наприклад, методом k-середніх) для групування студентів за рівнем залученості;
- регресійні моделі для прогнозування оцінок;
- дерева рішень та наївний баєсівський класифікатор для ідентифікації учнів, які потенційно можуть мати труднощі в навчанні.

У процесі тестування програмного засобу були використані анонімізовані дані з навчального курсу, проведеного на базі Google Classroom. Застосування аналітики дозволило виявити, що студенти з найвищим рівнем активності демонструють на 30–40% вищі результати на тестуваннях, порівняно з менш активними. Також було виявлено, що зниження кількості входів у систему часто передує зниженню оцінок на 1–2 тижні.

У перспективі планується додати функціональність адаптивних рекомендацій для студентів — система зможе пропонувати додаткові матеріали або вправи на основі слабких місць, виявлених в аналізі. Також передбачається інтеграція з мобільними застосунками для оперативного доступу до статистики.

Отже, запропонований програмний засіб має потенціал стати універсальним інструментом підтримки викладання у цифровому освітньому середовищі, забезпечуючи адаптивність, масштабованість та орієнтацію на конкретні потреби закладу освіти

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Зварич І. "Моніторинг навчально-пізнавальної активності учнів як показник якості освітніх послуг" // Вісник післядипломної освіти, 2020.* https://doi.org/10.32405/2218-7650-2020-13(42)-73-86 .

*2. Шегда А. "Моніторинг розвитку навчальної діяльності учнів" // Інститут модернізації змісту освіти, 2023.*

УДК 681.52(043.2)

**Д.С. Шевчук**
**О.М. Глазок**
*Державний Університет «Київський авіаційний інститут», Київ*

# СУЧАСНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ ДОНАВЕДЕННЯ В БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТАХ

У наш час тема розвитку безпілотних літальних апаратів (БПЛА) є як ніколи важливою і актуальною. Сучасний світ стрімко змінюється завдяки інноваційним технологіям, що відкриває нові можливості для застосування БПЛА у різних сферах – від оборонної промисловості до цивільного використання в логістиці, сільському господарстві, рятувальних місіях, екологічному моніторингу. Одна із найперспективніших галузей досліджень є розробка систем донаведення, які відіграють ключову роль у забезпеченні високої точності а надійності польотів. Також важливо зазначити, що інтеграція сучасних технологій, таких як штучний інтелект та алгоритми обробки даних в режимі реального часу, значно підвищує ефективність БПЛА. Це сприяє не лише кращому виконанню поставлених завдань через зменшення впливу зовнішніх факторів, допомога у виявленні цілі, автоматичний обхід перешкод, але й забезпечує можливість виконання складних завдань в умовах при яких раніше це було б неможливо.

Важливість систем донаведення для БПЛА полягає у забезпеченні їх здатності ефективно виконувати завдання навіть у найскладніших умовах. Сучасні технології дозоляють інтегрувати дані з кількох сенсорних систем, зокрема з камер високої роздільної здатності та інерційних вимірювальних блоків, що забезпечує багатовимірний аналіз навколишнього середовища та адаптивне управління апаратом. Наприклад, завдяки використанню інформації з даних сенсорів і оптичних систем, БПЛА може точна визначити своє положення у просторі та самостійно корегувати свою траєкторію польоту у режимі реального часу, що дозволяє забезпечити непередбачуваність траєкторії ускладнюючи процес виявлення і відстеження БПЛА противником. [1]

Також, важливою є розробка нових законів донаведення для кооперативного управління декількома БПЛА, що відкриває можливості для виконання ширшого спектру завдань, таких як

обліт цілей, розвідка і моніторинг, а також сприяє підвищенню їх ефективності. Так завдяки використанню методів оптимізації траєкторій та динамічному коригуванню на основі даних з різних сенсорних модулів, система може оперативно реагувати на змінні умови, що забезпечує більш ефективне виконання завдань. [2] Також кооперативне управління декількома БПЛА, набагато підвищує їх операційну ефективність, адже сучасні алгоритми кооперативного управління розподіляють місію на завдання, які розподіляються між БПЛА. [4]

Одна із важливих технологій - автономна посадка БПЛА на рухомі платформи, що дозволяє зберегти в цілісності бойову одиницю або ж знищити рухому ціль, здійснюється за рахунок систем донаведення, що базуються на багатосенсорній інтеграції, що значно покращує точність і надійність автономної посадки на рухомі платформи. [3] Це дає великий простір можливостей тактичного планування завдань, використання БПЛА і збільшує радіус дій місій для переслідування, спостереження і ліквідування ворога, а також підвищує їх ефективність.

