

MINISTRY OF EDUCATION AND
SCIENCE OF UKRAINE

STATE UNIVERSITY
"KYIV AVIATION INSTITUTE"

FACULTY OF COMPUTER
SCIENCE AND TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ І НАУКИ
УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК
ТА ТЕХНОЛОГІЙ



Abstracts of
XXV International conference of
higher education students
and young scientists

**POLIT.
CHALLENGES OF SCIENCE TODAY**

Modern information and communication
technologies in aviation

Kyiv 2025

Тези доповідей
XXV Міжнародної науково-практичної
конференції здобувачів
вищої освіти і молодих учених

**ПОЛІТ.
СУЧАСНІ ПРОБЛЕМИ НАУКИ**

Сучасні інформаційні та комунікаційні технології
в авіації

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

Тези доповідей
XXV Міжнародної
науково-практичної конференції здобувачів
вищої освіти і молодих учених

ПОЛІТ.
СУЧАСНІ ПРОБЛЕМИ НАУКИ

Сучасні інформаційні та комунікаційні технології в авіації

ПОЛІТ. СУЧАСНІ ПРОБЛЕМИ НАУКИ. Сучасні інформаційні та комунікаційні технології в авіації: Тези доповідей XXV Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених, Київ, 2025, Державний університет «Київський авіаційний інститут» / Редакційна колегія К. Семенова [та ін.]. – К.: КАІ, 2025. – 273 с.

Матеріали науково-практичної конференції містять узагальнення доповідей науково-дослідних робіт здобувачів вищої освіти та молодих учених у галузі «Інформаційні технології».

*Рекомендовано до друку Вченою радою факультету комп'ютерних наук та технологій
(Протокол № 6 від 14 квітня 2025 р.)*

Голова оргкомітету:

К. Семенова, в. о. президента, Державний університет «Київський авіаційний інститут».

Заступники голови оргкомітету:

С. Гнатюк, проректор з наукових досліджень та трансферу технологій, доктор технічних наук, професор, Державний університет «Київський авіаційний інститут».

Андрій Фесенко, декан факультету комп'ютерних наук та технологій, к.т.н., доцент

Члени оргкомітету:

Т. Охріменко, к.т.н., старший дослідник, заступник декана

А. Молчанов, к.т.н., заступник декана

Н. Журавель, заступник декана

О. Поліщук, к.е.н, доц., заступник декана

О. Нечипорук, д.т.н., проф., завідувач кафедри

А. Савченко, д.т.н., проф., завідувач кафедри

П. Приставка, д.т.н., проф., завідувач кафедри

В. Козловський, д.т.н., проф., завідувач кафедри

І. Ластівка, д.т.н., проф., завідувач кафедри

А. Ільєнко, к.т.н., доц., завідувач кафедри

Ю. Іскренко, к.т.н, завідувач кафедри

О. Гріненко, к.т.н., завідувач кафедри

Є. Артамонов, к.т.н., доц., доцент кафедри ІКС

Ю. Коваленко, к.п.н., доц., доцент кафедри КБ

О. Дорош, ст. викладач кафедри КСМ

О. Охремчук, асистент кафедри Кім

О. Піскунов, к.ф.-м.н., доц., доцент кафедри ПМ

Л. Терещенко, к.т.н., доц., доцент кафедри ІПЗ

Scientific publication

POLIT.
Challenges of science today
Modern information and communication technologies in aviation

***Abstracts of
XXV International
conference of higher education students
and young scientists***

Kyiv, 1-4 April 2025
Published in the author's edition

Наукова публікація

ПОЛІТ.
СУЧАСНІ ПРОБЛЕМИ НАУКИ
Сучасні інформаційні та комунікаційні технології в авіації

***Тези доповідей
XXV Міжнародної
науково-практичної конференції здобувачів
вищої освіти і молодих учених***

Київ, 1-4 квітня 2025
Публікується у авторській редакції

Підп. до друку 10.06.2024. Електронне видання.

Формат 60x84/16. Видавець і виготовник

Державний університет «Київський авіаційний інститут» 03058. Київ – 58, проспект Любомира Гузара, 1
Свідectvo про внесення до Державного реєстру України суб'єктів видавничої справи ДК № 977 від 05.07.2002

УДК 81'33(075)

СТВОРЕННЯ СИСТЕМИ АВТОМАТИЧНОГО АНОТУВАННЯ АУДІО ФАЙЛІВ ДЛЯ УКРАЇНСЬКОЇ МОВИ

Ольга Солодка, Михайло Юрукін

Київський національний університет імені Тарас Шевченка, Київ

Науковий керівник – Ольга Супрун, к.ф.-м.н., доц.

Ключові слова: автоматичне анотування, фонетика, розпізнавання мовлення

Автоматичне анотування аудіо є надзвичайно актуальною темою у сучасному світі. Воно знаходить широке застосування у різноманітних галузях, таких як розпізнавання мелодій (наприклад, Шазам) [1], «оцифровування» літературних творів, зокрема аудіокниг, а також допомагає фонетистам у деталізованому аналізі мовлення. Автоматизація процесів дозволяє значно оптимізувати час та зусилля, які витрачаються на ручну обробку аудіоданих. Для української мови, з її багатою фонетичною системою, відсутність автоматизованих рішень у цій сфері створює суттєві труднощі для дослідників, викладачів і розробників.

Анотування аудіо надзвичайно важливе у фонетиці, оскільки воно дозволяє точніше і швидше аналізувати акустичні характеристики мовлення, знижує потребу у ручній роботі, яка є часо- та ресурсозатратною, особливо у програмі Praat [2], де користувачі змушені самотійно виконувати сегментацію та інші дії. У публічному доступі наразі немає систем автоматичного анотування, які б відповідали потребам української мови та її фонетичних особливостей. Розроблення такої системи створить нові можливості для дослідників із різних дисциплін: лінгвістики, нейронаук, освіти.

В основі запропонованої системи лежить алгоритм, описаний у схемі (рис. 1). Перший етап передбачає прийом аудіофайлу, який потребує анотації. Аудіофайл розділяється на окремі сегменти на основі змін акустичних характеристик, таких як паузи або рівень енергії сигналу. Далі сегменти класифікуються як мовлення або немовлення за допомогою алгоритму, що враховує оцінки впевненості.

Мовленнєві сегменти групуються відповідно до мовця через кластеризацію за акустичними ознаками. Кожен кластер відповідає сегментам, що, ймовірно, належать одному мовцю. Це забезпечує ефективність подальшого аналізу, зокрема дозволяє розділяти сегменти між різними мовцями навіть у великому аудіозаписі. Також цей підхід може використовуватися в архівах для зручного пошуку сегментів із промовами певної людини.

Наступний крок передбачає розпізнавання мовлення із ідентифікацією слів та синхронізацією їх із часовими позначками, що дозволяє отримати текстову транскрипцію з точними часовими рамками кожного слова. Це зручно для подальшого аналізу чи використання в пошукових системах.

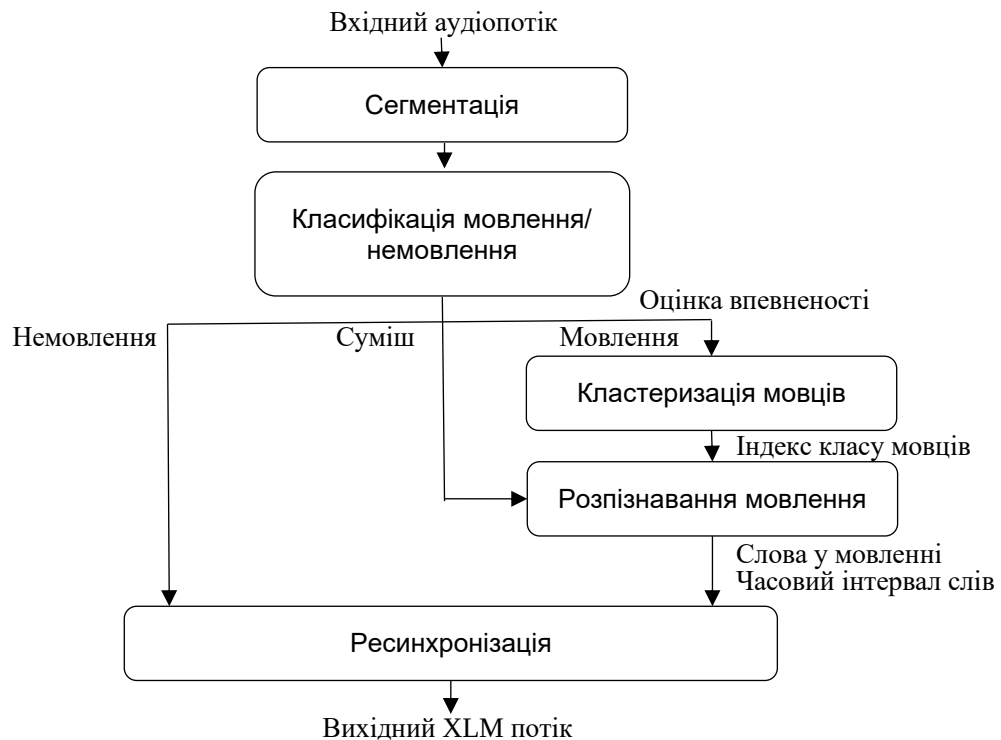


Рис. 1. Блок-схема системи анотації аудіофайлів

Всі дані сегментації, класифікації, кластеризації та розпізнавання формуються у структурований XML-документ для зручного зберігання та подальшого оброблення. Такі XML-документи можуть використовуватися для інтеграції з іншими інструментами або програмами, що працюють із мовними даними.

Висновок

Розроблення системи автоматичного анотування аудіофайлів для української мови є важливим кроком для розвитку мовознавчих досліджень. Ця система полегшить роботу фонетистів і науковців, дозволяючи їм зосередитися на аналізі даних, а не на їхній підготовці.

Список використаних джерел:

1. An Automatic Annotation System for Audio Data Containing Music. URL: <https://dspace.mit.edu/bitstream/handle/1721.1/80547/43551492-MIT.pdf?sequence=2> (Last accessed: 20.03.2025).
2. Praat. URL: <https://www.fon.hum.uva.nl/praat/> (Last accessed: 20.03.2025).

УДК 159.98:004.4(043.2)

АДАПТИВНА СИСТЕМА МОНІТОРИНГУ ПСИХОЛОГІЧНОГО СТАНУ КОРИСТУВАЧІВ НА БАЗІ ANDROID З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Антон Юрченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олексій Глазок, к.т.н., доц.

Ключові слова: психологічний моніторинг, машинне навчання, Android, мобільна психодіагностика, адаптивні системи

Вступ. Сучасні розробки у сфері мобільних технологій демонструють потенціал використання смартфонів для збору психологічних даних. Проте існуючі рішення часто не враховують індивідуальні особливості користувачів та демонструють низьку адаптивність.

Мета дослідження – розробка концепції та прототипу адаптивної системи моніторингу психологічного стану користувачів для платформи Android з використанням алгоритмів машинного навчання.

Матеріали та методи. Дослідження проведено на платформі Android API 28+ із використанням архітектури MVVM [1] та інструментів Android Jetpack [3]. Для машинного навчання застосовано TensorFlow Lite [2] та попередньо навчену модель аналізу тексту.

Психодіагностика базується на скороченій шкалі депресії Бека [4], опитувальнику Спілбергера [5]. Дані зберігаються локально за допомогою бібліотеки Room.

Функціональність системи тестували на вибірці з 5 добровольців (віком 20–23 роки) протягом 2 тижнів. Аналізувалися щоденні опитування та текстові записи користувачів.

Результати. Розроблена система складається з трьох функціональних модулів: модуль збору даних, модуль аналізу та обробки, модуль адаптивних рекомендацій. Аналіз текстових записів із використанням NLP дозволяє виявляти емоційне забарвлення. Попереднє тестування показало 65% точності у розпізнаванні негативних змін стану порівняно зі стандартизованими методиками.

Попереднє тестування на малій вибірці показало, що система розпізнає негативні зміни психологічного стану з точністю близько 65% у порівнянні з контрольними оцінками, зробленими на основі повних версій стандартизованих опитувальників (рис. 1).

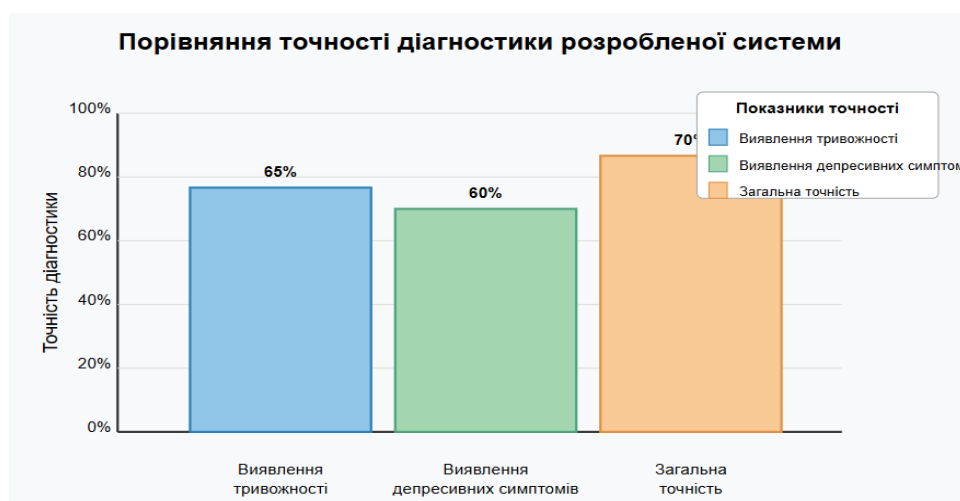


Рис. 1. Порівняння точності діагностики розробленої системи з контрольними методиками

Модуль рекомендацій пропонує користувачам базові поради, ґрунтовані на когнітивно-поведінковій терапії. Більшість учасників відзначили підвищену обізнаність щодо свого психологічного стану.

Висновок

Розроблений прототип демонструє можливість використання адаптивних методів для моніторингу психологічного стану на базі мобільного додатку. Отримані результати можуть бути застосовані для подальшої розробки персоналізованих інструментів підтримки психічного здоров'я.

Список використаних джерел

1. Model-View-ViewModel (MVVM). URL: <https://learn.microsoft.com/en-us/dotnet/architecture/maui/mvvm>.
2. LiteRT overview. URL: <https://ai.google.dev/edge/litert>
3. Jetpack libraries. URL: <https://developer.android.com/jetpack/androidx/explorer>
4. Aaron T. Beck, Robert A. Steer, Margery G. Carbin. Psychometric properties of the Beck Depression Inventory: Twenty-five years of evaluation, – Clinical Psychology Review. – Volume 8, Issue 1. – 1988. Pages 77-100. DOI: 10.1016/0272-7358(88)90050-5.
5. Spielberger, C. D. State-Trait Anxiety Inventory: Bibliography (2nd ed.) – Palo Alto, CA: Consulting Psychologists Press, 1989. – Pp. 3-11.

УДК 519.688 (043.2)

ІНТЕГРАЦІЯ ПРОСТОРОВИХ ДАНИХ У ЦИФРОВІ ІНФРАСТРУКТУРИ

Арсеній Григор'єв

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Світлана Кашкевич, ст. викладач

Ключові слова: картографічна проєкція, просторові дані, геокодування, ГІС, геометрія

Рух за відкриті дані стимулює державні установи, наукові та культурні організації до публікації інформації в Інтернеті. Незважаючи на те, що просторові дані, такі як карти, супутникові знімки та зображення вулиць, широко доступні через пошукові системи та веб-додатки, їх використання обмежене через відсутність узгодженості в методах представлення та структурування. В рамках ГІС (географічні інформаційні системи) важливо вирішити питання інтеграції просторових даних з різними джерелами в єдину інформаційну екосистему.

Багато просторових об'єктів можна описати через статичні властивості. Однак у деяких випадках важливо враховувати зміни цих властивостей у просторі та часі, що описується через покриття. Покриття є важливим інструментом для опису складної геометрії даних, оскільки воно дозволяє аналізувати не тільки точні розташування, а й динаміку змін на картах.

Згідно з [ISO-19123-1:2022], покриття є набором значень, кожне з яких відповідає певному елементу масиву точок або клітинок. Воно функціонує як математична функція, яка визначає значення в просторі, часі або їх комбінації. Прикладами покриттів є растрові дані, хмари точок і сіткові моделі, що можуть бути: 1D (часові ряди з даними з датчиків), 2D (супутникові знімки), 3D (геофізичні воксельні дані), або 4D (кліматичні моделі).

Прикладом покриття є хмара точок: набір точок у тривимірному просторі з додатковими атрибутами, такими як інтенсивність, колір або час. Цифрова карта висот для Нідерландів містить точні дані про висоти, середньою щільністю вісім вимірювань на кв. метр (рис. 1).

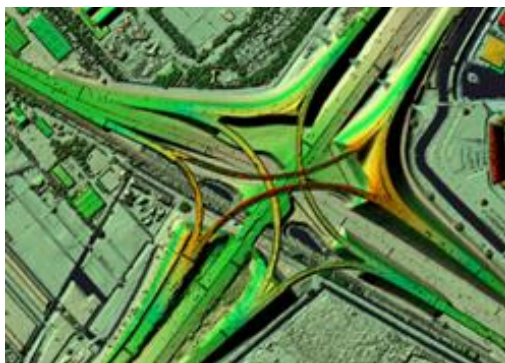


Рис. 1. Хмара точок, що відображає Prins Clausplein – складне перехрестя шосе.

Точкам надається колір для візуалізації висоти.

Покриття можна вважати особливим типом просторової речі, яка має певні властивості. Наприклад, «сегмент річки» може мати властивість «швидкість течії», що виражається через покриття. Просторові речі та покриття можуть бути пов'язані кількома способами:

- інформаційні сигнали в покриттях можуть використовуватися для виявлення наявності, розташування та типу просторових об'єктів, наприклад, варіація типу ґрунту в геофізичній свердловині;
- покриття може описувати зміни значень властивості просторової речі, що варіюються у межах цієї речі, наприклад, різні рівні покриття мобільної мережі в різних регіонах;
- покриття може забезпечувати спільну властивість для набору просторових об'єктів, що дозволяє здійснити дискретне вимірювання, як це відбувається при оцінці вологості ґрунту на основі даних із різних станцій.

Покриття визначається через три основні елементи:

- область покриття – набір точок у просторі та часі, де є значення даних;
- діапазон покриття – набір вимірних, змодельованих або спостережених значень для кожної точки в області покриття;
- метадані діапазону – опис значень покриття, що включає інформацію про одиниці вимірювання, визначення змінних та способи інтерполяції.

Одним з найскладніших аспектів є визначення області покриття, яка може варіюватися в широких межах, що вимагає чіткого визначення просторово-часової геометрії покриття, зокрема для багатовимірних сіток чи часових рядів.

Отже, покриття є структурою даних, що з'єднує точки в просторі та часі зі значеннями властивості. Це можна розглядати як математичну функцію, де значення даних є функцією координат, при цьому значення можуть бути не тільки числами, а й складними структурами.

Список використаних джерел:

1. Liu Shan, Zhang Min, Kadam Pranav, C.-C. Jay Kuo. 3D Point Cloud Analysis: Traditional, Deep Learning, and Explainable Machine Learning Methods – опубліковано 10 груд. 2021 р. – 146 с.
2. Sestras Paul, Bilașco Ștefan. Geodetic and UAV Monitoring in the Sustainable Management of Shallow Landslides [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mdpi.com/2072-4292/13/3/385>, опубліковано 22 січня 2021 р., видавництво: MDPI.

УДК 004.4 (043.2)

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ KUBERNETES ДЛЯ ПОТРЕБ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Софія Білокур

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олексій Глазок, к.т.н., доц.

Ключові слова: Kubernetes , контейнери , телекомунікації.

Сучасний світ постійно еволюціонує, і зростаюча потреба в безперервному обслуговуванні програм та додатків стає критично важливою. Телекомунікаційні системи повинні забезпечувати високу доступність, ефективність та надійність. У зв'язку з цим впровадження Kubernetes як платформи для управління додатками є надзвичайно актуальним. Ця технологія дозволяє автоматизувати процеси розгортання, управління та масштабування, що відповідає вимогам сучасного бізнесу.

Kubernetes (K8s) – це платформа з відкритим кодом, створена для автоматизації розгортання, управління та масштабування контейнеризованих додатків [3]. Щоб запустити застосунок у Kubernetes, спочатку потрібно упакувати його в один або кілька контейнерних образів, завантажити ці образи в реєстр контейнерів, а потім подати опис вашого застосунку на сервер API Kubernetes, також платформа автоматично змінювати розмір кластера (збільшувати чи зменшувати) в залежності від потреб розгорнутих додатків. Це дозволяє автоматизувати процеси розгортання, управління та масштабування, що відповідає вимогам сучасного бізнесу [1].

Її універсальність дає змогу працювати на фізичних або віртуальних кластерах у локальних, публічних, приватних і гібридних хмарних середовищах. Завдяки незалежності від конкретної інфраструктури кластери можуть бути встановлені на різних публічних і приватних хмарних платформах (AWS, Google Cloud, Azure, OpenStack), а також на фізичних серверах. Крім того, Google Container Engine може забезпечити розгорнутий кластер Kubernetes. Це робить схожим на ядро Linux, яке забезпечує узгодженість між різними апаратними платформами [2].

Використання такої інфраструктури стало необхідним для оптимізації процесів, підтримки надійності сервісів і прискорення впровадження інновацій [3]. Завдяки оптимізації використання ресурсів, Kubernetes допомагає зменшити споживання енергії, сприяючи сталому розвитку технологій у телекомунікаціях. Це має особливе значення в контексті розвитку 5G-технологій, віртуалізації мережевих функцій (NFV) і програмно-налаштованих мереж (SDN). [2]

У сфері телекомунікацій Kubernetes відіграє ключову роль у впровадженні 5G-технологій, які потребують високої адаптивності інфраструктури та динамічного масштабування [2]. Крім того, платформа допомагає зменшувати час простою сервісів і забезпечувати стабільність навіть за умов пікових навантажень телекомунікаційного сектору. Провідні міжнародні корпорації, такі як Vodafone, активно використовують Kubernetes для оптимізації 5G-мереж, управління трафіком і покращення обслуговування клієнтів [1].

Завдяки своїм можливостям платформа дозволяє операторам запускати мережеві сервіси ефективніше, масштабувати інфраструктуру та забезпечувати безперебійну роботу сервісів. Додаткові переваги включають скорочені конвеєри CI/CD, ефективне використання ресурсів, високу доступність, незалежність від середовища та

можливості самовідновлення системи шляхом автоматичного перезапуску або реплікації контейнерів [2]. Всі ці автоматизовані процеси і раціональне використання ресурсів допомагають суттєво зменшити витрати на підтримку інфраструктури. Використання Kubernetes породжує ряд актуальних наукових проблем, які потребують досліджень та розв'язання. Серед них – проблеми, пов'язані з організацією масштабування та оптимізації ресурсів, проблеми безпеки, продуктивності мережі та організації зберігання даних.

Висновок

Kubernetes є потужною платформою, що здатна задовольнити потреби сучасних телекомунікаційних систем, особливо зменшила навантаження на сервери, оскільки контейнеризація стала оптимальним рішенням для управління та передачі даних інфраструктурою.

Розширення функціоналу Kubernetes, додавання системи моніторингу, спрощення інтеграції Kubernetes з різними хмарними сервісами полегшить управління гібридними середовищами через платформу. Розробка універсальних API для легкого переміщення робочих навантажень між різними хмарами створить комфортне розподілення даними між користувачами та полегшить роботу операторам.

Список використаних джерел:

1. Що таке Kubernetes? /Документація по Kubernetes. Концепції. Огляд. – URL: <https://kubernetes.io/uk/docs/concepts/overview/what-is-kubernetes/>
2. Everything Kubernetes: A practical guide. URL: <https://iamondemand.com/wp-content/uploads/2019/11/Kubernetes-eBook.pdf>
3. Marko Lukša. Kubernetes in Action. – Manning, 2018. 624 pages.

УДК 004.4:004.93(043.2)

ПРОГРАМНИЙ ЗАСІБ СУПРОВОДУ ОБ'ЄКТІВ ДЛЯ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

Максим Маслюк

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олексій Глазок к.т.н., доц.

Ключові слова: БПЛА, супровід об'єктів, відеотрекінг, комп'ютерний зір, OpenCV, Raspberry Pi.

Вступ

Сучасні безпілотні літальні апарати (БПЛА) знаходять широке застосування у військовій, цивільній та комерційній сферах, зокрема для моніторингу, розвідки та транспортування вантажів. Однією з ключових задач є точне наведення на ціль, що потребує автоматизації процесів супроводу об'єктів. У сучасних дослідженнях [1, 2] розглядаються різні підходи до розпізнавання та супроводу об'єктів з використанням комп'ютерного зору та штучного інтелекту. Проте існують проблеми, пов'язані з обмеженими обчислювальними ресурсами бортових систем, що обумовлює актуальність розробки ефективних програмних рішень для таких задач.

Метою дослідження є експериментальний аналіз програмного засобу для супроводу об'єктів, який забезпечує точне до наведення прицілу безпілотного літального апарату на обрану ціль з використанням відеотрекінгу на основі алгоритмів MOSSE та CSRT в обмежених обчислювальних ресурсів.

Матеріали та методи: Предметом дослідження є програмний засіб, розроблений мовою Python з використанням бібліотеки OpenCV [3] для обробки зображень. В якості апаратної платформи використовується Raspberry Pi 4, що дозволяє імітувати роботу бортової системи БПЛА. Для супроводу об'єктів застосовано два методи відеотрекінгу: MOSSE (Minimum Output Sum of Squared Error) та CSRT (Channel and Spatial Reliability Tracker). MOSSE обраний через низькі вимоги до обчислювальних ресурсів, тоді як CSRT забезпечує вищу точність за рахунок більшого навантаження на систему. Також використано методи попередньої обробки зображень (фільтрація, контрастування) для підвищення точності розпізнавання цілі.

Результати: Розроблений програмний засіб дозволяє супроводжувати об'єкти у реальному часі. Експерименти з порівнянням методів трекінгу показали, що алгоритм MOSSE забезпечує високу швидкість обробки до 15 кадрів на секунду на Raspberry Pi 4, що робить його придатним для роботи на малопотужних пристроях. З іншого боку, алгоритм CSRT демонструє значно вищу точність, але потребує більше обчислювальних ресурсів, що знижує швидкість обробки до 8-10 кадрів на секунду. Експериментально доведено, що попередня обробка зображень підвищує стійкість обох алгоритмів до змін освітлення та фонових перешкод. Отримані результати демонструють можливість використання розробленого засобу для автономного наведення БПЛА на ціль у реальних умовах, з урахуванням компромісу між точністю та продуктивністю. Також використано методи попередньої обробки зображень (фільтрація, контрастування) для підвищення точності розпізнавання цілі [4, 5].

Висновки

Експериментальне дослідження показало, що програмний засіб із алгоритмом MOSSE є ефективним рішенням для систем з обмеженими обчислювальними ресурсами, забезпечуючи стабільний трекінг із високою швидкістю обробки. З іншого боку, програмний засіб із алгоритмом CSRT демонструє вищу точність супроводу об'єктів, що робить його придатним для завдань, де критичним є точне позиціонування, незважаючи на більші вимоги до обчислювальних потужностей.

Список використаних джерел:

1. Han, Ke. Image object tracking based on temporal context and MOSSE. /Cluster Computing. – June 2017. – Vol. 20 (2). – Pp. 1017-1023. DOI: 10.1007/s10586-017-0800-0 /
2. Xing, Daitao & Unlu, Halil & Evangeliou, Nikolaos & Tzes, Anthony. (2022). "Drone Surveillance Using Detection, Tracking and Classification Techniques"/ In book: Image Analysis and Processing. ICIAP 2022 Workshops /Lecture Notes in Computer Science. – August 2022. – Pp. 446-457. DOI:10.1007/978-3-031-13324-4_38.
3. OpenCV [Електронний ресурс] – Режим доступу до ресурсу: <https://opencv.org>.
4. David S. Bolme, J. Ross Beveridge, Bruce A. Draper, Yui Man Lui. Visual Object Tracking using Adaptive Correlation Filters /IEEE Computer Society Conference on Computer Vision and Pattern Recognition. – August 2010. DOI: 10.1109/CVPR.2010.5539960 [Електронний ресурс] – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/abstract/document/5539960>.
5. Lukezic, A., et al. Discriminative Correlation Filter with Channel and Spatial Reliability." IEEE Conference on Computer Vision and Pattern Recognition (CVPR)/ International Journal of Computer Vision. July 2018. DOI:10.1007/s11263-017-1061-3 [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/310953390_Discriminative_Correlation_Filter_with_Channel_and_Spatial_Reliability.

УДК 004.77:004.738.5:613.9:615.47:004.056

МОБІЛЬНИЙ ДОДАТОК ДЛЯ МОНІТОРИНГУ СТАНУ ЗДОРОВ'Я З ВИКОРИСТАННЯМ ФІЗИЧНИХ НОСІЇВ НА БАЗІ ІОТ

Олександр Гетьман

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Сергій Кравченко, д.т.н., доц.

Ключові слова: мобільний додаток, ІоТ, моніторинг здоров'я, носимі пристрої, кібербезпека.

Вступ

Сучасні технології Інтернету речей (ІоТ) значно розширюють можливості в сфері охорони здоров'я, забезпечуючи персоналізований моніторинг фізіологічних параметрів користувачів. В останніх дослідженнях [1, 2] розглядаються питання інтеграції ІоТ-пристроїв для медичного моніторингу, підкреслюючи їхню ефективність у ранньому виявленні захворювань та підтримці здорового способу життя. Водночас такі технології потребують ефективних рішень щодо безпеки даних і стабільності роботи.

Мета: Розробка мобільного додатку для моніторингу стану здоров'я з використанням фізичних носіїв на базі ІоТ, що забезпечує надійний збір, обробку та візуалізацію фізіологічних показників користувача.

Матеріали та методи: дослідження включає аналіз сучасних платформ для розробки ІоТ-рішень у сфері медицини. Для передачі даних використовуються бездротові протоколи (Bluetooth Low Energy, Wi-Fi). Методика дослідження включає реалізацію алгоритмів збору даних із фізичних носіїв (розумних годинників, фітнес-браслетів), їх обробку за допомогою статистичних методів і візуалізацію в мобільному додатку.

Результати. Розроблений мобільний додаток дозволяє збирати дані про серцевий ритм, рівень кисню в крові, артеріальний тиск та інші параметри з підключених ІоТ-пристроїв. Інформація передається у хмарне сховище для подальшої обробки та аналітики. Реалізовані алгоритми аналізу дозволяють ідентифікувати відхилення від норми та генерувати сповіщення для користувача.

Крім того, забезпечена інтеграція з електронними медичними системами для оперативного доступу лікарів до даних пацієнта. Результати тестування показують високу точність передачі даних та стабільність роботи системи.

Висновки

Мобільний додаток для моніторингу стану здоров'я на базі ІоТ може значно покращити якість медичного обслуговування за рахунок безперервного збору та аналізу фізіологічних параметрів користувача. Отримані результати можуть бути використані для подальшого вдосконалення системи та її впровадження у сферу телемедицини.

Список використаних джерел

1. Smith J., Brown K. IoT-Based Health Monitoring Systems. Journal of Medical Informatics, 2023.
2. Lee R., Kim S. Wearable Health Devices and IoT Integration. International Conference on IoT Technologies, 2022.

УДК 004.891:629.7(043.2)

ІНТЕЛЕКТУАЛЬНИЙ ЗАСІБ КЕРУВАННЯ РУХОМ БПЛА В УМОВАХ МІСЬКОЇ ЗАБУДОВИ

Олена Вязнікова

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олексій Глазок, к.т.н., доц.

Ключові слова: БПЛА, алгоритм, штучний інтелект, датасет, нейромережа

Вступ. 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.

Мета дослідження – розробка інтелектуального засобу керування рухом БПЛА для автоматичного обльоту перешкод в умовах міської забудови. Ключовим елементом цієї розробки є поєднання нейронних мереж та алгоритмів, що забезпечують автономне розпізнавання та обхід перешкод.

Матеріали та методи. Дослідження проведено із застосуванням нейромережевої моделі YOLOv5 для розпізнавання міських об'єктів (дерева, ліхтарі, будинки, дорожні знаки, світлофори) на основі Open Images Dataset v7.

Дані підготовлено шляхом конвертації анотацій у формат YOLOv5 за допомогою інструменту Roboflow, а навчання нейромережі виконано у хмарному середовищі Google Colaboratory.

Для обльоту перешкод використано алгоритм D*-Lite, інтегрований у PX4. Моделювання польоту БПЛА та перевірка ефективності алгоритму здійснені у симуляторі Gazebo, що відтворює умови міської забудови з визначеними

Результати. У ході дослідження встановлено, що використання нейромережевих моделей для розпізнавання перешкод у поєднанні з алгоритмами пошуку оптимальних маршрутів значно покращує ефективність автономного керування БПЛА в умовах міської забудови. Аналіз датасетів, отриманих із Open Images Dataset v7, показав, що якість навчання моделі YOLOv5 безпосередньо залежить від правильності розмітки та репрезентативності вибраних класів об'єктів в анотаціях. Коригування анотацій і конвертація їх у формат, сумісний із YOLOv5, дозволяє підвищити точність розпізнавання ключових міських об'єктів, таких як дерева, ліхтарі, будинки, світлофори та дорожні знаки.

Результати тестування підтвердили, що використання хмарних середовищ, зокрема Google Colaboratory, є ефективним підходом для швидкого навчання моделей, оскільки воно забезпечує оптимальні обчислювальні ресурси для роботи з великими датасетами. Крім того, встановлено, що

алгоритм D*-Lite демонструє високу адаптивність у побудові маршруту обльоту перешкод, що підтверджено під час моделювання в симуляторі Gazebo. Виявлено закономірність, що ефективність уникнення перешкод суттєво залежить від якості інтеграції алгоритму в програмне забезпечення керування БПЛА, зокрема PX4. Отримані дані вказують на те, що поєднання методів машинного навчання та алгоритмічного планування маршруту дозволяє підвищити рівень автономності БПЛА та забезпечити рух у складних урбаністичних умовах.

Висновок. Розроблене програмне забезпечення демонструє актуальність поєднання штучного інтелекту разом із алгоритмами керування БПЛА та уникання ними перешкод. Синтез усіх зазначених технологій та інструментів можна використовувати у будь – яких галузях задля полегшення досягання цілей та економії ресурсів.

Список використаних джерел:

1. A Comprehensive Review of AI-enabled Unmanned Aerial Vehicle: Trends, Vision, and Challenges. /Arxiv. URL: <https://arxiv.org/pdf/2310.16360> .
2. Л.С. Єршова, О.М. Шевченко. Особливості використання штучного інтелекту в умовах воєнного стану на території України. // Юридичний науковий електронний журнал. 2023. № 6. С. 410-413. DOI 10.32782/2524-0374/2023-6/95. URL: http://lsej.org.ua/6_2023/95.pdf.
3. Рухомі засоби Gazebo. PX4. URL: https://docs.px4.io/main/uk/sim_gazebo_gz/vehicles.html .
4. 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 .
5. YOLOv5. URL: <https://docs.ultralytics.com/models/yolov5/>.

УДК 681.52(043.2)

КЕРУВАННЯ РУХОМ ГРУПИ БПЛА ДЛЯ УНИКНЕННЯ СТАТИЧНИХ ТА ДИНАМІЧНИХ ПЕРЕШКОД

Юрій Шестопап

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олексій Глазок, к.т.н., доц.

Ключові слова: безпілотні літальні апарати, уникнення перешкод, траєкторії руху

Вступ

На сьогоднішній день використання безпілотних літальних апаратів (БПЛА) у цивільних і військових цілях зростає та вимагає точної координації між апаратами для спільного виконання завдань [1]. Управління групами БПЛА ускладнюється необхідністю автономного уникнення перешкод у динамічних середовищах. Сучасні методи уникнення перешкод ґрунтуються на поєднанні локальної та глобальної навігації, обробці сенсорних даних та побудові оптимальних траєкторій польоту.

Метою дослідження є аналіз існуючих методів уникнення статичних та динамічних перешкод для керування рухом групи БПЛА, що дозволяють безпечно та коректно змінювати траєкторію польоту з урахуванням динамічних змін у навколишньому середовищі.

Основні підходи до уникнення перешкод у груповому русі безпілотних літальних апаратів (БПЛА) враховують як глобальні, так і локальні аспекти планування маршруту. Одним із ключових методів уникнення

статичних та динамічних перешкод є використання потенційних полів, що дозволяє створювати віртуальну модель середовища, в якій цільові точки діють як центри притягання, а перешкоди – як центри відштовхування. Це забезпечує безперервну адаптацію траєкторії польоту відповідно до розташування об'єктів у просторі. Інший метод, а саме метод оптимізації траєкторії, яка використовується для мінімізації відхилення від запланованого маршруту, базується на алгоритмах пошуку найкоротшого шляху та визначенні оптимальної стратегії руху. Варто зазначити, що важливу роль у визначенні поточного положення БПЛА відіграють методи оптичного потоку та SLAM (Simultaneous Localization And Mapping), які дозволяють створювати та відтворювати карту середовища, а також здійснювати навігацію в умовах змінного середовища. Водночас, метод ORCA (Optimal Reciprocal Collision Avoidance) надає можливість групі БПЛА уникати зіткнень з перешкодами, аналізуючи відносні швидкості об'єктів та розраховуючи безпечні напрями руху кожного БПЛА без централізованого контролю. Ще одним підходом, що використовується для уникнення перешкод, є метод динамічних вікон (Dynamic Window Approach – DWA), який аналізує можливі напрямки руху, враховуючи динамічні характеристики БПЛА. Метод формує набір допустимих швидкостей та кутів повороту, що забезпечують виконання безпечного маневру. Він враховує не тільки геометричне розташування об'єктів, а ще й кінематичні параметри самого БПЛА, такі як максимальне прискорення, гальмування та інерційні обмеження, завдяки чому БПЛА може здійснювати маневри без різких змін курсу, що особливо необхідно при пересуванні в середовищі з великою кількістю перешкод. DWA не лише визначає безпечні шляхи уникнення перешкод, а також адаптує їх з точки зору плавності руху, що є обов'язковим для руху групи БПЛА. У поєднанні з попередніми методами, такими як ORCA та SLAM, підхід сприяє покращенню автономної навігації БПЛА в складних умовах середовища [2, с. 17-31].

Дослідження показало, що застосування методів уникнення статичних та динамічних перешкод значно зменшує ризик зіткнень та підвищує злагодженість руху групи БПЛА. Використання алгоритмів потенційних полів забезпечує плавну корекцію траєкторій в середовищах з невеликою кількістю перешкод, проте в складних умовах з великою кількістю перешкод існує вірогідність виникнення локальних мінімумів, що може спричинити затримку у виборі подальшого маршруту. Метод ORCA надає можливість уникати зіткнень маневруванням групи БПЛА без потреби у централізованому контролі, знижуючи затримки у прийнятті рішень. Методи оптичного потоку та SLAM застосовуються для роботи в змінних умовах, де відсутня заздалегідь відома карта середовища. Метод DWA сприяє коригуванню траєкторії в режимі реального часу, що значно впливає на маневреність руху групи БПЛА у динамічному середовищі. При комбінованому застосуванні декількох методів вдається збільшити точність систем уникнення статичних та динамічних перешкод, забезпечуючи безперервність польоту групи БПЛА навіть у складному середовищі.

Висновок. Використання методів уникнення статичних та динамічних перешкод надає можливість покращити автономність груп БПЛА та забезпечити безпечне виконання місій у динамічному середовищі. Отримані результати можуть бути застосовані у сферах аеророзвідки, рятувальних операцій та інших сфер, де існує необхідність в автономному ухваленні рішень.

Список використаних джерел:

1. Yoav Gottlieb, Tal Shima. UAVs Task and Motion Planning in the Presence of Obstacles and Prioritized Targets: Israel Institute of Technology, 2015. – 5 p.
2. Erika Mai. Obstacle Detection and Avoidance Techniques for Unmanned Aerial Vehicles: Master Degree Thesis. – Politecnico di Torino, 2020. – 126 p.

УДК 004.752:004.738.5:061.2

ПРОГРАМНИЙ МОДУЛЬ ОНЛАЙН-ПЛАТФОРМИ ДЛЯ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ**Анастасія Миколенко***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олена Монченко, к.т.н., проф.*

Ключові слова: волонтерська діяльність, збір коштів, онлайн-платформа.

Вступ. Цифрові рішення – це невід'ємна частина соціальної взаємодії у сучасному світі. В останні роки спостерігається активний розвиток онлайн-платформ, що дозволяють ефективніше координувати соціальні ініціативи та благодійні проекти [1]. Цифрові технології суттєво розширили можливості для громадських ініціатив, надаючи нові способи збору коштів і залучення волонтерів [2]. Цифровізація волонтерської діяльності не тільки сприяє ефективності та доступності допомоги, але й надає громадянам зручні інструменти для фінансової підтримки важливих соціальних проектів [3]. Завдяки цифровим інструментам, волонтерські організації можуть ефективно комунікувати з потенційними донорами та волонтерами, забезпечуючи прозорість використання зібраних коштів та підвищуючи довіру до своїх ініціатив. Цифровізація також дозволяє аналізувати дані про пожертви та волонтерську діяльність, що сприяє покращенню стратегій залучення ресурсів та підтримки соціальних проектів [4]. Веб-платформа для збору коштів на волонтерські ініціативи стає важливим ресурсом, що дозволяє максимально спростити процес отримання допомоги та забезпечити прозорість використання зібраних ресурсів. Платформа надає можливість створювати та підтримувати благодійні збори у зручному форматі та популяризувати важливість допомоги у сучасному світі.

Основна частина. Метою дослідження є розробка програмного модуля для онлайн-платформи збору коштів на волонтерські ініціативи. Основна мета модуля – забезпечити безпечну обробку фінансових транзакцій, автоматизувати процеси моніторингу прогресу зборів та створити механізми звітності для підтвердження цільового використання коштів. На основі аналізу була розроблена архітектура програмного модуля, яка включає компоненти для збереження та обробки фінансової інформації; сервіс автентифікації та авторизації; систему відстеження історії платежів; автоматизований генератор звітів про використання коштів.

Для реалізації програмного модуля було обрано сучасний стек технологій: середовище розробки Visual Studio Code; мову програмування TypeScript для забезпечення статичної типізації та покращеної безпеки коду; Node.js для серверної частини модуля; Express.js для створення API; MongoDB для збереження інформації про збори та внески; React.js для створення користувацького інтерфейсу;

Висновки. Робота присвячена розробці програмного модуля для онлайн-платформи збору коштів на волонтерські ініціативи. У ході роботи була створена архітектура модуля, що відповідає сучасним вимогам, та визначено стек технологій для його реалізації, включаючи TypeScript, Node.js, Express.js, MongoDB, та React.js. Впровадження даного модуля значно підвищить рівень довіри до благодійних ініціатив, забезпечуючи захист операцій та прозору звітність.

Список використаних джерел:

1. Благодійність в епоху цифрових технологій. URL: <https://bestfriends.com.ua/blog/blagodijnist-v-epohu-cifrovih-tehnologij>
2. Онлайн платформи та їхній вплив на розвиток спільнот. URL: <https://welfare.green/onlajjn-platformi-ta-ikhnijj-vpliv-na-rozvitok-spilnot>
3. Феномен фандрейзингу в Україні у 2024 році: уроки єдності, інновацій та сили волонтерства. URL: <https://egoistmagaz.in.ua/syspilstvo/fenomen-fandreyzynhu-v-ukrayini-u-2024-rotsi-uroky-yednosti-innovatsiy-ta-syly-volonterstva/>
4. Фандрейзинг в Україні: шляхи до залучення коштів. URL: <https://welfare.green/fandrejjzing-v-ukraini-shlyakhi-do-zaluchennya-koshtiv>

УДК 004.946 (043.2)

ПРОГРАМНИЙ МОДУЛЬ ВІЗУАЛІЗАЦІЇ КОМПОНЕНТІВ БПЛА З ВИКОРИСТАННЯМ AR-ТЕХНОЛОГІЇ

Аріна Кравченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник –Росінська Галина Павлівна, к.т.н., доцент

Ключові слова: доповнена реальність, БПЛА, візуалізація, програмний модуль, 3D-моделювання.

Програми електронного навчання з підтримкою AR відображають доповнений об'єкт на екрані та відтворюють 3D-прикладні концепції, які дозволяють учням навчатися та залучати. Загалом також широко використовується комп'ютерна графіка, яка дає змогу зафіксувати об'єкт і відобразити його в розширеному середовищі, а також здійснювати пошук щодо об'єкта. Це означає, що програма може отримувати зображення об'єктів із реального середовища та надавати детальний опис об'єкта. Ви також можете створити власну програму електронного навчання з доповненою реальністю з унікальною концепцією.

Використання технологій доповненої реальності (AR) у поєднанні з безпілотними літальними апаратами (БПЛА) відкриває нові перспективи в навчанні та тренуванні операторів. AR дозволяє створювати віртуальні шари, які накладаються на реальні зображення, покращуючи сприйняття просторових об'єктів та сприяючи ефективнішому аналізу конструкції БПЛА.

Основною метою є створення програмного модуля, який забезпечить інтерактивне 3D-відображення компонентів БПЛА в середовищі доповненої реальності. Для досягнення цієї мети передбачено:

- Створення інтерактивного 3D-відображення компонентів БПЛА у середовищі доповненої реальності. Це дозволить користувачам детально ознайомитися з конструкцією та функціональними особливостями кожного компонента.
- Розробка механізму взаємодії з моделями. Користувачі зможуть змінювати ракурс перегляду, масштабувати зображення та отримувати додаткову інформацію про складові частини БПЛА, що сприятиме глибшому розумінню матеріалу.

- Аналіз ефективності використання розробленого модуля у контексті навчання. Оцінка впливу AR-візуалізації на якість засвоєння знань та навичок операторів БПЛА.

Використання доповненої реальності в навчальних програмах для операторів БПЛА має кілька ключових переваг:

- Покращене сприйняття просторових об'єктів. AR дозволяє візуалізувати складні конструкції в реальному масштабі та контексті, що сприяє кращому розумінню їхньої будови та функціонування.

- Інтерактивність. Можливість взаємодії з віртуальними моделями в реальному часі підвищує залученість та мотивацію учнів.

- Доступність. AR-технології можуть бути використані на різних пристроях, таких як смартфони, планшети чи спеціалізовані окуляри, що робить навчання більш гнучким та доступним.

Висновок

Розробка та впровадження програмного модуля для AR-візуалізації компонентів БПЛА є перспективним напрямом, який може значно покращити якість навчання та підготовки операторів. Інтеграція доповненої реальності в освітній процес сприяє глибшому розумінню матеріалу, підвищує ефективність навчання та відкриває нові можливості для інтерактивного вивчення складних технічних систем.

Список використаних джерел:

1. Augmented Reality (AR) In Education: A Staggering Insight Into The Future. eLearning Industry. URL: <https://elearningindustry.com/augmented-reality-in-education-staggering-insight-into-future> (дата звернення: 23.03.2025).

2. Імерсивні технології в освіті: збірник матеріалів науково-практичної конференції, 16 листопада 2022 року / НАПН України, Інститут цифровізації освіти. Київ: 2022.

УДК 004.85(043.2)

ПРОГРАМНИЙ МОДУЛЬ НАПІВАВТОМАТИЧНОЇ РОЗМІТКИ ТА ПІДГОТОВКИ ДАТАСЕТІВ ДЛЯ YOLO

Володимир Балабан

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Юрій Дегтяр, ст. викл.

Ключові слова: Розмітка даних, комп'ютерний зір, машинне навчання, виявлення об'єктів, зв'язування даних.

Вступ. Розробка та впровадження систем комп'ютерного зору, зокрема алгоритмів виявлення об'єктів, є одним із пріоритетних напрямків сучасних інформаційних технологій. Модель YOLO (You Only Look Once) зарекомендувала себе як ефективний інструмент для детекції об'єктів у реальному часі завдяки високій швидкодії та точності. Проте, якість роботи моделі YOLO безпосередньо залежить від якості навчальних датасетів, створення яких є трудомістким процесом. Ручна розмітка зображень вимагає значних часових ресурсів і схильна до помилок, тоді як повністю автоматизовані методи часто не забезпечують необхідної точності. Метою роботи є створення

програмного застосунку на базі C# та WPF, який поєднує переваги автоматичних алгоритмів з можливістю ручної корекції для підвищення ефективності підготовки датасетів для YOLOv11.

Матеріали і методи. Для розробки програмного застосунку було обрано мову програмування C# у поєднанні з фреймворком WPF для створення сучасного графічного інтерфейсу. Архітектурна модель MVVM (Model-View-ViewModel) стала основою програмного рішення, забезпечуючи ефективне розділення бізнес-логіки та презентаційного шару.

Така архітектура не лише підвищує модульність коду, але й значно спрощує процеси тестування, розширення та підтримки продукту. Особливу роль у реалізації MVVM відіграє механізм зв'язування даних, який забезпечує автоматичну синхронізацію даних між моделлю та інтерфейсом користувача, мінімізуючи обсяг коду та зменшуючи ймовірність помилок при оновленні відображення.

Результати. Розроблений програмний застосунок на C# та WPF забезпечує ефективну напівавтоматичну розмітку зображень для створення навчальних датасетів YOLOv11. В результаті проведеної роботи:

- Створено інтуїтивно зрозумілий інтерфейс для розмітки зображень із застосуванням WPF.
- Забезпечено можливість класифікації об'єктів з візуальним відображенням різних класів.
- Реалізовано експорт даних у форматі, сумісному з YOLOv11.

Інтерфейс програми, побудований на WPF, забезпечує високу інтерактивність та чутливість при роботі з зображеннями, а реалізація паттерну зв'язування даних дозволяє миттєво відображати зміни в модель даних, що значно полегшує процес розмітки для користувачів з різним рівнем технічної підготовки.

Висновки. Розроблений програмний застосунок на C# та WPF для напівавтоматичної розмітки та підготовки датасетів для YOLOv11 демонструє ефективність гібридного підходу, що поєднує автоматичні алгоритми з можливістю ручної корекції. Використання паттерну зв'язування даних забезпечило тісну інтеграцію користувацького інтерфейсу з логікою програми, що підвищило ефективність взаємодії користувача з системою. Застосунок може бути використаний як у навчальних, так і в комерційних проектах комп'ютерного зору для підготовки якісних даних для навчання моделей YOLOv11. Подальший розвиток програми передбачає впровадження алгоритмів активного навчання та розширення функціоналу для підтримки різних форматів даних.

Список використаних джерел:

1. Документація по YOLOv11. URL: <https://github.com/ultralytics/ultralytics>
2. Документація по WPF. URL: <https://learn.microsoft.com/en-us/dotnet/desktop/wpf/?view=netdesktop-9.0>
3. Data binding overview (WPF .NET), URL: <https://learn.microsoft.com/en-us/dotnet/desktop/wpf/data/?view=netdesktop-9.0>

УДК 004.056.52(043.2)

ПРОГРАМНИЙ МОДУЛЬ БАТЬКІВСЬКОГО КОНТРОЛЮ ЗА ДОСТУПОМ ДИТИНИ ДО ІНФОРМАЦІЇ У ПЕРСОНАЛЬНОМУ КОМП'ЮТЕРІ

Ярослав Приймак

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Надія Марченко, к.т.н., доц.

Ключові слова: програмний модуль, батьківський контроль, моніторинг активності.

У наш час діти мають необмежений доступ до інформаційних ресурсів, які можуть містити небажаний та травмуючий контент. Через відсутність нагляду підвищуються ризики негативного впливу інтернет-контенту на психоемоційний стан дитини. Численні дослідження чітко показують, що чимало користувачів соціальних мереж, особливо діти, можуть ставати жертвами кіберзлочинності та психологічного тиску [1]. Ці небезпеки включають інформаційні маніпуляції, різноманітний шкідливий контент, а також часте та майже неконтрольоване споживання інформації, що може помітно негативно впливати на розвиток дитини [2] – тому розробка програмного модуля батьківського контролю є актуальним завданням.

Для реалізації програмного модуля була обрана мова програмування C#. Програма має виконувати такі функції: фільтрація контенту, моніторинг активності та обмеження часу використання комп'ютера. Блокування веб-сайтів виконується шляхом внесення їх доменних імен у локальний файл hosts, що перенаправляє запити до цих ресурсів на локальну IP-адресу (127.0.0.1). Для блокування програм використовується перехоплення процесів Windows через API-функцію CreateToolhelp32Snapshot, що дозволяє виявляти запущені додатки. Моніторинг активності реалізовано шляхом ведення журналу відвіданих веб-ресурсів і запущених програм. Також були впроваджені часові обмеження для контролю активності використання ПК з можливістю встановлення індивідуальних налаштувань, вони реалізуються через системний таймер, котрий відстежує активний час користування комп'ютером та конкретними програмами. Для забезпечення безпеки передбачено систему авторизації користувача.

Дана програма реалізує три основні функції: контент-фільтрацію, моніторинг активності та обмеження по часу. Фільтрація споживаного контенту відбувається за допомогою настроюваного блокування веб-сайтів та програм. Система моніторингу активності записує інформацію про відкриті програми та відвідані інтернет-ресурси. Крім цього, є можливість налаштування надсилання оповіщень батькам про спроби доступу до заблокованих веб-ресурсів або програм. Функція обмеження часу дозволяє встановлювати як загальні ліміти використання комп'ютера, так і окремі часові інтервали для певних програм або веб-сайтів. Це сприяє раціональному розподілу часу дитини між навчанням, відпочинком та розвагами.

Висновок

Розроблений програмний модуль батьківського контролю є ефективним рішенням обмеження доступу дітей до небажаної інформації та регулюванням часу користування комп'ютером. Простота використання та можливість адаптації під індивідуальні потреби робить його зручним інструментом для батьків. На відміну від багатьох комерційних рішень, дана система має гнучке налаштування. Подальші дослідження можуть бути спрямовані на інтеграцію штучного інтелекту для аналізу контенту в реальному часі, а також розширення функціональності шляхом додавання контролю за соціальними мережами та месенджерами.

Список використаних джерел:

1. Дубовий Д.О., Вітківська О.С. Проблеми безпеки користувачів соціальних мереж (віктимологічний аспект). – 2021.
2. Артемов В.Ю. Ризики, які виникають в ході використання соціальних мереж Інтернеті: психологічний аспект. – 2020.

УДК 004.51 (043.2)

ПРОГРАМНИЙ МОДУЛЬ ВІДСЛІДКУВАННЯ РУХУ ГРОМАДСЬКОГО ТРАНСПОРТУ

Максим Пономар

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Надія Марченко, к.т.н., доц.

Ключові слова: відслідковування транспорту, парсинг даних, громадський транспорт, API, візуалізація даних.

Вступ

Розвиток міського транспорту вимагає сучасних технологічних рішень для покращення якості перевезень. Важливо забезпечити пасажирів точною та актуальною інформацією про рух громадського транспорту, що дозволить оптимізувати їхні поїздки та скоротити час очікування. Одним із таких рішень є розробка програмного модуля для відслідковування руху громадського транспорту, що базується на парсингу даних із веб-ресурсу Easy Way. Даний ресурс містить інформацію про маршрути, розклади та фактичне місцезнаходження транспорту. У цій роботі розглянуто методи збору, обробки та візуалізації отриманих даних.

Матеріали і методи

Для реалізації програмного модуля використовуються сучасні програмні засоби та методи обробки даних. Основною мовою програмування є Python, що забезпечує широкі можливості для роботи з веб-ресурсами та базами даних. Парсинг інформації здійснюється за допомогою бібліотек BeautifulSoup і Selenium, що дозволяють отримувати дані як із статичних, так і з динамічних веб-сторінок. Отримані дані обробляються за допомогою Pandas, а для їхнього збереження використовується база даних,

наприклад, SQLite або PostgreSQL. Доступ до інформації реалізовано через веб-сервер на Flask, що дозволяє надавати API для взаємодії з іншими сервісами. Зібрані дані структуровано у форматах JSON або CSV та інтегровано з картографічними сервісами, такими як Google Maps API або OpenStreetMap, для їхньої візуалізації. Це дозволяє користувачам отримувати актуальну інформацію про рух транспорту та прогнозувати його прибуття на зупинки.

Результати

Було розроблено функціональний програмний модуль, що дозволяє автоматично отримувати та обробляти інформацію про рух громадського транспорту. Основні можливості модуля включають:

- Автоматизований збір даних із сайту Easy Way, що працює у фоновому режимі.
- Фільтрацію та оновлення отриманих даних у базі, що дозволяє зберігати лише актуальну інформацію.
- Побудову API, яке надає доступ до даних про поточне місцезнаходження транспорту.
- Інтерактивний веб-інтерфейс для перегляду маршрутів та прогнозування часу прибуття транспорту на зупинки.
- Можливість інтеграції з мобільними додатками або сторонніми сервісами через API.

Розроблений модуль дозволяє пасажирам оперативно отримувати інформацію про рух транспорту, що сприяє підвищенню зручності користування громадським транспортом та зменшенню часу очікування на зупинках.

Висновки

Розроблений модуль забезпечує автоматизований збір, обробку та візуалізацію даних про рух громадського транспорту, що підвищує зручність для пасажирів. Він дозволяє отримувати актуальну інформацію в реальному часі, прогнозувати прибуття транспорту та інтегрувати дані з мобільними додатками. Подальший розвиток може включати тестування у реальних умовах та розширення функціональності для оптимізації маршрутів і співпраці з транспортними службами.

Список використаних джерел:

1. Документація EasyWay API: <https://www.eway.in.ua/ua/api> – офіційна документація для доступу до даних про маршрути та рух транспорту.
2. libcurl: бібліотека для виконання HTTP-запитів і отримання даних. URL: <https://curl.se/libcurl/>.
3. SQLite: <https://www.sqlite.org/> – база даних для зберігання та обробки даних.
4. OpenStreetMap API: <https://wiki.openstreetmap.org/wiki/API> – API для картографічних даних та інтеграції карт.

УДК 004.8 (043.2)

СИСТЕМА РОЗПІЗНАВАННЯ ГОЛОСОВИХ КОМАНД КОМП'ЮТЕРОМ ЗА ДОПОМОГОЮ C#

Ігор Марецький

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Голего, старший викладач

Ключові слова: розпізнавання мови, C#, штучний інтелект, голосове управління, автоматизація.

Розпізнавання людської мови є однією з ключових технологій сучасних комп'ютерних систем. Воно широко застосовується у віртуальних асистентах, системах автоматизації та програмному забезпеченні для осіб з обмеженими можливостями. Використання мови програмування C# та інструментів для обробки голосових сигналів дозволяє ефективно реалізовувати голосове управління в програмних продуктах [2].

Метою даного дослідження є аналіз можливостей реалізації системи розпізнавання усних команд за допомогою мови C# та бібліотек для їх подальшого опрацювання, а також дослідження ефективності роботи алгоритмів перетворення голосу в текст.

Системи розпізнавання мовлення базуються на штучному інтелекті та методах обробки природної мови. Вони використовують нейронні мережі та алгоритми машинного навчання для аналізу голосових сигналів і перетворення їх у слова. Одним з ключових елементів є лінгвістична модель, яка дозволяє враховувати контекст сказаного, що значно підвищує точність розпізнавання. Основним є ідентифікація мови за принципом аналізу акустичних характеристик голосу, його частотного спектру. Ці параметри дозволяють системам аналізувати окремі фонети та лексеми, навіть у складних акустичних умовах [1].

Для реалізації розпізнавання усних інструкцій використано мову програмування C# та сучасні бібліотеки для мовного аналізу System.Speech.Recognition. Методика дослідження включає розробку тестового додатка, який приймає голосові команди та виконує відповідні дії. Аналіз здійснено шляхом тестування системи на різних мовних моделях та акцентах користувачів.

Система успішно розпізнає мовлення та виконує відповідні дії. Браузер Edge і Notepad відкриваються без проблем, а запуск Discord залежить від правильного шляху до файлу. Команда закриття додатків передбачена, але не реалізована. Ідентифікація працює добре при стандартній англійській вимові, але акцент і фоновий шум можуть впливати на точність. Відгук системи швидкий, а використання ресурсів мінімальне. Бібліотека System.Speech.Recognition дозволяє легко реалізувати голосове управління, але поступається сучасним AI-моделям за точністю [1].

Розглянута технологія може бути інтегрована в різні програмні рішення, зокрема в системи розумного будинку, керування ПК та мобільними пристроями, а також у додатки для користувачів з обмеженими можливостями. Використання C# та бібліотек для мовного аналізу дозволяє створювати

адаптивні інтерфейси, що підвищують зручність взаємодії з комп'ютером і автоматизують виконання повсякденних завдань. Крім того, подібні рішення можуть застосовуватися в робототехніці, де голосові команди використовуються для керування механізмами або виконання складних сценаріїв. Подальше вдосконалення алгоритмів розпізнавання дозволить підвищити точність роботи систем навіть у шумних середовищах та для різних мовних акцентів.

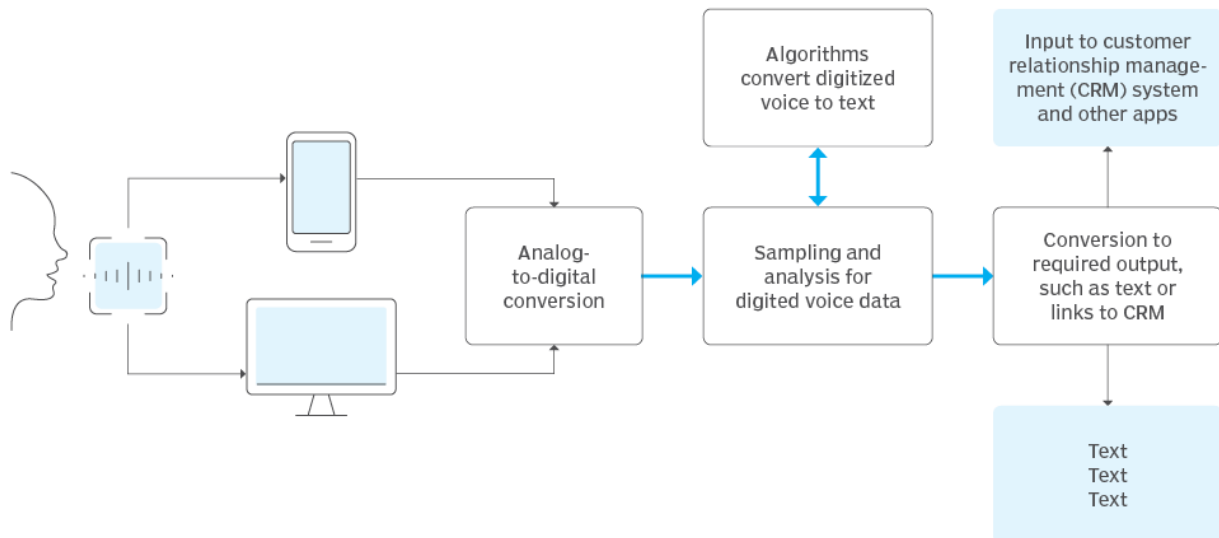


Рис.1. Етапи переходу від мови до тексту

Висновки

Розроблена система демонструє можливість ефективного використання мови C# для голосового управління. Подальші дослідження можуть включати покращення алгоритмів шумозахисту та адаптацію до різних мов і діалектів.

Список використаних джерел:

1. Пауль Кірман. Що таке розпізнавання мовлення? [Електронний ресурс]. URL: <https://www.techtarget.com/searchcustomerexperience/definition/speech-recognition>
2. Вікіпедія. [Розпізнавання мовлення](#).

УДК 004.22 (043.2)

ОПТИМІЗАЦІЯ ПАСИВНИХ СИСТЕМ НАВЕДЕННЯ: МЕТОДИ ОБРОБКИ СИГНАЛІВ ТА АЛГОРИТМ MUSIC**Роман Корчемний***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олена Нечипорук, д.т.н., проф.*

Ключові слова: пасивні радіолокаційні системи (ПРС), алгоритм MUSIC, обробка сигналів, моніторинг, навігація.

Пасивні радіолокаційні системи (ПРС) є важливим компонентом сучасних технологій навігації, моніторингу та безпеки. Вони отримують сигнали від сторонніх джерел, таких як мобільні мережі чи супутники, що забезпечує їхню скритність і низьке енергоспоживання. Сучасні дослідження спрямовані на підвищення точності ПРС шляхом вдосконалення методів обробки сигналів, серед яких особливу роль відіграє алгоритм MUSIC. Цей алгоритм забезпечує високу роздільну здатність та здатність одночасно працювати з кількома джерелами сигналу, що робить його ефективним інструментом для тактичного моніторингу, контролю повітряного простору та громадської безпеки.

Основним напрямком удосконалення пасивних систем є інтеграція сучасних програмних модулів, які поєднують широкий спектр методів обробки сигналів. Від фільтрації та коваріаційного аналізу до використання машинного навчання та нейронних мереж – ці технології дозволяють підвищити ефективність ПРС навіть у складних середовищах із високим рівнем шуму та багатошляховим поширенням сигналів. Методи Track-Before-Detect, крос-кореляційний аналіз та синтез апертури дозволяють значно покращити точність визначення цілей, забезпечуючи надійність навіть у міських або віддалених районах.

Алгоритм MUSIC демонструє особливу ефективність у пасивних системах наведення завдяки високій точності та стійкості до перешкод. Він дозволяє ідентифікувати та відстежувати об'єкти навіть за низького рівня сигналу, що є критично важливим для стратегічних та тактичних завдань. Завдяки можливості працювати у багатоканальних системах, цей алгоритм забезпечує точність та надійність роботи ПРС, що робить їх важливим інструментом у сфері оборони, екологічного моніторингу та навігації.

Сучасні тенденції розвитку пасивних систем наведення передбачають інтеграцію штучного інтелекту, використання нових алгоритмів обробки сигналів, а також впровадження мереж 5G та енергоефективних технологій. Завдяки цьому ПРС продовжують удосконалюватися, забезпечуючи високу точність, скритність та ефективність роботи у різних сферах. Поєднання адаптивних технологій

та алгоритму MUSIC значно розширює можливості пасивних систем, роблячи їх надійним та перспективним рішенням для навігації, моніторингу та розвідки.

Список використаних джерел:

1. IEEE Transactions on Industrial Informatics information for authors. URL: <https://ieeexplore.ieee.org/document/6631538>
2. Phased Array System Toolbox. URL: <https://www.mathworks.com/help/phased/ug/direction-of-arrival-estimation.html>
3. Supplemental Files. URL: https://www.researchgate.net/publication/331882259_Performance_comparison_of_MUSIC_and_ESPRIT_algorithms_in_DOA_estimation

УДК 004.942 (043.2)

РОЛЬ СИМУЛЯЦІЇ ІОТ-ПРИСТРОЇВ У РОЗРОБЦІ ЕФЕКТИВНИХ СИСТЕМ УПРАВЛІННЯ МІСЬКИМ ПАРКУВАННЯМ

Артем Чинник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Голего, старший викладач

Ключові слова: Інтернет речей (IoT), симуляція, розумне паркування, Cooja, Contiki OS, моделювання, управління паркінгом, міська інфраструктура, Smart City, сенсорна мережа, передача даних, паркомісця, тестування, мережеві втрати, цифровізація, проектування IoT-систем.

Із кожним роком кількість автомобілів у містах України зростає, що створює нові виклики для організації дорожнього руху та ефективного використання паркувального простору. Проблема нестачі паркомісць, нераціонального їх розміщення та відсутності оперативної інформації про завантаженість паркінгів є типовими для багатьох населених пунктів. Традиційні підходи, що базуються на ручному обліку або розміщенні табличок, не можуть задовольнити потреби сучасного динамічного міста [1]. У зв'язку з цим виникає необхідність у впровадженні розумних технологій, які дозволяють автоматизувати процес управління паркуванням і підвищити комфорт для водіїв. Одним із перспективних напрямів є застосування систем на основі Інтернету речей (IoT), які забезпечують онлайн-моніторинг і контроль за станом паркувального простору [2].

Повноцінне розгортання IoT-систем потребує значних фінансових ресурсів, часу та людських зусиль. Зазвичай, проблеми та помилки виявляються вже на стадії впровадження, що призводить до додаткових витрат і затримок [3]. Складність полягає також у необхідності передбачення різноманітних сценаріїв поведінки системи в реальному середовищі. Тестування в польових умовах, особливо у великому місті, може бути технічно неможливим або надто дорогим. Через це симуляція – тобто віртуальне моделювання поведінки IoT-пристроїв і їхньої взаємодії – стає вкрай актуальною [6].

Ця робота спрямована на обґрунтування доцільності використання симуляцій IoT-пристроїв на етапі проєктування систем управління паркуванням, а також аналіз їхніх переваг порівняно з традиційними методами розробки та впровадження таких рішень [3].

Для моделювання роботи систем управління паркінгом на основі IoT можуть використовуватись такі симуляційні середовища, як Cooja, NS-3, OMNeT++ [4; 5]. Вони дозволяють змодельовати мережеву взаємодію сенсорів, передачу та втрату даних, різні топології розміщення пристроїв та навіть вплив зовнішніх чинників. У симуляціях можна перевірити, як система реагує на зміну трафіку, втрату зв'язку, збільшення кількості користувачів, перевірити алгоритми прийняття рішень контролером та протестувати поведінку серверної частини.

Для перевірки функціонування системи управління паркуванням була змодельована базова IoT-мережа з використанням симуляційного середовища Cooja, що входить до складу операційної системи Contiki OS [4]. Модель відтворює умовну ділянку міста з 10 паркувальними місцями, кожне з яких обладнане віртуальним сенсором наявності автомобіля. Сенсори періодично передають дані про статус паркомісця (вільне/зайняте) до центрального вузла (gateway), який, у свою чергу, надсилає агреговану інформацію на сервер управління.

У моделі реалізовано:

- Топологію мережі типу «зірка», де всі сенсори безпосередньо з'єднані з головним вузлом.
- затримки передачі даних, типові для міського середовища (100–300 мс).
- втрату пакетів у 5–10% випадків для перевірки стійкості системи.
- зміни статусу паркомісць у випадковому порядку з інтервалом 20–60 секунд (імітація прибуття та від'їзду автомобілів).
- формат передачі даних у вигляді простих JSON-повідомлень, які можна легко адаптувати до реальної серверної інфраструктури.

Модель дозволила виявити потенційні проблеми синхронізації даних, перевірити швидкість оновлення інформації на сервері та визначити оптимальний інтервал між сеансами зв'язку сенсорів і центрального вузла, щоб зменшити навантаження на мережу [3].

Використання симуляції дає змогу виявити помилки в логіці ще до початку фізичної реалізації. Наприклад, в моделюванні можна з'ясувати, що пристрої неефективно розподіляють навантаження між собою, або що дані передаються із запізненням, що може спричинити некоректну роботу паркінгового контролера. Крім того, симуляція дозволяє дослідити оптимальне розміщення сенсорів, протестувати кілька варіантів конфігурації без витрат на фізичне обладнання [3]. У навчальному процесі симуляція є чудовим інструментом для ознайомлення студентів із принципами роботи IoT-систем, а для інженерів – способом швидкої перевірки ідей без ризиків [2].

Висновок

Симуляція IoT-пристроїв – це не просто зручний інструмент, а необхідний етап сучасного проєктування «розумних» міських систем, зокрема систем управління паркінгом. Вона дозволяє зменшити витрати, уникнути помилок на ранніх етапах, підвищити надійність і масштабованість майбутнього рішення. У світлі розвитку концепції Smart City та цифровізації міської інфраструктури, симуляція є важливим кроком до впровадження ефективних, доступних та технологічно досконалих рішень у сфері міського управління [6].

Список використаних джерел:

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376. <https://doi.org/10.1109/COMST.2015.2444095>
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
3. Shah, R., & Kumar, R. (2022). Simulation Tools for IoT-Based Smart Parking Systems: A Review. <https://www.researchgate.net/publication/361497319>
4. Cooja Simulator - Contiki OS Wiki. <https://github.com/contiki-os/contiki/wiki/Cooja-Simulator>
5. OMNeT++ Network Simulator. <https://omnetpp.org/>
6. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, 58, 49–69. <https://doi.org/10.1007/s11277-011-0288-5>

УДК 004.8 (043.2)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ МОНІТОРИНГУ СТАНУ АВІАЦІЙНОЇ ТЕХНІКИ В РЕАЛЬНОМУ ЧАСІ

Юлія Бойко

Фаховий коледж інженерії, управління та землевпорядкування Державного некомерційного підприємства "Державний університет "Київський авіаційний інститут", Київ

Науковий керівник – Наталія Рябчук, викладач-методист

Ключові слова: Інтернет речей, моніторинг, авіаційна техніка, реальний час, діагностика.

Сучасні авіаційні системи потребують високого рівня надійності та безпеки. Інтернет речей (IoT) відкриває нові можливості для моніторингу стану авіаційної техніки в реальному часі, що сприяє підвищенню безпеки польотів та зниженню витрат на технічне обслуговування.

Метою дослідження є аналіз застосування IoT-технологій для моніторингу стану авіаційної техніки в реальному часі, а також оцінка їх впливу на безпеку польотів.

Для дослідження було використано методи аналізу літературних джерел, моделювання роботи IoT-систем у сфері авіаційної техніки, а також аналіз практичних кейсів впровадження таких технологій у реальних умовах експлуатації авіатранспорту.

Сучасні IoT-сенсори забезпечують постійний збір даних про ключові параметри роботи авіаційної техніки, такі як температура двигунів, вібрації, тиск у гідравлічних системах, витрата палива та інші

показники. Ці дані передаються у реальному часі до наземних центрів обробки інформації через бездротові мережі, що дозволяє оперативно реагувати на відхилення від норми.

Зібрані дані аналізуються за допомогою алгоритмів машинного навчання для прогнозування можливих поломок. Наприклад:

- виявлено, що підвищення вібрацій понад норму може свідчити про зношення підшипників двигуна;
- аналіз температурних показників дозволяє прогнозувати перегрів окремих компонентів задовго до критичного стану.

Це дозволяє авіакомпаніям планувати технічне обслуговування заздалегідь, зменшуючи кількість непередбачуваних простоїв літаків.

Використання IoT сприяє оптимізації роботи літаків:

- зниження витрат палива завдяки аналізу польотних даних і корекції маршрутів;
- підвищення точності прогнозування залишкового ресурсу компонентів, що дозволяє уникати надмірного ремонту.

Завдяки IoT-системам кількість аварійних ситуацій через технічні несправності зменшиться у порівнянні з традиційними методами моніторингу. Це досягається завдяки ранньому виявленню потенційних проблем і можливості їх усунення до виникнення критичних ситуацій.

IoT-платформи інтегруються з існуючими системами управління польотами і технічного обслуговування. Наприклад, використання хмарних платформ дозволяє централізовано зберігати та аналізувати великі обсяги даних, забезпечуючи доступ до них у будь-який момент.

Висновок

Технології Інтернету речей відкривають значні можливості для оптимізації процесів моніторингу та обслуговування авіаційної техніки. Їхнє впровадження дозволяє підвищити безпеку польотів, знизити витрати на технічне обслуговування та продовжити термін служби авіаційного обладнання. Подальші дослідження у цій сфері мають бути спрямовані на вдосконалення методів аналізу великих даних та підвищення надійності IoT-систем у критичних умовах експлуатації.

Список використаних джерел:

1. GlobalLogic Ukraine. (n.d.). End-to-End IoT Рішення. GlobalLogic. URL: <https://www.globallogic.com/ua/technology-capabilities/end-to-end-iot/>
2. DusunIoT. (2023, July 14). Віддалений моніторинг IoT: керування активами та відстеження умов з будь-якої точки світу. DusunIoT. URL: <https://www.dusuniot.com/uk/blog/iot-remote-monitoring-managing-assets-and-tracking-conditions-from-anywhere-in-the-world/>
3. Allbest. (n.d.). Використання Інтернету речей у виробництві та логістиці. Allbest. URL: https://revolution.allbest.ru/marketing/01492178_0.html
4. SkyPlanner. (n.d.). Інтернет речей: Розширення можливостей виробництва. SkyPlanner. URL: <https://skyplanner.ai/uk>

УДК 004.89 (043.2)

АНАЛІЗ ТЕХНІЧНИХ СТРАТЕГІЙ ТА КІБЕРЗАГРОЗ НА ІНТЕЛЕКТУАЛЬНІ ТРАНСПОРТНІ СИСТЕМИ В УМОВАХ КІБЕРВІЙНИ

Олександра Ярошенко

Фаховий коледж інженерії, управління та землевпорядкування Державного некомерційного підприємства Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Рябчук, викладач-методист

Ключові слова: інтелектуальні системи, штучний інтелект, кібервійна, критична інфраструктура.

Інтелектуальні авіаційні системи стають невід'ємною частиною сучасної авіації, забезпечуючи безперебійну взаємодію між повітряними суднами, диспетчерськими службами та наземною інфраструктурою. Водночас із зростанням автоматизації збільшується ймовірність кібератак, які можуть вплинути на безпеку польотів та функціонування транспортної галузі.

Як студентка, що вивчає інформаційно-психологічні впливи в кіберпросторі та стандарти безпеки, я можу відзначити, що загрози в авіаційній галузі мають не лише технічний, а й психологічний аспект. Військові та державні структури країни-агресора використовують кібератаки не тільки для безпосереднього впливу на авіаційні системи, а й для створення інформаційного хаосу та підриву довіри до авіаційних перевезень. Це особливо важливо в умовах війни, коли будь-яка нестабільність у критичній інфраструктурі може призвести до паніки та зриву стратегічних операцій.

Особливої уваги потребує захист від атак на авіаційні системи з боку кіберпідрозділів країни-агресора. За останні роки було зафіксовано численні випадки атак на критичну інфраструктуру України, включаючи аеропорти, авіакомпанії та диспетчерські служби.

Одним із найгучніших прикладів недавніх кібератак на критичну інфраструктуру України стала атака на «Укрзалізницю». Вона продемонструвала, наскільки вразливими можуть бути транспортні системи, що покладаються на автоматизоване управління та цифрову інфраструктуру. Хоча ситуація була оперативно виправлена, цей випадок показав, що в умовах війни кібернапади можуть мати не лише економічні наслідки, а й впливати на безпеку громадян.

Якщо порівнювати цей інцидент із можливими атаками на авіаційну інфраструктуру, то наслідки можуть бути ще серйознішими. Вразливість систем управління повітряним рухом та навігаційних систем може призвести до катастрофічних подій. Особливо це стосується військової авіації, яка зараз відіграє ключову роль у протистоянні з агресором. На даний момент цивільна авіація України не функціонує через загрозу ракетних ударів, однак після завершення бойових дій постане питання відновлення роботи авіаперевезень. Саме тому вже зараз необхідно розробляти ефективні стратегії захисту від потенційних кібератак.

Зважаючи на загрози, що виникають для транспортної інфраструктури, зокрема для авіації, я, як молодий майбутній спеціаліст, пропоную розробити стратегію кіберзахисту, яка б враховувала міжнародний досвід та специфіку сучасної війни. Основними напрямками, на мою думку, повинні стати: масштабне впровадження багаторівневої автентифікації для доступу до авіаційних систем, що допоможе мінімізувати

ризика несанкціонованого доступу, впровадження SIEM-систем, які дозволяють моніторити кіберзагрози в режимі реального часу та оперативно реагувати на потенційні атаки, використання протоколів PKI дозволяє захистити канали зв'язку та запобігти несанкціонованому доступу до даних, використання штучного інтелекту для аналізу кіберзагроз та прогнозування можливих атак на основі великих масивів даних, що дозволить покращити ефективність превентивних заходів, інтеграція кібербезпеки у військово-авіаційні операції, враховуючи ризики, пов'язані з безпілотними літальними апаратами та іншими сучасними технологіями, активна співпраця з міжнародними партнерами для обміну інформацією про кібератаки та розробки єдиних стандартів безпеки, що допоможе зміцнити загальний рівень захисту на глобальному рівні. Перспективним напрямом є інтеграція технологій блокчейну, які забезпечують прозорість та безпеку авіаційних операцій шляхом децентралізації та унеможливлення модифікації даних без авторизації.

Висновок

Результати дослідження підтверджують важливість розробки ефективних стратегій кіберзахисту для авіаційних систем, зважаючи на зростаючі загрози в умовах гібридної війни. Отримані результати підкреслюють необхідність впровадження багаторівневої автентифікації, активного моніторингу загроз та використання штучного інтелекту для прогнозування потенційних атак. Ці стратегії можуть значно підвищити рівень безпеки транспортної інфраструктури, зменшуючи ризики від кібератак, які можуть призвести до серйозних наслідків для безпеки логістики та стабільності країни. Важливість цих результатів полягає в їхній практичній застосовності для розробки національних та міжнародних стандартів кібербезпеки в транспортній галузі, а також для використання в підготовці фахівців з кібербезпеки та в рамках стратегій захисту критичної інфраструктури держави.

Список використаних джерел:

1. Ільєнко А.В., Ільєнко С.С. Сучасний стан забезпечення кібернетичної безпеки цивільної авіації України та світу // Cybersecurity Education Science Technique. 2020.
2. ICAO Cybersecurity Strategy. International Civil Aviation Organization, 2019.
3. Kazmirchuk, S., Ilenko A., Ilenko S. Digital signature authentication scheme with message recovery based on elliptic curves. ICCSEEA 2019.

УДК 004.056 (043.2)

РОЛЬ МІЖНАРОДНИХ СТАНДАРТІВ МОВНОЇ ПІДГОТОВКИ ДЛЯ СФЕРИ БЕЗПЕКИ

Юлія Голодюк

*Національна академія Служби безпеки України, Київ**Науковий керівник – Анастасія Вавіленкова, д.т.н., проф.*

Ключові слова: міжнародні стандарти, мовна підготовка, фахівці сектору безпеки, військова освіта, професійна компетентність.

Вступ. Забезпечення національної безпеки та оборони України залишається найбільш актуальною проблемою держави, особливо сьогодні, в умовах постійно існуючих та потенційних загроз. Це обумовлює необхідність пошуку ефективних механізмів для своєчасного запобігання загроз та їх деструктивних чинників, а також підтримання такого оборонного потенціалу держави, який гарантуватиме її воєнну безпеку. Однією з ключових ланок вирішення цих завдань є підвищення ефективності професійної підготовки фахівців сектору безпеки та оборони. Нагальним є дослідження сучасних тенденцій професійної підготовки фахівців сектору безпеки та оборони у зарубіжних країнах, особливо в тих, що розвиваються, з огляду на схожі з Україною економічні та військово-політичні процеси, які впливають на національну безпеку та обумовлюють уразливість держави, зростання викликів та посилення загроз [1].

Метою цього дослідження є аналіз міжнародних стандартів мовної підготовки для силових структур, фахівців у сфері безпеки та охорони, а також методів їхнього впровадження та основних викликів, з якими стикаються фахівці у цій сфері.

Матеріали і методи. Володіння іноземними мовами для військовослужбовців, правоохоронців та аналітиків є не тільки перевагою, а ще й необхідністю для міжнародного співробітництва, виконання міжнародних завдань, проведення переговорів та координації дій з правоохоронними органами іноземних держав. Для такої взаємодії потрібні єдині вимоги до рівня знань та навичок працівників сектору безпеки та оборони. Існує безліч систем оцінювання, але основні це STANAG 6001, ILR Scale у США та шкала CEFR в Європі.

Результати. STANAG (Standartization Agreement, Стандарт НАТО) – міжнародний договір, що діє в країнах НАТО та країнах-партнерах. Одна із численних угод цього договору, а саме STANAG 6001, стосується стандартів володіння іноземною мовою для військовослужбовців. В Україні іспит проводиться відповідно до наказу Міністра оборони України. Іспит складається з чотирьох частин: письмо, аудіювання, читання, говоріння. Саме навчання проводиться у межах стандартизованих мовленнєвих рівнів (СМР): СМР 0 (Відсутність практичного вміння); СМР 0+ (Завчений мінімум); СМР 1 (Виживання); СМР 1 + (Виживання +); СМР 2 (Функціональний); СМР 2+ (Функціональний +); СМР 3 (Професійний); СМР 4 (Експертний) [2]. Шкала ILR Scale (Interagency Language Roundtable) вимірює мовні здібності у всіх чотирьох комунікативних навичках – аудіювання, читання, говоріння та письмо. Кожна навичка має свої власні дескриптори рівня і оцінюється від 0 (без володіння) до 5 (функціональна рідна професійна майстерність). Плюсіві рівні призначаються, коли рівень кваліфікації вищий за базовий рівень, але не відповідає критеріям наступного вищого базового рівня. CEFR (Common European Framework of Reference for Languages) – це Загальноєвропейська система оцінювання мовних компетенцій, розроблена Радою Європи для

уніфікації стандартів володіння іноземними мовами. CEFR визначає шість рівнів володіння мовою: A1 (Beginner) – початковий рівень, базові навички спілкування на прості теми. A2 (Elementary) – розширене розуміння простих фраз і можливість вести нескладний діалог. B1 (Intermediate) – самостійне використання мови у стандартних ситуаціях повсякденного життя. B2 (Upper-Intermediate) – вільне розуміння складних текстів та ведення професійної комунікації. C1 (Advanced) – високий рівень володіння мовою з розумінням складної термінології та професійної лексики. C2 (Proficient) – рівень носія мови, здатність ефективно функціонувати в будь-якому мовному середовищі.

Висновки. В умовах глобалізації та міжнародного співробітництва України з іншими державами STANAG, ILR Scale, CEFR є важливим інструментом для оцінки та стандартизації мовних навичок військових і силових структур. Завдяки іноземним навчанням, фахівцям та співробітництву Україна отримує безперервний досвід, нові розробки зброї, нові тактики проведення та організації бою. Також це дає змогу просувати Україну на міжнародній арені, де вона показує досвідчених фахівців у сфері безпеки та оборони, які здатні вдосконалювати свої знання та вміння на рівні з представниками країн великої сімки. Таким чином, міжнародні мовні стандарти відіграють важливу роль у забезпеченні підготовки військових та правоохоронців, а їх подальше вдосконалення та використання допоможе у підвищенні ефективності міжнародної взаємодії та виконання стратегічно важливих задач у сфері безпеки та оборони.

Список використаних джерел:

1. Артющин Г., Тушко К. «СУЧАСНІ ТЕНДЕНЦІЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ У КРАЇНАХ, ЩО РОЗВИВАЮТЬСЯ», Збірник наукових праць НАДПСУ: Хмельницький, Видавництво НАДПСУ, 2024. No 3(38). 218 с (дата звернення 22.03.2025).
2. Що таке STANAG 6001? - JIT. URL: <https://www.jit.academy/shho-take-stanag-6001/> (дата звернення 22.03.2025).

УДК 004.932.2 (043.2)

ВИЯВЛЕННЯ ОСОБЛИВИХ ЗОН ЯК ОСНОВА МЕТОДУ ТОПОГРАФІЧНОЇ СПОРІДНЕНOSTІ ЗОБРАЖЕНЬ

Роман Джебраїлов, Вадим Боровик

Інститут інформаційних технологій та систем НАН України, Київ

Науковий керівник – Олександр Волков, к.т.н., ст.досл.

Ключові слова: комп'ютерний зір, особливі точки, особливі зони, автономна навігація, повітряна платформа.

Як відомо, функціонування різних повітряних платформ супроводжується недоліками в роботі їх навігаційних систем: система на основі сигналів глобальних навігаційних супутникових систем є вразливою до природних і штучних перешкод, інерційна система має проблему постійного накопичення похибки [1], системи TERCOM та DSMAC спираються лише на попередньо підготовлені дані [2], методи одночасної локалізації і картографування V-SLAM [3, 4] та візуальної одометрії [5, 6] можуть працювати лише в приміщенні або на вулиці, у методі топографічної кластеризації візуальних зображень іноді

неможливо виділити особливі точки або їх може бути дуже багато, що ускладнює їх перебір і співставлення [7]. Таким чином, актуальним є питання про розроблення більш досконалої системи автономної навігації повітряних платформ на основі технологій комп'ютерного зору.

Мета дослідження – розробити принципово новий метод співставлення зображень природного ландшафту поверхні землі для задач автономної навігації повітряних платформ.

Для досліджень пошуку спільних ознак на зображеннях використані методи комп'ютерного програмного моделювання та порівняння, а саме були створені за допомогою бібліотеки підпрограм комп'ютерного зору й оброблення зображень з відкритим кодом OpenCV комп'ютерні програми, що моделюють систему автономної навігації повітряної платформи, та здійснено їх порівняльний аналіз між собою.

Нами був розроблений метод топографічної спорідненості зображень на основі виявлення особливих зон, який складається з п'яти етапів:

1. Підготовка базового та поточного зображень, яка полягає у застосуванні фільтра усереднення для розмиття зображень з метою покращення виявлення особливих зон;
2. Пошук особливих зон за допомогою за принципом пошуку локальних максимумів оператора Лапласа або так званим «простим методом»;
3. Фільтрація особливих зон за їх розміром і місцем розташування;
4. Пошук геометрично подібних трикутників, утворених центрами особливих зон, за довжинами й кутами їх внутрішніх сторін;
5. Додавання четвертої точки до трикутників для більшої вірогідності їх подібності;
6. Визначення висоти, повороту та подоланої відстані повітряної платформи.

Особливі зони та їх центри (1, 2, 3, 4), центри зображень (5, 7), та точка переміщення центру поточного зображення відносно базового представлені на рис. 1.

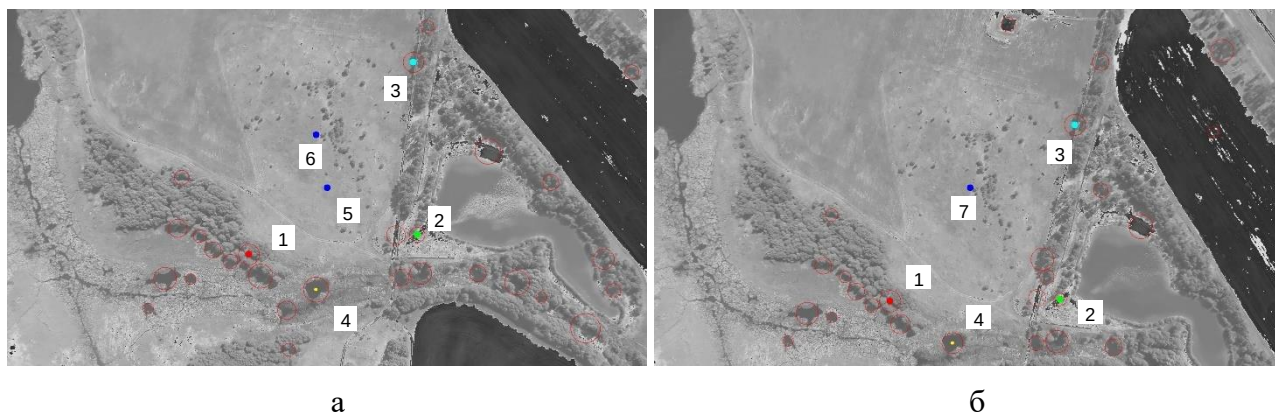


Рис.1. Базове (а) та поточне (б) зображення природного ландшафту поверхні землі з висоти

Висновок

Запропонований метод топографічної спорідненості зображень забезпечує можливість розрахувати параметри руху повітряної платформи відносно земної поверхні достатньо точно та може працювати зі

складними зображеннями природного ландшафту, такими як чисте поле, на відміну від методу топографічної кластеризації візуальних зображень [7].

Список використаних джерел:

1. Герасимов С., Коломійцев О., Пустоваров В. Особливості визначення точності вимірювань інерціальних приладів визначення координат. Системи управління, навігації та зв'язку. 2018. № 6(52). С. 3–8.
2. Irani G., Christ J. Image processing for Tomahawk scene matching. Johns Hopkins APL Technical Digest. 1994, No. 3, pp. 250–264.
3. Durrant-Whyte H., Bailey T. Simultaneous localization and mapping: part I. IEEE Robotics and Automation Magazine. 2006, No. 2, pp. 99–110.
4. Durrant-Whyte H., Bailey T. Simultaneous localization and mapping (SLAM): part II. IEEE Robotics and Automation Magazine. 2006, No. 3, pp. 108–117.
5. Scaramuzza D., Fraundorfer F. Visual odometry [tutorial]. Part I: The first 30 years and fundamentals. IEEE Robotics and Automation Magazine. 2011, No. 4, pp. 80–92.
6. Scaramuzza D., Fraundorfer F. Visual odometry: part II: matching, robustness, optimization, and applications. IEEE Robotics and Automation Magazine. 2012, No. 2, pp. 78–90.
7. Система автономної навігації безпілотної літального апарата на основі топографічної кластеризації візуальних зображень : пат. UA 121833 C2 Україна : 2020.01. № а 2019 05904 ; заявл. 29.05.2019 ; опубл. 27.07.2020, Бюл. № 14. 18 с.

УДК 004.056 (043.2)

КІБЕРЗАХИСТ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ УКРАЇНИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

Євген Скляренко, Максим Величко

Національна академія Служби безпеки України, Київ

Науковий керівник – Анастасія Вавіленкова, д.т.н., проф.

Ключові слова: кібербезпека, кібератаки, кіберзахист, кібернетичний фронт, критична інфраструктура.

Вступ. Сучасна війна виходить далеко за межі традиційних бойових дій, охоплюючи все нові і нові сфери, серед яких особливе місце посідає кіберпростір, особливо останніми роками. В умовах збройної агресії проти України кібернетичний фронт набув особливого значення, оскільки атаки на критичні інформаційні системи можуть паралізувати державне управління, фінансову систему, енергетику, транспортну інфраструктуру та військовий зв'язок. Це загрожує не лише національній безпеці, а й життєдіяльності всього суспільства. Актуальність дослідження зумовлена безпрецедентним зростанням кількості та складності кібератак, спрямованих на стратегічно важливі об'єкти [1,2]. Від початку повномасштабного вторгнення Україна зіткнулася з масовими DDoS-атаками, спробами проникнення до державних реєстрів, атаками на фінансову систему та енергетичний сектор. російська федерація застосовує комплексну стратегію гібридної війни, у якій загрози кіберпростору виступають не лише як засіб дестабілізації, а й як інструмент інформаційного впливу та розвідки.

Метою доповіді є аналіз сучасних викликів кібербезпеки критичних інформаційних систем України та формулювання ефективних стратегій їхнього захисту та адаптації до умов воєнного часу. Це передбачає дослідження кіберзагроз, оцінку стану кіберзахисту, розгляд чинної нормативно-правової бази, а також визначення шляхів посилення стійкості кіберінфраструктури.

Матеріали і методи. Адаптація передбачає й підвищення рівня кіберобізнаності серед державних службовців, військових, бізнесу та громадян. Запровадження систематичних навчань, тестування на проникнення,

кібернавчань та обов'язкової сертифікації фахівців дозволяє знизити ризики, пов'язані з людським фактором. Також держава розширює нормативно-правове регулювання у сфері кіберзахисту, створюючи законодавчу базу для чіткої взаємодії держави та приватного сектору в умовах кіберзагроз. Особливий акцент робиться на законодавчому закріпленні вимог до операторів критичної інфраструктури щодо обов'язкових заходів безпеки та відповідальності за недотримання стандартів.