У сучасних умовах стрімкого розвитку технологій безпілотних систем відзначається тенденція до інтеграції БПЛА із іншими безпілотними системами. Така кооперація забезпечує синергію між різними типами апаратів, дозволяючи закривати слабкі сторони один одного і використовувати сильні сторони кожного з них для виконання комплексних завдань у надзвичайно складних умовах. Так, за результатами дослідження «A Novel Cooperative Design for USV-UAV Systems: 3-D Mapping Guidance and Adaptive Fuzzy Control», було показано, що за рахунок кооперативної схеми управління між безпілотними літальними апаратами(БПЛА) і безпілотними надводними апаратами(БПНА) підвищувалась точність синхронізації платформ і зменшувався необхідний час на комунікацію, що призводило до підвищеної оперативності виконання завдань. [5] Та в кооперація різних видів безпілотних апаратів було помічено приріст в стійкості до зовнішніх впливів, значні зменшення затрат часу на комунікацію і виконання розрахунків, через ефективне розділення задач між різними апаратами. [7] Це все показує нові простори планування операцій і реагування в реальному часу на непередбачувані зміни під час них.

З програмної точки зору, підвищення рівня автономності БПЛА досягається завдяки застосуванню адаптивних механізмів керування у системах донаведення та інших автономних системах. Ці алгоритми в сучасній точці розвитку, аналізуючи поточні параметри системи, дозволяють БПЛА самостійно, в залежності від навколишніх умов, корегувати свою траєкторію польоту в автоматичному режимі, а при управлінні на відстані корегують положення БПЛА для кращого управління. [6]

**Висновок.** Розвиток систем донаведення для БПЛА є критично важливим для підвищення їх тактичних можливостей, що дозволяє значно розширити застосування цих апаратів як у військовій так і в цивільній сферах. Завдяки впровадженню адаптивних алгоритмів, моделей кооперативного управління і інших інноваційних технологій, які збільшують стійкість до зовнішніх збурень, БПЛА здатні ефективно виконувати складні комплексні завдання, корегувати траєкторію польоту мінімізую ризики їх виявлення в режимі реального часу. Така кооперація і інтеграція систем надає можливість не лише зменшити втрати бойових одиниць, а й створювати нові тактичні можливості, що відкриває нові простори для застосування БПЛА у ширшому діапазоні.

## ВИКОРИСТАНІ ДЖЕРЕЛА


1. *Julius A. Marshall, Robert B. Anderson, Wen-Yu Chien, Eric N. Jonson, Andrea l`Afflitto. A Guidance System for Tactical Autonomous Unmanned Aerial Vehicles/ Journal of Intelligent & Robotic Systems.-2021.-Vol. 103.-Article number 71. DOI: 10.1007/s10846-021-01526-8. URL:https://link.springer.com/article/10.1007/s10846-021-01526-8%20*

2. *Mia Zhang, Chengyu Liang, Jingsong Mei. Robust guidance law for cooperative aerial target circumnavigation of UAVs based on composite system theory/ Journal Aerospace Science and Technology.-2023-Vol. 140-Article number 108439. DOI: 10.1016/j.ast.2023.108439 URL: https://www.sciencedirect.com/science/article/abs/pii/S127096382300336X?via%3Dihub*

3. *Ching-Wei Chang, Li-Yu Lo, Hiu Ching Cheung, Yurong Feng, An-Shik Yang, Chih-Yung Wen. Proactive Guidance for Accurate UAV Landing on a Dynamic Platform: A Visual-Inertial Approach/ Journal Sensors.-2022.-Vol. 22.-Issue 1. DOI: 10.3390/s2201040.*

*URL: https://www.mdpi.com/1424-8220/22/1/404*

*4. Min Zhang, Jiangbo Jia, Jingsong Mei. A composite system theory-based guidance law for cooperative target circumnavigation of UAVs/ Journal Aerospace Science and Technology.-2021-Vol. 118-Article number 107034. DOI: 10.1016/j.ast.2021.107034*

*URL: https://www.sciencedirect.com/science/article/abs/pii/S1270963821005447?via%3Dihub*

*5. Jiqiang Li, Guoqing Zhang, Qihe Shan, Weidong Zhang. A Novel Cooperative Design for USV-UAV Systems: 3-D Mapping Guidance and Adaptive Fuzzy Control/ Journal IEEE Transactions on Control of Network Systems.-2022.-Vol.10.-Issue 2.-Pp. 564-474. DOI: 10.1109/TCNS.2022.3220705*