З огляду на досвід кібервійни, стратегія передбачає застосування концепції «активної оборони», що включає заходи з виявлення, відслідковування та нейтралізації загроз ще на ранніх стадіях. Це вимагає комплексного підходу, в якому поєднуються юридичні, технологічні та організаційні механізми. Окремим напрямом є розвиток національної криптографічної стійкості, що включає перехід на постквантові алгоритми шифрування та розробку власних технологій для захисту державних комунікацій.

Результати. Збройна агресія проти України паралельно перейшла в вимір кіберпростору, особливо щодо об'єктів критичної інформаційної інфраструктури (ОКІІ). В умовах гібридної війни кіберпростір став одним із головних полів бою, де під загрозою є державні органи, військові структури, фінансові установи, енергетичний сектор, телекомунікації та інші об'єкти критичної інфраструктури.

Одним із ключових викликів є масштабованість і складність кібератак. Противник застосовує різноманітні методи – від DDoS-атак, спрямованих на виведення з ладу веб-ресурсів, до складних атак із використанням шкідливого програмного забезпечення (віреїв-вірусів), які можуть знищувати дані та порушувати роботу цілих систем. Особливо небезпечними є кібератаки на енергетичний сектор, що може призвести до дестабілізації життєво важливих послуг, що стало очевидно після атаки на Прикарпаттяобленерго в 2015 році.

Другим важливим викликом є спеціалізовані операції в кіберпросторі, що поєднуються з інформаційно-психологічними атаками. Кіберагресори поширюють дезінформацію, зламують державні інформаційні ресурси для зміни або знищення даних, а також здійснюють фішингові атаки, спрямовані на посадових осіб та критично важливі підприємства [3].

Державне та приватне партнерство у сфері кібербезпеки також зазнає серйозних випробувань. Багато підприємств критичної інфраструктури перебувають у приватній власності, що ускладнює контроль за їхнім рівнем кіберзахисту [4]. Відсутність уніфікованих стандартів і механізмів оперативного реагування на кібератаки створює додаткові ризики.

Далі поговоримо про загальні напрямки реалізації нормативно-правової бази в довготривалих аспектах. Стратегії адаптації та розвитку кіберзахисту ОКІ України формуються з урахуванням постійної потенційної загрози з боку держави-агресора. У відповідь на ці загрози державна політика кібербезпеки орієнтована на створення гнучкої, адаптивної та багатоселонної системи захисту, здатної ефективно протидіяти як традиційним, так і новим формам кібератак. Основним напрямом є інтеграція національної системи кіберзахисту з міжнародними структурами та стандартами, що включає тісну співпрацю з НАТО, ЄС та іншими союзниками, а також дотримання норм NIST, ISO/IEC 27001 та рекомендацій Європейського агентства з кібербезпеки (ENISA).

Важливою складовою адаптації є розвиток технологічного потенціалу через модернізацію кіберінфраструктури державних установ та приватного сектору. Це передбачає впровадження сучасних рішень для моніторингу мережевого трафіку, виявлення аномалій та раннього реагування на інциденти. Державні органи, зокрема Державна служба спеціального зв'язку та захисту інформації України (ДССЗІ) у співпраці з СБУ,

активно впроваджують системи автоматизованого аналізу загроз та технології штучного інтелекту для прогнозування атак [5]. Розвиток національної системи кіберінцидентів і оперативне обмінювання даними між відомствами значно підвищує стійкість критичних інформаційних систем до зовнішніх впливів.

Висновки. Загалом, у ході дослідження було розглянуто виклики та стратегії адаптації системи кіберзахисту критичних інформаційних систем України в умовах збройної агресії. Аналіз нормативно-правової бази, міжнародного досвіду та технологічних рішень засвідчив, що держава активно розвиває багатоварштовну систему кібероборони, інтегруючи її з глобальними стандартами та посилюючи власний технологічний потенціал. Окреслені підходи до кіберстійкості, зокрема модернізація інфраструктури, розширення нормативного регулювання, активізація міжнародної співпраці та впровадження концепції активної оборони, підтверджують, що Україна адаптується до нових загроз і формує ефективну систему протидії. Досягнення мети дослідження доводить, що розвиток кіберзахисту є не лише відповіддю на сучасні виклики, а й фундаментальним елементом забезпечення національної безпеки в умовах гібридної війни.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 23.03.2025).
2. Указ Президента України «Про Стратегію кібербезпеки України» від 26 серпня 2021 року № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013> (дата звернення: 23.03.2025).
3. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 23.03.2025).
4. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20> (дата звернення: 23.03.2025).
5. Постанова Кабінету Міністрів України «Про затвердження Порядку реагування на кіберінциденти та кібератаки» від 29 березня 2022 року № 348. URL: <https://zakon.rada.gov.ua/laws/show/348-2022-%D0%BF> (дата звернення: 23.03.2025).

УДК 004.78 (043.2)

ІНТЕЛЕКТУАЛЬНІ КІБЕРНЕТИЧНІ СИСТЕМИ В РОБОТОТЕХНІЦІ

Анастасія Ліснічук, Ангеліна Бухало

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Євген Артамонов, к.т.н., доц.

Ключові слова: інтелектуальні системи, робототехніка, кібернетика

Вступ

Технологічний розвиток у сфері робототехніки, обчислювальних архітектур і пристроїв, а також систем зберігання інформації, одним словом – кібернетичні системи. Інтеграція інтелектуальних кібернетичних систем у робототехніку є одним із основних напрямків сучасних досліджень, що поєднують штучний інтелект, кібернетику та робототехніку для створення автономних і адаптивних систем. Ці системи здатні аналізувати дані, приймати рішення та адаптуватися до змінних умов, що робить їх незамінними в різних галузях.

Мета: дослідити вплив інтелектуальних кібернетичних систем на розвиток робототехніки, проаналізувати підходи до їх впровадження та визначити перспективи подальшого розвитку.

Матеріали та методи: основні підходи до створення інтелектуальних систем керування:

1. Фіксовані алгоритми – застосовуються у програмованих роботах, де всі дії чітко визначені та не змінюються під час виконання завдань.

2. Адаптивні системи – дозволяють роботам змінювати поведінку залежно від навколишніх умов, використовуючи методи машинного навчання та обробки великих обсягів даних.

3. Системи штучного інтелекту – забезпечують автономність, навчання на основі досвіду та можливість прийняття рішень у непередбачуваних ситуаціях.

Метою створення інтелектуальної системи керування є забезпечення того, щоб робот працював ефективно, безпечно та відповідав очікуванням у певній програмі. Залежно від складності завдання та операційної системи, система керування може бути простою або дуже складною, використовуючи передові методи, такі як машинне навчання, адаптивне керування або доповнена реальність.

Результати

Інтелектуальні кібернетичні системи значно розширюють можливості робототехніки, дозволяючи автоматизувати складні процеси в різних сферах. Сфери застосування роботів досить великі. Техніка стає не просто автоматичною, а «розумною», багато простих для нас пристроїв також стають роботизованими. Однією з найбільших сфер застосування роботів є промисловість, особливо в автоматизації виробничих процесів. Впровадження промислових роботів сприяє підвищенню ефективності, покращенню якості та оптимізації виробничих витрат. Активне впровадження інтелектуальних кібернетичних систем також спостерігається в медицині, транспорті, обороні та енергетиці. Вони автоматизують виробництво, покращують діагностику, керують безпілотним транспортом, підсилюють військові технології та оптимізують енергомережі. Це підвищує ефективність, безпеку та зменшує вплив людського фактора.

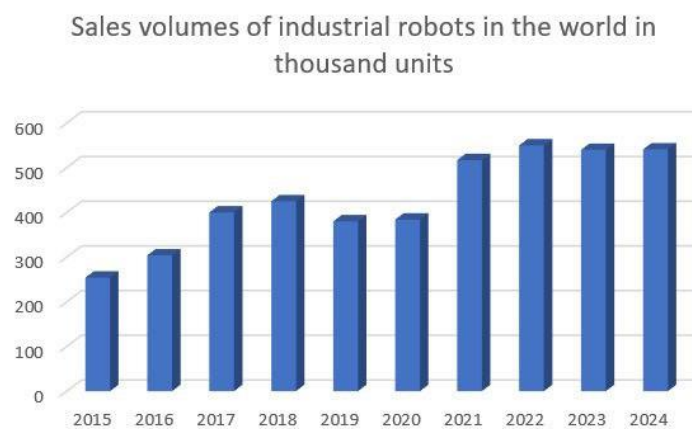


Рис 1. Діаграма обсягів продажу промислових роботів у світі

Висновок

Інтелектуальні кібернетичні системи є ключовим етапом розвитку робототехніки, сприяючи її автономності та ефективності. Їх подальше вдосконалення дозволить розширити можливості автоматизації та оптимізувати складні процеси в різних галузях.

Список використаних джерел

1. Advanced Intelligent Systems 2 (12), 2000120, 2020
2. Jordan, E. (2024). Cybernetics Unveiled: Exploring the Science of Communication and Control in Systems
3. Evgeny Chepin. Procedia Computer Science 190, 130-136, 2021

УДК 004.85.056 (043.2)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ СИСТЕМ ВИЯВЛЕННЯ ЗАГРОЗ

Володимир Бойко

*Державний університет «Київський авіаційний
інститут», Київ*

Науковий керівник – Козловський Валерій д.т.н., проф.

Ключові слова: штучний інтелект, машинне навчання, кібербезпека, виявлення загроз, аналіз трафіку.

Вступ

Інформаційна безпека є критично важливою складовою функціонування сучасних комп'ютерних систем та мереж. Постійне збільшення кількості кібератак, зокрема атак нульового дня, багатовекторних атак та автоматизованих загроз, вимагає застосування більш ефективних методів захисту. Традиційні методи, такі як сигнатурний аналіз і евристичні підходи, вже не завжди забезпечують достатній рівень безпеки через складність та динамічність атак. У зв'язку з цим штучний інтелект (ШІ) відіграє ключову роль у підвищенні ефективності систем виявлення загроз, дозволяючи автоматизувати процеси аналізу мережевого трафіку та виявлення аномалій.

Основна частина

Штучний інтелект є потужним інструментом у виявленні загроз, дозволяючи ефективно аналізувати великі обсяги даних та знаходити аномальні патерни. У дослідженні запропоновано використання трьох методів штучного інтелекту, реалізованих у середовищі Python: глибокі нейронні мережі (DNN), рекурентні нейронні мережі (RNN) та автоенкодера (AE).

Методологія дослідження базується на моделюванні сценарію мережевого трафіку. Нормальний трафік представлений 1000 зразками, аномальний трафік – 200 зразками, що включають як відомі загрози, так і нові невідомі атаки. Дані нормалізовано методом MinMaxScaler для забезпечення коректної роботи алгоритмів машинного навчання.

Глибокі нейронні мережі використовують багатошарову архітектуру, що включає щонайменше три приховані шари. Вони навчаються на великих обсягах даних та використовують функції активації, такі як ReLU та Softmax, для класифікації трафіку.

Переваги:

- Висока точність при класифікації загроз.
- Здатність до навчання на великих обсягах даних.
- Ефективне розпізнавання складних патернів атак.

Недоліки:

- Високі обчислювальні витрати.
- Потреба у великих обсягах даних для ефективного навчання.

– Складність інтерпретації отриманих результатів.

Рекурентні нейронні мережі (RNN)

Рекурентні нейронні мережі із застосуванням LSTM-моделей ефективно аналізують послідовні дані та виявляють часові залежності у мережевому трафіку. Це дозволяє ідентифікувати довготривалі атаки, зокрема ботнет-атаки та DDoS-кампанії.

Переваги:

- Аналіз часових залежностей у трафіку.
- Ефективність для виявлення складних атак, що розвиваються в часі.
- Висока точність в аналізі послідовних даних.

Недоліки:

- Тривалий процес навчання.
- Велике споживання ресурсів при роботі з великими наборами даних.
- Можливість виникнення проблеми затухання градієнта.

Автоенкодери (AE)

Автоенкодери використовуються для виявлення аномалій. Вони стискають вхідні дані у латентне представлення, а потім відновлюють їх. Висока похибка відновлення сигналізує про потенційну загрозу. AE є ефективними для виявлення невідомих атак, проте можуть генерувати велику кількість хибнопозитивних спрацьовувань.

Переваги:

- Ефективне виявлення нових аномалій та атак нульового дня.
- Висока здатність до узагальнення на основі попередніх атак.
- Автоматична адаптація до змін у мережевому трафіку.

Недоліки:

- Висока ймовірність хибнопозитивних спрацьовувань.
- Потреба у тонкому налаштуванні гіперпараметрів.
- Складність у поясненні прийнятих рішень.

Результати експериментального дослідження показали ефективність використання запропонованих методів. Глибокі нейронні мережі (DNN) досягли точності класифікації у 97%, рекурентні нейронні мережі (RNN) продемонстрували ефективність у виявленні атак з часовими залежностями із точністю 95%, а автоенкодери (AE) виявили нові аномалії з рівнем хибнопозитивних спрацьовувань у 8%. Комплексне застосування цих методів дозволяє суттєво підвищити рівень безпеки інформаційних систем та ефективність моніторингу загроз.

Висновки

Зростання складності атак вимагає застосування інтелектуальних методів виявлення загроз. Дослідження демонструє, що DNN ефективно класифікує відомі загрози, RNN дозволяє аналізувати

часові патерни, а АЕ забезпечує виявлення нових аномалій. Впровадження цих методів у системи моніторингу кібербезпеки дозволить підвищити ефективність виявлення атак та захисту інформаційних систем.

Список використаних джерел

1. Машинне навчання в кібербезпеці. URL: <https://www.cybersecurity-ai.com>
2. Osadchyi, Y., Yesina, M., Onopriienko, V. The application of deep learning for network intrusion detection // Computer Science and Cybersecurity. – 2023. – № 2. – С. 45–53. URL: <https://periodicals.karazin.ua/cscs/article/view/23123>
3. Захист інформаційних систем за допомогою нейронних мереж. URL: <https://cyber-ai-defense.org>
4. Лахно, В., Ткач, Ю., Петренко, Т. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks // Information and controlling system. – Харків, 2016. – № 4/9(82). – С. 32–44. URL: <https://journals.uran.ua/eejet/article/view/85600>.

УДК 519.688 (043.2)

ІНТЕРАКТИВНИЙ ПРОГРАМНИЙ ДОДАТОК ДЛЯ АНАЛІЗУ АЛГОРИТМІВ СОРТУВАННЯ

Єлизавета Приймак

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Світлана Кашкевич, ст. викладач

Ключові слова: алгоритми сортування, інтерактивний додаток, візуалізація, продуктивність, програмне забезпечення

Вступ

Алгоритми сортування відіграють ключову роль у комп'ютерних науках, забезпечуючи впорядкування даних для подальшої обробки чи аналізу. Сучасні дослідження [1, 2] вказують на потребу в інтерактивних інструментах, які дозволяють не лише оцінити продуктивність алгоритмів, але й візуалізувати їхню роботу для кращого розуміння. Актуальність теми зумовлена зростанням обсягів даних та необхідністю швидкого вибору оптимального алгоритму залежно від умов задачі.

Мета: розробити інтерактивний програмний додаток для аналізу та порівняння алгоритмів сортування з можливістю візуалізації їхньої поведінки в реальному часі.

Дослідження базується на аналізі трьох класичних алгоритмів сортування: сортування бульбашкою, швидке сортування та сортування злиттям. Для реалізації додатку використано мову програмування C++. Об'єктами аналізу були масиви чисел розміром від 10 до 10 000 елементів, згенеровані випадковим чином. Оцінка продуктивності проводилася за двома параметрами: час виконання (в секундах) та кількість операцій порівняння. Для порівняння алгоритмів використано статистичний метод із вимірюванням середнього часу виконання на 100 запусках для кожного розміру масиву.

Результати

Розроблений інтерактивний додаток забезпечує зручний інструмент для аналізу алгоритмів сортування, дозволяючи користувачу обирати алгоритм, налаштовувати розмір масиву (від 10 до 10 000 елементів) та затримку між ітераціями для детального спостереження за процесом сортування. На рис. 1 представлено інтерфейс додатка під час виконання сортування бульбашкою для масиву з 74 елементів. Стовпчики відображають значення

елементів масиву, де червоним кольором виділено елементи, які порівнюються на поточному кроці, що дає змогу наочно простежити за переміщенням елементів. Панель управління, розташована зліва внизу, дозволяє обирати один із трьох алгоритмів (сортування бульбашкою, швидке сортування, сортування злиттям), змінювати розмір масиву та затримку між ітераціями. Інформаційна панель, розміщена зліва вгорі, містить опис обраного алгоритму, що полегшує розуміння його логіки для користувачів.

Аналіз продуктивності алгоритмів показав значні відмінності залежно від розміру масиву. Для масивів із 10–100 елементів різниця в часі виконання між алгоритмами незначна: сортування бульбашкою завершує роботу за 0.001–0.003 секунди, швидке сортування – за 0.0005–0.001 секунди, а сортування злиттям – за 0.001–0.002 секунди. Проте для масивів із 10 000 елементів сортування бульбашкою потребує в середньому 5.2 секунди, що відповідає часовій складності $O(n^2)$. Швидке сортування завершує роботу за 0.03 секунди ($O(n \log n)$), а сортування злиттям – за 0.05 секунди ($O(n \log n)$). Кількість операцій порівняння також зростає пропорційно до часової складності: для сортування бульбашкою на масиві з 10 000 елементів виконано близько 50 мільйонів порівнянь, тоді як швидке сортування потребує лише 120 000 порівнянь.



Рис. 1. Інтерфейс інтерактивного додатка під час виконання сортування бульбашкою для масиву з 74 елементів

Функціонал додатка включає можливість збереження результатів у файл, що зручно для подальшого аналізу. Візуалізація процесу сортування у вигляді стовпчиків допомагає користувачам, зокрема студентам, краще зрозуміти внутрішню логіку алгоритмів, а налаштування затримки дозволяє детально простежити кожен крок.

Список використаних джерел:

1. Knuth D. E. The Art of Computer Programming, Volume 3: Sorting and Searching. 2nd ed. Addison-Wesley, 1998.
2. Goodrich M. T., Tamassia R. Algorithm Design and Applications. Wiley, 2015.
3. Skiena S. S. The Algorithm Design Manual. 3rd ed. Springer, 2020

УДК 004.9:336.7

РОЛЬ БЛОКЧЕЙН У ЗАБЕЗПЕЧЕННІ ПРОЗОРОСТІ ФІНАНСОВИХ ПРОЦЕСІВ

Сергій Подельський

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олена Нечипорук, доктор технічних наук, професор.*

Ключові слова: Блокчейн, Фінансові процеси, Децентралізація, Бухгалтерський облік, Смарт-контракти, Автоматизація.

Вступ. Прозорість фінансових процесів є критично важливою для довіри до фінансових систем і протидії шахрайству. Сучасні дослідження вказують на вразливість традиційних підходів через складність верифікації та ризики маніпуляцій. Блокчейн пропонує інтелектуальні рішення для підвищення прозорості завдяки децентралізації та криптографії.

Мета. Дослідити потенціал блокчейну як інтелектуальної кібернетичної системи для забезпечення прозорості у фінансових процесах.

Матеріали та методи. Досліджено блокчейн як технологію з властивостями незмінності й розподіленого управління. Об'єктами аналізу стали фінансові процеси: бухгалтерський облік, банківські операції, AML/KYC. Застосовано системний аналіз для оцінки впливу блокчейну на прозорість і порівняльний метод для зіставлення традиційних та децентралізованих систем.

Результати. Блокчейн забезпечує незмінність даних через децентралізовану архітектуру, ускладнюючи маніпуляції. Смарт-контракти автоматизують угоди, знижуючи витрати й усуваючи посередників. У бухгалтерському обліку автоматична верифікація скорочує час перевірки на 30–40% порівняно з традиційними методами. Дослідження показують, що прозорість зростає завдяки доступності даних і відстеженню транзакцій у реальному часі, що відповідає стандартам AML/KYC.

Криптографія блокує спроби шахрайства, а децентралізація підвищує довіру до системи. На рисунку 1 ілюструється залежність прозорості від впровадження блокчейну: традиційні системи мають 20% прозорості, гібридні – 60%, а повністю децентралізовані – 95%.

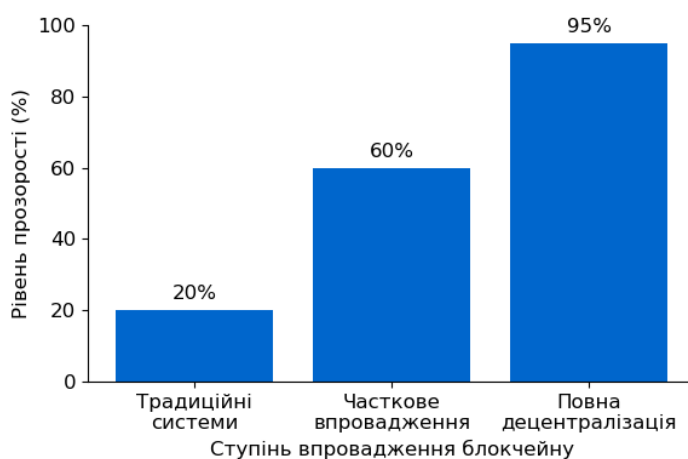


Рисунок 1. Залежність рівня прозорості фінансових процесів від ступеня впровадження блокчейну (за даними системного аналізу).

Застосування охоплює банківські операції, страхування та глобальну інфраструктуру, де блокчейн оптимізує процеси й посилює безпеку.

Висновок

Блокчейн трансформує фінансові процеси через інтелектуальні механізми, підвищуючи прозорість і ефективність. Його впровадження перспективне для цифрової економіки.

Список використаних джерел

1. Балазюк О.Ю., Пилявець В.М. Технологія блокчейн: дослідження суті та аналіз сфер використання. Економіка та суспільство, 2022.
2. Tapscott, D. and Tapscott, A. (2016) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin, New York, 2016.

УДК 004.8(043.2)

НЕЙРОМЕРЕЖЕВІ ПІДХОДИ ДО ФОРМУВАННЯ РЕКОМЕНДАЦІЙ МЕДІАКОНТЕНТУ ПРИ ОБМЕЖЕНИХ ОБСЯГАХ ДАНИХ

Валентин Черкай

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Голего, старший викладач

Ключові слова: рекомендаційні системи, медіаконтент, малооб'ємні дані, машинне навчання, нейронні мережі.

У сучасних умовах зростання обсягу цифрового контенту значну увагу приділяють системам рекомендацій. Проте ефективність традиційних підходів знижується при обмеженій кількості доступних даних, що характерно для нових або нішевих медіа-платформ. Останні дослідження [1, 2] пропонують використання нейронних мереж для роботи в умовах малооб'ємних даних. Особливу увагу приділяють гібридним методам, що поєднують переваги різних підходів, таких як колаборативна фільтрація та контентно-орієнтовані методи.

Метою роботи є розробка та аналіз ефективності методів формування рекомендацій медіаконтенту на основі нейронних мереж в умовах малого обсягу даних. Зокрема, досліджується можливість використання гібридних архітектур, що поєднують колаборативні фільтри та контентно-орієнтовані підходи для забезпечення високої точності рекомендацій.

У дослідженні використано методи машинного навчання, зокрема гібридні нейронні мережі, що поєднують глибоке навчання та факторизацію матриць. Запропонована система базується на автоенкодері, що формує латентні представлення користувачів і медіаконтенту, а також на факторизаційній моделі, яка сприяє подоланню проблеми недостатності даних. Додатково застосовується механізм попереднього навчання на схожих наборах даних, що дозволяє покращити узагальнюючу здатність моделі. Для перевірки ефективності моделей застосовано набір даних із симульованими користувацькими переглядами, що містить анонімізовану інформацію про вподобання

та історію взаємодій. В якості метрики оцінювання точності використано показник NDCG (Normalized Discounted Cumulative Gain).

Запропонована модель представляє собою комбінацію автоенкодера та факторизаційної машини, що дозволяє покращити якість рекомендацій в умовах обмеженої кількості даних. У порівнянні з традиційними підходами, такими як колаборативна фільтрація, модель демонструє вищу точність передбачень, особливо для нових користувачів та медіаконтенту з низькою популярністю. Використання комбінованої архітектури покращило персоналізацію рекомендацій та зменшило похибки в прогнозуванні уподобань користувачів. Аналіз продемонстрував, що попереднє навчання на схожих наборах даних значно підвищує ефективність рекомендаційної системи, зменшуючи проблему холодного старту. Крім того, результати показали, що адаптивне оновлення ваг мережі відповідно до змін у вподобаннях користувачів дозволяє покращити довготривалу ефективність рекомендацій.

Висновки. Розроблена система формування рекомендацій медіаконтенту на основі нейронних мереж є ефективним інструментом для платформ із обмеженою кількістю користувачів або контенту. Застосування гібридної архітектури дозволяє покращити персоналізацію та адаптацію рекомендацій під індивідуальні уподобання. Подальші дослідження можуть бути зосереджені на оптимізації архітектури моделі, зокрема використанні трансформерів для покращення обробки послідовностей взаємодій користувачів. Також перспективним напрямком є дослідження механізмів самонавчання моделей у реальному часі, що дозволить адаптувати рекомендації до змінних уподобань користувачів.

Список використаних джерел:

1. Zhang, Y., & Yang, Q. (2020). A Survey on Deep Learning for Recommender Systems. IEEE Transactions on Knowledge and Data Engineering.
2. Koren, Y., Bell, R., & Volinsky, C. (2009). Matrix Factorization Techniques for Recommender Systems. Computer, 42(8), 30-37.

УДК 004.67 (043.2)

ОСНОВНІ КОМПОНЕНТИ ЗАСТОСУНКУ ДЛЯ ПЕРЕВІРКИ ДОКУМЕНТІВ ВНУТРІШНЬО ПЕРЕМІЩЕНИХ ОСІБ

Ярослав Бортник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Апенько, д.т.н., доц.

Ключові слова: внутрішньо переміщені особи, перевірка документів, автентифікація, електронна ідентифікація, захист персональних даних, інтеграція з реєстрами

З початком повномасштабної агресії проти України кількість внутрішньо переміщених осіб (ВПО) зросла до мільйонів. Ефективне управління цими потоками, надання допомоги, правовий захист та забезпечення державних послуг потребують оперативної та достовірної перевірки документів ВПО. У відповідь на цей виклик постає необхідність створення цифрових рішень, зокрема мобільних або вебзастосунків, які б автоматизували процес перевірки, знижували навантаження на соціальні служби та

мінімізували людський фактор. Основна мета такого застосунку – гарантувати точність, швидкість та безпеку при роботі з персональними даними у надзвичайних умовах.

Сучасний застосунок для перевірки документів ВПО повинен мати низку базових, але технологічно складних компонентів, кожен із яких забезпечує окрему функціональну роль у загальному процесі перевірки. Першим критичним елементом є модуль автентифікації та авторизації. В умовах обробки персональних даних застосунок повинен гарантувати доступ лише для уповноважених осіб – представників соціальних служб, волонтерських організацій чи правоохоронних органів [1, 2]. Це досягається через впровадження двофакторної автентифікації, інтеграцію з національними системами ідентифікації, зокрема Дія або BankID, і логування всіх дій користувачів.

Другим компонентом є інтерфейс завантаження та сканування документів. Він повинен підтримувати зчитування інформації з внутрішніх і закордонних паспортів, довідок ВПО, посвідчень, цифрових QR-кодів тощо. У цьому компоненті доцільно реалізувати розпізнавання тексту (OCR), що дозволяє автоматично витягувати дані зі сканованих або сфотографованих документів. Це не тільки пришвидшує перевірку, а й мінімізує ризик помилки при ручному введенні.

Ключову роль відіграє модуль перевірки достовірності документів [2], що працює за принципом звірки з офіційними базами даних. Такий модуль повинен мати API-зв'язок з реєстрами Міністерства соціальної політики, Державної міграційної служби, Мінцифри або інших відомств, які мають підтвердження статусу особи. Також може використовуватись верифікація електронного підпису або цифрових печаток, якщо документи подано в електронному вигляді.

Важливим є блок обробки персональних даних із вбудованими політиками конфіденційності та захисту згідно з вимогами GDPR та українського законодавства. Дані повинні зберігатись тимчасово або з шифруванням, із чітким контролем доступу. Особливої актуальності цей компонент набуває в умовах війни, коли витік інформації може загрожувати життю та безпеці ВПО.

Ще один суттєвий елемент – аналітичний модуль, що дозволяє систематизувати інформацію про кількість перевірених осіб, регіони їх походження, частоту використання підроблених документів тощо. Такі дані можуть бути критично важливими для ухвалення рішень органами влади або координації гуманітарної допомоги.

Висновок. Створення швидкісного, зручного та безпечного застосунку для перевірки документів внутрішньо переміщених осіб вимагає системного підходу до архітектури та глибокого розуміння як технологічних, так і соціальних аспектів. Такий інструмент має не лише підвищити ефективність роботи служб, а й стати гарантом безпеки для людей, які втратили дім. Комплексність, захищеність та адаптивність є трьома ключовими критеріями, що мають визначати розробку подібного рішення.

Список використаних джерел:

1. G. M. P. Sarangi et al., "Automated Financial Document Processing using Machine Learning Techniques," IEEE Transactions on Automation Science and Engineering, vol. 18, no. 2, pp. 654-665, 2021. (Дата звернення: 22.03.2025).
2. M. T. Ribeiro, S. Singh, and C. Cardie, "Why Should I Trust You? Explaining the Predictions of Any Classifier," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016. (Дата звернення: 22.03.2025).

УДК 004.7 (043.2)

ВИМОГИ ДО ПРОГРАМНОЇ СИСТЕМИ ОБРОБКИ ЗАЯВ НА ПОСЕЛЕННЯ В ГУРТОЖИТОК

Максим Усик

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Євген Артамонов, к.т.н., доц.

Ключові слова: заява на поселення, студентський гуртожиток, автоматизована система, електронний документообіг, пріоритезація заяв

Процес поселення студентів у гуртожитки – одна з ключових адміністративних функцій навчального закладу, яка потребує ретельної організації, контролю й автоматизації. Особливої актуальності питання набуває в умовах масовості подання заяв, обмеженого фонду вільних місць та потреби враховувати індивідуальні особливості заявників. Відсутність цифрового інструменту призводить до неефективної роботи комісій, втрат часу, дублювання інформації та зростання кількості помилок. Саме тому виникає потреба у розробці програмної системи, здатної централізовано обробляти заявки на поселення. Формулювання чітких вимог до такої системи – перший крок до її успішного впровадження.

Формування вимог до програмної системи розпочинається з аналізу потреб ключових користувачів: студентів, представників студентських рад, співробітників деканатів та адміністрації гуртожитків. Очікування різних категорій користувачів суттєво впливають на склад функціональних і нефункціональних вимог.

До функціональних вимог належать:

- реєстрація та аутентифікація користувача з інтеграцією в систему єдиного входу ВНЗ або використанням електронного підпису (наприклад, через Дія або університетські облікові записи);
- подання електронної заяви з вибором типу кімнати, гуртожитку, обґрунтуванням пільг або індивідуальних умов поселення;
- динамічна перевірка статусу заявки: «подано», «на розгляді», «схвалено», «відхилено», «в очікуванні підтвердження»;
- завантаження супровідних документів (скан-копії посвідчень, довідок, рішень соціальних служб тощо);
- модуль пріоритезації та автоматичного ранжування заявок, заснований на встановлених критеріях: соціальний статус, відстань до навчального закладу, успішність, наявність дітей, інвалідність тощо;
- інтерфейс для комісії, що дозволяє розглядати заявки, перевіряти документи, приймати рішення і формувати списки на поселення;
- інтеграція з базами студентів, навчальних планів та гуртожитків, що дозволяє виключити дублювання даних і підвищує надійність;

До нефункціональних вимог належать:

- надійність і відмовостійкість системи, враховуючи високе навантаження в періоди масового подання заяв [1].
- безпека персональних даних, що обробляються відповідно до Закону України «Про захист персональних даних» та принципів GDPR.
- можливість масштабування, у разі підключення нових факультетів, гуртожитків або навчальних закладів [2].
- адаптивний інтерфейс, який працює однаково ефективно на ПК, планшетах і смартфонах;
- можливість генерації звітів для адміністрації, у тому числі для зовнішніх аудитів, формування статистики або звітування в міністерства.

Не менш важливо врахувати юридичні та регламентні аспекти: положення про порядок поселення, обмеження по термінах подачі заяв, процедуру подачі апеляцій. Система має враховувати ці правила автоматично, зменшуючи адміністративне навантаження.

Висновок

Програмна система обробки заяв на поселення в гуртожиток є необхідним компонентом сучасної цифрової інфраструктури ВНЗ. Її впровадження дозволить зробити процес поселення більш ефективним, прозорим і справедливим. Визначені функціональні та нефункціональні вимоги демонструють, що система має враховувати не лише технічні, але й соціальні, правові та адміністративні аспекти. Подальші дослідження можуть бути спрямовані на проєктування модулів системи та проведення експериментального впровадження на базі конкретного університету.

Список використаних джерел:

1. Haverbeke M. Eloquent JavaScript: A Modern Introduction to Programming. No Starch Press, 2018. 472 с.
2. Banks A., Porcello E. Learning React / A. Banks, E. Porcello. O'Reilly Media, 2020. 350 с.

УДК 004.78 (043.2)

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС СУШКИ ПЛАСТИКУ

Максим Маліновський

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Артамонов Є.Б., к.т.н., доц.

Ключові слова: Сушка для пластику, філамент, 3D принтер

На сьогодні 3D принтери набувають все більшої популярності у побутових користувачів та комерційних підприємствах котрі намагаються отримати належну якість своїх виробів, тому сушіння філаменту(мононитки) стає невід'ємною частиною процесу друку.

Мета: розробка апаратно-програмного комплексу для ефективного контролю та управління процесом сушки філаменту, що дозволить тримати під контролем процес сушіння.

Об'єктом дослідження є процеси дегідратації полімерних матеріалів. Для контролю параметрів сушіння використовується датчик температури та вологості, інтегрована з мікроконтролерною платформою. Основні методи дослідження включають експериментальне моделювання, аналіз та статистичну обробку даних для оптимізації алгоритмів керування.

В результаті розроблено апаратно-програмний комплекс, що складається з: мікроконтролерної системи керування сушильною установкою, датчиків для відслідковування параметрів у реальному часі та програмного алгоритму адаптивного регулювання параметрів.

Розроблений комплекс дозволяє керувати процесом сушіння філаменту. Отримані результати можуть бути в подальшому використано у виробничих процесах.

Список використаних джерел:

1. Wevolver. How to Dry Filament: PA, TPU, PLA, PVA & PET. URL: <https://www.wevolver.com/article/how-to-dry-filament>
2. Prusa3D. Drying filament. URL: https://help.prusa3d.com/article/drying-filament_332086

УДК 004.3 (043.2)

СИСТЕМА ОБЛІКУ ТА КЕРУВАННЯ ОБЛАДНАННЯМ НА ПІДПРИЄМСТВІ

Владислава Урсова

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ольга Самойліченко, д.т.н., доц.

Ключові слова: облік обладнання, автоматизація, управління активами, ERP-система, технічне обслуговування.

У сучасних умовах ефективно управління матеріальними активами підприємства відіграє ключову роль у підвищенні продуктивності та зниженні операційних витрат. Відсутність належного контролю за обладнанням може призвести до нераціонального використання ресурсів, збільшення витрат на обслуговування та ризику простоїв у виробництві. У зв'язку з цим автоматизація обліку обладнання стає необхідною умовою для стабільного функціонування підприємства та оптимального використання його активів [1].

Дослідження спрямоване на аналіз та впровадження системи обліку та керування обладнанням, яка дозволяє відстежувати місцезнаходження, технічний стан та історію обслуговування кожної одиниці. Основними елементами такої системи є база даних обладнання, засоби ідентифікації (наприклад, RFID-мітки або штрихкоди), програмне забезпечення для обліку та аналітики, а також інтеграція з ERP-системами підприємства [2].

Використання системи управління активами, такої як IBM Maximo, дозволяє підприємствам переходити від планового технічного обслуговування до обслуговування на основі фактичного стану обладнання, що сприяє продовженню життєвого циклу активів, зменшенню несподіваних простоїв та підвищенню продуктивності

команди [1]. Крім того, застосування прогнозного технічного обслуговування, заснованого на реальних даних та аналітиці, дозволяє передбачати та запобігати відмовам обладнання, що знижує ризик простоїв та продовжує загальний термін служби важливих активів [2].

Застосування прогнозного технічного обслуговування за допомогою SAP Predictive Asset Insights дозволяє аналізувати дані з датчиків IoT та інших джерел для прогнозування можливих відмов обладнання. Це дає змогу своєчасно планувати ремонтні роботи, що знижує ризик аварійних поломок та продовжує термін служби активів [3].

Результати впровадження таких систем свідчать про значне покращення ефективності управління активами, зниження витрат на технічне обслуговування та зменшення кількості незапланованих простоїв виробничого обладнання. Таким чином, впровадження автоматизованої системи обліку та керування обладнанням сприяє підвищенню ефективності управління активами підприємства, що в довгостроковій перспективі забезпечує стабільність його роботи та конкурентоспроможність на ринку [1,2].

Висновок

Запропонована система обліку та керування обладнанням підвищує ефективність використання ресурсів підприємства, сприяє зниженню експлуатаційних витрат і мінімізації простоїв. Отримані результати можуть бути використані для подальшого вдосконалення методів управління активами та інтеграції сучасних цифрових технологій у виробничі процеси.

Список використаних джерел:

1. IBM Maximo Asset Management V7.1 - IBM Redbooks. URL: <https://www.redbooks.ibm.com/redbooks/pdfs/sg247640.pdf>
2. Introducing Predictive Maintenance with SAP Predictive Asset Insights. URL: https://www.sap-press.com/introducing-predictive-maintenance-with-sap-predictive-asset-insights_5353/
3. Thompson B. Introducing Predictive Maintenance with SAP Predictive Asset Insights. – SAP Press, 2021. – 312 с. URL: https://www.sap-press.com/introducing-predictive-maintenance-with-sap-predictive-asset-insights_5353/3

УДК 681.52(043.2)

АКТУАЛЬНІСТЬ РОЗРОБКИ СИСТЕМ ДОНАВЕДЕННЯ В БПЛА

Денис Шевчук

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Глазок Олексій Михайлович, к.т.н., доц.

Ключові слова: донаведення, безпілотні літальні апарати (БПЛА), координація безпілотних систем, еволюційні алгоритми, кооперативне управління.

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 безпілотних літальних апаратів (БПЛА) полягає у забезпеченні їх здатності ефективно виконувати завдання навіть у найскладніших умовах. Сучасні технології дозволяють 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 точно 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 нам, 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 мінімізують 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.

Список використаних джерел:

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 004.77(043.2)

ПРОГРАМНИЙ МОДУЛЬ МОНІТОРИНГУ СТАНУ КОМП'ЮТЕРІВ У ЛОКАЛЬНІЙ МЕРЕЖІ

Владислав Степанін

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Масловський Борис, к.т.н., доц.

Ключові слова: Моніторинг, збір даних, обробка даних, автоматизація, локальна мережа.

Вступ. Розробка та впровадження систем моніторингу стану комп'ютерів у локальних мережах є одним із пріоритетних напрямків сучасних інформаційних технологій. Така система дозволяє своєчасно виявляти збої, аналізувати продуктивність та забезпечувати безперебійну роботу мережі. Автоматизоване відстеження стану комп'ютерів зменшує ризики, пов'язані з несправностями апаратного та програмного забезпечення. Метою роботи

є створення програмного модуля для моніторингу стану комп'ютерів у локальній мережі, реалізованого на основі сучасного технологічного стеку: мови програмування **C# (.NET 8)**, серверного фреймворку **ASP.NET Core** з використанням **SignalR**, а також використання **PostgreSQL** для зберігання даних і **Redis Backplane** для обміну повідомленнями. Цей підхід забезпечує швидку обробку даних і інтеграцію між різними компонентами системи.

Матеріали і методи. Для розробки програмного модуля було обрано мову програмування **C#** у поєднанні з **.NET 8**, що дозволяє використовувати новітні можливості платформи. Для серверної частини обрано фреймворк **ASP.NET Core**, що забезпечує високу продуктивність і можливість роботи з багатьма одночасними підключеннями. За допомогою **SignalR** реалізовано можливість двостороннього зв'язку в реальному часі між сервером і клієнтами, що забезпечує миттєве оновлення інформації на клієнтських пристроях.

Дані зберігаються у **PostgreSQL**, що забезпечує надійність та масштабованість системи. Для обміну повідомленнями між різними компонентами системи використовується **Redis Backplane**, що дозволяє масштабувати систему та зменшити затримки в обробці повідомлень.

Програмний модуль використовує технології **WMI (Windows Management Instrumentation)** та **SNMP (Simple Network Management Protocol)** для збору інформації про стан комп'ютерів у локальній мережі. Дані включають показники навантаження на процесор, використання оперативної пам'яті, стан дискових накопичувачів та активні процеси. Інтерфейс програми дозволяє відображати інформацію в реальному часі у вигляді таблиць і графіків, а також надсилати сповіщення при виявленні критичних змін у роботі комп'ютерів.

Результати. Розроблений програмний модуль на **C#** та **ASP.NET Core** з **SignalR** забезпечує ефективний моніторинг стану комп'ютерів у локальній мережі. В результаті проведеної роботи:

- Створено серверний модуль для збору та обробки даних про стан комп'ютерів.
- Створено функцію автоматичного збору даних з комп'ютерів за допомогою **WMI** та **SNMP**.
- Надано можливість експорту отриманих даних для подальшого аналізу.

Висновки. Розроблений програмний модуль для моніторингу стану комп'ютерів у локальній мережі надає функціонал для автоматизації відстеження стану систем. Використання сучасного технологічного стеку, включаючи **ASP.NET Core**, **SignalR**, **PostgreSQL**, **Redis Backplane** дозволило створити гнучку та ефективну систему для моніторингу, яка забезпечує своєчасне виявлення проблем і оптимізацію продуктивності мережі. Подальший розвиток модуля передбачає інтеграцію з хмарними сервісами для централізованого управління та підтримку мобільних пристроїв для віддаленого моніторингу.

Список використаних джерел:

1. Документація по WMI. URL: <https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>
2. Документація по ASP.NET. URL: <https://learn.microsoft.com/en-us/aspnet/core/?view=aspnetcore-9.0>
3. Документація по SignalR. URL: <https://learn.microsoft.com/en-us/aspnet/core/signalr/introduction?view=aspnetcore-8.0>
4. Документація по Redis. URL: <https://redis.io/docs/latest/>
5. Документація по PostgreSQL. URL: <https://www.postgresql.org/docs/>

УДК 004.8:519.2:551.5 (043.2)

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ПРОГНОЗУВАННЯ ПОГОДНИХ УМОВ НА ОСНОВІ АЛГОРИТМІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Зоряна Сліпченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ольга Кравченко, к.т.н.

Ключові слова: програмний засіб, прогнозування погоди, великі дані, інтелектуальний аналіз даних, алгоритм Априорі.

Вступ. У сучасному світі точне прогнозування погоди є важливим завданням для багатьох сфер діяльності, включаючи сільське господарство, транспорт та енергетику [1]. Традиційні методи прогнозування базуються на фізичних моделях атмосфери, але вони мають обмежену точність через високу варіативність метеорологічних процесів [2]. Використання методів інтелектуального аналізу даних дозволяє покращити прогнозування, обробляючи великі обсяги історичних даних та виявляючи приховані закономірності. Одним із таких методів є алгоритм Априорі, що використовується для пошуку асоціативних залежностей між метеорологічними параметрами.

Мета. Розробка програмного засобу для прогнозування погодних умов на основі алгоритмів інтелектуального аналізу даних.

Матеріали та методи. Для реалізації прогнозування використовується алгоритм Априорі, що дозволяє знаходити часті шаблони в великих наборах даних [3]. В якості вхідних даних застосовуються історичні метеорологічні показники, такі як температура, вологість, атмосферний тиск та швидкість вітру. Дані обробляються за допомогою методів машинного навчання та візуалізуються у вигляді прогнозів погоди на основі виявлених закономірностей (правил асоціацій). Програмний засіб реалізовано мовою Python із використанням бібліотек Pandas, Scikit-learn та Matplotlib.

Результати. Розроблений програмний засіб дозволяє аналізувати великі обсяги метеорологічних даних та виявляти залежності між основними кліматичними показниками. Використання алгоритму Априорі забезпечує автоматичне формування правил для прогнозування змін погодних умов. Інтерфейс програмного засобу забезпечує зручність використання для кінцевих користувачів.

Висновки. Розроблений програмний засіб демонструє ефективність алгоритмів інтелектуального аналізу даних для прогнозування погодних умов та може бути використаний у різних сферах господарської діяльності.

Список використаних джерел

1. Kalnay, E. (2002). Atmospheric Modeling, Data Assimilation and Predictability. 2nd Edition. Cambridge University Press. 2012. P.341
2. Wilks, D. S. Statistical Methods in the Atmospheric Sciences. 4th Edition, Elsevier. 2020. P.818.
3. Agrawal, R., Srikant, R. Fast Algorithms for Mining Association Rules. Proceedings of the 20th International Conference on Very Large Data Bases (VLDB). 1994. P.487-499.

УДК 004.9:620.9 (043.2)

ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ АНАЛІЗУ, МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕНЕРГОРЕСУРСАМИ

Максим Литвинюк

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Юлія Вітрук, к.т.н., доц.

Ключові слова: інформаційні системи, енергоресурси, моніторинг, управління, Big Data, штучний інтелект.

У сучасних умовах цифрової трансформації підвищується актуальність ефективного використання енергоресурсів. Інформаційні системи аналізу, моніторингу та управління енергоресурсами сприяють оптимізації енергоспоживання, зниженню витрат та підвищенню екологічної безпеки. У цій роботі розглядаються основні підходи до побудови таких систем, їх архітектурні рішення, а також технології збору, обробки та візуалізації даних.

Сучасні тенденції енергозбереження вимагають нових підходів до управління енергоресурсами. Використання інформаційних систем дозволяє здійснювати оперативний контроль за споживанням енергії, прогнозувати її використання та автоматизувати процеси управління. Впровадження таких систем є важливим для промислових підприємств, муніципальних установ та житлового сектору.

Основні компоненти інформаційної системи:

1. Збір даних – сенсори та IoT-пристрої реєструють показники енергоспоживання в реальному часі.
2. Обробка даних – програмні алгоритми аналізують отримані дані, виявляючи аномалії та тенденції.
3. Візуалізація та звітність – інтерактивні панелі керування та аналітичні звіти допомагають користувачам ухвалювати рішення.
4. Автоматизоване управління – використання штучного інтелекту та машинного навчання для оптимізації енергоспоживання.

Для забезпечення ефективного управління енергоресурсами застосовуються методи математичного моделювання, прогнозування споживання та автоматизованого керування. Важливу роль відіграє використання технологій Big Data та штучного інтелекту для обробки великих обсягів інформації та визначення оптимальних стратегій управління.

Висновок

Розвиток інформаційних систем аналізу, моніторингу та управління енергоресурсами є ключовим напрямком підвищення енергоефективності. Інтеграція сучасних цифрових технологій дозволяє не тільки знижувати витрати на енергоспоживання, але й сприяє зменшенню негативного впливу на

навколишнє середовище. Перспективи подальших досліджень включають удосконалення алгоритмів аналізу даних та розширення можливостей систем автоматизованого управління.

Список використаних джерел:

1. Баранов О.І., Ковальчук В.В. Інтелектуальні системи моніторингу та управління енергоспоживанням // Енергетика України.
2. Василенко С.М. Інформаційні технології в управлінні енергоресурсами: сучасний стан та перспективи // Сучасні інформаційні технології.
3. Khan M.A., Lee S. Smart Energy Management Systems: Concepts, Technologies, and Future Directions // Renewable and Sustainable Energy Reviews. – 2020. – Vol. 130. – P. 109876.

УДК 004.78 (043.2)

ПРИНЦИПИ ОЦІНКИ КОЕФІЦІЄНТУ ПРОДУКТИВНОСТІ ІОТ-СИСТЕМИ

Олексій Коломієць

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Володимир Артемчук, д.т.н., с.н.с.

Ключові слова: ІоТ-система, коефіцієнт продуктивності, метрики, пропускна здатність, сенсорна мережа, обробка даних

Інтернет речей (Internet of Things, ІоТ) охоплює мільярди пристроїв, які щосекунди генерують, передають і обробляють величезні обсяги даних. Такі системи проникають у всі сфери – від «розумного дому» до промислової автоматизації та охорони здоров'я. Зі зростанням масштабів і складності ІоТ-систем, постає потреба в об'єктивному вимірюванні їх ефективності [1]. Для цього застосовується поняття коефіцієнта продуктивності, що є інтегральною характеристикою здатності системи обробляти інформаційні потоки, виконувати задачі в реальному часі та масштабуватись без втрати якості обслуговування. Принципи оцінки цього коефіцієнта мають враховувати специфіку ІоТ: розподіленість, гетерогенність пристроїв, обмежені ресурси та чутливість до затримок [2].

Продуктивність ІоТ-системи – це не просто швидкість передачі даних чи обчислень. Це комплексна характеристика, яка поєднує апаратні, мережеві та програмні параметри. Оцінка продуктивності базується на принципах, що дозволяють перетворити технічні вимірювання на значущі метрики системного рівня.

Першим принципом є модульність і багаторівневість оцінки. ІоТ-система складається з сенсорного рівня, мережевого рівня, обчислювального ядра (локального або хмарного) та рівня користувацької взаємодії. Для кожного з них визначаються окремі показники – затримка, надійність, пропускна здатність, кількість оброблених запитів, рівень втрат пакетів, час реакції тощо. Підсумковий коефіцієнт продуктивності формується як агрегат цих часткових показників, з урахуванням вагових коефіцієнтів залежно від критичності кожного рівня для конкретного застосування.

Другий принцип – адаптивність метрик до типу ІоТ-системи. Наприклад, для систем «розумного міста» критичною є масштабованість і здатність обслуговувати тисячі одночасних запитів, тоді як для медичних ІоТ-рішень важливішими є надійність і мінімальні затримки. Це означає, що коефіцієнт

продуктивності не може бути універсальним – він повинен будуватись на адаптованих, контекстних метриках.

Третій принцип – баланс між обсягом переданої інформації та ресурсами, які витрачаються на її обробку. Важливо не лише оцінити, скільки пристроїв обслуговує система, але й скільки енергії, трафіку і обчислювальної потужності витрачається на обробку одиниці інформації. Це дозволяє порівнювати різні IoT-рішення за ефективністю їх функціонування в умовах обмежених ресурсів.

Четвертий принцип – інтеграція з реальними сценаріями використання. Продуктивність не повинна вимірюватись лише синтетичними тестами. Необхідно враховувати типові сценарії – наприклад, кількість збоїв під час передачі даних з датчика температури до хмарного сервера у період пікового навантаження, або середній час реакції «розумного» контролера на зміну стану системи.

П'ятий принцип – часова динаміка. Коефіцієнт продуктивності має відображати зміну характеристик у часі: деградацію при перевантаженні, затримки у вечірній період або просідання продуктивності після оновлення. Без урахування таких коливань метрики будуть неповними або хибними.

У процесі аналізу були сформульовані основні принципи оцінки коефіцієнта продуктивності IoT-системи:

- система оцінки повинна охоплювати всі рівні архітектури – від сенсора до хмари;
- загальний коефіцієнт має враховувати ефективність використання ресурсів, динаміку продуктивності у часі та реальні умови експлуатації;
- запропоновані підходи дозволяють побудувати формалізовану модель для автоматизованої оцінки IoT-продуктивності у виробничих або дослідницьких середовищах.

Висновок

Оцінка коефіцієнта продуктивності IoT-системи є критично важливим етапом у проектуванні, тестуванні та експлуатації розподілених обчислювальних платформ. Врахування структурної складності, мінливості навантаження та контексту використання дозволяє забезпечити об'єктивне вимірювання ефективності. Запровадження чітких принципів і метрик відкриває шлях до створення стандартів продуктивності IoT-рішень, що, у свою чергу, сприятиме їх більш широкому впровадженню у ключових секторах економіки.

Список використаних джерел:

1. Damor D. IoT Security Threats and Solutions [Електронний ресурс]. Режим доступу: <https://www.einfochips.com/blog/iot-securitythreats-and-solutions/> (Дата звернення: 24.03.2025).
2. Garg H. Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware / H. Garg, M. Dave // 4th International Conference on Internet of Things: Smart Innovation and Usages. Ghaziabad, India, 2019. P. 1-6. (Дата звернення: 22.03.2025).

УДК 004.7 (043.2)

АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ СИСТЕМ ДОСТАВКИ В РЕСТОРАННІЙ ДІЯЛЬНОСТІ

¹Назар Сосновський, ²Артем Дехтяренко¹Державний університет «Київський авіаційний інститут», Київ,²Фаховий коледж інженерії, управління та землевпорядкування Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Євген Артамонов, к.т.н., доц.

Ключові слова: ресторан, система доставки, логістика, замовлення онлайн,

Ресторанний бізнес зазнає суттєвих трансформацій під впливом цифровізації та зміни споживацьких моделей поведінки. Однією з ключових тенденцій останнього десятиліття є стрімке зростання попиту на послуги доставки готових страв. Для ресторану доставка – це не просто логістика, а окремий канал продажів зі своєю інфраструктурою, IT-рішеннями та клієнтським досвідом. Побудова ефективної системи доставки потребує інтеграції технологій, аналітики та операційної гнучкості. Аналіз принципів, на яких базуються такі системи, дозволяє зрозуміти фактори успіху та уникнути поширених помилок при запуску або масштабуванні служби доставки в ресторанному середовищі.

Система доставки в ресторанній діяльності охоплює не лише фізичне переміщення товару до клієнта, а й усі етапи – від формування замовлення до контролю виконання. Її побудова спирається на кілька ключових принципів.

Перший принцип – інтегрованість процесів. Замовлення має надходити безпосередньо з інтерфейсу клієнта (мобільний застосунок, сайт, кол-центр) у внутрішню облікову систему ресторану або POS-систему. Це дозволяє автоматично запускати процес приготування, уникати помилок та дублювання, а також швидко реагувати на зміни в замовленні.

Другий – реальний час як стандарт. Усі компоненти системи повинні взаємодіяти в режимі реального часу: статус замовлення, кур'єра, наявність продуктів, зміна маршрутів доставки тощо.

Третій принцип – гнучкість логістичної моделі. Сучасна система доставки може бути: власною (in-house), через маркетплейс (Glovo, Bolt Food), гібридною або франчайзинговою. Вибір залежить від масштабу ресторану, його бюджету, лояльності клієнтів та географії. Ефективна система дозволяє легко перемикастись між моделями, зберігаючи контроль за якістю.

В розробленій системі все коригування меню проводиться в розділі єдиного меню можна обрати тільки категорії для системи інтеграції з Глово (рис. 1).

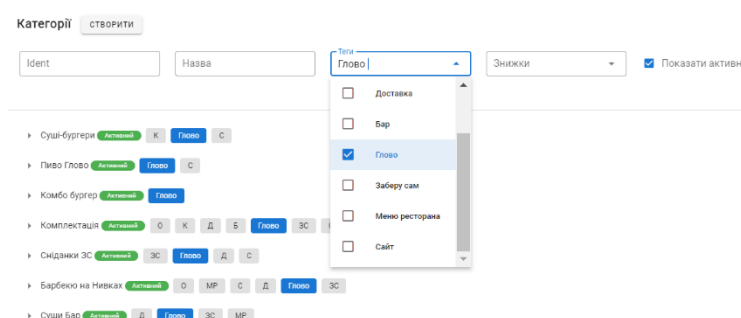


Рис. 2. Категорії для Глово

Вікно (рис. 2) є інтерфейсом для управління меню ресторанів, інтегрованим з платформою Glovo, розробленим за допомогою мови програмування PHP та бази даних MySQL. Вікно дозволяє користувачам переглядати, оновлювати та управляти меню ресторанів, інтегрованих з Glovo.

#	Назва	Glovo ID	Статус	Статус оновлення	Дії
26	вул. Рогнідницька, 5/14 Коня	ghofa698988	Активний	Помилка оновлення	Оновити меню в Glovo, Переглянути JSON, [іконки]
25	ДК Миколайчука 614019 GLOVO суши	614019	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
24	ДК Миколайчука GLOVO бургер	614006	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
23	ДК Миколайчука 614010 GLOVO вок	614010	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
22	ДК Миколайчука 614029 Glovo піца	614029	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
21	пр-т Правди, 47	1008806	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
20	пр-т Оболонський, 19	1001828	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
19	вул. Райси Окіпної, 3	1003372	Активний	Не підняв статус	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]
18	м.Вишневе, вул. Святошинська, 27Е	1003371	Активний	SUCCESS	Оновити статус, Оновити меню в Glovo, Переглянути JSON, [іконки]

Рис. 2. Розроблене вікно інтеграції

Висновок

Системи доставки в ресторанній діяльності є не просто допоміжними інструментами, а центром цифрової взаємодії з клієнтами. Принципи їх побудови базуються на швидкості, точності, прозорості, гнучкості та орієнтації на користувача. З огляду на зміну ринку, успішна система доставки – це результат технічної інтеграції, логістичного менеджменту та досвіду клієнта. Майбутні дослідження повинні зосередитись на використанні штучного інтелекту в прогнозуванні попиту, адаптивному управлінні кур'єрами та інтеграції з фінансовими й CRM-системами.

УДК 004.7 (043.2)

РЕФАКТОР-ПОМІЧНИК ЯК ІНСТРУМЕНТ ДЛЯ ЗНИЖЕННЯ ТЕХНІЧНОГО БОРГУ ТА БОРОТЬБИ ІЗ ЗАСТАРІЛИМ КОДОМ

Олексій Фещенко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олена Нечипорук, д.т.н., професор

Ключові слова: рефакторинг, технічний борг, середовище розробки, надання рекомендацій.

Технічний борг є однією з головних проблем, що впливають на розвиток програмного забезпечення. Його накопичення може значно знизити ефективність розробки, ускладнити підтримку і збільшити витрати на обслуговування продукту. Сучасні інструменти рефакторингу, зокрема вбудовані в середовища розробки, допомагають виявляти проблеми в коді та автоматизувати процеси оптимізації. Проте навіть у найпоширеніших редакторах не завжди можна ефективно боротися з усіма аспектами технічного боргу.

Для дослідження були обрані популярні середовище розробки та інструменти для аналізу коду, такі як Visual Studio, IntelliJ IDEA, Eclipse, а також SonarQube та ReSharper. Оцінка цих інструментів проводилася за кількома критеріями: точність виявлення проблем, здатність пропонувати рефакторинг рішень, ефективність підтримки складних проєктів. Для цього було вибрано кілька реальних проєктів з відкритим кодом, в яких проводився аналіз на предмет дублювання коду, складності функцій та архітектурних недоліків.

Visual Studio має вбудовані інструменти аналізують синтаксичні помилки і надають базові рекомендації щодо рефакторингу. Однак інструмент не завжди здатен виявити складні архітектурні проблеми. IntelliJ IDEA пропонує потужні функції рефакторингу для Java, виявляючи дублювання коду та складні конструкції. Проте підтримка інших мов обмежена. Eclipse має схожі функції з IntelliJ IDEA, але потребує додаткових плагінів для повного аналізу. Інструменти для рефакторингу менш ефективні. SonarQube є незалежним інструментом, який глибоко аналізує технічний борг, виявляючи не тільки помилки в коді, але й недоліки в архітектурі. Підходить для інтеграції з CI/CD системами. ReSharper - плагін для Visual Studio, що покращує рефакторинг, надаючи точні рекомендації. Однак потребує додаткових ресурсів для інтеграції.

Для створення більш ефективного Рефактор-помічника можна застосувати кілька інноваційних підходів. Один з них – читання та аналіз коду в реальному часі за допомогою асистента. Це дозволить миттєво виявляти проблеми під час написання коду та надавати рекомендації щодо його покращення на основі аналізу поточних змін. Інструмент, який відстежує кожну зміну, може підказувати правильні підходи до рефакторингу або попереджати про потенційні помилки, не чекаючи завершення всього коду.

Ще один важливий елемент – це аналіз коду за допомогою штучного інтелекту. Інтелектуальні алгоритми можуть вивчати та аналізувати великі обсяги коду, виявляючи неочевидні помилки, які можуть бути пропущені традиційними інструментами. Наприклад, такі алгоритми можуть не лише знаходити помилки синтаксису чи стилю, але й виявляти складні логічні помилки чи проблеми з архітектурою, пропонуючи автоматичні варіанти їх виправлення.

Також вартує запровадити можливість аналізу коду інших програмістів. Це дозволить відстежувати та застосовувати кращі практики, які використовуються в інших проєктах. Наприклад, помічник може порівнювати написаний код з кращими зразками на відкритих платформах, таких як GitHub, пропонуючи на основі порівняння рекомендації щодо його покращення. Такий аналіз може допомогти розробникам швидше знаходити оптимальні рішення для складних завдань, зокрема в питаннях оптимізації та масштабування коду.

Ще одним способом підвищення ефективності рефакторингу є імпорт моделей-помічників, створених іншими програмістами. Наприклад, програмісти можуть обмінюватися інструментами, які вже оптимізують певні типи коду, чи використовувати їх в своїх проєктах. Це дозволить зекономити час

на розробку нових рішень і інтегрувати перевірені методи покращення коду, вже створені іншими спеціалістами.

Висновок

Інструменти для рефакторингу коду, такі як Visual Studio, IntelliJ IDEA, SonarQube, здатні полегшити виявлення технічного боргу. Однак для досягнення кращих результатів необхідно розробити спеціалізоване програмне забезпечення, яке б зосереджувалося на комплексному аналізі архітектури і забезпечувало глибокі рекомендації щодо рефакторингу.

Список використаних джерел:

1. Learn Visual Studio Refactor code. URL: <https://learn.microsoft.com/en-us/visualstudio/ide/refactoring-in-visual-studio?view=vs-2022> (Last accessed: 26.03.2025).
2. IntelliJ IDEA Code refactoring. URL: <https://www.jetbrains.com/help/idea/refactoring-source-code.html> (Last accessed: 26.03.2025).
3. ReSharper Refactorings. URL: https://www.jetbrains.com/help/resharper/Refactorings__Index.html (Last accessed: 26.03.2025).

УДК 004.87 (043.2)

АНАЛІЗ ЗАДАЧ ОБРОБКИ І МОНІТОРИНГУ ЗАМОВЛЕНЬ ІНТЕРНЕТ-МАГАЗИНУ

Станіслав Нікішин

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Євген Артамонов, к.т.н., доц.

Ключові слова: інтернет-магазин, замовлення, моніторинг замовлень, статус доставки, валідація даних, автоматизація

Електронна комерція є однією з найдинамічніших сфер цифрової економіки. У центрі її функціонування перебуває механізм обробки та моніторингу замовлень – ключовий бізнес-процес, що забезпечує безперервну взаємодію між клієнтами, складом, службами доставки та фінансовими системами. Надійність і ефективність цього процесу безпосередньо впливають на рівень клієнтського сервісу, швидкість доставки, точність розрахунків і здатність компанії масштабуватись. Успішне функціонування інтернет-магазину неможливе без чіткого розуміння задач, пов'язаних із цим етапом життєвого циклу замовлення.

Задачі обробки замовлень охоплюють весь шлях – від моменту створення замовлення клієнтом до його фізичного виконання. Перший блок задач пов'язаний із формуванням та валідацією замовлення. Система повинна перевірити наявність товарів, достовірність обраних параметрів (розмір, колір, кількість), правильність контактних та платіжних даних. У цьому ж етапі виконується перевірка на дублікати, шахрайські дії та обмеження за регіонами доставки.

Наступна група задач стосується обробки замовлення в бекенді: резервування товарів на складі, генерація рахунків, підготовка замовлення до відвантаження, взаємодія з кур'єрськими службами та

сторонніми логістичними провайдерами. Важливо забезпечити автоматичну синхронізацію цих дій з ERP або WMS-системами, щоб уникнути втрати або затримки замовлення.

Третя категорія задач – моніторинг статусів замовлення в реальному часі. Кожен етап (прийнято, в обробці, на складі, передано до доставки, доставлено) повинен відображатись як у внутрішньому інтерфейсі менеджера, так і у профілі клієнта [1]. Важливо, щоб система підтримувала як автоматичні статуси (на основі API з логістами), так і ручне оновлення, якщо частину логістики виконує персонал магазину. Особливої уваги заслуговує обробка помилок і винятків, зокрема відсутність товару після підтвердження, затримка доставки або збої в оплаті. Система має вміти вчасно інформувати користувача, пропонувати альтернативи (наприклад, інші варіанти доставки або заміну товару), генерувати службові сповіщення для відповідального персоналу.

Ще один блок – аналітика та аудит замовлень. IT-система повинна надавати менеджерам доступ до статистики виконання замовлень, рівня повернень, середнього часу доставки, кількості замовлень у статусі очікування, прострочених або скасованих. Це дає змогу виявляти вузькі місця та оптимізувати процеси.

Також важливими є задачі, пов'язані з інтеграцією з платіжними системами (LiqPay, Stripe, PayPal), забезпеченням безпеки транзакцій, створенням сповіщень по email/SMS/месенджерах, а також механізмами підтвердження отримання товару.

В результаті аналізу задач обробки і моніторингу замовлень виявлено:

- основними технічними точками контролю є: валідація даних, управління статусами, синхронізація з логістикою та системами складу, обробка винятків;
- критичними для бізнесу є завдання оперативного оновлення статусів та вчасного реагування на зміни – затримки, недоступність товарів, помилки оплати;
- впровадження інструментів аналітики та автоматичних сповіщень значно підвищує контроль над якістю виконання замовлень [2];
- комплексність задач вимагає модульного підходу до побудови програмного забезпечення інтернет-магазину.

Висновок

Обробка і моніторинг замовлень в інтернет-магазині – це багаторівневий процес, який поєднує клієнтський інтерфейс, бекенд-сервіси, логістику, фінансові операції та моніторинг. Ефективна реалізація цього процесу потребує не лише автоматизації, а й впровадження адаптивних рішень, здатних реагувати на динамічну поведінку користувачів та ринку. Аналіз задач показує, що ключем до успішного функціонування інтернет-магазину є прозорість, контроль, інтеграція і швидкість обробки замовлень.

Список використаних джерел:

1. Методичні вказівки до лабораторних робіт з дисципліни «Дослідження і проектування інтерфейсів користувача» для студентів напряму підготовки 123 – «Комп'ютерна інженерія» /Укл.: А. С. Посадська, В. В. Нехай. – Чернігів: ЧНТУ, 2018. – 32 с
2. Miraz, M. H., Ali, M., and Excell, P. S. Adaptive user interfaces and universal usability through plasticity of user interface design. Computer Science Review 40 (2021), 100363

УДК 004.89:629.3.05 (043.2)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ФІЛЬТРА КАЛМАНА ДЛЯ ІНТЕГРАЦІЇ ДАНИХ GPS І IMU

Андрій Радченко, Тарас Залозний

Державний університет «Київський авіаційний інститут», Київ,

Науковий керівник – Юлія Авер'янова, д.т.н., проф.

Ключові слова: фільтр Калмана, навігаційна система, зашумлене середовище, інтеграція сенсорів, прогнозування положення

Навігаційні системи, що поєднують дані з GPS-приймачів та інерціальних вимірювальних одиниць (IMU), є ключовими компонентами у безпілотному транспорті, мобільній робототехніці, розумних дронах та геодезичних приладах. Однак їх точність значно знижується в умовах обмеженої доступності сигналів GPS (наприклад, у міських каньйонах, тунелях, закритих приміщеннях) або при значному зашумленні сигналів від акселерометрів та гіроскопів. Для забезпечення безперервної та надійної оцінки положення і швидкості в таких умовах необхідно застосовувати методи фільтрації і прогнозування стану системи. Одним із найефективніших підходів є використання фільтра Калмана, що дозволяє об'єднувати зашумлені дані з різних джерел у єдину оцінку стану з мінімальною середньоквадратичною похибкою.

Фільтр Калмана є ітеративним алгоритмом оцінювання стану динамічної системи у разі наявності гаусового шуму у вхідних даних [1]. У контексті GPS/IMU інтеграції він виконує дві основні функції: прогноз стану (на основі IMU) та корекцію прогнозу (коли доступні GPS-дані). Це дає змогу використовувати швидку частоту оновлення IMU, навіть коли GPS надає інформацію з низькою частотою або перериваннями [2].

IMU-дані (лінійне прискорення, кутова швидкість) дають змогу отримати короткотерміновий прогноз траєкторії об'єкта, однак похибка у цих обчисленнях накопичується з часом (drift). Дані з GPS, у свою чергу, дають абсолютну позицію, але з меншою частотою та залежністю від доступності супутників [3]. Фільтр Калмана поєднує ці джерела, враховуючи їхні дисперсії, щоб зменшити сумарну похибку.

У межах дослідження були проведені моделювання двох сценаріїв:

- ідеальні умови – без шуму у GPS і IMU;
- зашумлене середовище – GPS-сигнал переривчастий, IMU має гаусовий шум.

У кожному циклі фільтр Калмана використовував зашумлені вимірювання GPS для корекції прогнозованих значень. На кожному кроці інновація (різниця між вимірюванням і прогнозом) була значною, але фільтр Калмана значно зменшив цю помилку за допомогою коефіцієнта Калмана, що призвело до більш точного положення та швидкості.

На кожному кроці фільтр Калмана зменшував невизначеність у системі, що проявлялося у зменшенні елементів коваріаційної матриці після корекції та адаптувався до умов високого рівня шуму датчиків GPS і IMU. Про це свідчить зменшення похибок положення та швидкості на кожному кроці корекції, навіть за наявності великої початкової невизначеності через шум.

Результати моделювання та експериментів засвідчили:

- зменшення середньої похибки позиціонування в зашумлених умовах у 2–3 рази при використанні фільтра Калмана у порівнянні з окремим використанням GPS або IMU;
- стабільність визначення швидкості і положення навіть при відсутності GPS протягом коротких періодів (до 5–10 секунд);
- гнучкість моделі щодо варіацій частоти IMU та періодичності GPS-повідомлень;
- зниження впливу високочастотного шуму IMU за рахунок згладжування фільтром та динамічної адаптації до якості даних.

Висновок

Фільтр Калмана є ефективним інструментом для інтеграції даних GPS та IMU в умовах зашумленого середовища. Його здатність передбачати стан у разі втрати GPS, зменшувати ефект шуму та забезпечувати плавність траєкторій робить його незамінним у критичних застосуваннях. З урахуванням варіативності навігаційного середовища та сенсорного шуму, застосування Баєсівських методів фільтрації стає стандартом у розробці високоточних систем позиціонування. Подальші дослідження будуть спрямовані на адаптивні фільтри (Unscented Kalman Filter або Extended Kalman Filter), що краще працюють із нелінійними системами.

Список літератури:

1. X. Zhang, Y. Bai, S. Chai. (2018). State Estimation for GPS Outage Based on Improved Nonlinear Autoregressive Model, in: Proceedings of the IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 23-25 November 2018. doi:10.1109/icseess.2018.8663875.
2. P. Matisko, V. Havlena. (2012). Optimality tests and adaptive Kalman filter, IFAC Proceedings Volumes 45. 1523-1528. doi:10.3182/20120711-3-be-2027.00011.
3. J. Sun, L. Tao, Z. Niu, B. Zhu. (2020). An Improved Adaptive Unscented Kalman Filter With Application in the Deeply Integrated BDS/INS Navigation System, IEEE Access 8. 95321-95332. doi:10.1109/access.2020.2995746.

УДК 004.89 (043.2)

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ ДЛЯ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Дмитрій Студзінський

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олена Нечипорук, д.т.н., професор*

Ключові слова: кібербезпека, штучний інтелект, машинне навчання, аналіз загроз, виявлення аномалій.

Сучасний розвиток інформаційних технологій супроводжується збільшенням ризиків кіберзагроз, що вимагає удосконалення механізмів захисту. Традиційні методи виявлення атак часто мають низьку ефективність у розпізнаванні новітніх загроз. Використання інтелектуальних алгоритмів машинного навчання дозволяє покращити систему безпеки шляхом автоматизованого аналізу аномалій у трафіку [1, 2].

Метою дослідження є розробка методів застосування машинного навчання для кібербезпеки, що підвищують точність виявлення атак та зменшують кількість хибнопозитивних результатів.

У дослідженні використано методи обробки великих даних та алгоритми глибокого навчання, такі як нейронні мережі та кластеризація. Дані для навчання моделі зібрані з відкритих джерел, зокрема KDD Cup 99 та CICIDS2017. Оптимізація алгоритмів проводилася шляхом адаптації параметрів моделі та використання графічних процесорів для прискорення обчислень.

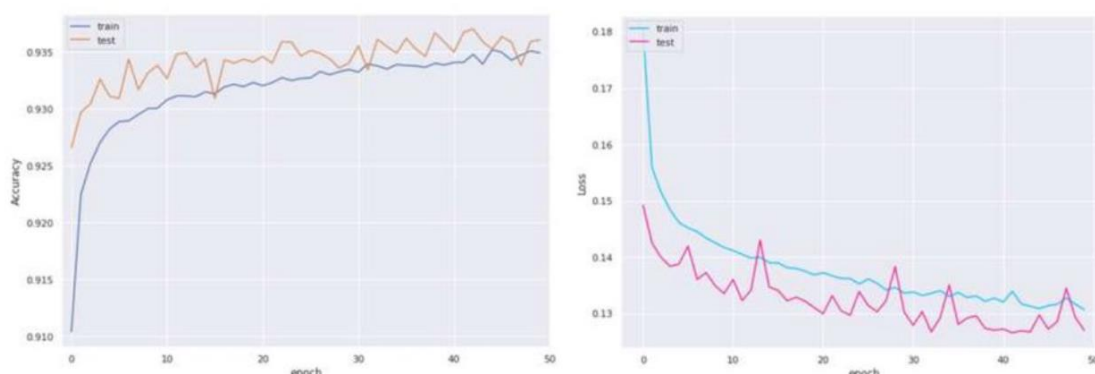


Рис.1. Порівняння точності виявлення загроз традиційними методами та з використанням машинного навчання

Розроблена модель досягла точності 98% у класифікації мережевого трафіку на безпечний і загрозливий. Використання методів поведінкового аналізу дозволило зменшити частку хибнопозитивних спрацьовувань на 20% у порівнянні з класичними підходами до виявлення загроз.

Висновок

Впровадження машинного навчання в системи кібербезпеки дозволяє підвищити рівень захисту інформаційних ресурсів та зменшити ймовірність успішних атак. Запропоновані алгоритми можуть бути використані у фінансовій сфері, державних установах та корпоративних мережах.

Список використаних джерел:

1. Sommer R., Paxson V. Машинне навчання для виявлення вторгнень у мережу. Симпозіум IEEE з безпеки та конфіденційності, 2010.
2. García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E. Виявлення мережевих вторгнень на основі аномалій: методи, системи та виклики. Computers & Security, 2009.

УДК 004.87 (043.2)

ПРИНЦИПИ РОБОТИ БОТУ РОЗКЛАДУ УНІВЕРСИТЕТУ**Андрій Карвасарський***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Євген Артамонов, к.т.н., доц.*

Ключові слова: розклад, бот, моніторинг занять, статус доставки, валідація даних, автоматизація

У цифрову епоху автоматизація щоденних інформаційних процесів є не розкішшю, а необхідністю. В межах освітнього середовища особливу роль відіграє доступ до актуального розкладу занять, що стосується як студентів, так і викладачів. Ручний або частково автоматизований підхід до оновлення й розповсюдження розкладу часто спричиняє затримки, помилки й непорозуміння. Рішенням цієї проблеми є впровадження інтелектуального боту, здатного у зручній формі надавати розклад у відповідь на запити користувачів через популярні платформи (Telegram, Viber, Facebook Messenger тощо).

Комплекс програмного коду являє собою систему для автоматизованого отримання та надання розкладу занять студентам Київського авіаційного інституту (КАІ). Система складається з декількох ключових компонентів, кожен з яких виконує свою визначену функцію для забезпечення безперебійного доступу користувачів до актуального розкладу.

Першим важливим елементом є парсер, представлений класом ParseController. Його основне завдання полягає в автоматизованому зборі та обробці даних розкладу безпосередньо з вебсайту КАІ. Для цього парсер використовує бібліотеку Guzzle для здійснення HTTP-запитів до веб сервера університету та бібліотеку Symfony DomCrawler для ефективної навігації та вилучення необхідної інформації з HTML-коду веб сторінок.

Функціональність парсера охоплює отримання переліку всіх існуючих факультетів, збір списку академічних груп для кожного факультету та, найважливіше, вивантаження детального розкладу занять для кожної окремої групи. Зібрані та оброблені дані потім зберігаються в структурованому вигляді у базі даних, зокрема в таблицях

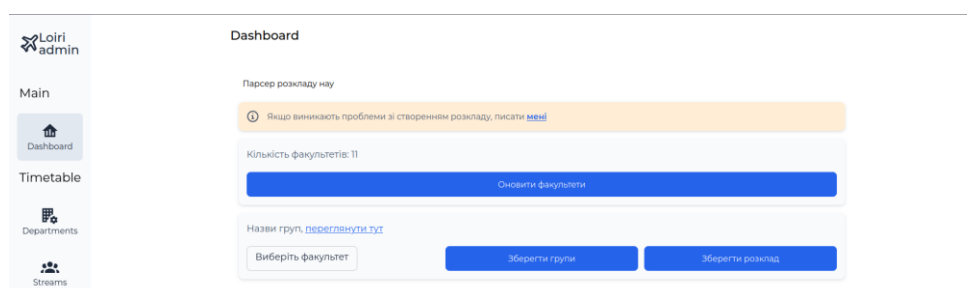


Рис. 1. Вікно веб-інтерфейса боту розкладу університету

Departments, Groups, Stream та Timetable. Ці дані слугують першоджерелом інформації для подальшого використання іншими компонентами системи, такими як Telegram-бот та потенційний веб сайт.

Другим ключовим компонентом є Telegram-бот, розроблений для забезпечення зручного та оперативного доступу студентів до розкладу занять через популярний месенджер Telegram. Блок коду визначає набір команд, на які реагує бот. Кожна команда виконує певну функцію: від вітання користувача та надання загальної інформації про бота (/start, /help) до надання можливості вибору своєї академічної групи (/selectgroup) та безпосереднього отримання актуального розкладу на різні періоди часу (/time, /lesson, /today, /tomorrow, /day, /week). Для реалізації взаємодії з Telegram API використовується бібліотека Nutgram, яка спрощує обробку команд та надсилання відповідей користувачам. Додатково реалізована функція підписки (/subscription), яка має основу для реалізації автоматичних сповіщень. Для покращення візуального сприйняття повідомлень використовується HTML-форматування.



Рис. 2. Вікно Telegram-бота розкладу університету

Висновок

Бот розкладу є прикладом ефективного використання автоматизації в освітньому процесі. Його розробка базується на принципах інтеграції, персоналізації, зручності, безперервної доступності та аналітичного зворотного зв'язку. Така система покращує управління навчальним процесом, підвищує прозорість та зменшує навантаження на персонал. Перспективи розвитку включають впровадження ШІ для адаптації до індивідуального графіку, синхронізацію з мобільними календарями та розширення функціоналу до повноцінного студентського помічника.

УДК 004.87 (043.2)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ АЛГОРИТМУ ЛЕВЕНШТЕЙНА ДЛЯ КАТЕГОРИЗАЦІЇ КОРИСТУВАЧІВ НАВЧАЛЬНИХ СИСТЕМ

Костянтин Радченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Євген Артамонов, к.т.н., доц.

Ключові слова: алгоритм Левенштейна, категоризація користувачів, навчальні системи, траєкторія дій, кластеризація, поведінковий аналіз, адаптивне навчання, освітня аналітика

З поширенням електронного навчання зростає потреба у персоналізованому підході до користувачів навчальних систем, зокрема в автоматичній категоризації студентів за стилем навчання, активністю або траєкторією взаємодії з платформою. Одним із найкращих підходів до такої класифікації є аналіз послідовностей дій користувача та визначення схожості між ними. У цьому контексті застосування алгоритму Левенштейна, який обчислює відстань редагування між двома рядками, дозволяє порівнювати траєкторії використання системи та групувати студентів із подібними поведінковими шаблонами. Такий метод відкриває можливості для глибшого розуміння навчального процесу, виявлення ризикових категорій та оптимізації адаптивного контенту.

Алгоритм Левенштейна, або метрика редагування, визначає мінімальну кількість операцій (вставка, видалення, заміна символу), необхідних для перетворення одного рядка в інший. У випадку навчальних систем, такими "рядками" виступають послідовності дій користувача, зафіксовані в логах системи: відкриття модуля, проходження тесту, завантаження файлу, спілкування на форумі тощо. Кожна подія кодується умовним символом, а повна взаємодія за певний період – у вигляді строки.

Для прикладу:

- користувач А: A-B-B-C-D-E;
- користувач Б: A-B-D-E.

Відстань Левенштейна дорівнює 2 (видалення В та С).

Цей показник використовується як міра подібності, на основі якої користувачів можна об'єднувати в кластери. Для обробки великої кількості таких "поведінкових рядків" застосовуються методи машинного навчання – зокрема, кластеризація на основі відстаней (наприклад, K-means або DBSCAN із попередньо обчисленою матрицею відстаней).

Перевагою алгоритму Левенштейна є простота реалізації та інтерпретації результату. Якщо група користувачів має схожі послідовності, можна припустити наявність типового навчального шаблону: пасивні слухачі, активні експлорери, стратегічні виконавці тощо. Це дає змогу:

- налаштовувати інтерфейс під стиль навчання;
- виявляти користувачів із нетиповими чи хаотичними траєкторіями;

- прогнозувати ризик непроходження курсу;
- виводити рекомендації для викладача щодо втручання.

Однак алгоритм Левенштейна не враховує контекст подій (що саме зробив студент), лише їхню позицію і порядок. Наприклад, проходження тесту після прочитання лекції і перед ним мають однакову "вартість" заміни. Тому метод часто доповнюється ваговими коефіцієнтами подій або комбінується з іншими метриками (наприклад, часовими).

У дослідженні було проведено симуляцію та аналіз логів поведінки студентів на LMS Moodle, де послідовності дій були представлені у вигляді рядків, а Левенштейнівські відстані обчислені попарно між усіма користувачами. Застосована кластеризація дозволила виявити три основні типи користувачів з різними підходами до навчання.

Висновок

Застосування алгоритму Левенштейна для аналізу поведінки користувачів у навчальних системах є перспективним напрямом для створення адаптивного та гнучкого цифрового освітнього середовища. Він дозволяє виявляти подібності в траєкторіях користування платформою, формувати поведінкові кластери та підвищувати якість персоналізованого навчання. Подальші дослідження можуть бути спрямовані на поєднання цього методу з часовими метриками, семантичним аналізом подій та гібридними підходами на основі нейронних мереж.

УДК 004.9:351.78 (043.2)

МОБІЛЬНИЙ ДОДАТОК ДЛЯ ЕКСТРЕНОГО ОПОВІЩЕННЯ ТА ВИКЛИКУ СЛУЖБ БЕЗПЕКИ

Авраменко Ангеліна

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Голего, ст.викладач

Ключові слова: екстрений, оповіщення, служби безпеки, мобільний додаток

У сучасному світі швидке інформування та виклик служб безпеки, як пожежна-рятувальна служба чи швидка медична допомога є надзвичайно важливими, оскільки будь-яка хвилина чи година може коштувати життя. Особливо якщо це стосується проблем зі серцем чи мозку. Відомі випадки зупинки серця, свідчать, що кожна хвилина без медичної допомоги зменшує ймовірність виживання людини на 7-10% [1].

Майже кожна людина стикалась з ситуаціями, коли потрібна була допомога спеціалізованих служб, але через брак знань чи інших індивідуальних проблем чи ситуацій не змогла отримати таку бажану допомогу, тому впровадження спеціалізованих мобільних додатків для екстреного оповіщення є актуальною в сучасному світі.

Об'єкт дослідження: мобільний додаток для екстреного оповіщення та виклику служб безпеки. Основні властивості: виклик служб безпеки, можливість передачі інформації. Для наукового обґрунтування результатів дослідження були використані методи аналізу даних та обробки.

Аналіз показав, що впровадження мобільних додатків для екстреного оповіщення та виклику(інформування) служб безпеки підвищує ефективність реагування на надзвичайні ситуації. Зокрема, такі додатки дозволяють швидко передавати інформацію про місцезнаходження користувача та характер події до відповідних служб [2]. Крім того, використання таких мобільних додатків дозволяє користувачам у незвичайній ситуації чи з обмеженими можливостями отримати бажану допомогу. Таким чином мінімізуються ситуації, де люди з обмеженими можливостями не отримують відповідну допомогу від обраної служби безпеки.

Висновки

Для безпеки кожної людини та населення в цілому розробка і впровадження мобільних додатків для екстреного оповіщення є вкрай важливими. Вони не тільки забезпечують зручну та оперативну комунікацію з службами, а й дозволяють швидко отримати необхідну допомогу у критичних ситуаціях. Крім того, такі технології сприяють інтеграції осіб з обмеженими можливостями у систему екстреного реагування, забезпечуючи їм рівний доступ до необхідної підтримки. Впровадження подібних рішень здатне покращити ефективність роботи екстрених служб, мінімізувати вплив людського фактору та значно знизити рівень смертності та травматизму під час надзвичайних ситуацій. Подальші дослідження у цій сфері сприятимуть удосконаленню системи безпеки, роблячи її більш доступною, надійною та ефективною.

Список використаних джерел:

1. The Importance of Quick Response Times in Cardiac Arrest Cases. Lifeline EMS. URL: <https://lifeline-ems.com/the-importance-of-quick-response-times-in-cardiac-arrest-cases/>.
2. sylniukraine. Мобільні додатки, що здатні допомогти під час небезпечної ситуації. БФ "Сильні". URL: <https://www.sylni.org/post/мобільні-додатки-що-здатні-допомогти-під-час-небезпечної-ситуації>.

УДК 004.87 (043.2)

МОДЕЛЮВАННЯ ПРОЦЕСУ КЕРУВАННЯ АВТОМОБІЛЕМ НА ЗАЗДАЛЕГІДЬ СТВОРЕНОМУ ТРЕКУ

Даніїл Крант

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Євген Артамонов, к.т.н., доц.

Ключові слова: моделювання, керування автомобілем, симулятор, траєкторія руху, автономне керування, фізична модель, віртуальна симуляція

У сучасних умовах розвитку транспортних технологій моделювання процесу керування автомобілем стає важливим інструментом для тестування алгоритмів автономного руху, перевірки динамічних характеристик транспортного засобу та навчання систем штучного інтелекту без ризику для життя та обладнання. Особливу цінність має симуляція на заздалегідь створених треках, які можуть відображати реальні або змодельовані дорожні умови. Такі системи використовуються у сфері робототехніки, автоспорту, безпілотного транспорту та професійної підготовки водіїв. Ключовим завданням у таких системах є забезпечення реалістичної взаємодії між об'єктом (автомобілем), трасою та віртуальним середовищем.

Розроблена система є програмним комплексом, що моделює процес керування автомобілем на заздалегідь створеному треку. При цьому враховуються реалістична фізика руху, наявність перешкод та конкурентне середовище з іншими “віртуальними гравцями”. В процесі моделювання збираються чисельні параметри дій водія (сила натиску на педаль газу, гальма, кут повороту керма) та параметри стану системи (швидкість, положення на треку тощо).

Основна мета створення комплексу – отримати структуровані та порівняльні дані про стиль та ефективність керування автомобілем різними водіями. Оскільки ці дані фіксуються у форматі, подібному до CAN-шини, їх можна інтегрувати з інформацією, отриманою безпосередньо з реальних транспортних засобів. Це відкриває можливість комплексного аналізу поведінки водіїв як у віртуальних, так і в реальних умовах.

На основі зібраних логів проведено порівняння профілів водіїв, що дозволяє глибше зрозуміти закономірності у стилі їзди та дослідити вплив різних чинників на поведінку водія. Також ці дані можуть бути використані для прогнозування ймовірності певних подій та налаштування алгоритмів адаптивних систем безпеки, що підлаштовуються під конкретний тип водіння.

Використання програмного комплексу має й практичну складову (рис. 1):

- програмне визначення профілю водія і адаптація параметрів ТЗ під нього;
- адаптація систем безпеки під профіль водія;
- оцінка агресивності манери їзди водія для подальшого аналізу страховою компанією.

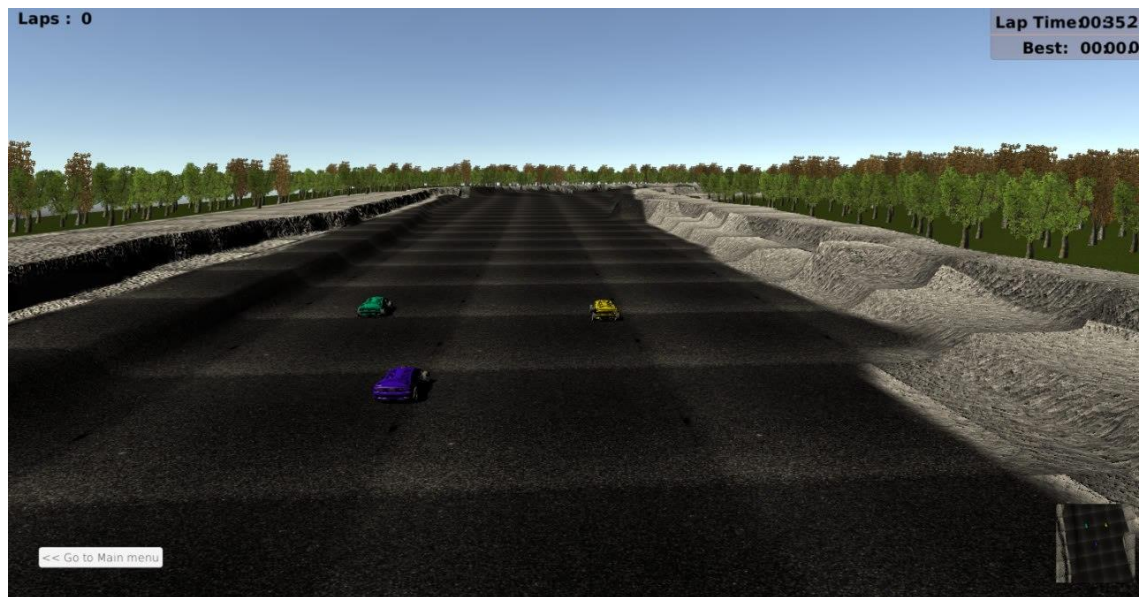


Рис. 1. Інтерфейс розробленого комплексу

Особливу увагу приділено можливості масштабованого збору даних: система зберігає кожен експеримент у форматі, придатному для подальшої аналітики та навчання моделей штучного інтелекту. Це дозволяє застосовувати алгоритми класифікації або кластеризації стилів водіння, проводити регресійний аналіз на основі показників ефективності проходження треку та виявляти залежності між поведінкою водія і конкретними дорожніми умовами.

Висновок

Моделювання процесу керування автомобілем на заздалегідь створеному треку є потужним інструментом для розробки, верифікації та навчання навігаційних і керувальних систем. Воно дозволяє безпечно тестувати різні сценарії поведінки транспортного засобу, адаптувати алгоритми до нестандартних умов та забезпечувати глибоку аналітику процесу. Подальші напрями розвитку включають використання нейромережевих підходів до керування, мультиагентні симуляції та поєднання моделі з реальними транспортними даними для гібридного навчання.

УДК 004.415 (043.2)

СИСТЕМА КЕРУВАННЯ БПЛА НА БАЗІ ARDUINO

Іван Якобчук

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Євген Артамонов, к.т.н., доц.*

Ключові слова: мікроконтролер, Arduino, радіомодуль, програмний код.

Безпілотні літальні апарати (БПЛА) знаходять широке застосування у сфері моніторингу, картографії та наукових досліджень. БПЛА на сьогоднішній день широко представлені в різних конструктивних виконаннях. Є конструкції коптерного типу і літакового. Їх об'єднує електронна складова системи керування і передачі та приймання інформації. В системі керування одним із ключових компонентів БПЛА є польотний контролер, який забезпечує стабілізацію та керування польотом. Використання мікроконтролерних платформ, зокрема Arduino, дозволяє створити ефективні та доступні рішення для таких систем за оптимальний бюджет залежно від задачі, що вирішується. Складовими системи керування, представлені на рисунку 1, є радіомодуль з антеною, мікроконтролер, на зовнішні пристрої вводу та виводу інформації. Для зручного візуального контролю параметрів польоту на пульті керування інтегровано OLED дисплей.

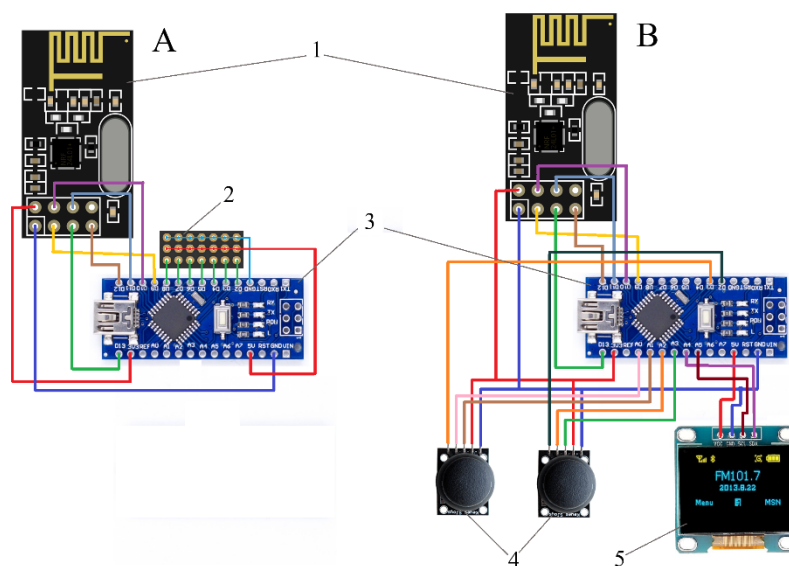


Рис.1. Елементи системи керування БПЛА:

А – приймач, що встановлюється на БПЛА; В – пульт керування БПЛА; 1 – радіомодуль з антеною; 2 – PWM порт підключення зовнішніх пристроїв; 3 – мікроконтролер Arduino;
4 – елементи системи вводу інформації; 5 – елементи системи виводу інформації.

Для реалізації процесу передачі даних було використано модуль NRF24L01 та бібліотеки nRF24L01.h та RF24.h для програмування обміну даними між модулями. Завдяки зовнішній антені дальність зв'язку може досягати понад 2 км на відкритій місцевості.