*URL: https://ieeexplore.ieee.org/document/9942343*

*6. Ximan Wang, Spandan Roy, Stefano Fari, Simone Baldi. Adaptive Vector Field Guidance Without a Priori Knowledge of Course Dynamics and Wind/ Journal IEEE Transactions on Control of Network Systems.-2022.-Vol. 27.-Issue 6.-Pp. 4597-4607. DOI: 10.1109/TMECH.2022.3160480.*

*URL: https://ieeexplore.ieee.org/document/9756038*

*7. Bin-Bin Hu, Hai-Tao Zhang, Bin Liu, Jianing Ding, Yifan Xu, Chuanshang Luo, Haosen Cao. Coordinated Navigation Control of Cross-Domain Unmanned Systems via Guiding Vector Fields/ Journal IEEE Transactions on Control of Network Systems.-2023.-Vol. 32.-Issue 2.-Pp. 550-563. DOI: 10.1109/TCST.2023.3323766.*

*URL: https://ieeexplore.ieee.org/document/10294277*

УДК 681.52

**Ю.К. Шестопал**
*Державний Університет «Київський авіаційний інститут», Київ*

# КЕРУВАННЯ РУХОМ ГРУПИ БПЛА ДЛЯ УНИКНЕННЯ СТАТИЧНИХ ТА ДИНАМІЧНИХ ПЕРЕШКОД

Застосування безпілотних літальних апаратів (БПЛА) в сільському господарстві, логістиці, будівництві та інших сферах людської діяльності зростає, а також потребує впровадження покращеної координації між апаратами для виконання поставлених завдань та цілей в стані групи. Координація та керування груп БПЛА ускладнюється через необхідність автономного уникнення перешкод в умовах змінного середовища. Існуючі методи уникнення перешкод полягають в побудові оптимальних траєкторій польоту, поєднанні локальної та глобальної навігації та обробці сенсорних даних.

Мета дослідження – аналіз методів та підходів уникнення перешкод під час керування рухом групи безпілтоних літальних апаратів, що забезпечують безпечну зміну траєкторії польоту групи БПЛА з урахуванням динамічних змін у навколишньому середовищі.

Для успішного уникнення перешкод під час групового польоту БПЛА необхідно враховувати як глобальні, так і локальні аспекти планування маршруту. Ключовим методом уникнення перешкод є використання потенційних полів або непотенційних функцій [1], що надає змогу побудувати середовище, в якому віртуальні сили притягання до бажаних областей та сили відштовхування від перешкод коригують траєкторію польоту. Метод ORCA (Optimal Reciprocal Collision Avoidance) надає групі БПЛА можливість уникати зіткнень з перешкодами, аналізуючи відносні швидкості об’єктів та розраховуючи безпечні напрями руху кожного БПЛА. Геометричні методи уникнення перешкод полягають в моделюванні траєкторій руху як самих БПЛА, так і виявлених перешкод. Одним із підходів є розрахунок зон загрози, в яких можливе зіткнення та визначення мінімальної безпечної дистанції. Якщо БПЛА наближається до перешкоди, то його траєкторія коригується таким чином, щоб уникнути входження апарату в цю зону, причому чим ближче перешкода, тим суттєвіші зміни траєкторії. Застосування геометричних методів можливе при роботі

як із статичними, так і з динамічними перешкодами, проте їх використання потребує відповідної точності сенсорних даних. Перспективним сучасним напрямком є застосування генеративних алгоритмів для підвищення точності роботи датчиків БПЛА [2].

Проведене дослідження продемонструвало, що застосування підходів та методів уникнення перешкод значно зменшує ризик зіткнень та покращує координацію руху БПЛА в стані групи. Використання алгоритмів потенційних полів забезпечує плавну корекцію траєкторій в середовищах з невеликою кількістю перешкод, проте в складних умовах з великою кількістю перешкод можуть виникнути проблеми стосовно затримки у виборі подальшого маршруту. Метод ORCA надає можливість кожному БПЛА самостійно коригувати маршрут, тим самим зменшуючи ймовірність зіткнень. Геометричні методи дозволяють прогнозувати ризик зіткнень на основі параметрів руху перешкод і коригують траєкторію так, щоб забезпечити мінімальну зміну курсу при максимальному рівні безпеки.