Два радіомодулі зв'язуються між собою на частоті 2.4 МГц по одній із 128 доступних адрес з унікальним ключем. Перед процесом передачі даних інформація зберігається в пакет даних для стиснення і зменшення часу передачі даних.

На рисунку 2 представлено фрагменти коду для передачі даних між радіомодулями.

<pre> 1 #include <SPI.h> 2 #include <nRF24L01.h> 3 #include <RF24.h> 4 5 RF24 radio(9, 10); // CE, CSN 6 const byte address[6] = "00001"; 7 8 struct ControlData { 9 int throttle; 10 int yaw; 11 int pitch; 12 int roll; 13 }; 14 15 ControlData data; 16 17 void setup() { 18 Serial.begin(9600); 19 radio.begin(); 20 radio.openWritingPipe(address); 21 radio.setPALevel(RF24_PA_MIN); 22 radio.stopListening(); 23 } 24 25 void loop() { 26 // Отримання даних від пульта керування 27 data.throttle = analogRead(A0); 28 data.yaw = analogRead(A1); 29 data.pitch = analogRead(A2); 30 data.roll = analogRead(A3); 31 32 // Передача даних 33 radio.write(&data, sizeof(data)); 34 35 delay(50); 36 } 37 </pre>	<pre> 1 #include <SPI.h> 2 #include <nRF24L01.h> 3 #include <RF24.h> 4 #include <Servo.h> 5 6 RF24 radio(9, 10); // CE, CSN 7 const byte address[6] = "00001"; 8 9 struct ControlData { 10 int throttle; 11 int yaw; 12 int pitch; 13 int roll; 14 }; 15 16 ControlData data; 17 18 Servo motor1, motor2, motor3, motor4; 19 20 void setup() { 21 Serial.begin(9600); 22 radio.begin(); 23 radio.openReadingPipe(0, address); 24 radio.setPALevel(RF24_PA_MIN); 25 radio.startListening(); 26 27 motor1.attach(3); 28 motor2.attach(5); 29 motor3.attach(6); 30 motor4.attach(9); 31 } 32 33 void loop() { 34 if (radio.available()) { 35 radio.read(&data, sizeof(data)); 36 37 // Контроль двигунів (спрощено) 38 motor1.write(map(data.throttle, 0, 1023, 0, 180)); 39 motor2.write(map(data.throttle, 0, 1023, 0, 180)); 40 motor3.write(map(data.throttle, 0, 1023, 0, 180)); 41 motor4.write(map(data.throttle, 0, 1023, 0, 180)); 42 } 43 } 44 </pre>
--	---

а

б

Рис.2. Коди передачі (а) та отримання (б) даних.

Висновок

Розуміння принципів робототехніки та знання низькорівневих мов програмування дозволяє самому розробити програму для керування нескладними системами БПЛА, які можна зібрати на базі доступних мікроконтролерів.

Список використаних джерел:

1. Документація по Arduino. URL: <https://arduino.cc>

УДК 004.8(043.2)

ІНТЕЛЕКТУАЛЬНИЙ ПРОГРАМНИЙ ЗАСІБ АВТОМАТИЗОВАНОГО ПІДБОРУ ПАРАМЕТРІВ АЛГОРИТМІВ OPENCV ДЛЯ ПОКРАЩЕННЯ ЯКОСТІ ЗОБРАЖЕНЬ НА ОСНОВІ МЕТОДУ DEEP Q-LEARNING

Євгеній Боданов, Каріна Кисіль*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олексій Глазок, к.т.н., доц.*

Ключові слова: Deep Q Learning, OpenCV, обробка зображень, нейромережі, автоматизація

Актуальність теми. Автоматизація вибору оптимальних параметрів алгоритмів обробки зображень є критично важливим завданням для успішного застосування алгоритмів комп'ютерного зору у сферах, медицини, безпеки, робототехніки та автономних систем. В задачах, пов'язаних з обробкою зображень, отриманих з бортової камери БПЛА, якість зображень має прямий вплив на точність навігації, ефективність розпізнавання об'єктів та моніторингу місцевості. Традиційні алгоритми, хоч і швидкі, не завжди забезпечують високу якість через складність підбору оптимальних параметрів, тоді як глибокі нейромережі потребують значних ресурсів і часу на обробку. Використання підходу Deep Q Learning [1, 2] для автоматичного налаштування параметрів OpenCV дозволяє значно прискорити та покращити цей процес.

Мета дослідження: розробити та дослідити метод автоматичного вибору оптимальних параметрів алгоритмів обробки зображень на основі поєднання нейромережі Deep Q Learning та бібліотеки OpenCV.

Матеріали і методи. У роботі використано бібліотеку OpenCV для обробки зображень та метод Deep Q Learning для автоматизації вибору параметрів. Для тренування нейромережі було використано датасет DIV2K, що містить кольорові зображення високої якості. Підготовлено два набори даних: оригінальні та спотворені гаусівським шумом (середнє значення 50, дисперсія 150). Для оцінки якості застосовувалися метрики Peak Signal-to-Noise Ratio (PSNR) та Structural Similarity Index (SSIM) [3,4].

Архітектура нейромережі включає три згорткові шари CNN для вилучення просторових ознак та два повнозв'язні шари DQN для прийняття рішень про параметри алгоритмів OpenCV. Використовувався метод experience replay для стабілізації навчання.

Навчання здійснювалося протягом 10 епох із використанням оптимізатора Adam, швидкістю навчання 0.001 та дисконт-фактором (gamma) 0.99. Тренування нейромережі проводилося на ноутбучі з процесором Intel Core i5 та 16 ГБ оперативної пам'яті, з використанням графічної підсистеми Intel(R) Iris(R) Xe Graphics.

Результати: Розроблено нейромережевий програмний засіб, який здійснює автоматичний підбір оптимальних параметрів рівня шумозаглушення та розміру шаблонного вікна алгоритму шумозаглушення Non-Local Means (fastNlMeansDenoisingColored).

Тестування розробленої системи показало значне покращення обробки за метриками PSNR і SSIM. Зокрема, середнє значення PSNR збільшилось з 10.60 дБ до 13.39 дБ, а значення SSIM – з 0.11 до 0.28.

Використання CNN у поєднанні з Deep Q-Network забезпечило адаптивний підбір параметрів, значно покращуючи якість зображень, особливо за умов високого рівня шуму. При цьому нейромережа ефективно узагальнювала отриманий досвід для нових зображень.

Висновки

Запропонований метод має наукову новизну, що полягає у використанні Deep Q Learning для автоматичного налаштування параметрів алгоритмів OpenCV. В ході дослідження розроблено прототип програмного засбу, який може бути інтегрований у медичні системи, системи відеоспостереження, а також у бортові інформаційні системи БПЛА для підвищення якості зображень. Подальші дослідження передбачають створення комплексного модуля для автоматизованої обробки зображень, який включатиме етапи шумозаглушення, усунення ефекту туману, адаптивного підвищення контрастності та детекції країв з автоматичним підбором оптимальних параметрів на кожному етапі за допомогою Deep Q Learning.

Список використаних джерел:

1. Ramaswamy A., Hüllermeier E. Deep Q-Learning: Theoretical Insights from an Asymptotic Analysis. – ArXiv. – 2021. – URL: <https://arxiv.org/abs/2008.10870>.
2. Hester T., Vecerik M., Pietquin O. et al. Deep Q-learning from Demonstrations. – ArXiv. – 2017. – URL: <https://arxiv.org/abs/1704.03732>.
3. 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.
4. Hlazok O., Bodanov Ye. Image quality assessment based on no-reference methods /The 1st International Scientific and Practical Conference “Research in Science, Technology and Economics”, January 22-24, 2025: proceedings. – Luxembourg, Luxembourg. – 2025. – Pp. 66-68.

УДК 004.056.5(045)

УДОСКОНАЛЕНИЙ ПРОГРАМНИЙ МОДУЛЬ АВТЕНТИФІКАЦІЇ НА ОСНОВІ СХЕМИ МЕРКЛЕ-ДЕМГАРДА

Арешков Мирослав

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: автентифікація, гешування, динамічна сіль, безпека

Вступ

Процес автентифікації є ключовою складовою будь-якої системи захисту інформації, а також першою «лінією оборони» перед зловмисником. Для впровадження нових рішень щодо побудови надійних протоколів автентифікації необхідно дослідити шлях формування сучасних рішень захисту[1], а також їх структуру та загрози, з якими вони зустрічались[2-3].

Метою даної роботи є дослідження теоретичних основ застосування вдосконалених геш-функцій у процесах автентифікації користувачів, зокрема розгляду схеми Меркле-Демгарда з динамічною сіллю та секретним «перцем» для підвищення стійкості до атак грубою силою.

Для подальшої модифікації геш-функції були досліджені структури їх побудови. На сьогоднішній день схема Меркле-Демгарда є найвідомішою та найпоширенішою основою для побудови

криптографічних геш-функцій. До таких функцій належать MD-5, SHA-1 та сімейство SHA-2. Вона має такі властивості як стійкість до колізій і захищеність від атак типу подовженого повідомлення. Далі саме вона буде мною модифікована і порівняна із іншими існуючими структурами, а саме: структурою Рабіна, структурою Девіса-Мейєра, структурою Матіаса-Мейєра-Озіса, а також структура Міагуччи-Пренеля.

Всі вони, на відміну від попередника, використовують у якості компресійної функції блочний шифр. Між собою їх підходи до шифрування відрізняються і майже кожна є модифікацією попередників, де додаткове ускладнення збільшує рівень захищеності вихідного геш-значення.

Для наукового обґрунтування доцільності модифікованої структури були використані методи вимірювання та порівняння усіх вищезазначених структур.

Аналіз схем формування геш-функцій дозволив визначити підходи до їх удосконалення. Була розроблена модифікація структури Меркле-Демґарда, яка використовує динамічну сіль і секретний «перець» для підвищення стійкості до атак. Ця схема представлена на рис. 1.

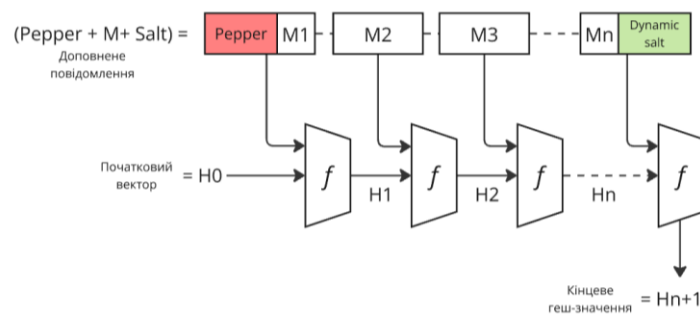


Рис.1. Модифікована структура Меркле-Демґарда

$$H_i = f(H_{i-1} (P + (M_i + S))_i),$$

де H_i – ітеративне геш-значення; f – компресійна функція; M_i – i -тий блок доповненого повідомлення; S – динамічна сіль; P – секретний перець.

Наявність динамічної солі у алгоритмі не тільки збільшує час формування складного початкового значення перед передачею того до геш-функції, але і зобов'язує запускати її для генерації нового геш-значення при кожному новому сеансу користувача до системи. Модифікація Меркле-Демґарда використовує 512-бітові блоки, що підвищує її стійкість до криптографічних атак. Завдяки цьому вона має високий рівень захисту, а підтримка довгих блоків робить її перспективною для застосування в системах із підвищеними вимогами до криптографічної стійкості.

Проведений аналіз ефективності різних структур для автентифікації дозволяє виділити ключові аспекти їхньої продуктивності та рівні захисту. При порівнянні за швидкістю виконання отримано такі дані: 0.033мс, 0.052мс, 0.066мс, 0.082мс, 0.098мс відповідно до зазначених вище структур і 0.073мс у модифікації Меркле-Демґарда.

У даній роботі представлено комбіновану концепцію реалізації схеми автентифікації на базі модифікованої схеми Меркле-Демґарда. Завдяки використанню динамічної солі та секретного «перцю» забезпечується стійкість до атак на довжину повідомлення, перебору хешів та підбору колізій, що робить

її перспективною для застосування в корпоративних інформаційних системах, фінансових технологіях і системах моніторингу кіберзагроз.

Список використаних джерел:

1. Євсєєв С. П., Йохов О. Ю., Король О.Г. Гешування даних в інформаційних системах: монографія. Харків: ХНЕУ, 2013. 312 с.
2. Cryptographic Hash Functions and Attacks. URL: <https://pdfs.semanticscholar.org/b312/007ceb0918779c7cc4453489b6fc02bb0462.pdf> (Last accessed: 26.03.2025).
3. Miyaguchi–Preneel Snefru Cryptographic Blockchain URL: <https://www.ijirmps.org/papers/2022/3/1551.pdf> (Last accessed: 26.03.2025).

УДК 004.056.55:003.26

ДОСЛІДЖЕННЯ КРИПТО-СТЕГANOГРАФІЧНОГО НАПРЯМУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Денис Одноочко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: стеганографія, криптографія, крипто-стеганосистема, шифрування.

У сучасному цифровому просторі, де обмін даними є невіддільною частиною повсякденного життя, забезпечення інформаційної безпеки набуває першочергового значення, адже кіберзлочинність стрімко розвивається, і вдалі спроби несанкціонованого доступу до конфіденційних даних можуть призвести до непоправних наслідків. Саме тому вивчення і використання способів програмного захисту є надзвичайно важливим в умовах сьогодення.

Для збереження конфіденційності інформації при пересиланні її відкритими каналами зв'язку традиційно використовують два способи програмного захисту: криптографічні та стеганографічні методи захисту. Сутність криптографічного захисту полягає в тому, що інформація зашифровується певним алгоритмом в нечитабельний формат. У свою чергу, стеганографічний захист – це приховування самого факту існування інформації шляхом вбудовування її в цифрові об'єкти (контейнери), що спричиняє деякі спотворення цих об'єктів [1]. Об'єднання методів криптографії та стеганографії створює перспективний напрямок програмного захисту інформації, що дозволяє розробити нові ефективні методи забезпечення інформаційної безпеки.

У межах дослідження крипто-стеганографічного напрямку було розглянуто основні методи шифрування інформації та її приховування в цифрових контейнерах. Об'єктами дослідження є криптографічні алгоритми та стеганографічні техніки. У дослідженні застосована експериментальна методика, що базується на аналізі криптографічних і стеганографічних підходів для створення більш надійної системи захисту інформації. Для наукового обґрунтування результатів дослідження використаний **статистичний метод**, який полягав в аналізі наявних способів адаптивного багатопланового захисту інформації.

Структура загального вигляду крипто-стаганосистем зображена на рисунку 1. Шифрування вихідного тексту відбувається за допомогою криптографічного алгоритму. Найчастіше для цього використовуються такі симетричні шифри, як потоковий шифр RC4, блоковий AES, а також застарілі Blowfish та DES.

Для приховування шифротексту в цифровому контейнері використовуються різні стеганографічні методи модифікації носія. Одним із найпоширеніших є метод найменш значущих бітів (LSB). Оскільки розподіл незначущих бітів найчастіше близький до білого шуму, вбудовані дані повинні мати той самий характер. Це досягається шляхом попереднього шифрування повідомлення або його стиснення [2]. Інколи замість LSB застосовуються частотні методи, такі як DCT та DWT, які дозволяють приховувати інформацію у спектральних компонентах файлу.

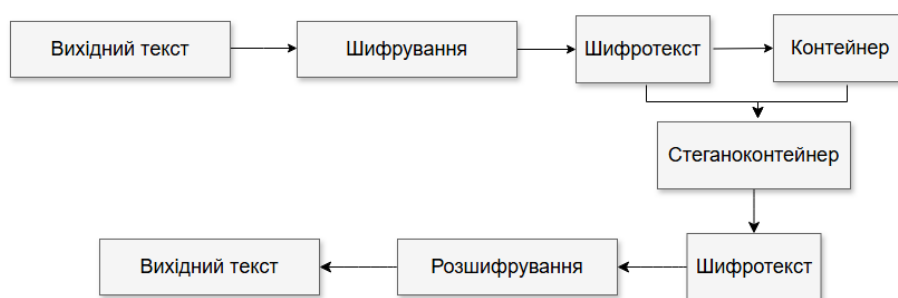


Рис.1. Загальна схема крипто-стаганосистеми

Під час отримання стеганоконтейнера одержувач витягує прихований шифротекст за допомогою ключа. Він може безперешкодно прочитати інформацію, що прихована від зломисників. Однак доцільно використовувати додатково асиметричне шифрування, адже використання симетричних шифрів не гарантує достатньої захищеності прихованої інформації. Таким чином можна зашифрувати ключ симетричного шифру асиметричним алгоритмом шифрування, щоб ускладнити криптоаналіз зломисників.

Важливо пам'ятати, що жодна система не є абсолютно безпечною, із розвитком технологій можуть з'явитися нові методи виявлення стеганографічних змін. Тому для високого рівня безпеки необхідно постійно оновлювати алгоритми, враховуючи нові загрози.

Висновок

У дослідженні підтверджено ефективність поєднання криптографії та стеганографії для забезпечення багатоварового захисту інформації. Отримані результати можуть бути використані для розробки більш стійких систем прихованої передачі даних у сфері управління інформаційною та кібербезпекою.

Список використаних джерел:

1. Кухарська Н.П., Кордунова Ю.С., Хомич І.В. Використання гібридного “криптографія+стеганографія” підходу для розв’язання задач захисту інформації. Електронний репозитарій ЛДУ БЖД. 2019. URL: <https://sci.ldubgd.edu.ua/bitstream/123456789/6741/1/1.pdf> (дата звернення: 20.03.2025).
2. Кузнецов О.О. Євсєєв С.П. Король О.Г. Стеганографія : підручник. Харків : ХНЕУ, 2011. 150 с. URL: <http://repository.hneu.edu.ua/bitstream/123456789/2289/1/Стеганография.pdf> (дата звернення: 20.03.2025).

УДК 004.8

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ КІБЕРБЕЗПЕКИ В АВІАЦІЙНІЙ ГАЛУЗІ

Дімітрій Ізотов

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ірина Лозова, ст.викладач

Ключові слова: Штучний інтелект, кібербезпека, авіація, автоматизація, виявлення загроз

Вступ. Штучний інтелект (ШІ) стрімко змінює сферу кібербезпеки, особливо в критичних галузях, таких як авіація. Завдяки автоматизації рутинних задач, таких як моніторинг мереж і виявлення аномалій, ШІ допомагає швидше реагувати на кібератаки, забезпечуючи безпеку авіаційних систем і даних. Це особливо важливо для авіації, де затримки можуть мати серйозні наслідки.

Дослідження показують, що ШІ може аналізувати великі обсяги даних у реальному часі, виявляти підозрілу активність і навіть пропонувати рішення для усунення вразливостей. Наприклад, компанії як Darktrace використовують ШІ для виявлення відхилень у поведінці мереж, що може бути адаптовано для авіації. [1]

Матеріали та методи. Об'єктом дослідження є технології ШІ, застосовані в контексті кібербезпеки авіаційної галузі, з акцентом на їхню ефективність, якість виявлення загроз і доступність для впровадження. Методи включали огляд наявної літератури, аналіз кейсів і вивчення поточних практик галузі.

Для збору даних використовувалися веб-пошуки та аналіз звітів Європейського агентства з авіаційної безпеки (EASA) та наукових публікацій у галузі кібербезпеки авіації.

Результати

1. Виявлення загроз і аномалій на основі ШІ: ШІ-алгоритми, такі як машинне навчання (ML) і нейронні мережі, аналізують дані польотів і мережевий трафік для ідентифікації аномальної поведінки, яка може свідчити про кібератаку. Наприклад, кластерний аналіз даних бортових самописців (FDR) дозволяє виявляти аномальні рейси, що може вказувати на потенційні загрози безпеки. [2]

2. Автоматизоване реагування та усунення наслідків: ШІ автоматизує реагування на виявлені загрози, наприклад, ізолюючи скомпрометовані системи чи застосовуючи патчі безпеки. Це забезпечує швидке й ефективне управління інцидентами, що критично важливо для авіації. ШІ може миттєво діяти, блокуючи шкідливий трафік чи відновлюючи системи до безпечного стану, що зменшує час реакції. [2]

3. Оцінка та управління вразливостями за допомогою ШІ: ШІ аналізує конфігурації систем і код для виявлення потенційних вразливостей та пропонує кроки для їх усунення. Це дозволяє проактивно зміцнювати безпеку, запобігаючи атакам до їх виникнення. Наприклад, інструменти сканування коду використовують ШІ для ідентифікації вразливостей, що може бути адаптовано для авіаційного ПЗ.

4. Симуляції та тренування з використанням ШІ: ШІ створює реалістичні симуляційні середовища для тренування фахівців з кібербезпеки, дозволяючи їм відпрацьовувати навички в безпечних умовах. Такі платформи використовують ШІ для моделювання кібератак, що допомагає підготуватися до реальних сценаріїв. [3]

5. Переваги використання ШІ:

– Ефективність: Автоматизує рутинні задачі, зменшуючи навантаження на персонал і економлячи ресурси.

- Точність: Покращує точність виявлення загроз, зменшуючи кількість помилкових тривог.
- Проактивність: Дозволяє вживати превентивні заходи, такі як оцінка вразливостей, для запобігання атакам.
- Масштабованість: Обробляє великі обсяги даних і масштабується разом із зростанням авіаційних систем, забезпечуючи безперервний моніторинг.

Висновок. Штучний інтелект має значний потенціал для покращення кібербезпеки та захисту інформації в авіаційній галузі. Автоматизуючи рутинні задачі, підвищуючи точність виявлення загроз і надаючи інструменти для тренувань, ШІ сприяє створенню більш безпечних і стійких авіаційних систем.

Список використаних джерел:

1. Darktrace Security Management. URL: <https://darktrace.com/products/network> (дата звернення 15.03.2024)
2. Anomaly detection in aircraft data using Recurrent Neural Networks (RNN) URL: <https://ieeexplore.ieee.org/document/7486356> (дата звернення 15.03.2024)
3. AI-Powered Attack Simulation: Stress-Testing Your Cyber Defenses URL: <https://akitra.com/ai-powered-attack-simulation/> (дата звернення 15.03.2024)

UDC 004.934

DEVELOPMENT OF THE ARCHITECTURE OF THE NEURAL NETWORK MODEL OF BIOMETRIC AUTHENTICATION BASED ON THE FACE AND IRIS IMAGE

Oleh Tereikovskiy

The State University "Kyiv Aviation Institute", Kyiv

*Scientific advisors – Olexandr Korchenko, D.Sc., prof.,
Corresponding Member of the National Academy of Sciences of Ukraine,
Honored Worker of Science and Technology of Ukraine,
Andrii Mishchenko, D.Sc., prof.,*

Keywords: neural network, critical infrastructure facility, face image, iris, biometric authentication

Introduction

In modern conditions, biometric authentication plays a key role in protecting information systems [3]. Due to the high uniqueness of biometric characteristics, the prevalence of means of their registration and the provenance of neural network technologies, one of the most promising approaches is authentication based on neural network analysis of facial and iris images [1, 3].

Purpose

Development of a neural network model that provides effective authentication using facial and iris images, taking into account expected operating conditions.

Materials and methods

The development is based on an approach that involves a modular architecture of a neural network model in which each module corresponds to one of ten separate biometric authentication tasks, which is advisable to solve using a separate neural network [1]. When determining the expected operating conditions, attention was

focused on eliminating interference during video recording, recognizing spoofing attacks and promptly updating data on the list of legitimate users. When developing the modules, neural network tools of the MTCNN, RetinaFace, BlazeFace, U-Net, DeepPixBiS, FaceNet, Face Mesh, OpenFace, Face Alignment Network, MobileNet, Siamese Network, Two_channel Networks types were used.

Results

As a result of the research, a modular neural network model of biometric authentication was developed, which consists of interconnected modules designed to solve tasks that usually require the use of a separate neural network model, thereby increasing the flexibility and adaptability of the system [3]. A mechanism has been developed that allows each module to determine the most effective type and parameters of a neural network tool adapted to solve the corresponding task in specific operating conditions [2].

The originality of the model also lies in the development of author's versions of neural networks that allow implementing several important functions. In particular, this is the analysis of the emotional state of a registered person to recognize spoofing attacks by the naturalness of emotions, as well as the detection of spoofing attacks based on the analysis of background objects, which allows you to effectively detect attempts to deceive the authentication system. In addition, the model provides the ability to recognize a person without the need for additional training of the neural network by using the Siamese and Two_channel approaches, which makes the model convenient for practical implementation in real conditions, where constant data updating can be difficult or resource-consuming. Another important advantage is the ability to authenticate a person even under conditions of partial face overlap by obstacles, by selecting and analyzing open areas of the face. This allows you to effectively recognize the identity of a staff representative not only during entry control to an information system object, but also during the performance of official duties by a person. Prospects for further research are related to the development of a method for biometric authentication of a staff representative of a critical infrastructure object using an image of the face and iris, taking into account the need to recognize spoofing attacks and operational adaptation to the conditions of usage.

Conclusions

The problem of developing a neural network model of biometric authentication using facial and iris images has received a new solution. The proposed solutions can be used in the development of neural network tools for biometric authentication of information system users.

Sources list

1. Korchenko, O.; Tereikovskiy, I.; Ziubina, R.; Tereikovska, L.; Korystin, O.; Tereikovskiy, O.; Karpinskyi, V. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. *Applied Sciences*. 2025, 15, 2553.
2. Hamdani, N.; Bousahba, N.; Bousbai, A.; Braikia, A. Face Detection and Recognition Using Siamese Neural Network. *International Journal of Computing and Digital System* 2023, 14(1), 889–897.
3. Yergesh, A.K. Development of an advanced biometric authentication system using iris recognition based on a convolutional neural network. *Herald of Science* 2024. 2, 5 (74), 615-625.

УДК 004.7

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ У ВІДКРИТОМУ СЕГМЕНТІ МЕРЕЖІ**Наталія Петляк***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Юрій Кльоц, к.т.н., доц.*

Ключові слова: виявлення аномалій, мережевий трафік, гібридний метод виявлення аномалій

Вступ. Забезпечення кібербезпеки у відкритих сегментах мереж аеропортів є важливим завданням, оскільки такі мережі піддаються численним атакам та можуть використовуватися зловмисниками для несанкціонованого доступу або проведення атак на інфраструктуру підприємства чи сторонні ресурси [1-2]. Аналіз сучасних підходів до виявлення аномального трафіку показує, що традиційні методи або занадто чутливі, що призводить до хибних спрацьовувань, або не здатні виявити нові загрози чи суттєво впливати на продуктивність мережі [3]. Метою дослідження є підвищення ефективності виявлення атак у відкритому сегменті мережі аеропорту шляхом розроблення гібридної моделі виявлення аномального трафіку, що поєднує можливості сигнатурного аналізу Snort із поведінковими методами. Об'єктом дослідження є процес виявлення аномального трафіку. Для реалізації моделі використано: сигнатурний метод аналізу для виявлення відомих атак; поведінковий аналіз, що ґрунтується на статистичних методах оцінки самоподібності трафіку; алгоритм нечіткої логіки для класифікації мережевої активності.

Результати. Запропонована система складається з кількох модулів, що взаємодіють між собою для ефективного виявлення аномального трафіку у відкритому сегменті мережі аеропорту. Основним компонентом є Snort, який перехоплює мережевий трафік і здійснює його попередню обробку. Препроцесор, вбудований у Snort, виконує дефрагментацію IP-пакетів, відновлення TCP-з'єднань і структурування даних перед подальшим аналізом. До Snort підключена зовнішня бібліотека, в якій реалізовано гібридний метод аналізу трафіку, що включає три послідовні етапи класифікації. Якщо один із методів не дає чіткої відповіді щодо класифікації трафіку, то система автоматично переходить до наступного рівня аналізу. На першому етапі використовується метод класифікації трафіку за ознаками, який аналізує пакети на відповідність заздалегідь визначеним множинам дозволених або заборонених даних. Цей підхід працює на основі статичних правил та сигнатур атак, що дозволяє швидко ідентифікувати загрози, відомі системі. Якщо отриманий трафік чітко підпадає під визначену категорію, система ухвалює рішення без додаткового аналізу. Однак цей метод не завжди здатний розпізнати нові або модифіковані атаки, які не входять до попередньо заданих сигнатур. У разі невизначеності система переходить до другого етапу аналізу. Другий рівень передбачає оцінку самоподібності трафіку, яка виконується за допомогою коефіцієнта Херста. Цей метод базується на аналізі часових рядів мережевого потоку та визначенні відхилень від типового мережевого навантаження. У нормальному стані трафік демонструє самоподібну поведінку, яку можна оцінити через коефіцієнт Херста (H). Значення H у межах

0,5–1 свідчить про сильну кореляцію даних у часі та прогнозовану поведінку трафіку, тоді як значення, близькі до 0.5, вказують на випадковість процесу. Якщо ж коефіцієнт Херста виходить за межі очікуваних значень або демонструє аномальні зміни, це може свідчити про DDoS-атаки, ботнет-активність або інші загрози. У разі недостатньої впевненості в результатах система переходить до третього етапу аналізу. На останньому рівні використовується нечіткий метод класифікації трафіку, який дозволяє ухвалювати рішення навіть у разі невизначеності чи неповних вхідних даних. Нечітка логіка оцінює мережеву активність за кількома параметрами, такими як кількість з'єднань за одиницю часу, обсяг переданих даних, відхилення від типового патерну поведінки користувачів. Використання нечітких множин дозволяє уникнути жорсткого поділу параметрів трафіку, натомість кожен пакет отримує певний рівень належності до потенційної загрози. Завдяки цьому система значно знижує кількість хибних спрацьовувань і може ефективно класифікувати навіть складні атаки, які не були розпізнані попередніми методами. Оскільки цей метод є найбільш гнучким, саме він приймає остаточне рішення щодо класифікації трафіку. Після аналізу система ухвалює рішення щодо подальшої обробки трафіку. Якщо трафік визнано безпечним, він передається без обмежень. У разі виявлення потенційної загрози відбувається блокування з'єднання.

Висновок

Запропонована система дозволяє підвищити точність виявлення аномального трафіку та зменшити кількість хибних спрацьовувань у відкритих сегментах мережі.

Список використаних джерел:

1. L. Florido-Benítez L. The Importance of Cybersecurity for Airports in Marketing Activities. *Airport Marketing Strategies, Emerald Publishing Limited*. 2024 PP. 165-183. DOI: 10.1108/978-1-83608-082-420241009
2. C. Aranzazu-Suescun, L. F. Zapata-Rivera, O. G. -M. Saenz and J. M. Christensen. Securing IoT Surveillance Airport Infrastructure. *International Conference on Smart Applications, Communications and Networking (SmartNets)*. 2024. PP. 1-7, DOI: 10.1109/SmartNets61466.2024.10577747.
3. С. Мостовий, Н. Петляк, І. Голота. Дослідження ефективності інструментів виявлення і запобігання вторгнень на вузли в корпоративних мережах. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2023. Вип. 2, с. 5–8.

УДК 004.056.5

ДОСЛІДЖЕННЯ ПОШИРЕНИХ ВРАЗЛИВОСТЕЙ ВЕБДОДАТКІВ

Денис Слис

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: кібербезпека, вразливості вебдодатків, OWASP Top 10, статичний аналіз коду, динамічний аналіз, машинне навчання, автоматизоване виявлення вразливостей, кіберзагрози.

На сьогодні у сучасному цифровому середовищі вебдодатки стали невід'ємною складовою бізнес-процесів та повсякденного життя – від фінансових операцій до соціальних комунікацій. Більшість компаній використовують

вебсервіси для підтримки своєї діяльності, що зумовлює зростання попиту на веброзробку. Водночас із розширенням функціональності вебтехнологій зростає і кількість вразливостей у них, що ставить під загрозу конфіденційність, цілісність і доступність даних користувачів. За даними OWASP та інших досліджень, саме вразливості вебдодатків часто стають причиною успішних кібератак. Зловмисники активно націлюються на вебдодатки, оскільки ті нерідко містять критично важливі персональні чи фінансові дані і водночас можуть мати слабкі місця через помилки розробки або некоректну конфігурацію. Вразливості вебдодатків призводять до значних збитків компаній – як прямих фінансових, так і репутаційних втрат, а також правових наслідків.

Вебдодатки сьогодні належать до найбільш атакованих компонентів інформаційних систем. За останніми дослідженнями Verizon, майже половина всіх інцидентів кібербезпеки пов'язана саме з вебдодатками. Згідно з Verizon DBIR 2024, вебдодатки стали основним вектором початкового проникнення: їх залучено приблизно у 50% проаналізованих порушень безпеки [1]. У 2023 році, за даними звіту Verizon, атаки через вебдодатки були використані у 80% зафіксованих інцидентів і призвели до 60% витоків даних. Така статистика підкреслює критичність захисту вебсервісів. Масштаб загрози підтверджується і кількісно: наприклад, лише за 2023 рік засобами компанії Barracuda було заблоковано понад 18 млрд атак на вебдодатки та API (у середньому ~1,7 млрд атак на місяць) [2]. Це вказує на те, що в середньому вебресурси піддаються безперервним автоматизованим спробам зламу.

Статистика свідчить, що зловмисники найбільше націлюються на фінансовий сектор: так, у період з листопада 2022 по жовтень 2023 року у фінансовій індустрії було зафіксовано 184 інциденти атак через вебдодатки – більше, ніж у будь-якій іншій галузі [3]. Другим за кількістю став інформаційний сектор (144 атаки), а третє місце посіли професійні та комерційні послуги (близько 127 інцидентів). Ці дані корелюють з мотивами нападників: фінансові системи обробляють грошові транзакції, а отже є найпривабливішими; інформаційні служби і бізнес-послуги володіють значними масивами персональних даних, що теж становлять цінність. Окрім зростання абсолютної кількості атак, спостерігається тривожна тенденція збільшення частки інцидентів, у яких зловмисники експлуатують відомі вразливості для проникнення. За даними Verizon DBIR 2024, кількість успішних зламів, здійснених через експлуатацію вразливостей, зросла майже втричі (на 180%) порівняно з попереднім роком.

Проведений аналіз підтверджує, що безпека вебдодатків залишається одним з найактуальніших і найскладніших напрямків кібербезпеки. Кількість атак на вебресурси продовжує зростати разом із розширенням сфер застосування вебтехнологій – від мобільних додатків до хмарних сервісів і API для IoT. У цих умовах організаціям потрібно впроваджувати комплексний підхід до безпеки вебдодатків. Такий підхід має включати як технічні засоби, так і процеси: починаючи від дотримання кращих практик безпечного програмування та регулярного аналізу коду (SAST/DAST) на етапах розробки, до інтеграції засобів безпеки в CI/CD конвейси та проведення постійного моніторингу трафіку. Забезпечення безпеки вебдодатків є безперервним процесом, що вимагає випереджувального мислення.

Дослідження присвячене аналізу вразливостей вебдодатків, їх впливу на безпеку інформаційних систем та методам їх усунення. Проведено огляд сучасних загроз, тенденцій розвитку атак та міжнародних стандартів класифікації вразливостей (OWASP Top 10, CWE Top 25, MITRE ATT&CK тощо). Розглянуто методи тестування безпеки (SAST, DAST, IAST) та можливості застосування AI/ML

для автоматизованого виявлення загроз. Оцінено економічні, репутаційні та правові наслідки вразливостей. Запропоновано комплексний підхід до кіберзахисту, що включає передові методи аналізу безпеки та використання сучасних інструментів захисту для мінімізації ризиків.

Список використаних джерел:

1. Verizon, «2024 Data Breach Investigations Report». [Електронний ресурс]. Режим доступу: <https://www.verizon.com/business/resources/T807/reports/2024-dbir-data-breach-investigations-report.pdf>. (Last accessed: 21.03.2025).
2. Barracuda. «Threat Spotlight: Attackers Targeting Web Applications Right Now», 2024. [Електронний ресурс]. Режим доступу: <https://blog.barracuda.com/2024/02/07/threat-spotlight-attackers-targeting-web-applications-right-now> (Last accessed: 21.03.2025).
3. Statista, «Cybercrime Target Industries 2024». [Електронний ресурс]. Режим доступу: <https://www.statista.com/statistics/221293/cyber-crime-target-industries/> (Last accessed: 21.03.2025).

УДК 004.056.5

ВИКОРИСТАННЯ ГЛИБОКОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ

Олександр Копитін

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: мережевий трафік, кібератака, штучний інтелект, глибоке навчання, методи обробки природної мови.

З розвитком цифрових технологій та зростанням обсягу мережевого трафіку загрози кібербезпеці стають усе складнішими та витонченішими. Традиційні системи виявлення вторгнень (IDS) часто використовують сигнатурні методи, що мають обмежену ефективність при виявленні нових або модифікованих атак [1]. Використання штучного інтелекту (ШІ), зокрема глибокого навчання (Deep Learning) та методів обробки природної мови (NLP) для аналізу логів дозволяє покращити виявлення загроз завдяки самонавчанню та адаптації до нових типів атак [2].

Метою дослідження є розробка методики застосування глибокого навчання для аналізу мережевого трафіку та виявлення аномалій, які можуть свідчити про кібератаки. Основними завданнями є: аналіз існуючих методів детекції мережевих атак; використання згорткових нейронних мереж (CNN) та рекурентних нейронних мереж (RNN) для обробки послідовностей мережевого трафіку; розробка та тренування моделі нейромережевого аналізу для класифікації нормального та шкідливого трафіку; оцінка продуктивності розробленої системи в порівнянні з класичними підходами.

Для аналізу трафіку використано методи глибокого навчання, такі як LSTM (Long Short-Term Memory) та трансформерні моделі, що добре підходять для аналізу послідовних даних. Розроблено модель, яка працює в три етапи: попередня обробка даних: з мережевого трафіку виділяються ключові характеристики (пакети, часова послідовність, порти, протоколи тощо); навчання моделі: модель LSTM аналізує послідовності запитів та виявляє аномалії на основі патернів поведінки; класифікація та реагування: класифікатор CNN визначає, чи є трафік потенційно небезпечним, та активує відповідні захисні механізми.

Експерименти проведено на наборі даних CICIDS2017, що містить реальні та синтетично згенеровані атаки, такі як DDoS, SQL-ін'єкції, фішингові атаки та атаки типу «людина посередині» (MitM) [3].

Розроблена система демонструє значну ефективність у виявленні атак порівняно з традиційними IDS: Точність класифікації досягає 97.5%; кількість помилково позитивних спрацювань знижено на 40% порівняно з класичними методами; система адаптується до нових атак завдяки механізмам самонавчання.

Висновок

Застосування глибокого навчання у сфері аналізу мережевого трафіку значно підвищує ефективність виявлення атак, зменшуючи кількість помилкових спрацювань та покращуючи швидкість реагування. Поєднання LSTM для аналізу послідовностей та CNN для класифікації дозволяє ефективно детектувати складні загрози в режимі реального часу. Подальші дослідження можуть бути спрямовані на інтеграцію запропонованої системи в сучасні SIEM-рішення (Security Information and Event Management) для комплексного моніторингу кібербезпеки.

Список використаних джерел:

1. Аналіз методів виявлення кіберінцидентів. ResearchGate. URL: https://www.researchgate.net/publication/375837851_Analiz_metodiv_viyavlennia_kiberincidentiv (Last accessed: 15.03.2025).
2. Гільгурт, О. В. Застосування алгоритмів машинного навчання для виявлення прихованих кіберзагроз на об'єктах енергетичної інфраструктури. Наукові праці ДонНТУ. 2024. URL: https://iktv.donntu.edu.ua/wp-content/uploads/2024/11/05_gilgurt.pdf. (Last accessed: 15.03.2025).
3. Набір даних оцінки виявлення вторгнень. UNB. URL: <https://www.unb.ca/cic/datasets/ids-2017.html/> (Last accessed: 11.03.2025).

УДК 342.738.004.056.5:004.738.5

ДЕРЖАВНА ПОЛІТИКА УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Олександр Ткаченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: соціальні мережі, інформаційний вплив, правове регулювання, державна інформаційна політика, інформаційна безпека, інформаційний простір, інформаційне законодавство.

У сучасному світі, де цифрова трансформація проникає у всі сфери життя, інформація стає найціннішим ресурсом, що визначає економічний, соціальний і культурний рівень розвитку суспільства. У постіндустріальну епоху соціальні мережі набувають стратегічного значення як основні канали комунікації, обміну знаннями та формування громадської думки. Ці платформи не лише забезпечують оперативний доступ до новин і різноманітного контенту, але й створюють умови для масового поширення інформації, що може як позитивно впливати на суспільство, так і використовуватись як інструмент маніпуляцій, дезінформації та пропаганди. Україна, інтегруючись у глобальний інформаційний простір, зобов'язана створити ефективну правову базу для регулювання діяльності соціальних мереж, яка має забезпечити баланс між гарантіями свободи слова та захистом національної безпеки і громадського порядку. Основоположним документом є Конституція України, яка гарантує

право на свободу вираження думки, проте передбачає можливість обмежень задля захисту інтересів суспільства, національної безпеки, громадського порядку та прав інших осіб [1]. Це створює правове підґрунтя для втручання держави в інформаційний простір, включно із соціальними мережами, у випадках, коли існує загроза важливим суспільним чи державним інтересам. Також важливим є **Закон України «Про інформацію»**, який визначає рамки вільного поширення інформації та відповідальність за дезінформацію, що може завдати шкоди державі чи суспільству. Він є ключовим у боротьбі з інформаційними атаками та маніпуляціями в соцмережах. [2]. Не менш важливим є **Закон України «Про захист персональних даних»** спрямований на забезпечення конфіденційності інформації, що обробляється цифровими платформами. Він гарантує дотримання прав на приватність і передбачає санкції за їх порушення. [3]. Ключовим елементом правової системи є також Закон України «Про національну безпеку України», який визнає інформаційну безпеку як одну із складових загальної безпеки держави, що дозволяє державі вживати заходів проти дестабілізуючих інформаційних впливів, зокрема через соціальні мережі [4].

Закон України «Про медіа» регулює діяльність цифрових платформ та соціальних мереж, забезпечуючи плюралізм думок, захист національних інтересів і прав користувачів. Він визначає обов'язки постачальників інформації, впроваджує механізми протидії дезінформації та гарантує незалежність медіа [5]. **Закон України «Про електронні комунікації»** встановлює правові засади функціонування цифрових мереж, захисту персональних даних та діяльності операторів зв'язку. Він регламентує кібербезпеку, державний контроль за електронними комунікаціями та запобігання кібератакам, гармонізуючи законодавство з європейськими стандартами [6]. Окрім цього, законодавство у сфері кібербезпеки, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», встановлює регуляторні механізми, які передбачають відповідальність за поширення фейкових новин, пропаганди та закликів до насильства у цифровому середовищі, що є прямими загрозами в соціальних мережах [7].

Положення Кримінального кодексу України також передбачають кримінальну відповідальність за діяльність, що порушує інформаційну безпеку держави або підриває суспільний лад, включаючи незаконну передачу конфіденційної інформації через інформаційно-телекомунікаційні системи та інтернет.

Регулювання інформаційних впливів у соціальних мережах відображає складність і багатовимірність сучасних викликів. Українське законодавство прагне сформулювати збалансовану систему, що забезпечує як гарантії свободи слова, так і ефективний захист державних і суспільних інтересів. Проте в умовах сучасних гібридних загроз, коли соціальні мережі можуть виступати як засіб дестабілізації, так і інструмент захисту, необхідно постійно вдосконалювати правову базу та посилювати контроль за інформаційними потоками, зберігаючи при цьому основоположні демократичні цінності.

Список використаних джерел:

1. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (Last accessed: 19.03.2025).

2. Закон України «Про інформацію». URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (Last accessed: 19.03.2025).
3. Закон України «Про захист персональних даних». URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (Last accessed: 19.03.2025).
4. Закон України «Про національну безпеку України». URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (Last accessed: 19.03.2025).
5. Закон України «Про медіа». URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text> (Last accessed: 19.03.2025).
6. Закон України «Про електронні комунікації». URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (Last accessed: 19.03.2025).
7. Закон України «Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (Last accessed: 19.03.2025).

УДК 004.056:004.7:621.39

БЕЗПЕКА СУЧАСНИХ МЕСЕНДЖЕРІВ: ВИКЛИКИ, РИЗИКИ ТА ШЛЯХИ ПОДОЛАННЯ

Денис Осташко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: месенджер, безпека інформації, конфіденційність, шифрування, анонімність, централізація, децентралізація, відкритий код, метадані.

Сучасні месенджери є невід'ємною частиною цифрового спілкування, проте вони мають низку проблем, пов'язаних із безпекою, конфіденційністю та доступністю. Оскільки обмін повідомленнями є ключовим аспектом особистої та корпоративної комунікації, важливо розглянути потенційні загрози та способи їх мінімізації. У цій роботі розглянуто основні недоліки популярних месенджерів, таких як Telegram, WhatsApp, Viber, Signal та Element, а також запропоновано можливі шляхи їх вирішення. Однією з основних проблем сучасних месенджерів є централізація та залежність від серверів. Більшість популярних месенджерів використовують централізовану архітектуру, що створює вразливість до атак на сервери. WhatsApp та Telegram зберігають повідомлення на своїх серверах, що потенційно дозволяє доступ до них стороннім особам у разі злому або вимог від урядів [1]. Ще однією серйозною проблемою є недостатній рівень конфіденційності. Хоча месенджери заявляють про безпеку своїх сервісів, вони можуть збирати метадані про користувачів, такі як інформація про те, хто, коли і з ким спілкується. WhatsApp, наприклад, використовує наскрізне шифрування, але зберігає метаінформацію, яку може передавати третім особам [2]. У Telegram за замовчуванням відсутнє наскрізне шифрування для звичайних чатів, що робить його вразливим до атак [3]. Закритий вихідний код також є значною проблемою. Деякі месенджери, як Viber, не мають відкритого вихідного коду, що унеможливорює незалежний аудит безпеки. У закритих системах користувачі не можуть перевірити, чи справді використовувані алгоритми шифрування є безпечними, що створює ризик використання вразливих або застарілих механізмів захисту [4]. Питання анонімності та ідентифікації користувачів залишається

актуальним. Signal вимагає реєстрації за номером телефону, що може ставити під загрозу анонімність користувачів. Аналогічна ситуація спостерігається у WhatsApp та Viber, де користувачі змушені пов'язувати свій акаунт із мобільним номером. Це дозволяє провайдерам або державним органам встановлювати особу користувача та потенційно відстежувати його активність [5]. Ще однією важливою проблемою є продуктивність та доступність. Децентралізовані рішення, такі як Element, можуть мати труднощі з продуктивністю через складність синхронізації між серверами. Водночас централізовані месенджери можуть обмежувати доступ у певних країнах або зазнавати перебоїв через перевантаження серверів, що впливає на стабільність зв'язку. Щоб вирішити проблему централізації, необхідно використовувати децентралізовані мережі або блокчейн. Це дозволить знизити залежність від єдиних серверів та підвищить стійкість системи до атак. Наприклад, протокол Matrix, на якому базується Element, надає можливість створення незалежних серверів, що зменшує ризики централізованих рішень [5]. Шифрування є важливим механізмом захисту даних, тому всі месенджери повинні використовувати наскрізне шифрування для всіх типів чатів за замовчуванням. Крім того, розробники повинні впроваджувати квантово-стійкі алгоритми, що дозволить захистити повідомлення від майбутніх загроз з боку квантових комп'ютерів. Щоб забезпечити конфіденційність, слід мінімізувати збір метаданих. Користувачі повинні мати можливість приховувати свою активність через механізми Tor або VPN. Також варто розглядати альтернативні підходи до автентифікації, такі як реєстрація без номера телефону або використання децентралізованих ідентифікаційних систем, що забезпечить вищий рівень анонімності. Відкритий вихідний код та можливість незалежного аудиту є важливими для забезпечення прозорості. Усі месенджери повинні надавати можливість незалежного аудиту вихідного коду, що підвищить рівень довіри користувачів. Це вже реалізовано в Signal, але відсутнє в таких месенджерах, як Viber, що створює ризики для безпеки. Підвищення зручності та продуктивності також має важливе значення. Оптимізація алгоритмів синхронізації та розробка інтуїтивного інтерфейсу допоможуть зробити захищені месенджери більш доступними для користувачів.