**Висновок.** Застосування методів уникнення перешкод при русі БПЛА в стані групи покращує автономність групи та забезпечує безпечне виконання поставлених оператором цілей та місій у динамічному середовищі. Результати дослідження можуть бути використані при розробці автономних систем управління БПЛА для виконання складних місій, таких як таких як пошуково-рятувальні операції та доставка вантажів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Olexiy M. Glazok. A non-potential Target Function for Controlling the UAVs Group Flight in Presence of Concave Obstacles /2019 IEEE 5th Int. Conf. "Actual Problems of Unmanned Aerial Vehicles Developments" (APUAVD), October 22-24, 2019: proceedings. – IEEE, 2019. – Pp. 238-241. DOI:10.1109/APUAVD47061.2019. 8943870.*

2. *Нечипоренко В. А. Методи керування БПЛА із застосуванням комп'ютерного зору //Вчені записки. – 2024. – С. 52024217.*

УДК 004.7-048.34(043.2)

**О.І. Шкляр**
*Державний Університет «Київський авіаційний інститут», Київ*

# АНАЛІЗ НАЯВНИХ МЕТОДІВ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ХМАРНИХ ІНФРАСТРУКТУРАХ

Хмарні інфраструктури сьогодні є основою для більшості сучасних інформаційних систем [1]. Одним із важливих аспектів ефективного функціонування таких систем є балансування навантаження. Балансування навантаження дозволяє забезпечити високу доступність, ефективне використання ресурсів та масштабованість в хмарних середовищах. З огляду на різноманітність архітектур і методів реалізації, питання вибору оптимального підходу для конкретної інфраструктури набуває особливої актуальності.

Балансування навантаження — це процес рівномірного розподілу вхідного трафіку або задач між кількома серверами чи ресурсами для забезпечення високої продуктивності та доступності системи. В умовах хмарних інфраструктур цей процес є важливим для уникнення перевантаження окремих вузлів та забезпечення безперервної роботи додатків або сервісів [2, 3].

Основні методи балансування навантаження

1. Класичні методи балансування навантаження:

1.1. Розподіл на основі кругової адресації (Round-robin).

1.2. Балансування на основі мінімального навантаження.

2. Методи балансування на основі вмісту запиту:

2.1. Балансування на основі IP-адреси: Цей метод використовує IP-адресу клієнта для визначення сервера, до якого буде спрямовано запит.

2.1.1. Геш: розподіляти запити згідно з геш-таблицею.

2.2. Балансування на основі типу запиту: У цьому випадку методи балансування враховують тип запиту (наприклад, статичний контент чи динамічні обчислення), спрямовуючи їх на відповідні сервери.

3. Інтелектуальні методи:

3.1. Динамічне балансування навантаження: Сучасні методи базуються на аналізі реального часу й адаптуються до змінних умов навантаження. Це може включати в себе алгоритми машинного навчання або предсказувальні моделі, які дозволяють

на основі історичних даних прогнозувати майбутнє навантаження та оптимізувати розподіл ресурсів.

3.2. Автоматичне масштабування: Хмари зазвичай мають вбудовану функцію автоматичного масштабування, яка дозволяє додавати чи видаляти ресурси в залежності від поточного навантаження. Це дозволяє досягти високої доступності та ефективного використання ресурсів при змінному трафіку.

3.2.1. Алгоритм генетичного балансування навантаження.

Переваги та недоліки методів

1. Класичні методи:

Переваги: Проста реалізація, низька затримка, зручність для середовищ з однаковими серверами.

Недоліки: Не враховують змінність навантаження, можуть призводити до нерівномірного використання ресурсів, недостатньо гнучкі для складних архітектур.

2. Інтелектуальні методи:

Переваги: Висока адаптивність, можливість враховувати реальний стан системи, ефективне використання ресурсів.

Недоліки: Складність реалізації, велика потреба в обчислювальних потужностях для аналізу даних в реальному часі.

Аналіз наявних методів балансування навантаження в хмарних інфраструктурах показує, що правильний вибір підходу залежить від специфіки задач і архітектури. Класичні методи є простими та ефективними для базових сценаріїв, в той час як інтелектуальні методи і автоматичне масштабування дозволяють досягти кращої адаптивності і оптимізації в умовах змінного навантаження.

## ВИКОРИСТАНІ ДЖЕРЕЛА

*1. Huang, D. Data (2021) Center Infrastructure Management. Data Center Handbook. Wiley. C. 627–644.*

*2. Божуха Д.І., Байбуз О.Г., Мащенко Л.В. (2022) Про підходи дослідження системи хмарних обчислень. Актуальні проблеми автоматизації та інформаційних технологій. Том 26. С. 18-30.*

*3. Buyya, R., Broberg, J., Goscinski, A. (2011) Cloud Computing: Principles and Paradigms. Wiley.*

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
**XVI МІЖНАРОДНОЇ**
**НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

«КОМП'ЮТЕРНІ СИСТЕМИ
ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2025)

27–28 березня 2025 року

*Тези доповідей надруковані в авторській редакції*
*однією із двох*
*робочих мов конференції: українською, англійською.*