Хоча сучасні месенджери мають низку проблем, їх можна вирішити шляхом впровадження децентралізованих моделей, наскрізного шифрування, мінімізації збору метаданих та підтримки відкритого коду. Покращення продуктивності та зручності використання сприятиме більш широкому впровадженню захищених комунікаційних платформ, що є важливим кроком у побудові безпечного цифрового середовища майбутнього.

Список використаних джерел:

1. WhatsApp Privacy Policy. <https://www.whatsapp.com/legal/privacy-policy> (Last accessed: 21.03.25)
2. Telegram Security FAQ. <https://telegram.org/faq> (Last accessed: 21.03.25)
3. Viber Privacy Policy. <https://www.viber.com/en/terms/viber-privacy-policy> (Last accessed: 21.03.25)
4. Signal Support. <https://support.signal.org> (Last accessed: 21.03.25)
5. Matrix.org Documentation. <https://matrix.org/docs> (Last accessed: 21.03.25)

УДК 004.056.5

РОЛЬ МАШИННОГО НАВЧАННЯ В СУЧАСНИХ СИСТЕМАХ ОЦІНКИ РИЗИКІВ**Софія Маляренко***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Анна Ільєнко, к.т.н., доц.*

Ключові слова: соціальні машинне навчання, оцінка ризиків, прогнозування загроз.

Критична інфраструктура сучасних держав зазнає дедалі складніших кібератак, які можуть мати серйозні наслідки для національної безпеки, економіки та суспільства. Традиційні методи оцінки ризиків часто виявляються недостатньо ефективними для виявлення складних загроз та їхньої динаміки. У цьому контексті машинне навчання набуває ключового значення, дозволяючи автоматизувати процес аналізу ризиків та підвищувати точність прогнозування. Зокрема, у дослідженні [1] розглядається адаптивна модель оцінки ризиків, яка враховує мінливість зовнішнього середовища та використовує методи машинного навчання для більш точного прогнозування загроз. Робота [2] демонструє підхід до проєктування та навчання штучного інтелекту для оцінки ризиків, що дозволяє покращити управління кіберзагрозами. Крім того, у статті [3] аналізуються методи інтелектуального аналізу даних для оцінки ризиків кібератак у критичній інфраструктурі, що підкреслює важливість глибокого аналізу великих обсягів інформації для виявлення потенційних загроз. Таким чином, інтеграція методів машинного навчання в системи оцінки кіберризиків критичної інфраструктури є актуальним напрямом досліджень, що сприяє покращенню стійкості та безпеки ключових об'єктів.

Метою даного дослідження є аналіз та обґрунтування ролі машинного навчання у сучасних системах оцінки ризиків кібербезпеки критичної інфраструктури, а також визначення підходів до підвищення ефективності прогнозування та управління кіберризиками за допомогою методів штучного інтелекту.

Дослідження ґрунтується на аналізі наукових публікацій та сучасних підходів до використання машинного навчання в системах оцінки ризиків. Об'єктом дослідження є методи машинного навчання, які застосовуються для ідентифікації та прогнозування кіберзагроз. Використано метод системного аналізу для оцінки особливостей застосування машинного навчання у сфері кібербезпеки, порівняльний аналіз для вивчення ефективності різних алгоритмів оцінки ризиків, а також аналіз літературних джерел для узагальнення наукових підходів щодо застосування штучного інтелекту в цій галузі.

Машинне навчання відіграє ключову роль у підвищенні точності оцінки кіберризиків, що особливо важливо для критичної інфраструктури, де атаки можуть мати катастрофічні наслідки. У сучасній науковій літературі розглядаються кілька основних підходів до використання штучного інтелекту в цій сфері. Методи виявлення аномалій дозволяють ідентифікувати нетипову поведінку в мережевому трафіку, що є ефективним для виявлення невідомих загроз. Автоенкодера та глибокі нейронні мережі забезпечують високу точність детектування аномалій, що дозволяє швидко реагувати на потенційні загрози. Методи класифікації атак базуються на алгоритмах машинного навчання, таких як Random Forest, XGBoost та нейронні мережі, які дозволяють розрізняти різні типи загроз на основі попередньо зібраних даних. Прогностичне моделювання ризиків ґрунтується на використанні історичних даних та алгоритмів глибокого навчання для передбачення потенційних атак і вразливостей у системах

критичної інфраструктури. Аналіз наукових джерел показав, що комбіноване використання методів виявлення аномалій, класифікації атак та прогностичного аналізу дозволяє зменшити кількість помилкових спрацьовувань та покращити адаптивність систем безпеки до нових загроз. Крім того, ефективність моделей машинного навчання значною мірою залежить від якості вхідних даних, тому важливим напрямом подальших досліджень є покращення методів збору, фільтрації та аналізу інформації про потенційні загрози.

Висновок

Машинне навчання є ефективним інструментом для оцінки кіберризиків у критичній інфраструктурі, оскільки дозволяє автоматизувати процес аналізу загроз, підвищити точність їхнього виявлення та зменшити ймовірність помилкових спрацьовувань. Поєднання методів виявлення аномалій, класифікації атак та прогностичного аналізу сприяє підвищенню ефективності систем кібербезпеки.

Список використаних джерел:

1. Михайлов, Н. О. (2024, October). Адаптивна модель планування проєктів та оцінки ризиків із використанням машинного навчання. In The 5th International scientific and practical conference “Problems of science development in the context of global transformations”(October 01–04, 2024) Zagreb, Croatia. International Science Group. 2024. 310 p. (p. 119).
2. Михайлов, Н. О. (2024, December). Проектування та навчання моделі штучного інтелекту для планування й оцінки ризиків проєктів. In The 16th International scientific and practical conference “New ways of improving outdated methods and technologies”(December 17–20, 2024) Copenhagen, Denmark. International Science Group. 2024. 385 p. (p. 54).
3. Сукачова, С. М. (2024). Оцінка ризиків кібератак у критичних інфраструктурах на основі інтелектуального аналізу даних. Ukrainian Journal of Computing Innovations, (<https://doi.org/10.5281/zenodo.14565881>).

УДК 004.056.5

ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ТА КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В АВІАЦІЙНОМУ ЗВ'ЯЗКУ: РАДІОТЕХНІЧНІ ЗАСОБИ ТА ПОТЕНЦІЙНІ РИЗИКИ

Пасюков Анатолій

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анна Ільєнко, к.т.н., доц.

Ключові слова: авіаційні системи зв'язку, кібербезпека, доступність інформації, конфіденційність, CPDLC.

Сучасні авіаційні системи зв'язку відіграють критично важливу роль у забезпеченні безпеки та ефективності польотів. Основні вимоги до таких систем включають забезпечення високого рівня доступності та конфіденційності інформації. Враховуючи зростаючі кіберзагрози та технологічні виклики, питання захисту даних у радіотехнічних засобах набуває особливої актуальності [1]. Особливу увагу привертають механізми забезпечення доступності та конфіденційності інформації, які включають впровадження сучасних протоколів зв'язку, криптографічних методів захисту та механізмів автентифікації. Попри значний прогрес у стандартизації безпеки, такі системи залишаються вразливими до атак на мережевому рівні, що може призвести до втрати зв'язку, підміни даних або несанкціонованого доступу. У зв'язку з цим актуальним є дослідження ефективності існуючих методів захисту та пошук оптимальних рішень, які забезпечують баланс між рівнем безпеки та продуктивністю авіаційних систем зв'язку.

Мета дослідження: аналіз сучасних методів забезпечення доступності та конфіденційності інформації в авіаційних системах зв'язку, оцінка їх стійкості до кіберзагроз та виявлення оптимального балансу між рівнем захисту і продуктивністю систем.

Одним із ключових аспектів забезпечення доступності інформації є використання сучасних протоколів зв'язку, які здатні працювати у складних умовах електромагнітних завад. Наприклад, технологія Controller-Pilot Data Link Communications (CPDLC) дозволяє зменшити залежність від голосового зв'язку, що підвищує надійність передачі критично важливих команд [2]. Проте, навіть такі системи залишаються вразливими до атак на мережевому рівні, що може призвести до втрати зв'язку між повітряним судном та наземними службами [3].

Конфіденційність даних в авіаційному зв'язку забезпечується шляхом впровадження механізмів шифрування та автентифікації. Одним із нормативних документів, який регулює цей аспект, є стандарт DO-326A, що визначає вимоги до кібербезпеки в авіаційних системах [4]. Впровадження цих вимог дозволяє мінімізувати ризики несанкціонованого доступу до даних та їх модифікації.

Проте існують і технічні обмеження. Наприклад, використання криптографічних алгоритмів може впливати на швидкість обробки інформації, що є критичним для реального часу управління польотами. Тому необхідний баланс між рівнем захисту та продуктивністю системи [5].

У сучасних умовах важливим є також міжнародне регулювання, яке забезпечує уніфікацію підходів до безпеки авіаційного зв'язку. Наприклад, регламент ЄС 552/2004 встановлює вимоги до інтероперабельності систем зв'язку в європейському повітряному просторі [6]. Такі нормативні акти сприяють узгодженню стандартів безпеки на глобальному рівні.

Висновок

Таким чином, забезпечення доступності та конфіденційності інформації в авіаційному зв'язку вимагає комплексного підходу, що включає технічні рішення, нормативне регулювання та оперативний контроль за кіберзагрозами. Подальші дослідження у цій сфері можуть бути спрямовані на розробку нових методів захисту даних, що поєднують високу ефективність та мінімальний вплив на продуктивність систем. Важливим аспектом є також впровадження механізмів адаптивної безпеки, які здатні виявляти та нейтралізувати загрози в режимі реального часу. Окрім технічних заходів, значну роль відіграє підвищення рівня кібергігієни серед авіаційного персоналу та розробка стратегій швидкого реагування на інциденти. Узгодження міжнародних стандартів безпеки та їх адаптація до нових технологічних викликів сприятиме підвищенню загального рівня захисту авіаційних комунікаційних систем.

Список використаних джерел:

1. International Civil Aviation Organization. (2011). Doc 9880 Part IV-B: Amendment proposals July 2011.
2. International Civil Aviation Organization. (n.d.). Global TBO concept (Version 0.11). Re
3. AFuzion. (n.d.). DO-326A & ED-202A aviation cyber security.
4. Parasoft. (n.d.). DO-178C software compliance for aerospace and defense.
5. Military Embedded Systems. (n.d.). Incorporating DO-326A security airworthiness into the software development life cycle.
6. European Parliament & Council of the European Union. (2004). Regulation (EC) No 552/2004 on the interoperability of the European Air Traffic Management network.

УДК 004.056.5

ДОСЛІДЖЕННЯ СУЧАСНИХ КІБЕРІНЦЕНДЕНТІВ**Скальський Максим***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Анна Ільєнко, к.т.н., доц.*

Ключові слова: кіберінциденти, кіберзахист, кібератака.

У сучасному світі цифрові технології стали невід'ємною частиною всіх сфер життя. Оскільки комп'ютерні системи використовуються повсюдно – від серверів великих корпорацій до персональних мобільних пристроїв – їх захист набув критичного значення. Забезпечення кібербезпеки стало одним із ключових завдань як для організацій, так і для окремих користувачів. Метою дослідження є аналіз актуальних проблем у сфері кібербезпеки. Окрему увагу приділено вивченню тенденцій щодо зростання кількості кібератак та необхідності постійного вдосконалення навичок та знань у сфері кібербезпеки для фахівців та організацій. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, за минулий рік (2023) опрацювала 2543 кіберінциденти, що на 15,9% більше ніж за 2022 рік, коли Україна стикнулася з величезною кількістю атак у зв'язку з повномасштабною російською агресією проти нашої держави. [1].

Зі зростанням кількості та складності кібератак необхідно вдосконалювати заходи кібербезпеки. З метою посилення захисту було видано “Наказ Адміністрації Держспецзв'язку від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту»” [2]. Важливо постійно контролювати безпеку власних пристроїв, оскільки проникнення зловмисників може залишатися непоміченим протягом тижнів, місяців чи навіть років. Згідно зі звітами, у більшості випадків несанкціонований доступ до інформаційно-комунікаційних систем об'єкта атаки здійснюється заздалегідь (за рік або більше). Для цього зловмисники використовують скомпрометовані облікові записи VPN, а також експлуатують вразливості програмного забезпечення або помилки в налаштуваннях публічно доступних систем. За даними звіту оперативного центру реагування на кіберінциденти ДЦКЗ, за 2023 рік “безпосередньо аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5% більше ніж за результатами 2022 року.”[4]. У звіті 2024 року щодо кібератак було сказано наступне: “У процесі аналізу цих подій було виявлено та опрацьовано 1042 кіберінциденти. Переважна більшість з них стосувалася поширення шкідливого програмного забезпечення.”[5].

Окрім вище згаданого шкідливого ПЗ, існують й інші типи кібератак, адже “Кібератаки спрямовані на пошкодження важливих документів і систем у корпоративній або персональній комп'ютерній мережі, а також отримання доступу до них.” [6], тому й для різних цілей повинні бути і різні способи, що краще підходять для їх виконання.

Серед найпоширеніших помилок, які допускають підприємства, це “Відсутність багатофакторної автентифікації (2FA).”[7]. Для перевірки наявності таких помилок, а дуже часто це не єдине слабе місце мережі, необхідно періодично підвищувати кваліфікацію та проводити курси/лекції у кіберсфері. Проте, хоч і було

сказано що це для підприємств, відвідувати такі заходи та розширювати свої знання та розуміння у даній сфері може кожен бажаючий.

Ефективний захист від кібератак вимагає проактивного підходу, оскільки усвідомлення загроз часто настає лише після їх реалізації. Тому важливо заздалегідь розуміти механізми атак та методи протидії. Аналіз реальних інцидентів кібербезпеки демонструє значні наслідки таких атак, що спростовує хибне уявлення про їхню малоймовірність для конкретного користувача чи організації.

Розуміння загроз та їхніх наслідків формує мотивацію до підвищення рівня обізнаності та практичних навичок у сфері кіберзахисту. Це, у свою чергу, сприяє більш ефективному розпізнаванню атак, їхньому запобіганню та мінімізації потенційних втрат.

Список використаних джерел:

1. Державна служба спеціального зв'язку та захисту інформації України: <https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti>
2. Наказ Адміністрації Держспецзв'язку від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту»: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2025-54-pro-zatverdzhennya-bazovikh-zakhodiv-z-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-bazovikh-zakhodiv-z-kiberzakhistu>
3. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року: <https://cert.gov.ua/article/6277822>
4. Державна служба спеціального зв'язку та захисту інформації України: <https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanih-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz>
5. 2024 РІЧНИЙ ЗВІТ ст.6: <https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006>
6. Що таке кібератака?: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack>
7. Державна служба спеціального зв'язку та захисту інформації України: <https://cip.gov.ua/ua/news/naitipovishi-pomilki-pidpriyemstv-ta-organizacii-pri-kiberatakakh-rekomendaciyi-cert-ua>

UDC: 004.056.55.

A MODEL FOR PROTECTING WEBSITES FROM HTML ATTACKS: FROM VULNERABILITY DETECTION TO STRUCTURAL SOLUTIONS

Olena Kovalchuk

State University 'Kyiv Aviation Institute', Kyiv

Scientific supervisor – Yuliia Kovalenko, Associate professor

Keywords: website security, cyberattacks, protection, XSS (Cross-Site Scripting), HTML Injection, Clickjacking, user data, phishing, testing, hacker attacks, Penetration Testing, Automated Scanners.

Protecting websites is crucial as cyberattacks on web resources grow yearly. Developers must implement reliable security methods to counter threats like XSS, HTML Injection, and Clickjacking, which can lead to data theft, content manipulation, or full control over a web application.

An XSS attack involves injecting a malicious script into a web page, which allows the attacker to execute code in the victim's browser. This can lead to session hijacking, user redirection, or the display of malicious content.

HTML Injection allows an attacker to inject arbitrary HTML code into a web page, which can change its content or structure. This can be used for phishing, changing the interface, or creating fake forms to collect user data.

Clickjacking is an attack in which a user is tricked into clicking on elements of a web page without realising it. To do this, the attacker uses invisible frames that cover the real content. This can lead to undesirable actions, such as providing access to confidential data or making payments without the user's knowledge.

To protect a web resource, it is necessary to identify potential threats at the development and testing stages. The main methods of vulnerability detection include:

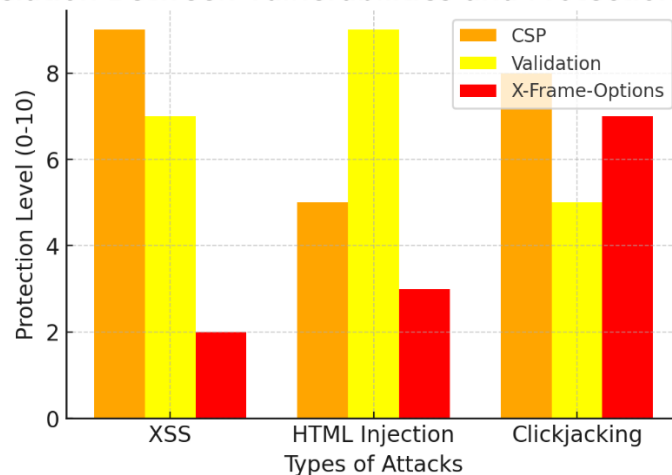
1. **Static Analysis** - code analysis without its execution to identify vulnerabilities and errors at the development stage.
2. **Dynamic Testing** - testing the application while it is running to find problems with performance, security, and stability.
3. **Security Audit** - a comprehensive system security check, including code analysis and testing in a real environment.
4. **Fuzz Testing** is the input of random or specially created data to detect vulnerabilities (for example, buffer overflows).
5. **Penetration Testing** - simulation of hacker attacks to identify weaknesses in system security.
6. **Automated Scanners** - tools for automatically searching for vulnerabilities in code, web applications and servers.

Once the vulnerabilities are identified, it is necessary to implement protection measures. The main methods include:

Method	Description	Example of implementation	Protects against
Content Security Policy (CSP)	An HTTP header that restricts the sources of executable code and downloaded resources.	Content-Security-Policy: script-src 'self';	Malicious code insertion (XSS)
Input Data Validation	Verification and screening of the entered data to prevent HTML injections.	htmlspecialchars(\$input) in PHP, encodeURI(input) in JavaScript	HTML injections, XSS
Protection against ClickjackingMethod	Using the header to prevent the site from opening in frames.	X-Frame-Options: DENY	Clickjacking attacks

The following diagram shows how effective these protection methods are:

Correlation Between Vulnerabilities and Protection Methods



Conclusion

Protecting websites from HTML attacks requires a comprehensive approach that includes identifying vulnerabilities, analysing them, and implementing structural security measures. The use of CSPs, input validation, and security headers can significantly reduce the risk of attacks. Adherence to these principles will ensure stable and secure operation of web resources.

References:

1. Kaur G., Bedi P. Prevention of HTML injection attack using pattern matching technique // Procedia Computer Science. – 2017. – Vol. 115. – P. 377–384. – DOI: 10.1016/j.procs.2017.09.093.
2. Mavroeidis V., Bromander S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece, 2017. – P. 91–98. – DOI: 10.1109/EISIC.2017.20.

УДК 004.056(043.2)

ПРОБЛЕМИ ЗАХИСТУ GNSS ВІД АТАК

Катерина Стукальська

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олена Дубчак, старший викладач

Ключові слова: атаки, GNSS, Jamming, Spoofing, AI

Як відомо, глобальні навігаційні супутникові системи (Global Navigation Satellite System, GNSS) є джерелом даних позиціонування, навігації та часу. [1] GNSS широко застосовуються в різних галузях у всьому світі та доступні будь-кому для використання в реальному часі. GNSS ґрунтуються на географічних координатах об'єкта, фіксуючи відстань до розташованих на орбіті супутників. Серед GNSS можна виділити такі відомі системи, як GPS (Global Positioning System), США, або GALILEO, Європа.[2]

Активне використання GNSS загострює питання захисту від сучасних загроз і атак, що впливають на стабільність і надійність функціонування навігаційних систем.

Мета – провести аналіз атак на GNSS і методів захисту від них.

Виділяють дві основні категорії навмисних атак на приймачі GNSS: фізичні (несигнальні) атаки; атаки на рівні сигналу в просторі GNSS (сигнальні). Несигнальні атаки виконуються безпосередньо шляхом фізичного втручання або маніпуляції. Прикладом сигнальних атак є Jamming (глушіння) і Spoofing (підміна), тобто атаки на GNSS - сигнали, які передаються супутниками, що впливають на спроможність приймача точно встановлювати місцерозташування, швидкість і час.[1] Існує підтип Spoofing - Meaconing (підробка), за якого сигнали GNSS передаються повторно, що потребує простішого обладнання в порівнянні з тим, яке необхідно для атаки типу Spoofing. [3]

Атака типу Spoofing сигналів розповсюджена в різних сферах: від машинобудівництва та авіаційної галузі – до комп'ютерних ігор. Атака Spoofing GPS серйозно вплинула на цивільну авіацію у вересні 2023 року, і наразі особливо відчутний вплив таких атак існує біля зон озброєних конфліктів. [4]

Одним із простих методів захисту від Spoofing є аналіз потужності сигналу та його характеристик. З метою виявлення неспівпадіння з реальними сигналами супутників і визначення підробок проводиться моніторинг потужності GPS – сигналу, що дозволяє відстежити відхилення показників потужності сигналу, а також час їхнього надходження, частоту та фазу. Серед ефективних методів захисту від зазначених типів атак експерти пропонують використання технологій штучного інтелекту (Artificial

Intelligence, AI), зокрема, фільтрацію на основі алгоритмів машинного навчання, що дозволяє розпізнавати аномалії, які можуть вказувати на Spoofing. Взаємодія з інерційними навігаційними системами (Inertial Navigation System, INS) допомагає відслідковувати невідповідності даних з різних супутникових джерел, що може забезпечувати автономну навігацію доки не буде відновлено довіру до GPS - сигналів.[5] Для захисту від навмисних завад також вимикають джерела сигналу або застосовують «розумну антену» (Controlled Reception Pattern Antenna, CRPA) для його придушення. Експертна спільнота вважає також достатньо ефективними засобами автентифікацію сигналу, що дозволяє виявити підробку, а також використання шифрування сигналу, що запобігає виникненню Spoofing. [4]

Інша сигнальна загроза, глушіння, викликає не менше проблем, оскільки пристрої глушіння легші у виготовленні за пристрої підробки і, отже, є доступнішими. На відміну від Spoofing, де структура сфальшованого сигналу має бути імітованою та схожою на справжній, глушіння є простішим у реалізації. Навіть невеликі за розміром пристрої глушіння можуть мати радіус дії в кілька метрів. [6]

Проведений аналіз методів захисту від атак на GNSS – приймачі показав, що більш надійними є методи машинного та глибокого навчання, що підвищують стійкість до радіочастотних перешкод. Ці новітні технології ефективно застосовуються для виявлення та класифікації завад і створенні сценаріїв щодо протидії завадам як в статичному, так і в динамічному середовищах. [7]

Висновок: На сьогодні поширеними атаками на GNSS є Jamming і Spoofing, для протидії яким застосовуються унікальні методи, що сприяють їх виявленню та боротьбі з ними. Залежно від виду та причини можливої атаки доцільно фокусувати увагу на конкретному методі. Проте кожен вид захисту окремо не гарантує повної безпеки, тож, використовуючи комбінації з кількох методів, можна забезпечити вищий рівень надійності. Новітні технології AI, зокрема, машинного навчання, ефективні як проти атак типу Spoofing, так і проти Jamming. У разі більшої потреби захисту від атак типу Spoofing варто також додатково використовувати методи шифрування.

Список використаних джерел:

1. Parisa Borhani-Darian. Detecting GNSS spoofing using deep learning// EURASIP Journal on Advances in Signal Processing. 18 January 2024. URL: <https://asp-urasipjournals.springeropen.com/articles/10.1186/s13634-023-01103-1>
2. Панченко І. В., Бондаренко Д. М., Липський О. А. Аналіз підходу до захисту від завад супутникових навігаційних приймачів БПЛА. URL: https://journal.viti.edu.ua/downloads/MITIT_5_2024.pdf
3. Free Article: Jamming and Spoofing// The Nautical Institute. 25/01/2024. URL: <https://www.nautinst.org/resources-page/free-article-jamming-and-spoofing.html>
4. GPS Spoofing. Final report of the GPS Spoofing WorkGroup. September 6, 2024. URL: <https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf>
5. Мустафаєв О. В. Сучасні технології захисту від GPS спуфінгу у системах навігації. URL: https://tech.vernadskyjournals.in.ua/journals/2024/5_2024/part_1/12.pdf
6. Katarina Radoš, Marta Brkić and Dinko Begušić. Recent Advances on Jamming and Spoofing Detection in GNSS. 2024. URL: <https://www.mdpi.com/1424-8220/24/13/4210>
7. Ali Ghanbarzadeh, Muhammad Soleimani and Hossein Soleimani. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning //School of Electrical

УДК 004.8.056:656.7(043.2)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ В АВІАЦІЙНІЙ ІНФРАСТРУКТУРІ

Вікторія Карпенко

Державний університет “Київський авіаційний інститут”, Київ

Науковий керівник - Ольга Бурбела, старший викладач

Ключові слова: штучний інтелект, кібербезпека, авіаційна інфраструктура, виявлення загроз, машинне навчання.

Авіаційна галузь є однією з найуразливіших до кіберзагроз через високу ступінь автоматизації, складність систем управління польотами та важливість безперервного функціонування критичної інфраструктури. Класичні засоби захисту вже не відповідають сучасним вимогам, що обумовлює актуальність впровадження інтелектуальних технологій. У роботі проаналізовано можливості використання технологій штучного інтелекту (ШІ) для забезпечення кібербезпеки авіаційної інфраструктури. Розглянуто ключові переваги та виклики впровадження систем на основі машинного навчання для виявлення аномальної активності та кіберзагроз у реальному часі. Окреслено перспективи подальшого розвитку даного напрямку з урахуванням ризиків, пов'язаних з хибними спрацюваннями, якістю даних та браком кваліфікованих кадрів.

Аналітичний аналіз переваг і недоліків ШІ в системах ІБ авіації. Штучний інтелект, зокрема алгоритми машинного навчання та глибокого навчання, відкривають нові можливості для:

- виявлення невідомих раніше загроз;
- аналізу великих обсягів телеметрії;
- проактивного реагування на інциденти.

Інтеграція ШІ в системи кібербезпеки має численні переваги, але супроводжується також низкою ризиків та обмежень, які необхідно враховувати на етапі впровадження. У таблиці 1 подано порівняльний аналіз використання ШІ.

Таблиця 1.

Аналітичний огляд переваг та недоліків використання ШІ в авіаційній кібербезпеці

Переваги	Недоліки / Обмеження
Швидке виявлення загроз у реальному часі	Можливі хибні спрацювання
Виявлення нових та невідомих типів атак	Необхідність якісного навчального датасету
Можливість аналізу великих обсягів трафіку та логів	Висока обчислювальна складність — потреба у потужному обладнанні
Адаптивність до нових загроз	Недостатня прозорість моделей
Прогнозування майбутніх інцидентів	Залежність від кваліфікації розробників
Інтеграція з поведінковими системами моніторингу	Складність інтеграції в існуючі системи захисту

Аналіз показав, що ШІ здатен успішно виявляти кіберзагрози завдяки глибокому навчанню та машинному навчанню. Зокрема, моделі ШІ здатні виявляти нетипову активність в мережевому трафіку, що може бути індикатором кібератак. Системи на основі ШІ, такі як системи виявлення вторгнень (IDS), продемонстрували високу точність у виявленні загроз у порівнянні з традиційними методами. Також

варто відзначити, що алгоритми ШІ можуть прогнозувати майбутні кіберінциденти на основі аналізу історичних даних, що дозволяє вжити проактивних заходів для їх запобігання.

Однак, незважаючи на значні досягнення, система ШІ має свої обмеження. Одним з основних ризиків є ймовірність хибних спрацьовувань, коли нешкідливі дії можуть бути помилково ідентифіковані як загроза. Також на ефективність ШІ може впливати якість даних, на яких він навчається. Дефіцит кваліфікованих фахівців у галузі кібербезпеки, здатних ефективно розробляти та підтримувати системи ШІ, також є значним обмеженням.

Висновок. Аналітичний підхід до оцінки використання ШІ в авіаційній кібербезпеці підтверджує його високу ефективність та інноваційність. Проте впровадження потребує ретельного врахування ризиків та обмежень. Рекомендовано поєднувати інтелектуальні рішення з традиційними методами безпеки, забезпечити постійне вдосконалення моделей та розвивати компетенції персоналу в галузі Data Science і кіберзахисту.

Список використаних джерел:

1. Корпоративна кібербезпека: Роль ШІ у захисті даних.
URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection>
2. ENISA. Artificial Intelligence Threat Landscape. – European Union Agency for Cybersecurity, 2023. – [Електронний ресурс]. – Режим доступу: <https://www.enisa.europa.eu/publications/artificial-intelligence-threat-landscape>
3. IATA. Aviation Cyber Security Strategy. – International Air Transport Association, 2023. – [Електронний ресурс]. – Режим доступу: <https://www.iata.org/en/policy/cyber-security>

УДК 004.7

ГІБРИДНІ ПІДХОДИ ДО АУТЕНТИФІКАЦІЇ ІОТ-ПРИСТРОЇВ У ХМАРНИХ СИСТЕМАХ

Іван Кукулевський, Євгеній Сокирка, Олена Толбатова

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Андрій Толбатов, к.т.н., доц.

Ключові слова: аутентифікація, IoT (Інтернет речей), хмарні системи, гібридні методи, криптографія, мультифакторна аутентифікація, машинне навчання.

Вступ. Сучасні хмарні технології забезпечують масштабовану інфраструктуру для обробки та зберігання великих обсягів даних, що генеруються IoT-пристроями [1]. У працях [2, 3] наголошується на важливості надійних механізмів аутентифікації, адже зростання кількості підключених пристроїв підвищує ризик несанкціонованого доступу. Гібридні методи, які поєднують симетричні, асиметричні та поведінкові підходи, пропонують більш гнучкі рішення для захисту IoT-середовищ [4, 5]. Таким чином, тема гібридної аутентифікації є надзвичайно актуальною для зменшення вразливостей і забезпечення стійкості IoT-систем.

Матеріали і методи. У ході дослідження було змодельовано невелику мережу IoT-пристроїв, проміжний шлюз і хмарний сервер. IoT-пристрої мали обмежені обчислювальні ресурси, тому використовувалися переважно швидкі симетричні алгоритми шифрування (AES) із короткими ключами (128 біт). Водночас, для безпечної передачі цих ключів на початку з'єднання залучалися асиметричні алгоритми (RSA або ECC) [3]. Таке поєднання дає змогу знизити навантаження на датчики, оскільки після обміну ключами вони працюють зі спрощеним симетричним шифруванням.

Мультифакторна аутентифікація передбачала використання пароля, а також додаткових біометричних або поведінкових факторів (ритм введення пароля, перевірка відбитка пальця тощо). Їх застосовували лише тоді, коли виявляли підозрілі дії: наприклад, коли сенсор раптово почав надсилати нетипово велику кількість даних чи підключився з незвичної локації. Для виявлення таких підозрілих ситуацій застосовувалося машинне навчання. Зокрема, аналізувались журнали роботи пристроїв та їхні телеметричні дані (частота передачі, обсяг трафіку, час доби). На основі цих показників алгоритми (Isolation Forest, One-Class SVM чи Autoencoder) відокремлювали нормальну активність від потенційно небезпечної [5]. У разі виявлення нетипових дій система могла перевіряти пристрій повторно або вимагати додатковий біометричний фактор.

Ефективність кожного компонента оцінювалася за часом встановлення шифрованого з'єднання, обчислювальним навантаженням на пристрої, точністю виявлення аномалій і кількістю хибних спрацювань. Для узагальнення результатів порівнювалися середні значення метрик і проводилася статистична перевірка на наявність істотних відмінностей.

Результати. Комбінування асиметричної та симетричної криптографії дає змогу зменшити ризики витоку ключів, забезпечивши безпечний обмін ключовою інформацією на початковому етапі під'єднання. Далі використання симетричних шифрів мінімізує навантаження на обмежені ресурси IoT-пристроїв. Залучення мультифакторної автентифікації (біометрії чи поведінкових патернів) дозволило знизити ймовірність несанкціонованого доступу навіть за умови компрометації традиційних паролів. Окрім цього, застосування машинного навчання для динамічного аналізу потоків телеметрії та системних журналів дозволило виявити типові та нетипові патерни даних. Це дає змогу проактивно реагувати на аномалії та розривати небезпечні з'єднання.

Таким чином, гібридні методи аутентифікації, що поєднують криптографічні, поведінкові та алгоритмічні підходи, виявилися ефективнішими порівняно з традиційними однофакторними схемами. Вони підвищують рівень інформаційної безпеки та забезпечують масштабованість рішень у хмарних середовищах з великою кількістю IoT-пристроїв.

Висновок. Гібридні методи аутентифікації дозволяють покращити захист IoT-пристроїв у хмарних системах, поєднуючи безпечний обмін ключами, мультифакторні механізми та машинне навчання для виявлення аномалій. Отримані результати свідчать про перспективність такого підходу з огляду на підвищення безпеки та зменшення кількості успішних атак на IoT-інфраструктуру.

Список використаних джерел:

1. Raza S., Duquennoy S., Chung T. Ta ін. Securing IoT for smart home using IPSec-based security solution // *Future Generation Computer Systems*. – 2019. – Vol. 92. – P. 70–81.
2. Ammar M., Russello G., Crispo B. Internet of Things: A survey on the security of IoT frameworks // *Journal of Information Security and Applications*. – 2018. – Vol. 38. – P. 8–27.
3. Arfaoui G., Bures M., Balazs A. Lightweight cryptography for IoT: A survey // *Procedia Computer Science*. – 2020. – Vol. 176. – P. 1683–1692.
4. ДСТУ ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Київ: Держспоживстандарт України, 2010. – 32 с.
5. Zhang Q., Liang X., Lu R. Blockchain-based distributed trust management in IoT // *IEEE Transactions on Industrial Informatics*. – 2020. – Vol. 16(6). – P. 4146–4155.

УДК 004.056.5

МЕТОДИ НАЛАШТУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Тимошенко Михайло

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Юлія Коваленко, к.пед.н.доц.*

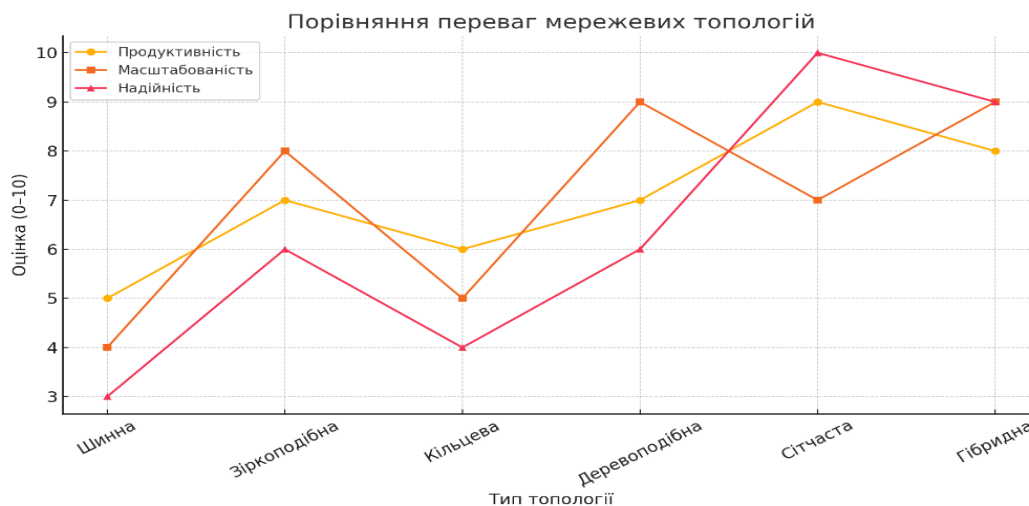
Ключові слова: локальні мережі, топологія мережі, протоколи маршрутизації, кібербезпека.

Локальні мережі (LAN) є основою для ефективного функціонування корпоративних інформаційних систем. Розуміння їхньої структури та принципів роботи є критично важливим для спеціалістів з кібербезпеки, оскільки без цих знань неможливо забезпечити захист даних та попереджати кібератаки. Зокрема, без базового розуміння механізмів передачі даних у мережах неможливо ефективно запобігати кіберзлочинам [1].

Одним із ключових аспектів побудови локальних мереж є їхня топологія, яка визначає:

- продуктивність – наскільки ефективно передаються дані в мережі;
- масштабованість – наскільки легко додавати нові пристрої;
- надійність – стійкість до відмов окремих вузлів або з'єднань.

На графіку представлено порівняння основних топологій локальних мереж за цими критеріями.



З аналізу представленого графіка видно, що сітчаста та гібридна топології мають найвищі оцінки за всіма критеріями. Вони забезпечують високу продуктивність і надійність, проте їх реалізація є складнішою та дорожчою порівняно з іншими варіантами. У той же час зіркоподібна топологія демонструє збалансовані показники між продуктивністю, масштабованістю та зручністю обслуговування, що робить її популярним вибором для корпоративних мереж.

Окрім вибору топології, важливим аспектом функціонування локальних мереж є маршрутизація, яка може бути:

- **статичною** – адміністратор вручну задає маршрути. Підходить для малих мереж, де зміни трапляються рідко;
- **динамічною** – маршрутизація відбувається автоматично за допомогою протоколів.

Протоколи динамічної маршрутизації:

- EIGRP (Enhanced Interior Gateway Routing Protocol) – оптимальний для мереж із обмеженими ресурсами, швидкий у налаштуванні, але менш масштабований.
- OSPF (Open Shortest Path First) – використовує ієрархічну структуру та ефективний для великих корпоративних мереж.
- BGP (Border Gateway Protocol) – основний протокол Інтернету, використовується для обміну маршрутною інформацією між автономними системами.

Параметр	Статична маршрутизація	EIGRP	OSPF	BGP
Ціль використання	Малі мережі	Середні мережі	Великі корпоративні мережі	Глобальні мережі
Кількість оптимальних пристроїв	<10	10-100	100+	Тисячі
Швидкість роботи	Висока	Висока	Висока	Відносно низька
Складність налаштування	Низька	Середня	Висока	Дуже висока
Потреба в ресурсах	Мінімальна	Помірна	Висока	Дуже висока

Отже, ефективне налаштування локальних мереж дозволяє не лише забезпечити стабільну роботу інформаційної інфраструктури, але й створити умови для проактивного захисту від зовнішніх і внутрішніх загроз. Без базових знань про побудову та конфігурацію мереж, зокрема про розмежування доступу (VLAN), контроль трафіку, застосування фаєрволів та мережевих політик, спеціаліст не зможе ефективно протидіяти сучасним викликам у сфері кібербезпеки. Крім того, врахування принципів безпеки ще на етапі проектування мережі дозволяє мінімізувати ризики компрометації систем і підвищити загальний рівень стійкості до атак.

Список використаних джерел:

1. Zahoor A., Ahmed E., Gani A., et al. A survey on security and privacy issues in edge-computing-assisted Internet of Things // *IEEE Internet of Things Journal*. — 2020. — Vol. 7, No. 7. — P. 5931–5945. DOI: 10.1109/IJOT.2020.2970996.

UDC: 004.056.55

A FORMAL MODEL FOR RISK ASSESSMENT WHEN USING CRYPTOGRAPHIC PROTOCOLS IN CLOUD NETWORKS

Mohylevets Maria

State University "Kyiv Aviation Institute", Kyiv

Scientific supervisor – Yuliia Kovalenko, Candidate of Pedagogical Sciences,

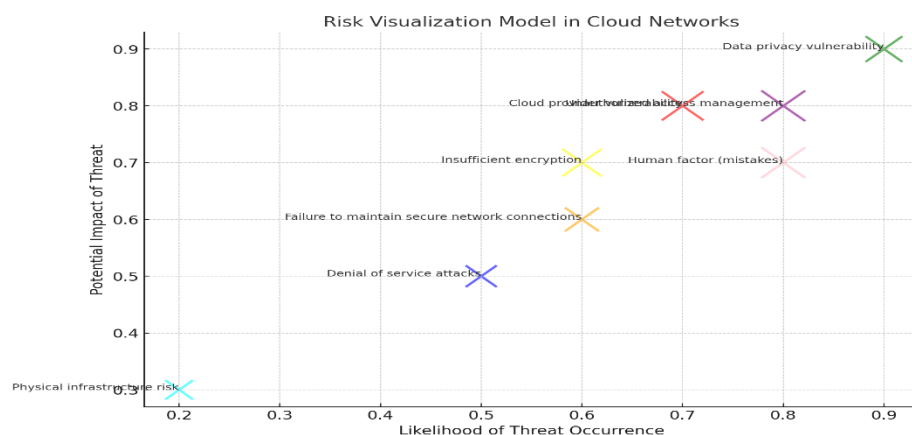
Associate Professor

Keywords: digitalisation, cybersecurity, privacy, data security, digital human rights, cryptography.

Modern society is rapidly digitising, leading to new challenges in the field of cybersecurity. The growing use of cloud technologies and cryptographic protocols for data protection raises an important question: how to ensure the security of information while maintaining a balance between confidentiality and access. Cryptography plays a key role in this context, as it helps to protect transmitted and stored information in cloud networks. However, new risks to the security of this data are emerging due to technological vulnerabilities and human error.

One of the main challenges is ensuring an adequate level of data protection in cloud networks. An important aspect of this is the use of formal models to predict possible threats and develop protection strategies. One of these models is mathematical methods. Modelling various attack scenarios using probability theory and vulnerability analysis techniques [1].

Threats to data security in cloud networks can range from attacks on communication channels to compromising cryptographic keys. Clouds provide remote access to data, it is important to consider the physical security of the infrastructure and proper key management. In addition, data access policies should be considered to ensure that data is protected from unauthorised access. Flaws in security settings or human error can cause serious breaches, so it is important to develop effective strategies to mitigate these risks.



The use of cryptographic protocols also requires constant monitoring and verification of compliance with current standards. Automated cryptographic risk assessment systems can help to identify vulnerabilities in protocols and their implementations in a timely manner, which can significantly reduce the likelihood of a successful attack. Monitoring network activity is also an important tool for detecting anomalies that may indicate a possible threat.

Threat category	Probability (0-1)	Potential impact (0-1)	Risk (index)	Countermeasures
Compromise of cryptographic keys	0.40	0.90	0.36	Implementation of hardware key storage (HSM), key rotation, use of protocols with forward secrecy
Attacks on communication channels	0.60	0.70	0.42	Traffic encryption (TLS/SSL), VPN, protection against MITM attacks
Improper access control	0.70	0.80	0.56	Role-based access policies (RBAC), multi-factor authentication
Human factor (errors)	0.80	0.60	0.48	Cybersecurity training for staff, automated configuration checking tools

A risk analysis table for cloud networks based on an assessment of the likelihood of threats and their potential impact. The graph shows a model that visualises these risks, allowing you to identify the most critical threats. Thus, to ensure an adequate level of security in cloud networks, it is necessary to develop formal risk assessment models that allow predicting threats and identifying strategies to minimise them.

List of references:

1. Stallings, W. *Cryptography and Network Security: Principles and Practice*. 7th ed. Boston: Pearson, 2017. 752 p. Bellare, M., & Rogaway, P. (1993). Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. *ACM SIGACT News*, 24(3), 62-73. URL: <https://www.scirp.org/reference/referencespapers?referenceid=2917777>
2. Kaufman, C., Perlman, R., & Speciner, M. *Network Security: Private Communication in a Public World*. 2nd ed. Upper Saddle River: Prentice Hall, 2002. 752 p.
3. Zissis, D., & Lekkas, D. "Addressing cloud computing security issues". *Future Generation Computer Systems*, vol. 28, no. 3, 2012, pp. 583–592. <https://doi.org/10.1016/j.future.2010.12.006>
4. Almorsy, M., Grundy, J., & Müller, I. "An analysis of the cloud computing security problem". *Proceedings of the 2010 APSEC Cloud Workshop*. Sydney: IEEE, 2010. pp. 1–6. <https://doi.org/10.1109/APSEC.2010.75>

UDC 004.056

USING THE THEORY OF LOGICAL-DYNAMIC SYSTEMS TO CONTROL SECURITY EVENTS OF COMPUTER STRUCTURES

Ieygen Samborskyi

State University "Kyiv Aviation Institute", Kyiv

Supervisor – Petro Pavlenko, Doctor of Technical Sciences, Professor.

Keywords: system, management, incident, security, computer structure.

Modern computer structures (CS), which are the basis for the management of critical objects (CS), are constantly affected by unauthorized interventions. The consequence of this may be the shutdown of critical infocommunication systems. Therefore, ensuring their reliable safety of functioning becomes an extremely urgent task.

In the context of the emergence of new threats to the information security of CS KO, in order to ensure their functional stability, it is proposed to use the theory of logical-dynamic systems (LDS) for modeling, analysis and synthesis of information and security event management systems (ISMS) [1].

The main goal of the research is to develop approaches to the synthesis of the structure of the algorithmic and software model (ISMS) using the LDS theory.

In the synthesis of control of computer security events in the mathematical model, formalization descriptions of its structural components are used:

$$S = (X, Y, Z, f, g', L, h). \quad (1)$$

Taking into account the axiomatics of LDS [1], and approaches to safety management of complex systems [2], the components of the model (1) are:

- $X = \{x_1, x_2, \dots, x_n\}$ – a set that describes the current states of the CS;
- $Y = \{y_1, y_2, \dots, y_m\}$ – a set that identifies security events in the CS;
- $Z = \{z_1, z_2, \dots, z_k\}$ – a set that describes the actions to implement security management;
- $f: X \times Y \rightarrow X$ – a function that formally describes changes in the states of the CS depending on the consequences of the destructive effects of security events;
- $g: X \times Y \rightarrow Z$ – the function of forming security management based on the current state and event of the CS security;
- $L = \{l_1, l_2, \dots, l_p\}$ – a set of logical conditions for ensuring the security state of the system;
- $h: X \rightarrow \{True, False\}_p$ – a function that describes a set of true or false logical conditions of states CS, $h(x) = (h_1(x), h_2(x), \dots, h_p(x))$, where $h_i(x)$ is the value of the truth of the logical condition l_i in possible states x ;
- $g': X \times Y \times \{True, False\}_p \rightarrow Z$ – an extended action selection function, which takes into account not only the state of the system and the event, but also the value of the truth of the logical conditions $g'(x, y, h(x)) = z \in Z$. It implements complex and context-sensitive safety responses in CS.

The developed dynamics of incident compensation will be presented in the form of a formalized model that implements step-by-step steps of this compensation and will be reflected in its form of an algorithm:

Step 1: /Initial State/ *The system is in the initial state $x_0 \in X$.*

Step 2: /Security incident occurs/ *Security event $y_i \in Y$.*

Step 3: /Change (transition) of states under the influence of a security event/ *The y_i system enters a new state $x_i' = f(x_i, y_i)$.*

Step 4: /Evaluate Boolean Conditions/ *L conditions are displayed by a new state: $h(x') = (b_1, b_2, \dots, b_p)$, where $b_i \in \{True, False\}$.*

Step 5: /Formation of managerial influences/ *Based on the new state x_i' and the security event y_i , the management of information and security events $z_i = g(x_i', y_i, h(x'))$ is formed.*

Step 6: /Implementation of managerial actions/ *The action z_i is worked out and changes the state of the CS.*

Step 7: /Repeat/ *When new safety events occur, the process from step 2 to step 6 is repeated cyclically.*

Conclusion

The application of the LDS theory is a promising direction for improving the efficiency of information security management in modern and prospective CS, and especially critical infrastructure facilities. The proposed algorithm can be implemented when modernizing existing and creating promising information management systems and security events of the CS.

References:

1. Rabchun D. I. Logical-dynamic model of the process of management of protection resources in the conditions of information confrontation. Modern information protection, 2016. No3. pp. 62-67.
2. Samborskyi I. I., Samborskyi Ie. I., Hol V. D., Peleshok Y. V., Sholokhov S. M. Synthesis of the model of management of complex dynamic objects taking into account the events of their security. Information Technology and Security. 2024. No1(22), pp. 4-16. <https://doi.org/10.20535/2411-1031.2024.12.1>.

UDC 004.056.005

THE ANALYSIS OF MODERN SYSTEMS FOR THE STATE ASSESSMENT OF CYBERSECURITY CLOUD SERVICES

Yevhenii Pedchenko, Mari Petrovska*State University «Kyiv Aviation Institute», Kyiv**Supervisor – Igor Ivanchenko, Candidate of Science (Engineering), associate professor.*

Keywords: cybersecurity, information security, criteria of cloud services assessment, informational impact, cybersecurity of cloud services

Modern cloud providers aim to provide their customers with high-quality service and availability of their systems to customers, but if the cloud provider has implemented an insufficient level of protection for its services, customers or businesses may suffer significant financial and reputational losses due to the lack of cybersecurity measures.

Today, the following standards/regulations are used to assess the security of cloud services HIPAA, PCI DSS, SOC 2, ISO 27001, NIST 80-145. However, neither describes clear requirements for the security of all components of cloud services, covering them only partially, as, for example, the ISO 27001 standard applies only to the ground part of cloud services. That is why the current issue is to compare the capabilities of modern assessment systems for building secure and sustainable cloud services with the ability to ensure the security of customer data [1].

The purpose of this research is to test the effectiveness of modern systems for assessment of the cybersecurity state of cloud services of information infrastructure facilities for a comprehensive assessment of the cybersecurity state of cloud service modules.

The innovativeness of this work is to determine the characteristic features of the modules of cloud services described in article [1] for the assessment of modern information systems built based on international standards and regulations of information security to determine their effectiveness in application.

To determine the effectiveness of the formed cloud service assessment modules, six of the most popular assessment systems were selected, such as IAAP (based on the HIPAA standard), GigaCloud (based on the PCI-DSS standard), SecureFrame (based on the SOC 2 standard), CertiKit (based on the ISO 27001 standard), Accenture (based on the NIST 80-145 standard) and CNIL (based on the GDPR). A comparison of these systems according to the formed assessment modules is presented in Table 1:

Table 1: Comparison of systems for assessment of cloud services cybersecurity

Cloud service module	Assessment systems					
	IAAP	GigaCloud	SecureFrame	CertiKit	Accenture	CNIL
Network module	+	+	+	+	-	Part.
Storage module	+	+	+	+	-	+
Server module	+	+	+	+	-	Part.
Virtualization module	Part.	Part.	Part.	Part.	+	Part.
OS module	+	+	+	+	-	Part.
Container Tech. module	Part.	Part.	Part.	Part.	+	Part.
Runtime module	-	Part.	-	Part.	-	-
Application module	+	+	+	+	-	+
Data module	+	+	Part.	+	-	+
Recommendations module	-	Part.	-	Part.	-	Part.

Result

An analysis of modern systems for assessment of the cybersecurity state of cloud services has shown that the assessment is based on the presented assessment systems, which are based on their assessment methods and are entirely based on modern standards and regulations of information security, and are entirely dependent on the subjective opinion of the auditors conducting the relevant assessment. This analysis has determined that the main disadvantage of existing assessment systems is the lack of a unified system covering all modules of the cloud service and the lack of comprehensive recommendations for eliminating the identified vulnerabilities during the assessment.

Conclusion

Through the comparison and analysis of modern systems for assessment of the cybersecurity state of cloud services, it was possible to determine that none of the evaluated systems fully covers all modules of cloud services and there is no clear list of criteria for assessing the cybersecurity of cloud services with clearly defined recommendations that will provide a clear action plan to improve the security of each of the cloud service modules.

References

1. Педченко Є.М., Іванченко І.С. Аналіз моделей та методів оцінювання стану кіберзахисності хмарних сервісів об'єктів інформаційної інфраструктури. *Безпека інформації*. 2024. Том. 30, №2. С. 279-287. URL: <https://doi.org/10.18372/2225-5036.30.19240> URL: <https://jrn1.nau.edu.ua/index.php/Infosecurity/article/view/19240>

УДК-004.056

АВТОМАТИЗОВАНІ СИСТЕМИ КІБЕРЗАХИСТУ В АВІАЦІЇ: РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ

Яковенко Богдан Андрійович

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ольга Кривокульська, асистент

Ключові слова: Штучний інтелект, авіація, авіаційна галузь, аналіз загроз

Авіація є однією з найбільш технологічно складних та критичних галузей, що потребує високого рівня кібербезпеки. Сучасні авіаційні системи мають підключення до Інтернету, що робить їх потенційними цілями для кібератак [1]. Інциденти, такі як демонстрація зламу Boeing 757 через радіочастотні методи [2] та компрометація IT-інфраструктури аеропорту «Бориспіль» у 2016 році, свідчать про недостатню ефективність традиційних методів захисту. У зв'язку з цим актуальним є застосування штучного інтелекту (ШІ) для виявлення загроз і забезпечення адаптивного реагування на атаки в авіаційних інформаційних системах.

Метою дослідження є дослідити ефективність використання штучного інтелекту в автоматизованих системах кіберзахисту авіації для виявлення, запобігання та нейтралізації загроз у режимі реального часу.

Таблиця 1

Аналіз методів ШІ у кіберзахисті авіації

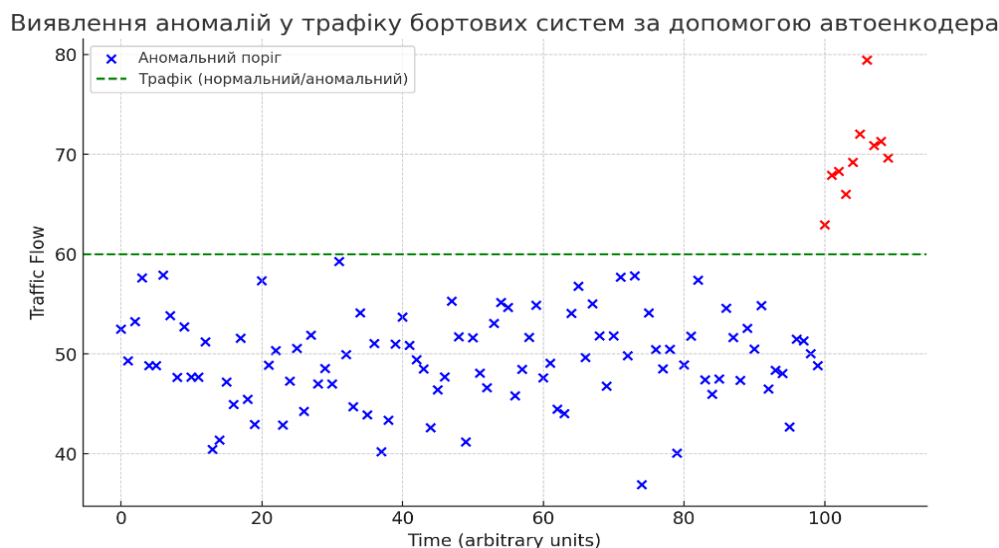
Метод	Призначення	Переваги	Недоліки	Ключові метрики
Автоенкодера	Виявлення аномалій у мережевому трафіку та системних логах	Виявляє нові та невідомі атаки, аналізує великі обсяги даних	Потребує великого обсягу навчальних даних	Мінімізація хибнопозитивних спрацювань, адаптація до нових загроз
Глибоке навчання (CNN, RNN)	Класифікація атак на основі патернів	Висока точність класифікації загроз	Високі обчислювальні витрати	Точність (ассигасу), повнота (recall), F1-міра
Поведінковий аналіз	Аналіз поведінки системи для виявлення підозрілих дій	Адаптивність до змін у поведінці загроз	Може давати хибні спрацювання при нестандартній поведінці	Виявлення відхилень від нормальної поведінки
Статистичний аналіз (класичні методи)	Визначення ефективності методів на основі точності, повноти та F1-міри	Об'єктивна оцінка ефективності методів кіберзахисту	Не завжди виявляє складні атаки в реальному часі	Аналіз ефективності та швидкості виявлення загроз

Для аналізу загроз використовувалися алгоритми машинного навчання, зокрема методи виявлення аномалій (автоенкодера), класифікації атак та поведінковий аналіз мережевого трафіку, було застосовано методи статистичного аналізу, для оцінки ефективності ШІ-систем, включаючи точність виявлення загроз (ассигасу), повноту (recall) та F1-міру.

Інтеграція ШІ в системи кіберзахисту авіації дозволяє суттєво скоротити час виявлення та реагування на загрози. Використання нейронних мереж забезпечує можливість розпізнавання складних та замаскованих атак, які не фіксуються традиційними сигнатурними методами. Автоенкодера продемонстрували високу ефективність у виявленні аномалій у трафіку бортових систем, дозволяючи прогнозувати потенційні загрози ще до їхнього безпосереднього впливу на польотні системи.

Зокрема, моделі глибокого навчання, застосовані для аналізу атак на системи ADS-B, дозволили виявити фальсифіковані сигнали літаків з точністю понад 96% [2]. Для аналізу мережевого трафіку аеропортових систем впровадження ШІ-моделей дало змогу запобігати DDoS-атакам на системи бронювання та автоматизовані авіаційні сервіси. Аналіз вхідних повідомлень електронної пошти за допомогою NLP-моделей дозволяє ідентифікувати фішингові атаки на персонал авіакомпаній, знижуючи ризик соціальної інженерії.

Важливим аспектом є захист самих алгоритмів ШІ від атак на цілісність навчальних даних. Зловмисники можуть маніпулювати даними, що навчають систему, впливаючи на її здатність виявляти аномалії. Впровадження додаткових механізмів валідації даних та криптографічних технологій дозволяє мінімізувати цей ризик.



Застосування штучного інтелекту в автоматизованих системах кіберзахисту авіації значно підвищує рівень безпеки шляхом прискореного виявлення загроз, аналізу поведінкових аномалій та автоматизованого реагування на атаки. Подальший розвиток таких систем потребує стандартизації підходів до впровадження ШІ, тісної співпраці авіакомпаній із технологічними компаніями та вдосконалення механізмів захисту самих алгоритмів від маніпуляцій зловмисників.

Список використаних джерел:

1. Feng, Q., & Xu, L. (2021). Artificial Intelligence for Cybersecurity in Aviation: A Review. *Journal of Aerospace Information Systems*, 18(5), 311-325.
2. Greenberg, A. (2017). The Feds Hijacked a Passenger Jet in 2016—To Prove a Point About Cybersecurity. *Wired*.

УДК 004.056.53

АНАЛІЗ СИСТЕМ ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Зандер Олександр, Мархай Антон, Кузьменко Микола

Державний університет «Київський Авіаційний Інститут», Київ

Науковий керівник – Кириленко Альона Юріївна, старший викладач

Ключові слова: несанкціонований доступ, автоматизована система, захист від НСД, програмний захист інформації.

Розвиток інформаційних технологій супроводжується зростанням загроз безпеки даних. Необхідність захисту інформації особливо актуальна у сфері державного управління, фінансів та критично важливих об'єктів інфраструктури. Метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її обробки в АС [1]. Шляхи захисту АС від несанкціонованого доступу, у загальному вигляді, можливо представити на Рис. 1

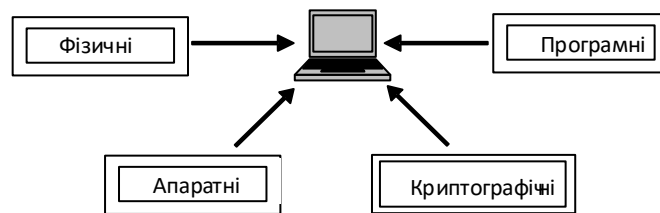


Рис 1. Шляхи захисту АС (ПЕОМ) від НСД

Проаналізуємо наступні рішення: «Лоза», «Гриф», **UALinux Secured*Pack**.

Система ЛОЗА™-1 / Система ЛОЗА™-2 — це програмні засоби захисту інформації від несанкціонованого доступу в автоматизованих системах класу «1». Система може працювати під керуванням операційних систем (ОС) Windows, Windows Server. Системи ЛОЗА™-1 / ЛОЗА™-2 реалізують всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу і для побудови системи захисту інформації. Можуть використовуватись для захисту інформації, що становить державну таємницю, — підтверджено експертним висновком №1095 [2].

«Комплекс «Гриф» (версії 4/версія 5) - засіб технічного захисту інформації від НСД, призначений для забезпечення захисту ІзОД, оброблюваної в АС класу 1 та 2, що побудовані на базі ПЕОМ, функціонуючі під керуванням ОС корпорації Microsoft. Комплекс може також використовуватись на робочих станціях та серверах інформаційних систем ІС. На відміну від політики довірчого керування доступом, яка реалізується штатними засобами захисту Windows, використання комплексу дозволяє забезпечити реалізацію політики адміністративного керування доступом до ІзОД. Повністю замінює штатні засоби власними, які реалізують захист інформації у вигляді даних довільного типу [3].

UALinux Secured*Pack є сукупністю функцій та механізмів безпеки в складі програмного забезпечення ОС призначених для реалізації захисту ІзОД, оброблюваної в АС класів 1, 2 та 3, що побудовані на базі ПЕОМ/Сервери (окремих та/або об'єднаних в локальну мережу), під управлінням ОС «UALinux Secured*Pack» [4].

При розгляді ефективності даних рішень в контексті реалізації захисту інформації кожен з варіантів має свої переваги та недоліки. Стосовно **Windows** орієнтованих систем вони є легшими в реалізації оскільки не потребують спеціалізованого персоналу для інсталяції та налаштування системи, не потребують спеціалізованого навчання персоналу для роботи з Windows. Однак, вони є залежними від ліцензійної моделі, що для великих компаній може бути не вигідним. Реалізація функціоналу є не такою гнучкою, порівняно з Linux - це буде сповільнювати темпи масштабування інформаційної мережі компанії. **UALinux Secured*Pack** забезпечує високий рівень захисту з можливістю кастомізації системи та її гнучкістю для налаштування під конкретні задачі компанії без сторонніх ліцензійних витрат. Однак потребує додаткових інвестицій на розгортання мережі, роботу кваліфікованих спеціалістів з налаштування та навчання персоналу для роботи з Linux. Можливо зазначити, що для користувачів АС 1 та 2 класу доцільно використовувати Систему Лоза, оскільки даний засіб простіший під час встановлення та налаштування. Для великих підприємств з швидкими темпами розвитку ІС та необхідністю гнучкого налаштування системи доцільно обрати **UALinux Secured*Pack**, що в довготривалій перспективі дозволить заощадити кошти, відмовившись від зайвих ліцензійних витрат.

Використовуючи метод порівняльного аналізу, вибір засобів захисту АС від НСД залежить від поставлених задач, бюджету, перспективності подальшого розвитку ІС. При цьому, перевага повинна надаватись засобам, що зручні при встановленні, налаштуванні та використанні.

Список використаних джерел

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22 (із змінами).
2. Технічний захист інформації. Електронний ресурс: <https://tzi.ua/ua/index.html>.
3. Інститут комп'ютерних технологій. Електронний ресурс: <https://www.ict.com.ua/?lng=1&sec=8&art=41>.
4. UALinux. Електронний ресурс: <https://ualinux.com/uk/uapack>

УДК 004.67

УДОСКОНАЛЕННЯ МЕТОДУ МОНІТОРИНГУ СТАНУ ВЕБ-САЙТУ ЗА РАХУНОК ВИЯВЛЕННЯ ПОМИЛОК В КОДІ САЙТУ

Ігор Мартинюк^{1,2}, Назар Заїка²

¹Державний університет «Київський авіаційний інститут», Київ

²Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ

Науковий керівник – Тетяна Охріменко, к.т.н., с.н.с.

Ключові слова: моніторинг, синтетичні тести, виявлення помилок, веб-сайт, помилки в коді.

Вступ. На сьогодні ІТ-системи стають все складнішими, через це організаціям потрібно інвестувати в інструменти моніторингу ІТ-систем. Такі інструменти надають можливість адаптуватися до розвитку технологій і зростаючим обсягам даних [1]. З огляду на це, питання моніторингу стану веб-сайту стає актуальним у контексті зростаючого обсягу даних, які зберігаються та обробляються [2].

Метою дослідження є вдосконалення методу моніторингу стану веб-сайту за рахунок додавання методу виявлення помилок у коді сайту, що підвищить рівень безпеки та безперебійності роботи таких веб-сайтів. Для задоволення поставленої мети дослідження були визначені наступні завдання: вибір системи збору даних та моніторингу, яка підтримує масштабування та необхідний набір метрик; аналіз можливостей та обмежень наявних методів збору даних та виявлення помилок за допомогою додаткових синтетичних тестів; вдосконалення методу моніторингу стану веб-сайту враховуючи виявлення помилок в коді сайту, а не лише за допомогою виявлення кодів стану HTTP; розробка методу інтеграції результатів синтетичних тестів в систему моніторингу для подальшого їх опрацювання та аналізу.

Висновок

У роботі проведено дослідження щодо вдосконалення виявлення ІТ-інцидентів за допомогою використання додаткових елементів перевірки системою моніторингу. Для цього було поєднані методи обробки та інтеграції даних, визначення доступності та моніторингу наявності помилок при роботі веб-сайту.

Список використаних джерел:

1. What's IT Monitoring? IT Systems Monitoring Explained. Joseph Nduhiu. URL: https://www.splunk.com/en_us/blog/learn/it-monitoring.html (Дата звернення: 24.03.2025)
2. Lizunov, Serhii, Yevhenii Filobok, and Maksym Vereshchaka. "Використання інтегрованих систем моніторингу ІТ-інфраструктури." Ukrainian Scientific Journal of Information Security 30.2 (2024): 353-357.

УДК 004.05:004.02

ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ ДИФЕРЕНЦІЙОВАНОЇ КОНФІДЕНЦІЙНОСТІ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ В ІНТЕЛЕКТУАЛЬНИХ МЕРЕЖАХ ІЗ ЗАСТОСУВАННЯМ ІОТ

Ірина Борисенко, к.т.н

Київський національний університет імені Тараса Шевченка, Київ

Ключові слова: диференційована конфіденційність, інтелектуальні мережі, ІоТ

Вступ. Розв'язання локальних задач проблеми оптимального управління безпекою інтелектуальних мереж із застосуванням ІоТ, веде до застосування різних методологічних основ. У результаті методологічної незалежності практичне використання локальних теорій зводиться до загальних оцінок, тому що локальні теорії об'єднані в загальну технологію управління на загальній основі логіко-експертних методів.

Ефективність процесів управління безпекою великою, а іноді й визначальною мірою залежить від сучасних технологій, які застосовуються в системі функції. Принциповим положенням управління безпекою є вибір математичної моделі, тому застосування методу диференційованої конфіденційності є доцільним. Диференційована конфіденційність криптографічна характеристика конфіденційності даних, яка може бути застосована для реалізації функцій в системах з інтелектуальними мережами із застосуванням ІоТ.

Мета. Метою дослідження є підвищення ефективності безпеки в інтелектуальних мережах із застосуванням ІоТ за рахунок використання методу диференційованої конфіденційності.

Матеріали та методи. Простий спосіб вивести функцію таким чином, щоб досягти диференційованої конфіденційності, полягає в використанні так званого «експоненціального механізму». Цей підхід передбачає побудову відповідної скінченної множини функцій $G = \{g_i, \dots, g_m\} \in R^T$, в якій кожна функція f_D має розумне наближення при деякій функції відстані d . Потім, коли на вхід подається D , вибирається функція шляхом вибірки з множини G з ймовірностями, заданими формулою.

$$P_D(g_i) \propto \exp\left\{\frac{-\alpha}{2S} d(g_i, f_D)\right\}, S \stackrel{\text{def}}{=} \sup_{D \sim D} d(f_D, f_D) \quad 1$$

Така методика забезпечує α -диференційовану конфіденційність в великих технічних системах. Цей метод концептуально привабливий своєю простотою, і в одно час залишається складним для застосування, оскільки набір функцій G може бути дуже великим, щоб забезпечити корисність виділеної функції (у сенсі очікуваної похибки). Оскільки алгоритм, який виводить результати з P_D , повинен отримати константу нормалізації до наведеного вище розподілу, він, очевидно, повинен обчислити ймовірності для кожного g_i , що може бути надзвичайно трудомістким.

Результати. Застосування експоненціального механізму по суті відповідає дискретизації простору функцій R^T . Альтернативою є дискретизація вхідного простору T та апроксимація функції, де частини

відповідають дискретизації T . Таким чином, апроксимацію можна розглядати як вектор з дійсними значеннями, з одним входом для значення кожного відрізка функції.

Висновки. Такі методи, можна інтерпретувати як виведення дискретної випадкової величини та виконання визначення конфіденційності по відношенню до σ -поля, що складається з степеневі множини G .

Застосування диференційованої конфіденційності створює анонімні дані шляхом додавання шуму в інтелектуальні мережі з застосуванням IoT. Доданий шум допомагає захистити конфіденційність та підвищити рівень безпеки та надійності роботи системи.

Список використаних джерел:

1. A. Bertinet and Thomas C. Agnan. Reproducing Kernel Hilbert Spaces in Probability and Statistics. Kluwer Academic Publishers, 2004.
2. P. Billingsley. Probability and Measure. Wiley-Interscience, 3 edition, 1995. O. Bousquet and A. Elisseeff. Stability and generalization. Journal of Machine Learning Research, 2:499–526, 2002.
3. A. Charest. Creation and Analysis of Differentially-Private Synthetic Datasets. PhD thesis, Carnegie Mellon University, 2012. K. Chaudhuri and D. Hsu. Convergence rates for differentially private statistical estimation. In ICML'12, 2012.
4. K. Chaudhuri and C. Monteleoni. Privacy preserving logistic regression. NIPS 2008, 2008.
5. K. Chaudhuri and C. Monteleoni. Differentially private empirical risk minimization. Journal of Machine Learning Research, 12:1069–1109, 2011.
6. S. Chawla, C. Dwork, F. McSherry, and K. Talwar. On the utility of privacy-preserving histograms. UAI, 2005. C. Dwork. Differential privacy. 33rd International Colloquium on Automata, Languages and Programming, pages 1–12, 2006.
7. C. Dwork and J. Lei. Differential privacy and robust statistics. Proceedings of the 41st ACM Symposium on Theory of Computing, pages 371–380, May–June 2009

UDC 004.056.005

OVERVIEW OF IDS CAPABILITIES FOR NETWORK TRAFFIC ANALYSIS

Bogdan Demianchuk, Diana Kozlovska, Vadym Storozhenko

State University «Kyiv Aviation Institute», Kyiv

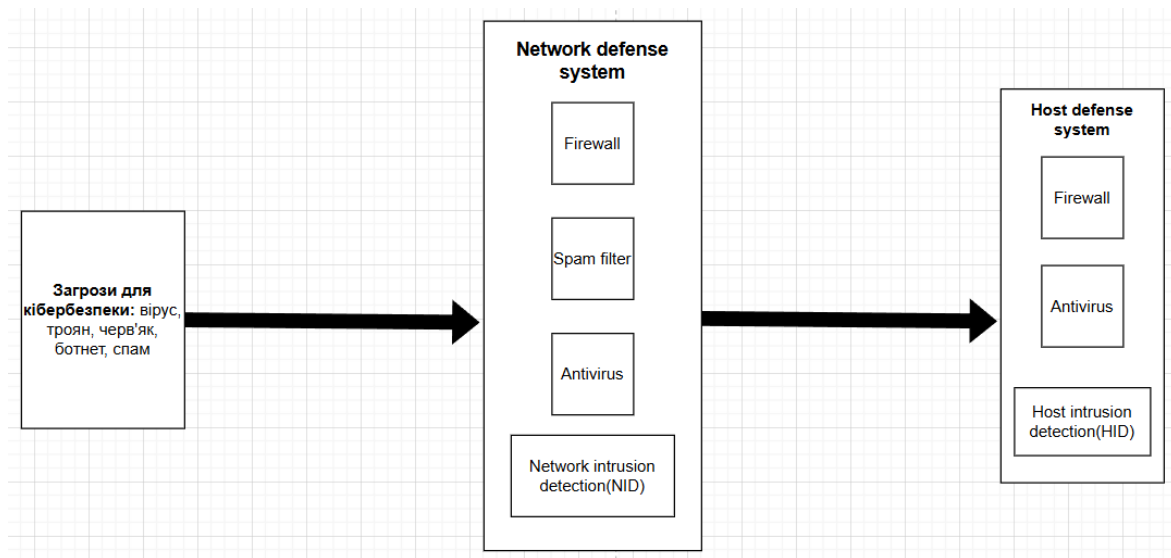
Keywords –Intrusion Detection System, IDS, NIDS, HIDS, cybersecurity, network traffic analysis, threat detection, security monitoring

Modern cyber threats are constantly evolving, demanding enhanced detection and response mechanisms. Traditional intrusion detection systems (IDS) and security information and event management (SIEM) tools provide basic protection but suffer from high false positive rates and limited ability to detect new attack types. Researchers are working to improve cybersecurity methods to ensure data confidentiality, integrity, and availability while effectively protecting networks.

IDS systems protect information, computers, and networks by ensuring confidentiality, integrity, and availability [1]. Cybersecurity solutions address threats like viruses and botnets at two levels: network and host. Networks are secured with firewalls and intrusion detection tools, while end-user devices rely on local security mechanisms [2]. An example is shown in Pic. 1.

At both security levels, an additional layer of protection is implemented in the form of NIDS and HIDS, key IDS variants, add an extra security layer [3]. IDS detects threats like unauthorized access, malware, and suspicious activity, alerting administrators. By analyzing data packets, logs, and system behavior, IDS enables real-time threat detection and

response. Popular IDS systems include: Some of the most popular IDS systems today are listed in Table 2, which highlights their main advantages and disadvantages/



Pic. 1. Standard Cybersecurity System

The experimental part tests the Security Onion SIEM system, integrating Suricata (IDS/IPS), Zeek (network analyzer), ELSA (log management), and Squil (event correlation). The main study objects are:

- The operation of the Suricata intrusion detection module;
- The effectiveness of the Security Onion comprehensive solution as a security monitoring platform.

Table 2
COMPARING DIFFERENT IDS SYSTEMS

System	Advantages	Disadvantages
Zeek	High scalability - Extensible via scripting - Supports behavior analysis - Free	- Complex setup - High computational power for large traffic
Suricata	- Flexible (Snort rules, Lua scripts) - Built-in protocol support - Free	- Complex configuration - Needs rule optimization
Security Onion	- Hybrid platform (Zeek, Snort, Suricata, Wazuh) - High scalability - Free	- Complex setup - Resource-intensive operation
Wazuh	- High scalability with agent support - Elastic Stack integration for SIEM - Automated event analysis - Free	- Requires agent installation on each device - Additional configuration needed
Cisco Secure IDS	- High performance - Deep Cisco integration - Professional support - High accuracy	- High license cost - Less flexible scalability due to closed ecosystem
IBM QRadar	- High scalability - AI-driven analytics - SIEM support - Partially free	- High cost - Requires expertise for setup
Snort	- Free - Flexible configuration - Strong community - Widespread use	- Moderate scalability - Needs rule optimization

1. Suricata Configuration

The Suricata configuration included two detection rule levels:

- **Standard rules (ET Open Ruleset)** – cover typical attack vectors with high accuracy.
- **Specialized rules** – experimental templates for testing adaptability to new threats, performance with anomalous patterns, and complex polymorphic attacks.

2. Datasets Used

To evaluate the accuracy of threat detection and minimize false positives, the following datasets were used: **KDD Cup 1999, NSL-KDD, CIC-IDS2017, UNSW-NB15**.

3. Research Results:

The testing revealed a high level of effectiveness of the Suricata system in countering modern network threats (Table 3).

Table 3
EFFECTIVENESS OF THREAT DETECTION (DETECTION RATE) BY ATTACK TYPE

Attack Type	Detection Rate	False Positives	Protection Level
DDoS Attacks	98%	2%	High
SQL Injection	94%	6%	High
Port Scanning	98,3 %	1,7%	High
Phishing	90,7%	9,3	Medium

4. Analysis of Results Based on Datasets

The testing conducted on different datasets revealed the following performance indicators for Suricata:

DETECTION ACCURACY AND FALSE POSITIVE RATE BY DATASET

Dataset	Accuracy (%)	False Positives	Main Attack Types
CIC-IDS2017	96	3.5	DDoS, Botnets, Phishing
UNSW-NB15	93	4.0	Exploits, Scanners, Analysis
NSL-KDD	89	5.2	DoS, Probing (Probe)

CONCLUSION

The study indicates that IDS systems vary in their strengths and weaknesses, affecting their suitability for specific scenarios. Open-source systems like Zeek, Suricata, and Snort offer great adaptability but require advanced configuration, while commercial tools like Cisco Secure IDS and IBM QRadar offer more comprehensive features at a higher cost. The choice of system depends on the infrastructure, expertise, and financial resources available. Future improvements should focus on integrating machine learning for automation and hybrid systems. The research showed that Suricata had a 92.6% detection rate and low false positives, proving the competitiveness of open-source systems

LITERATURE

- [1] Chernyk O. A. Intrusion Detection Systems // Proceedings of the International Scientific and Technical Conference "Information Models, Systems, and Technologies" (IMSTT-2023). – Ternopil: TNTU, 2023. – P. 126. – URL: https://elartu.tntu.edu.ua/bitstream/lib/44254/2/IMSTT_2023_Chernyk_O_A-Intrusion_detection_systems_126.pdf?utm_source=chatgpt.com (accessed on 13.03.2025)
- [2] Stolyar A. L. Analysis of Modern Anomaly Detection Methods in Computer Networks. 2023, URL: <https://doi.org/10.18372/2073-4751.74.17888> (accessed on 13.03.2025)
- [3] Kumar KN, Sukumaran S. A survey on network intrusion detection system techniques. International Journal of Advanced Technology and Engineering Exploration. 2018;5(47):385-393

УДК 004. 056

АНАЛІЗ ОЦІНКИ МЕТОДІВ І МОДЕЛЕЙ ОЦІНЮВАННЯ СТАНУ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ АВІАЦІЙНИХ ПІДПРИЄМСТВ

Андрій Біскупський

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ігор Іванченко, к.т.н, доц.

Ключові слова: оцінювання стану кібербезпеки, критична інфраструктура, авіаційне підприємство.

Широке впровадження авіаційними підприємствами інформаційно-комунікаційних технологій в операційні процеси – є життєво необхідним інструментом для нормального функціонування авіаційного транспорту. Як зазначається в [1] в авіаційному законодавстві України не сформовано критерії і немає системності до оцінювання стану кібербезпеки авіаційних підприємств. Тому розробка методів і моделей оцінювання стану критичної інформаційної інфраструктури є актуальною задачею.

Метою роботи є ґрунтовний аналіз існуючих методів і моделей оцінювання стану кібербезпеки критичної інформаційної інфраструктури авіаційних підприємств з урахуванням специфіки функціонування авіаційного транспорту, у відповідності до критеріїв визначених у наказі «Адміністрації державної служби спеціального зв'язку та захисту інформації» №601 від 06.10.2021 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» зі змінами в наказі №343 від 10.07.2022 [2], з метою визначення переваг та недоліків існуючих методів та моделей, визначення рівня їх відповідності заданим критеріям і обґрунтування розробки нових чи удосконалення існуючих методів та моделей.

В роботі [3] авторами монографії відібрані наступні методи оцінки ризиків: стандарт NIST 800-30, BSI-Standard 100-3, Стандарт ISO/IEC 27005:2008, Метод CRAMM, Метод на основі байєсовських мереж, Метод VAR, Методика COBRA Метод CRAMM, Метод Coras, Метод EBIOS, Метод ISAMM, Система RiskWatch, Інструментарій PTA, Система Enterprise Risk Assessor, Система vsRisk, Risk Assessment Tool, Система OCTAVE, Методика TRA, Методика FRAP, Методика Risk Matrix, Методика Mehari, Методика MAGERIT, Методика Information Security RA. Джерело [4] пропонує використовувати метод нечітких множин для виявлення вразливостей (FLVA – fuzzy logic for vulnerability assessment. В роботі [5] авторами запропоновано метод нечітких систем логічного висновку (FIS – fuzzy inference logic). В таблиці 1 зведені результати аналізу.

Таблиця 1. Критерії оцінки методів та моделей оцінювання стану кібербезпеки авіаційних підприємств.

	Методи і моделі оцінювання стану кібербезпеки									
	1	2	3	4	5	6	7	8	9	10
Клас заходу кібербезпеки	NIST 800-30	BSI-Standard 100-3	ISO/IEC 27005:2008	CRAMM	CORAS	EBIOS	ISAMM	RiskWatch	Інструментарій PTA	Система Enterprise Risk Assessor
Ідентифікація ризиків кібербезпеки	+	+	+	+	+	+	+	+	+	+
Кіберзахист	+	+	+	+	+	+	+	+	+	+
Виявлення кіберінцидентів	+	-	+	-	+	+	+	+	-	-
Реагування на кіберінциденти	+	+	+	+	+	+	+	+	+	+
Відновлення стану кібербезпеки	+	+	+	+	+	+	+	+	+	+

Таблиця 1. Критерії оцінки методів та моделей оцінювання стану кібербезпеки авіаційних підприємств (продовження).

	Методи і моделі оцінювання стану кібербезпеки										
	11	12	13	14	15	16	17	18	19	20	21
Клас заходу кібербезпеки	Система vsRisk	Risk assessment tool	OCTAVE	TRA	FRAP	Risk Matrix	MEHARI	MAGERIT	Information Security RA	FIS	FLVA
Ідентифікація ризиків кібербезпеки	+	+	+	+	+	+	+	+	+	+	+
Кіберзахист	+	+	+	+	+	+	+	+	+	+	+
Виявлення кіберінцидентів	-	+	+	+	+	+	+	+	+	+	+
Реагування на кіберінциденти	+	+	+	+	+	+	+	+	+	+	+
Відновлення стану кібербезпеки	+	+	+	+	+	+	+	+	+	+	+

Проведений аналіз оцінки методів та моделей оцінювання стану кібербезпеки за критеріями класів заходів кіберзахисту може бути використаний у якості основи для розробки та удосконалення методів та моделей оцінювання стану кібербезпеки критичної інфраструктури авіаційних підприємств.

Список використаних джерел:

1. Сидоренко В. М. Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі: автореф. дис. ... канд. техн. наук: 21.05.01 / В. М. Сидоренко. – Київ, 2018. – 23 с.
2. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури: Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації №601 від 06.10.2021 зі змінами наказу №343 від 10.07.2022 // Адміністрація державної служби спеціального зв'язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: [Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» \(зі змінами\)](#).
3. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія / О. Г. Корченко, С. В. Казмірчук, Б. Б. Ахметов. – Київ: Національний авіаційний університет, 2017. – 435 с.
4. Іванченко Є. В., Корченко О. Г., Бакалинський О. О., Мялковський Д. В., Верба Д. В., Зубков Д. А., Юдіна Д. О. Модель системи характеристик даних для оцінювання заходів кіберзахисту в Україні.
5. Al-Ali Mansour, AlMogren Ahmad. Fuzzy logic methodology for cyber security risk mitigation approach / Mansour Al-Ali, Ahmad AlMogren // King Saud University, Saudi Arabia. – Received: 19 April 2017, Revised: 30 May 2017, Accepted: 7 June 2017 // Journal of Digital Information Management. – 2017. – [Volume 8, number 3].

УДК 004.49

ЦІЛЕСПРЯМОВАНІ АТАКИ НА МОДЕЛІ ШТУЧНОГО ІНТЕЛЕКТУ: АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ

Сергій Бондаровець

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Охріменко, к.т.н., ст. дослідник

Ключові слова: цілеспрямовані атаки, штучний інтелект, кібербезпека.

Штучний інтелект (ШІ) дедалі частіше застосовується у критично важливих сферах, таких як автономний транспорт, медицина, фінанси та безпека. Вразливість моделей ШІ до цілеспрямованих атак створює серйозні ризики для їх надійності та безпечного використання [1]. Нападники можуть навмисно модифікувати вхідні дані, вводячи модель в оману, що призводить до неправильних або небезпечних

рішень [2]. На даний момент жоден із окремих методів і підходів до захисту не є універсальним рішенням: багато запропонованих методів було зламано адаптивними атаками [4].

Метою дослідження є аналіз основних загроз та методів захисту від цілеспрямованих атак на моделі штучного інтелекту.

Цілеспрямовані атаки можна класифікувати за тим, на якому етапі роботи моделі вони застосовуються, а саме:

Атаки ухилення (evasion attacks) – застосовуються на етапі прогнозування, коли змінені дані подаються на вхід моделі для викривлення її результатів [2].

Атаки на навчальні дані (data poisoning & backdoor attacks) – модифікація навчальних даних, щоб модель отримала неправильні закономірності [8].

Інверсійні атаки (model inversion attacks) – намагання відновити інформацію про навчальні дані, використовуючи вихідні значення моделі [7].

Атаки на крадіжку моделі (model extraction attacks) – надсилання великої кількості запитів до, наприклад, комерційного API, відстежуючи відповіді, щоб навчити власну модель, що дублює поведінку цільової [10].

Атаки визначення членства (membership inference attacks) – завдяки аналізу відповідей моделі нападник визначає, чи конкретний приклад використовувався під час навчання, що несе ризики розкриття конфіденційних даних [10].

Ін'єкція запитів (prompt injection attacks) – загроза для великих мовних моделей (LLMs), коли зловмисник вводить запити, що змушують модель ігнорувати її первісні обмеження та видавати приховану інформацію або небажаний контент [5].

Існуючі методи захисту можна поділити на три основні категорії (табл. 1):

Таблиця 1.

Існуючі методи захисту моделей штучного інтелекту

Категорія	Можливі методи захисту
Захист від атак ухилення	• Адверсаріальне навчання – модель навчається на викривлених прикладах, щоб розпізнавати атаки, але це вимагає значних обчислювальних ресурсів [3]. • Попередня обробка вхідних даних – зменшення роздільної здатності або використання автоматичних кодувальників для очищення сигналу [6]. • Сертифіковані методи – математичне доведення того, що невеликі зміни не змінять результат [9].
Захист від отруєння та прихованих атак [8]	• Фільтрація навчальних даних – перевірка на наявність аномалій. • Аналіз внутрішніх параметрів моделі – виявляє приховані тригери.
Захист від атак на конфіденційність та крадіжку моделей	• Диференційно-приватне навчання – додає шум під час навчання, щоб приховати окремі зразки [7]. • Обмеження вихідної інформації – надання лише найімовірнішого результату без ймовірностей [10]. • Водяні знаки у моделях – спеціальні патерни, що дозволяють відстежити вкрадені моделі [10].

Висновки

Попри досягнутий прогрес, існуючі методи захисту мають недоліки: обмежена універсальність – більшість захистів працює лише проти певного типу атак; компроміс між стійкістю та продуктивністю – захист від атак часто призводить до втрати точності або зростання витрат; нові вектори атак – швидкий розвиток технологій створює нові загрози. Важливим напрямком є розширення сертифікованих методів, покращення виявлення атак у режимі реального часу та інтеграція людини в процес перевірки аномалій. Цей аналіз проведено з метою систематизувати сучасні загрози для ШІ-моделей та оцінити ефективність наявних методів захисту від цілеспрямованих атак. Отримані результати дозволяють виявити ключові вразливості існуючих підходів і сформулювати основу для розробки більш універсальних, адаптивних і сертифікованих механізмів захисту в майбутніх дослідженнях.

Список використаних джерел:

1. N. Carlini and D. Wagner, «Towards Evaluating the Robustness of Neural Networks», 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2017, pp. 39-57.
2. Goodfellow, J. Shlens, and C. Szegedy, «Explaining and Harnessing Adversarial Examples», International Conference on Learning Representations (ICLR), 2015.
3. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, «Towards Deep Learning Models Resistant to Adversarial Attacks», International Conference on Learning Representations (ICLR), 2018.
4. Biggio and F. Roli, «Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning», Pattern Recognition, vol. 84, pp. 317–331, 2018.
5. X. Huang, M. Kwiatkowska, S. Wang, and M. Wu, «Safety Verification of Deep Neural Networks», Computer Aided Verification (CAV), 2017.
6. W. Xu, D. Evans, and Y. Qi, «Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks», Network and Distributed System Security Symposium (NDSS), 2018.
7. M. Nasr, R. Shokri, and A. Houmansadr, «Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks Against Centralized and Federated Learning», IEEE Symposium on Security and Privacy, 2019.
8. Y. Liu, X. Ma, J. Aafer, et al., «Trojaning Attack on Neural Networks», Network and Distributed System Security Symposium (NDSS), 2018.
9. E. Wong and J. Z. Kolter, «Provable Defenses Against Adversarial Examples via the Convex Outer Adversarial Polytope», International Conference on Machine Learning (ICML), 2018.
10. R. Shokri, M. Stronati, C. Song, and V. Shmatikov, «Membership Inference Attacks Against Machine Learning Models», IEEE Symposium on Security and Privacy (SP), 2017

УДК 004.89:004.056

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ: ПЕРСПЕКТИВИ, ВИКЛИКИ ТА ЕТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ

Багатко Анастасія

Національна академія Служби безпеки України (НА СБУ)

Науковий керівник – Анастасія Ігорівна Вавіленкова, д.т.н., професор

Ключові слова: штучний інтелект, кібербезпека, машинне навчання, кібератаки, етичні аспекти

Розвиток штучного інтелекту (ШІ) кардинально змінює підходи до забезпечення кібербезпеки. Сучасні наукові дослідження [1, 3] підтверджують значний потенціал ШІ у виявленні загроз, їх аналізі та автоматизованому реагуванні на кіберінциденти. Водночас впровадження цих технологій супроводжується низкою викликів, зокрема етичного характеру [2], що потребують комплексного розгляду.

Метою дослідження є аналіз можливостей, викликів і етичних дилем, пов'язаних із використанням штучного інтелекту у сфері кібербезпеки.

Для досягнення поставленої мети в дослідженні застосовано такі методи:

- **Аналітичний метод** – вивчення наукових праць і технічної документації з проблематики ШІ у кібербезпеці.
- **Порівняльний аналіз** – оцінка ефективності сучасних систем ШІ для виявлення загроз.
- **Метод моделювання** – тестування алгоритмів машинного навчання у сфері кіберзахисту.
- **Емпіричний метод** – аналіз практичних випадків застосування ШІ у реальних кіберінцидентах.

Сучасні дослідження підтверджують значний потенціал ШІ у таких аспектах:

1. **Автоматичне виявлення аномальної активності** у комп'ютерних мережах на основі поведінкового аналізу.
2. **Використання глибокого навчання** для прогнозування та ідентифікації кіберзагроз.
3. **Розширені системи багатфакторної автентифікації**, що використовують біометричні та поведінкові фактори.
4. **Самонавчальні системи**, здатні адаптуватися до нових тактик зловмисників.
5. **Автоматизоване виявлення фішингових атак** та аналіз шкідливого програмного забезпечення.

Незважаючи на високий потенціал, використання ШІ у сфері кібербезпеки пов'язане з низкою викликів:

1. **Вразливість алгоритмів до маніпуляцій** (наприклад, атаки на моделі машинного навчання).
2. **Хибнопозитивні та хибнонегативні результати**, що ускладнюють ефективний аналіз загроз.
3. **Високі вимоги до обчислювальних ресурсів** для навчання та роботи моделей ШІ.
4. **Обмежена пояснюваність рішень**, що ускладнює аудит і підзвітність алгоритмів.
5. **Потреба у кваліфікованих фахівцях**, здатних налаштовувати та підтримувати системи ШІ.

Окрім технічних аспектів, важливе значення мають етичні питання використання ШІ [2]:

1. **Ризик порушення конфіденційності** через використання ШІ для масового стеження.
2. **Автономність ухвалення рішень без участі людини**, що може призвести до непередбачуваних наслідків.
3. **Використання ШІ у кіберзлочинності**, наприклад, створення фішингових схем та глибоких фейків.
4. **Проблема відповідальності за дії ШІ** у випадку неправомірних рішень.
5. **Етична дилема щодо використання ШІ** в інформаційних війнах та дезінформаційних кампаніях.

Штучний інтелект відіграє важливу роль у сучасних системах кібербезпеки, підвищуючи ефективність виявлення загроз і реагування на інциденти. Водночас його використання супроводжується технічними, етичними та правовими викликами, що потребують комплексного підходу. Для успішного

впровадження технологій необхідно вдосконалювати алгоритми, забезпечувати їхню прозорість та розробляти механізми етичного регулювання.

Список використаних джерел

1. Дослідження сучасних підходів до застосування ШІ у кібербезпеці // Journal of Cybersecurity. 2023. № 4. С. 45–58.
2. Стаття про етичні аспекти використання ШІ у безпеці // Ethics & AI Review. 2022. № 2. С. 15–27.
3. Аналітичний звіт щодо вразливостей ШІ в кіберпросторі // Cybersecurity Analysis. 2024. № 1. С. 78–92.

УДК 004.9(043.2)

ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ТА УПРАВЛІННЯ ЗВІТНІСТЮ У СТАРТАП-КОМПАНІЯХ

Владислав Андросович

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Голего, старший викладач.

Ключові слова: бізнес-аналітика, дашборди, інтеграція даних, автоматизація звітності, предиктивна аналітика.

Сучасні стартап-компанії стикаються з необхідністю оперативного аналізу великих обсягів даних та прийняття обґрунтованих рішень в умовах обмежених ресурсів. Традиційні інструменти управління звітністю часто виявляються недостатньо гнучкими та потребують значних витрат на впровадження і підтримку, що ускладнює їх використання для компаній на ранніх стадіях розвитку.

Ефективне управління даними є критичним фактором успіху стартапів у сучасному динамічному бізнес-середовищі. Застосування інструментів візуалізації та аналітики, таких як Power BI та Python, дозволяє компаніям покращити процеси прийняття рішень та підвищити інвестиційну привабливість. Дослідження показують, що використання Power BI сприяє підвищенню ефективності бізнесу, зокрема, через інтеграцію з різними джерелами даних та можливості створення інтерактивних візуалізацій [1]. Крім того, поєднання Power BI з мовою програмування Python розширює аналітичні можливості, дозволяючи реалізовувати складніші моделі аналізу даних та машинного навчання [2].

Метою дослідження є розробка та апробація системи візуалізації та управління звітністю на основі інтеграції Power BI та Python для стартап-компаній, що забезпечить оптимізацію процесів аналізу даних, підвищення ефективності прийняття рішень та спрощення комунікації з інвесторами та клієнтами.

Об'єктом дослідження є процеси збору, аналізу та візуалізації бізнес-даних у стартап-компаніях різних галузей. Дослідження проводилось із застосуванням системного підходу до аналізу інформаційних потоків та експериментальної перевірки розроблених рішень.

У роботі використано платформу Microsoft Power BI для створення інтерактивних візуалізацій та Python з бібліотеками pandas, NumPy, scikit-learn для обробки даних і побудови прогностичних моделей. Для наукового обґрунтування результатів застосовано методи порівняльного аналізу та експериментальну перевірку ефективності на вибірці з декількох компаній з різних галузей та стадій

розвитку. Аналіз показує, що багато компаній витрачають понад 15 годин на тиждень на підготовку управлінської звітності, використовуючи переважно ручні методи обробки даних в електронних таблицях.

Існує пряма залежність між якістю візуалізації фінансових даних та швидкістю залучення інвестицій: стартапи з структурованими системами звітності закривають інвестиційні раунди набагато швидше порівняно з компаніями, що використовують неінтегровані інструменти.

Порівняльний аналіз інструментів бізнес-аналітики демонструє, що інтеграція Python та Power BI має найкраще співвідношення функціональності/вартість для стартапів з обмеженим бюджетом, забезпечуючи розширені можливості аналізу при мінімальних витратах на впровадження.

Критичними факторами успішного впровадження систем візуалізації у стартапах є: наявність чітко визначених ключових показників ефективності, структурованих джерел даних та базових компетенцій команди в роботі з аналітичними інструментами.

Концептуальна архітектура системи передбачає три взаємопов'язані модулі: збір та інтеграція даних з різних джерел за допомогою Python-скриптів; аналітична обробка з використанням алгоритмів машинного навчання; інтерактивна візуалізація в середовищі Power BI. На рис.1 представлено інтерфейс системи візуалізації даних у вигляді інтерактивного дашборду у Power BI та продемонстровано додаткові аналітичні можливості системи з деталізацією за категоріями.

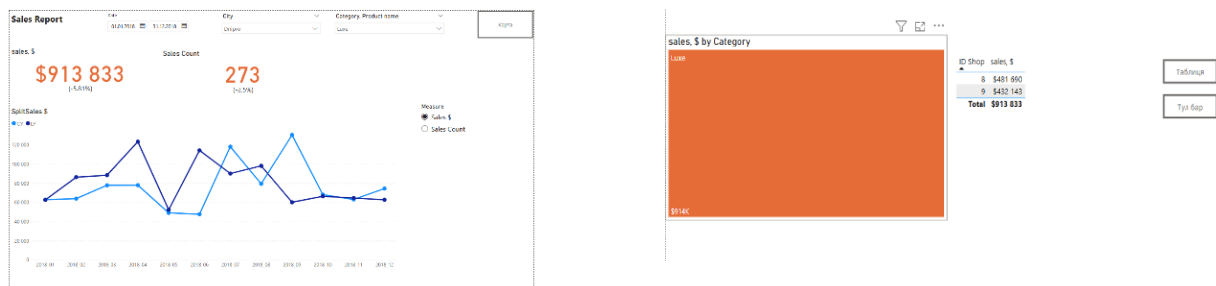


Рис. 1 Інтерфейс системи

Висновок. Запропонована інтеграція Power BI та Python є ефективним рішенням для стартапів, що дозволяє автоматизувати процеси збору, аналізу та візуалізації даних, оптимізуючи управління звітністю. Використання інтерактивних дашбордів та предиктивної аналітики сприяє підвищенню ефективності прийняття рішень та прискоренню залучення інвестицій. Розроблена концептуальна архітектура демонструє високу гнучкість та економічну доцільність для компаній з обмеженим бюджетом. Наукова новизна дослідження полягає у визначенні оптимальних підходів до інтеграції даних та адаптації аналітичних інструментів під специфіку стартап-проектів.

Список використаних джерел:

1. Pawashe, V. Startups get the big data power with Power BI. URL: <https://www.clariontech.com/blog/startups-get-the-big-data-power-with-power-bi> (Last accessed: 25.03.2025).
2. Microsoft. Create Power BI visuals using Python in Power BI Desktop. URL: <https://learn.microsoft.com/en-us/power-bi/connect-data/desktop-python-visuals> (Last accessed: 25.03.2025).

УДК 339.18-047.44:004.85(043.2)

АНАЛІЗ УСПІШНОСТІ ТОВАРІВ ТА ПРИБУТКОВОСТІ ІНТЕРЕНТ-МАГАЗИНУ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Євгеній Будков

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Тетяна Холявкіна, к.т.н., доц.*

Ключові слова: інтернет-магазин, електронна комерція, машинне навчання, прогнозування прибутковості, аналіз продажів, маржинальність, маркетингові стратегії, управління асортиментом, повернення товарів, персоналізація, big data.

Вступ. У наш час, в умовах шаленого розвитку електронної комерції досить часто інтернет-магазинам доводиться боротися з необхідністю результативного управління асортиментом товарів для підвищення рівня продажів та масштабування прибутковості бізнесу. Залучення до цього процесу машинного навчання надає підприємцям можливість аналізувати успішність продажів, знаходити певні закономірності в поведінці та вподобаннях клієнтів і прогнозувати майбутній прибуток. Дослідження базується на вивченні методів аналізу даних продажів і прогнозуванні прибутковості товарів у контексті мінімізації потенційних ризиків та оптимізації рекламних витрат.

Матеріали та методи

Дослідження базується на аналізі даних продажів інтернет-магазину за період з грудня 2023 року по грудень 2024 року. Було використано такі методи:

- Лінійна регресія для прогнозування прибутковості товарів;
- Кластеризація K-Means для сегментації товарів за популярністю;
- Random Forest для оцінки впливу різних факторів на результат продажів.

Дані містять параметри: артикул товару, категорія, маржинальність, кількість продажів, рейтинг користувачів, середній чек, витрати на рекламу та відсоток повернень (незаборів замовлень з пошти). Попередня обробка включала очищення від аномальних значень, нормалізацію показників та виявлення кореляцій між змінними.

Результати. Було проведено аналіз чинників, які впливають на прибутковість замовлень інтернет-магазину. Регресійна модель дала рівняння прогнозу прибутковості:

$$P = \left(S \times \frac{R}{5} \right) \times (P_{\text{од}} - C_{\text{од}}) - A - \left(\left(S \times \frac{R}{5} \right) \times P_{\text{од}} \times R_t \right)$$

де P – прогнозований прибуток, S – кількість продажів, R – рейтинг товару, A – витрати на рекламу, $P_{\text{од}}$ – вартість продажу одиниці, $C_{\text{од}}$ – собівартість одиниці, R_t – відсоток повернень

На основі кластеризації товарів (K-Means, $k = 3$) було виділено три групи:

1. **Успішні товари** (високий попит та маржинальність, низький рівень повернень).
2. **Потенційно-перспективні товари** (потенційно прибуткові при покращенні маркетингу).
3. **Нерентабельні товари** (низький попит, відсутність прибутку або вихід в мінус, високий рівень повернень).

Таблиця 1. Порівняльний аналіз кластерів товарів.

Кластер	Середня кількість продажів	Рейтинг	Витрати на рекламу	Відсоток повернень	Прибутковість
Успішні товари	150	4.8	10000	5%	45000
Потенційно-перспективні товари	80	4.2	6000	10%	18000
Нерентабельні товари	30	3.5	4000	20%	2000

Використання машинного навчання дозволяє зручно та швидко аналізувати продажі та прибутковість товарів інтернет-магазину. Проведений аналіз продемонстрував, що найбільший вплив на успішність товарів відіграє рейтинг, витрати на рекламу та маржинальність. В той час як відсоток повернень замовлень значно зменшує прибутковість магазину, незважаючи на велику кількість продажів.

Висновок. Проведене дослідження підтверджує той факт, що застосування машинного навчання в електронній комерції є ефективним та зручним інструментом для прогнозування прибутковості товарів. Зокрема, алгоритми регресійного аналізу та кластеризації допомагають оптимізувати асортимент і виявляти перспективні товари. Крім того, врахування відсотка повернень при обрахунку потенційної прибутковості є ключовим фактором для точнішого фінансового планування та розподілу рекламного бюджету, оскільки він має велике значення на результат.

Список використаних джерел:

1. Bishop C.M. Pattern Recognition and Machine Learning / C.M. Bishop. – Springer, 2006. – 738 с.
2. James G., Witten D., Hastie T., Tibshirani R. An Introduction to Statistical Learning / G. James, D. Witten, T. Hastie, R. Tibshirani. – Springer, 2013. – 426 с.
3. Пінцак І. Використання машинного навчання та аналізу даних для прогнозування тенденцій у електронній комерції / І. Пінцак // Науковий журнал. – 2024. – Вип. 1. – С. 45–52.

УДК 656.7:004.9

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ РЕСУРСАМИ АЕРОПОРТУ

Артем Буханенко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Апенько, к.т.н., доц.

Ключові слова: система управління, аеропорт, управління ресурсами, інформаційні технології, автоматизація.

Вступ. Сучасні аеропорти є складними інфраструктурними об'єктами, що вимагають ефективного управління ресурсами для забезпечення безперебійної роботи[1]. У праці розглядаються сучасні підходи до автоматизації процесів управління ресурсами аеропорту, які дозволяють зменшити витрати та підвищити ефективність роботи. Однак існує необхідність у створенні комплексної системи, що враховує специфічні вимоги аеропортів різного масштабу.

Матеріали та методи. Метою дослідження є розробка та аналіз інформаційної системи управління ресурсами аеропорту, що забезпечує централізоване управління основними логістичними та технічними процесами. У дослідженні використовувалися методи системного аналізу та математичного моделювання для розробки логіки функціонування системи. Система реалізована у вигляді програмного комплексу, що містить модулі управління персоналом, авіаційним транспортом, обслуговуючим транспортом, інвентарним ресурсом та паливним ресурсом. Для забезпечення взаємодії з іншими інформаційними системами аеропорту використані стандартизовані API.

Результати. Розробка інформаційної системи управління ресурсами аеропорту передбачала створення комплексного рішення, що дозволяє автоматизувати ключові процеси розподілу ресурсів та їх моніторинг у режимі реального часу. Основна увага приділялася гнучкості системи, її здатності адаптуватися до змін у робочому навантаженні та забезпеченню ефективної взаємодії між усіма службами аеропорту[2,3].

Розроблена система значно спрощує управління ресурсами та зменшує ризик виникнення конфліктів даних. Всі процеси розподілу персоналу, авіаційного транспорту, обслуговуючого транспорту та паливного ресурсу централізуються, що знижує ризик виникнення помилок і сприяє оперативному прийняттю рішень. Завдяки використанню централізованої бази даних і інтеграції з іншими інформаційними системами аеропорту, вдалося досягти більшої узгодженості між службами та зменшити час реагування на зміни у наявності та кількості ресурсів.

Під час моделювання роботи системи виявлено, що її використання дозволяє оптимізувати витрати на експлуатацію аеропортових ресурсів, оскільки зменшується кількість простоїв обладнання та покращується завантаженість технічних служб. Крім того, централізоване управління сприяє більш раціональному використанню інфраструктури аеропорту, що позитивно впливає на загальну ефективність його роботи. Таким чином, запропоноване рішення дозволяє створити єдине інформаційне середовище для управління всіма ключовими ресурсами аеропорту, забезпечуючи їх ефективний розподіл та мінімізуючи можливі затримки у виконанні операцій. Подальше вдосконалення системи може включати розширення її функціоналу, що дозволить ще більш точно планувати навантаження та адаптувати управлінські процеси до реальних умов експлуатації.

Висновок. Розроблена система управління ресурсами аеропорту забезпечує централізоване управління логістичними процесами та оптимізує використання ресурсів. Подальший розвиток системи може передбачати розширення функціоналу та інтеграцію з міжнародними платформами управління авіаційною інфраструктурою.

Список використаних джерел:

- 1.IATA (International Air Transport Association) Airport Development Reference Manua. URL: <https://www.scribd.com/document/742947545/IATA-Airport-Development-Reference-Manua-1-200/>.
- 2.Distributed systems: principles and paradigms. Книга, автор Ендрю Таненбаум. URL: https://vowi.fsinf.at/images/b/bc/TU_Wien-Verteilte_Systeme_VO_%28G%C3%B6schka%29_-_Tannenbaum-distributed_systems_principles_and_paradigms_2nd_edition.pdf
- 3.Hillier, F. S., & Lieberman, G. J. Introduction to Operations Research. URL: <https://bitshifters0.wordpress.com/wp-content/uploads/2015/03/intorduction-to-operations-research-7ed-hillier-lieberman-1240pp-mgh.pdf>

УДК 004.67:005.336.1(043.2)

ЯК ПРОГРАМНИЙ АНАЛІЗ ОБСЛУГОВУВАННЯ КОРИСТУВАЧІВ ПІДВИЩУЄ ЕФЕКТИВНІСТЬ УСТАНОВ

Микита Голодніков

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ігор Сябрук, ст. викл.

Ключові слова: програмний аналіз, обслуговування користувачів, ефективність установ, аналітичні системи, оптимізація ресурсів.

В сучасному світі швидко відбувається процес диджиталізації через що стрімко зростають обсягами даних, що генеруються в процесі обслуговування користувачів в державних і комерційних установах. Аналітика великих даних є ключовою технологією, що дозволяє установам оцінювати ризики та переваги різних стратегій, оптимізувати виробничі процеси, покращувати якість продукції та послуг, визначати переваги і потреби споживачів та багато іншого [1]. Використання аналітики у сфері менеджменту сприяє підвищенню ефективності персоналу та адаптації до сучасних цифрових рішень [2]. Також застосування аналітики у фінансовій сфері дає змогу покращити управління ризиками, витратами та ліквідністю компаній [3]. Програмний аналіз обслуговування користувачами стає важливим інструментом прийняття рішень та забезпечення ефективного розподілу ресурсів.

Метою роботи є висвітлення значення та переваг використання аналітики даних для підвищення ефективності державних і комерційних установ України.

Для наукового обґрунтування результатів досліджень, як аналіз даних впливає на підвищення ефективності установ використаний статистичний метод, а саме аналіз наукової роботи "ВПЛИВ АНАЛІТИЧНИХ ДАНИХ НА ЕФЕКТИВНІСТЬ ПІДПРИЄМСТВА" [1]. Дослідження також ґрунтується на аналізі графічних звітів світових і українських компаній з напрямку використання технологій аналізу даних.

Аналіз використання аналітики даних в українських галузях вказує на активне впровадження методів аналізу даних у всіх сферах [1]. Програмний аналіз суттєво впливає на роботу установ, сприяючи підвищенню їхньої ефективності, зокрема, зниженню адміністративних витрат, прискоренню обробки запитів користувачів та оптимізації управління ресурсною логістикою. Аналітичні системи позитивно впливають на продуктивність персоналу, забезпечують ефективний розподіл робочого навантаження та покращують якість управлінських рішень. Через застосування аналітичних систем спостерігається оптимізація фінансових процесів, а саме покращення прогнозування витрат, ефективніше планування бюджету, а також зниження фінансових ризиків. Компанії, які інтегрують аналітику даних, демонструють підвищену здатність адаптуватися до ринкових змін, що сприяє зміцненню їхньої позиції в умовах конкуренції. Компанія Amazon використовує технологію для аналізу даних про покупки, логістику, рекомендаційні системи та багато інших аспектів свого бізнесу. Google використовує технологію для обробки та аналізу даних, таких як пошукові запити, рекламні платформи, аналітика веб-трафіку та ін. IBM використовує технологію своїх рішень для аналізу та обробки даних, таких як аналітика бізнес-процесів, аналітика клієнтського досвіду, аналітика ринку та ін. Walmart використовує Big Data для аналізу

даних про продаж, логістику, а також для оптимізації поставок та управління запасами. Intel використовує Big Data для аналізу даних, пов'язаних із виробництвом, тестуванням та оптимізацією процесів виробництва [4].

Висновок. Програмний аналіз обслуговування користувачів відіграє ключову роль у підвищенні ефективності установ. Він є провідним інструментом у сучасному світі для підтримки та оптимізації надання послуг. Впровадження аналітичних інструментів сприяє розвитку організацій та підсилює їхні позиції в конкурентному середовищі.

Список використаних джерел:

1. Стеценко, О., & Бобров, Є. (2024). ВПЛИВ АНАЛІТИЧНИХ ДАНИХ НА ЕФЕКТИВНІСТЬ ПІДПРИЄМСТВА. Вчені записки Університету «КРОК», (4(76), 22–29. <https://doi.org/10.31732/2663-2209-2024-76-22-29>
2. Дороніна О., & Алярова А. (2020). АНАЛІТИКА ВЕЛИКИХ ДАНИХ ЯК ПРОГРЕСИВНИЙ ІНСТРУМЕНТ МЕНЕДЖМЕНТУ ПЕРСОНАЛУ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ. Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки) №1(41), 2020. <https://doi.org/10.31388/2519-884X-2020-41-174-182>
3. Супруненко С.А., Чорновол А.О., Гаврилюк В.М., 2024. ВИКОРИСТАННЯ АНАЛІТИКИ ДАНИХ ДЛЯ УПРАВЛІННЯ ФІНАНСОВИМИ ПРОЦЕСАМИ В ЦИФРОВОМУ СЕРЕДОВИЩІ УКРАЇНИ. ЕКОНОМІКА ТА СУСПІЛЬСТВО. <https://doi.org/10.32782/2524-0072/2024-62-51>

УДК 004.77:612.014.461(043.2)

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ВОДНОГО БАЛАНСУ НА ОСНОВІ АНАЛІЗУ ФІЗІОЛОГІЧНИХ ДАНИХ

Юрій Дядюк

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Холявкіна, к.т.н., доц.

Ключові слова: гідратація, інтелектуальна система, моніторинг водного балансу, веб-застосунок, персоналізовані рекомендації.

Вступ. Вода відіграє ключову роль у підтримці життєдіяльності людини, впливаючи на фізичне та когнітивне здоров'я. Проте багато людей нехтують достатнім рівнем гідратації, що може призводити до проблем зі здоров'ям. Існуючі рішення для контролю водного балансу часто не враховують індивідуальні фізіологічні параметри та стан здоров'я користувача. У зв'язку з цим розробка інтелектуальної системи, яка аналізуватиме фізіологічні показники та формуватиме персоналізовані рекомендації щодо споживання води, є актуальною проблемою.

Метою дослідження є створення веб-застосунку для моніторингу водного балансу, який використовує аналіз фізіологічних даних для персоналізації рекомендацій щодо гідратації.

Матеріали та методи. Дослідження базується на розробці веб-застосунку для моніторингу водного балансу. Використано такі методи:

- **Аналіз фізіологічних даних** – визначення добової потреби у воді з урахуванням ваги, рівня фізичної активності та стану здоров'я.
- **Розробка алгоритму персоналізованих рекомендацій** – застосування коригувальних коефіцієнтів для адаптації розрахунків до індивідуальних потреб користувача.
- **Веб-технології** – використання React для створення інтерфейсу, Node.js та Express.js для обробки серверних запитів, MongoDB для збереження даних.

• **Візуалізація результатів** – відображення списку споживання та інтеграція календаря для аналізу споживання води за певний період.

Результати. Розроблена система контролю водного балансу дозволяє автоматично розраховувати добову норму води на основі фізіологічних показників користувача. Алгоритм враховує стать, масу тіла та рівень фізичної активності, що дозволяє персоналізувати рекомендації та зробити їх максимально точними.

Для розрахунку добової потреби у воді використовуються такі формули:

- **Для жінок:** $V = (M \times 0,03) + (T \times 0,4)$
- **Для чоловіків:** $V = (M \times 0,04) + (T \times 0,6)$

Де: V – рекомендований обсяг води (літри на день), M – маса тіла (кг), T – час активного заняття спортом або іншої інтенсивної фізичної діяльності (години). Цей підхід дозволяє адаптувати норму води залежно від індивідуальних характеристик користувача.

Також було проаналізовано певні захворювання, які потребують коригування воб'ємі споживої води:

- **Діабет (1 та 2 тип)** – +0,5 л води на добу.
- **Серцеві захворювання** – -0,5 л води на добу.
- **Ниркові захворювання** – -0,5 л води на добу.
- **Гіпертонія (високий артеріальний тиск)** – -0,3 л води на добу.
- **Інфекційні захворювання та гарячка** – +0,5 л води на добу.
- **Під час вагітності та грудного вигодовування** – +0,7 л води на добу.

Висновок. Розроблений веб-застосунок для моніторингу водного балансу забезпечує персоналізовані рекомендації щодо гідратації на основі індивідуальних фізіологічних параметрів та стану здоров'я. Отримані результати можуть бути застосовані для покращення контролю за водним балансом і профілактики захворювань, пов'язаних з порушеннями гідратації.

Список використаних джерел:

1. Що таке водний баланс і чому він потрібен, 2020 [Електронний ресурс]. – Режим доступу: <https://eventukraine.com/health/shcho-take-vodniy-balans-i-chomu-treba-dotrimuvatisya-pitnogo-rezhimu/> – Назва з екрана. (Last accessed: 10.03.2025).
2. Good hydration may reduce long-term risks for heart failure, 2022 [Електронний ресурс]. – Режим доступу: <https://www.nhlbi.nih.gov/news/2022/good-hydration-may-reduce-long-term-risks-heart-failure> – Назва з екрана. (Last accessed: 10.03.2025).
3. «Як підтримувати водний баланс?», 2021 [Електронний ресурс]. – Режим доступу: <https://balanceinstitute.com.ua/diyetologiya/yak-pidtrymuvaty-vodnyj-balans> – Назва з екрана. (Last accessed: 11.03.2025).
4. «How Much Water Should You Drink Per Day?», 2023 [Електронний ресурс]. – Режим доступу: <https://www.healthline.com/nutrition/how-much-water-should-you-drink-per-day> – Назва з екрана. (Last accessed: 11.03.2025).
5. «Is Drinking More Water Actually Healthy? Maybe.», 2024 [Електронний ресурс]. – Режим доступу: <https://www.webmd.com/diet/news/20241210/drinking-water-actually-healthy-maybe> – Назва з екрана. (Last accessed: 11.03.2025).

УДК 624.21.097(043.2)

СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДЛЯ ШЛАГБАУМІВ "N-GATE"

Антон Жолобецький, Роман Степанюк

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олена Охремчук, асистент

Ключові слова: контроль доступу, шлагбаум, дистанційне управління, безпека об'єктів, автоматизація доступу, IOT, MQTT.

Вступ. Контроль доступу до територій є важливою частиною безпеки та зручності в житлових комплексах, офісних будівлях і паркінгах. Сучасні рішення часто обмежуються стандартними функціями без урахування потреб користувачів та адміністраторів. Розробка системи, яка поєднує зручний інтерфейс для користувачів із потужними інструментами адміністрування, є актуальною задачею.

Метою дослідження є створення системи контролю доступу "N-GATE" для управління шлагбаумами та точками проїзду з урахуванням потреб користувачів і адміністраторів.

Матеріали та методи.

Дослідження базується на розробці системи контролю доступу для шлагбаумів. Об'єктом дослідження є пункти проїзду (шлагбауми, ворота) та їх взаємодія з користувачами й адміністраторами. Використано такі методи:

- Аналіз функціональних вимог – визначення потреб користувачів (відкриття шлагбаумів, запит доступу) та адміністраторів (управління локаціями, історія).
- Проєктування архітектури – розробка клієнт-серверної системи з використанням сучасних вебтехнологій.
- Frontend: TypeScript, React, Zustand, Vite, Tailwind CSS, Ant Design, Axios.
- Backend: Python, FastAPI, PostgreSQL, SQLAlchemy, MQTT, JWT-авторизація.
- Тестування системи в різних умовах експлуатації

Результати. Розроблена система "N-GATE" забезпечує ефективний контроль доступу до шлагбаумів і воріт.

Основні можливості для користувачів:

- Перегляд доступних точок доступу на головному екрані додатка.
- Дистанційне відкриття шлагбаумів через кнопку "ВІДКРИТИ".
- Запит доступу до нових локацій шляхом введення коду локації.
- Управління профілем із редагуванням особистих даних (телефон, номери автомобілів).

Для адміністраторів реалізовано:

- Обробку запитів на доступ від користувачів.
- Створення та редагування локацій, точок доступу з налаштуванням параметрів.
- Перегляд історії використання (час, користувачі).
- Управління списком користувачів із можливістю їх редагування чи видалення.

Система побудована на основі клієнт-серверної архітектури. Frontend забезпечує інтуїтивний інтерфейс, а backend обробляє запити та бізнес-логіку, зберігає дані в PostgreSQL. Безпека забезпечена за допомогою контролю доступу користувачів до об'єктів, JWT-авторизації та HTTPS протоколом.

Висновок. Система "N-GATE" пропонує зручне рішення для контролю доступу до шлагбаумів, поєднуючи персоналізований підхід для користувачів із гнучкими інструментами адміністрування. Її можна застосовувати для підвищення безпеки та комфорту на об'єктах із регульованим доступом.

Список використаних джерел:

1. Security of Building Automation and Control Systems: Survey and future research directions, 2022. URL: <https://doi.org/10.1016/j.cose.2021.102527>.
2. A systematic literature review for authorization and access control: definitions, strategies and models, 2022. URL: <https://doi.org/10.1108/IJWIS-04-2022-0077> (Last accessed: 10.03.2025).
3. Enhancing JWT Authentication and Authorization in Web Applications Based on User Behavior History, 2023. URL: <https://doi.org/10.3390/computers12040078> (Last accessed: 11.03.2025).
4. Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance, 2024. URL: <https://doi.org/10.3389/frai.2024.1397480> (Last accessed: 11.03.2025).
5. Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN, 2023. URL: <https://doi.org/10.1016/j.csa.2023.100015> (Last accessed: 11.03.2025).

УДК 004.056

АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Богдан Кобільник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Вікторія Сидоренко, к.т.н., доц.

Ключові слова: критична інформаційна інфраструктура; нормативно-правове забезпечення; SWOT-аналіз; інформаційна безпека.

Цифровізація та гібридна агресія створюють нові загрози для інформаційної безпеки, що особливо актуально для проектування захищеної критичної інформаційної інфраструктури (КІІ) держави. Сьогодні, зростання кількості загроз, пов'язаних із розвитком інформаційних технологій, підвищує необхідність впровадження нових нормативно-правових рішень, які будуть актуальними в умовах сучасних викликів та ведення війни.

Нормативно-правова база України включає Закон «Про критичну інфраструктуру» (2021) та інші документи, що регулюють кібербезпеку, зокрема Стратегію кібербезпеки України (2021–2025), яка окреслює основні напрямки захисту критичних інформаційних систем. Крім того, прийнято численні підзаконні акти, що встановлюють стандарти захисту, категоризацію об'єктів, моніторинг безпеки, аудит, обмін інформацією про кіберінциденти та ведення державного реєстру КІІ [1].

Дослідження спрямоване на аналіз нормативно-правового забезпечення у сфері проектування захищеної критичної інформаційної інфраструктури держави з визначенням сильних і слабких сторін, можливостей і загроз за допомогою проведення SWOT-аналізу.

SWOT-аналіз нормативно-правового забезпечення у сфері проектування захищеної критичної інформаційної інфраструктури держави

Серед сильних сторін (**Strengths**) слід відзначити наявність спеціалізованого законодавства, яке вперше визначає поняття критичної інфраструктури та обов'язки суб'єктів, а також розвинену підзаконну базу з затвердженими вимогами і процедурами кіберзахисту. Додатково, створено ефективні координаційні механізми із залученням кращих міжнародних практик, що сприяє стабільному функціонуванню системи захисту та створенню основи для подальшого розвитку нормативно-правової бази.

Серед слабких сторін (**Weaknesses**) спостерігається неповна імплементація нормативної бази – практичні механізми, такі як реєстр об'єктів та аудит, перебувають у стадії впровадження. Виявлено також законодавчі прогалини щодо довгострокового розвитку та фінансування КІІ, нечіткий розподіл повноважень між суб'єктами, обмежені матеріальні та кадрові ресурси, а також недостатньо розвинені механізми відповідальності за невиконання вимог. Ці недоліки створюють ризики для неефективного застосування нормативних положень та можуть перешкоджати оперативному реагуванню на сучасні загрози.

Щодо можливостей (**Opportunities**), адаптація міжнародного досвіду, впровадження норм ЄС і НАТО у сфері захисту КІІ, а також підтримка союзників сприяють модернізації нормативної бази. Післявоєнне відновлення та розвиток державно-приватного партнерства, поряд із зростанням обізнаності суспільства про важливість кібербезпеки, відкривають нові перспективи для вдосконалення законодавства. Використання цих можливостей дозволить не лише модернізувати нормативно-правову базу, а й підвищити рівень національної кібербезпеки.

Зовнішні загрози (**Threats**) включають триваючу агресію та спрямовані кібератаки, що створюють високий рівень ризику для критичної інфраструктури. Крім того, стрімка еволюція кіберзагроз може випереджати оновлення законодавства, а економічні й політичні обмеження, людський фактор та залежність від імпортованих технологій залишаються важливими викликами. Ці фактори потребують негайного реагування та стратегічного планування для мінімізації потенційних наслідків для системи захисту [2-4].

Висновок. Результати проведеного аналізу нормативно-правового забезпечення у сфері проектування захищеної критичної інформаційної інфраструктури держави свідчать про існування базових механізмів для забезпечення певного рівня кібербезпеки, але також показують суттєві недоліки, що потребують оперативного удосконалення. Крім того, продовженням дослідження стане використання визначених у дослідженні можливостей, а саме адаптації міжнародного досвіду, впровадження норм ЄС для підвищення рівня національної кібербезпеки КІІ держави.

Список використаних джерел:

- 1.Melnyk, D. (2022). Захист національної критичної інфраструктури: актуальні проблеми та шляхи їх вирішення. *Адміністративне право і процес*, 3(38), 5–16.
- 2.Kudryashov, V. (2021). Державне регулювання критичної інфраструктури. *Фінанси України*, 7, 72–92.
- 3.Petrunenko, I. (2022). Regulation of cybersecurity of Ukraine's critical infrastructure: Legal aspects and standards of sustainable protection. *Law, Business and Sustainability Herald*, 2(3), 42–57.
- 4.Sokiran, M. (2021). Basic principles of public administration of critical information infrastructure: The example of Ukraine. *Advanced Space Law*, 7, 63–72.

УДК 004.77-045.43(043.2)

РОЛЬ АДАПТИВНОГО ДИЗАЙНУ У ПІДВИЩЕННІ КОНВЕРСІЇ ІНТЕРНЕТ-МАГАЗИНІВ

Олеся Кузьмич

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Тетяна Холявкіна, к.т.н., доц.*

Ключові слова: адаптивний вебдизайн, UX, Elementor, конверсія, мобільна оптимізація.

Вступ. Адаптивний вебдизайн є важливим елементом успішного інтернет-магазину, оскільки впливає на досвід користувачів та їхнє рішення щодо покупки. Важливість адаптивного дизайну зумовлена необхідністю оптимізації вмісту під різні пристрої та роздільну здатність екранів. Зі зростанням частки мобільного трафіку в електронній комерції оптимізація сайту під різні пристрої стає необхідністю для покращення конверсії. Адаптивний дизайн та продумана кольорова гамма сприятимуть вирішенню проблеми зниження відмов – тобто вони можуть збільшити час, який користувач проводить на сайті, та покращити конверсію – тобто відсоток відвідувачів, які здійснили покупку. Це важливо для досягнення успіху в електронній комерції та підвищення конкурентоспроможності магазину на ринку [1, 2].

Матеріали та методи. У дослідженні застосовувалися методи аналізу інтернет-магазинів, які використовують адаптивний дизайн, зокрема на платформі Elementor. Було проведено оцінку швидкості завантаження, рівня відмов, показника утримання користувачів та зручності навігації. Розглянуто ключові аспекти UI/UX-дизайну, що впливають на поведінку користувачів, зокрема кольорову гаму, розташування елементів та інтерактивність сайту. Застосування адаптивного дизайну безпосередньо впливає на зручність користувачів, що відображається у покращенні показників конверсії. Згідно з дослідженнями, спрощення навігації, зменшення часу завантаження сторінок і впровадження інтуїтивного UX-дизайну знижують рівень відмов на 20–30%.

Приклади впливу адаптивного дизайну на продажі:

- Amazon – завдяки покращенню адаптивного дизайну сайту вдалося скоротити час завантаження сторінки на 1 секунду, що призвело до збільшення доходу на 1.6 млрд доларів на рік.
- ASOS – редизайн мобільної версії сайту з урахуванням адаптивності сприяв підвищенню мобільних продажів на 30%.

Аналіз інтернет-магазинів продемонстрував, що оптимізація інтерфейсу для мобільних пристроїв сприяє підвищенню середнього часу перебування на сайті, що позитивно впливає на конверсію.

Висновок. Узагальнюючи, адаптивний дизайн є ключовим елементом розробки сучасних інтернет-магазинів, оскільки він забезпечує зручність і ефективність користування сайтом для широкого кола користувачів, підвищує їхній задоволення від покупок та сприяє успішності бізнесу в онлайн-сфері [3]. Інструменти, такі як Elementor, забезпечують просте та ефективне налаштування адаптивного інтерфейсу, що робить електронну комерцію доступнішою для широкого загалу підприємців.

Список використаних джерел:

1. Грабовський Ю. Проектування інтелектуального користувацького інтерфейсу для систем електронної підтримки освіти. ScienceRise. 2018. № 11. С. 36–39.
2. Грабовський Ю. Методи розроблення сайту івент-агентства. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. Т. 4. № 70. С. 70–76.
3. Грабовський Є. Методи створення мультимедійної онлайн-галереї. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. Т. 2, № 68. С. 102–107.

УДК 004.8(043.2)

ДОСЛІДЖЕННЯ ТОЧНОСТІ СИСТЕМ АВТОМАТИЗОВАНОГО ТАЙМ-ТРЕКІНГУ ТА ВИЯВЛЕННЯ СПОСОБУ ЇЇ ПІДВИЩЕННЯ

Власта Мельник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Холявкіна, к.т.н., доц.

Ключові слова: штучний інтелект, тайм-трекінг, аналіз, діяльність.

Вступ. Сучасна світова обстановка призвела до того, що більшість професій було переведено у дистанційний формат. Окрім того, нині присутній культ саморозвитку: кожен прагне стати кращою версією себе. Наслідком цього стало збільшення попиту на засоби для контролю витраченого часу, зокрема, автоматизоване ведення обліку часу – тайм-трекінг.

Матеріали та методи.

Для дослідження, обрано популярні засоби для тайм-трекінгу, а саме:

- Toggl Track;
- Clockify;
- Time Doctor;
- RescueTime;

Для дослідження точності систем автоматизованого тайм-трекінгу були застосовані емпіричний метод тестування програм, порівняльний метод аналізу їхніх характеристик, статичний метод вивчення документації.

Результати. Виконання завдання автоматизованого тайм-трекінгу потребує моніторингу активності користувача: класифікацію відвідуваних вікон та вебсторінок на контексті їх призначення та діяльності користувача, а також відстеження тривалості будь-яких виконаних з ними дій, враховуючи період неактивності.

Зазвичай, класифікація відбувається за рахунок великої бази даних, що понижує точність результатів тайм-трекінгу, адже не дозволяє врахувати особливості поточної виконуваної задачі та увесь контекст роботи.

Наприклад, користувач зазначив, що розробляє комп'ютерні ігри за допомогою мови C# в Unity. У такому разі, засіб для автоматизованого тайм-трекінгу враховуватиме лише ті ресурси, які стосуються безпосередньо зазначених технологій, проте, не братиме до уваги, наприклад, дослідження користувачем реалізації потрібних модулів для гри за допомогою інших технологій. Такий підхід не є інтелектуальним та гнучким, і як результат, спотворює справжні дані. Це пов'язано з тим, що система

автоматизованого тайм-трекінгу не має ніяких даних стосовно реальних проєктів користувача. З метою підвищення ефективності систем автоматизованого тайм-трекінгу варто впровадити розширений аналіз діяльності користувача шляхом вивчення контенту, який він створює та його взаємодії з іншими ресурсами. Це дозволить підвищити точність результатів роботи систем для тайм-трекінгу.

За допомогою використання штучного інтелекту призначеного для аналізу та створення графічних зображень, можна виявити, що в поточний момент ілюстратор малює дерево. На основі цього, система автоматизованого тайм-трекінгу може аналізувати та виявляти зв'язки між створеними елементами та відвідуваними вебресурсами — наприклад, якщо визначено що користувач шукає інформацію та зображення про структуру кори або анатомію листя, то такі дії можна автоматично класифікувати як робочі. Те ж саме стосується і файлів будь-якого іншого типу.

Висновок. Проведене дослідження дозволяє визначити шляхи покращення точності систем автоматизованого тайм-трекінгу. Впровадження комплексного інтелектуального аналізу поточних проєктів користувача та їхнього взаємозв'язку з іншими інформаційними ресурсами, а не лише сфери діяльності дозволяє забезпечити кращі результати роботи систем автоматизованого тайм-трекінгу.

Список використаних джерел:

1. Toggl. Toggl Track: програмне забезпечення для відстеження часу [Електронний ресурс] – Режим доступу: <https://toggl.com/> – Назва з екрана. (Last accessed: 16.03.2025).
2. Clockify. Clockify: безкоштовне програмне забезпечення для відстеження часу [Електронний ресурс] – Режим доступу: <https://clockify.me/> – Назва з екрана. (Last accessed: 16.03.2025).
3. Time Doctor. Time Doctor: програмне забезпечення для відстеження часу працівників [Електронний ресурс] – Режим доступу: <https://www.timedoctor.com/> – Назва з екрана. (Last accessed: 16.03.2025).
4. RescueTime. RescueTime: інструмент управління часом і продуктивністю [Електронний ресурс] – Режим доступу: <https://www.rescuetime.com/> – Назва з екрана. (Last accessed: 16.03.2025).
5. ШІ: хто твій батько? Історія розвитку та види штучного інтелекту. URL: <https://highload.tech/uk/shi-hto-tvij-batko-istoriya-rozvitku-ta-vidi-shtuchnogo-intelektu/> – Назва з екрана. (Last accessed: 17.03.2025).

УДК 004.946.5.056(043.2)

КІБЕРБЕЗПЕКА У ЦИФРОВОМУ СУСПІЛЬСТВІ: НОВІ ЗАГРОЗИ ТА СТРАТЕГІЇ ЗАХИСТУ

Ніколь Міщинська

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Холявкіна, к.т.н., доц.

Ключові слова: кіберзагрози, цифрова безпека, криптографія, атаки, протидія.

Розвиток цифрових технологій ускладнює кіберзагрози, що вимагає вдосконалення методів захисту інформаційного простору. Зростання атак АРТ (Advanced Persistent Threats) демонструє використання кіберпростору для політичного протистояння, а атаки на критичну інфраструктуру стали засобом гібридної війни [1].

Вступ. Сучасні загрози включають не лише DDoS та фішинг, а й складніші методи компрометації, зокрема маніпуляції нейромережами та використання квантових алгоритмів для зламу криптографії [2].

Постквантова криптографія ставить нові вимоги до безпеки даних, оскільки традиційні алгоритми (RSA, ECC) можуть втратити стійкість [3].

Матеріали та методи. Дослідження ґрунтується на контент-аналізі нормативних документів (ISO/IEC 27001, NIST SP 800-53), аналітичних звітів та випадків атак APT, DDoS, експлуатації вразливостей. Розглянуто концепції Zero Trust, машинного навчання у виявленні загроз, DevSecOps, а також стратегії кіберзахисту ЄС, США та України.

Результати. Аналіз основних векторів атак показує, що значна частина інцидентів пов'язана з людським фактором: інсайдерськими загрозами, соціальною інженерією та низьким рівнем цифрової гігієни [4]. Для зниження кіберризиків необхідний багаторівневий підхід, що включає Zero Trust-архітектуру, AI-аналіз поведінкових аномалій у трафіку та дотримання міжнародних стандартів кібербезпеки (ISO/IEC 27001, NIST SP 800-53) [5].

Особливу увагу слід приділити безпеці хмарних сервісів, адже уразливості в ланцюгах постачання ПЗ (наприклад, атака Sunburst у 2020 році) залишаються однією з головних загроз [7]. Використання Secure by Design і DevSecOps дозволяє мінімізувати ці ризики через автоматизований контроль безпеки [8].

Протидія кібератакам на державному рівні вимагає міжнародної координації, проте ефективність таких ініціатив, як Будапештська конвенція та NIS2, обмежується відмінностями у законодавстві [9]. Враховуючи автоматизацію атак та зростання загроз, кібербезпека має стати фундаментальним елементом цифрової інфраструктури, що потребує безперервної модернізації [10].

Висновок. Аналіз сучасних кіберзагроз показав зростання складності атак та необхідність впровадження багаторівневих стратегій захисту, таких як Zero Trust, DevSecOps та постквантова криптографія. Ефективна кібербезпека потребує безперервного моніторингу, адаптації до нових загроз та міжнародної координації.

Список використаних джерел:

1. Mindscope.biz.ua. (n.d.). Кібербезпека в епоху цифрової трансформації: Виклики та перспективи. Retrieved March 11, 2025, from <https://mindscope.biz.ua/kiberbezpeka-v-epohu-cyfrovyi-transformaciyi-vyklyky-ta-perspektyvy/> (date of access: 14.03.2025).
2. ResearchGate. (n.d.). Кібербезпека в цифровому навчальному середовищі. Retrieved March 11, 2025, from https://www.researchgate.net/publication/332716122_KIBERBEZPEKA_V_CIFROVOMU_NAVCALNOMU_SEREDOVISI (date of access: 14.03.2025).
3. Рада національної безпеки і оборони України. (2021). Проект Стратегії кібербезпеки України (2021–2025 роки). Retrieved March 11, 2025, from https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (date of access: 12.03.2025).
4. Програма розвитку ООН в Україні. (n.d.). Кращі практики управління кібербезпекою. Retrieved March 11, 2025, from https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf (date of access: 14.03.2025).
5. Капітон, А. М., & Прокудін, А. Ю. (n.d.). Кібербезпека в епоху цифрової трансформації. Житомирський державний технологічний університет. Retrieved March 11, 2025, from <https://conf.ztu.edu.ua/wp-content/uploads/2024/01/72.pdf> (date of access: 13.03.2025).
6. Вісник Хмельницького національного університету. (n.d.). Сучасні підходи до дослідження кібербезпеки та кібергігієни. Retrieved March 11, 2025, from <https://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/07/vknu-ts-2023-n3321-210-213.pdf> (date of access: 12.03.2025).
7. Запорізький національний університет. (n.d.). Кібербезпека та інформаційна безпека. Retrieved March 11, 2025, from https://moodle.znu.edu.ua/pluginfile.php/1275463/mod_resource/content/1/01_2_%D0%9F%D1%80%D0%B5%D0%B7%D0%B5

[%D0%BD%D1%82%D0%B0%D1%86%D1%96%D1%8F_%D0%B4%D0%BE_%D1%82%D0%B5%D0%BC%D0%B8_1.pdf](#) (date of access: 14.03.2025).

8. Coordynata.com.ua. (n.d.). Сучасні тенденції правового регулювання кібербезпеки та інтелектуальна власність. Retrieved March 11, 2025, from <https://coordynata.com.ua/sucasni-tendencii-pravovogo-reguluvanna-kiberbezpeki-ta-intelektualna-vlasnist> (date of access: 13.03.2025).

9. Стендер, С. В., Фротер, О. С., & Снітко, Ю. М. (2023). Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. Академічні візії, (26). Retrieved March 11, 2025, from <https://academy-vision.org/index.php/av/article/download/799/725/733> (date of access: 12.03.2025).

10. Academia.edu. (n.d.). Кібербезпека та кібергігієна: нова ера цифрових технологій. Retrieved March 11, 2025, from <https://www.academia.edu/98205745/> (date of access: 14.03.2025).

УДК 621.396.96

ПЕРСПЕКТИВИ ПІДВИЩЕННЯ АВТОНОМНОСТІ РОБОТИЗОВАНИХ ПЛАТФОРМ

Ігор Попов, Олексій Губський

Інститут інформаційних технологій та систем НАН України, Київ

Науковий керівник – Олександр Волков, к.т.н.

Ключові слова: автономність, роботизовані платформи, штучний інтелект, навігація.

Вступ. Автономні платформи є важливими для безпечного транспортування людей без залучення додаткового персоналу. Впровадження технологій штучного інтелекту (ШІ), машинного навчання (МН) та сенсорних систем дозволяє підвищити їхню автономність.

Мета: аналіз та розробка підходів до підвищення автономності платформ, що використовуються для транспортування людей у надзвичайних ситуаціях.

Матеріали та методи: Автономність платформ залежить від впровадження сучасних інтелектуальних систем керування. Поєднання алгоритмів машинного навчання, планування траєкторій та прогнозування поведінки середовища дозволяє підвищити ефективність їхньої роботи. Зокрема, комбінуючи класичні методи оптимізації з нейромережевими моделями аналізу даних можливо швидко адаптувати маршрути, а й передбачати потенційні ризики.

Розроблена класифікація SAE щодо ступеня автоматизації, де вищий ступінь збільшує кількість сценаріїв, які повинен розв'язати роботизована платформа. Незалежно від ступеня автоматизації, розробки, застосовані для автономного руху, можна згрупувати в три великі категорії: сприйняття, прийняття рішень і контроль, що підтверджується даними, отриманими від датчиків і засобів зв'язку платформи, що також дозволяє кооперативне водіння. [1]

Для підвищення автономності можливе поєднання методів МН та алгоритмів планування руху. Це дає змогу аналізувати та враховувати зміни середовища при прокладанні оптимального маршруту. Перспективним є використання гібридних алгоритмів, що поєднують класичне планування траєкторій із нейромережевими моделями прогнозування.

На практиці застосування одного типу датчиків не може гарантувати надійність результатів для різних сценаріїв. Тому поєднують кілька датчиків, щоб виявити перешкоди за допомогою їх злиття [2].

Застосування лідара, акустичних датчиків та камер забезпечує точне позиціювання в просторі та вчасне реагування на зміну умов руху.

Головним завданням є розробка систем, здатних автономно адаптуватися до мінливості середовища, складного контролю, систем зв'язку та ШІ на основі нейронних мереж. [3]. Особливу увагу слід приділити надійності зв'язку, що має зберігати стабільність навіть в умовах електронних перешкод або відсутності традиційних мережевих інфраструктур.

Платформи повинні бути адаптовані до роботи в умовах поганої видимості, пересіченій місцевості та швидко змінюваних зовнішніх умов. Це вимагає високої гнучкості в навігаційних системах та здатності до автономного коригування маршруту з урахуванням змін оточення. Крім того, для забезпечення безпеки платформ необхідно реалізувати надійний захист зв'язку від перехоплення сигналів керування та несанкціонованого втручання. Це включає використання шифрування даних, захищених протоколів зв'язку та механізмів, здатних виявляти загрози в реальному часі.

Результати. Враховуючи описані вище виклики та обмеження до роботизованих платформ при подальшому розвитку слід придати підвищену увагу часу на адоптацію системи до зміни умов зовнішнього середовища. Оскільки автономне ухвалення рішень, що базується на багаторівневих нейромережах, здатних самостійно реагувати на критичні ситуації лишається вразливим в момент переходу між моделями навігації.

Пропонується для моделювання автономної навігації до формули оптимального маршруту додати окремий елемент – час на адоптацію до змінних умов середовища:

$$T = \sum_{i=1}^n \frac{d_i}{v_i} + \sum_{j=1}^m P_j + C$$

де T – загальний час подолання маршруту, d_i – відстань на кожному відрізку шляху, v_i – швидкість на відповідному відрізку, P_j – час затримки на перешкодах або необхідних зупинках, а C – додатковий час на адаптацію до змінних умов середовища.

Висновок. Підвищення автономності роботизованих платформ є ключовим напрямом у сфері рятувальних технологій. Використання сучасних інтелектуальних систем, та безпечних комунікаційних технологій дозволить значно підвищити ефективність рятувальних операцій. Запровадження новітніх підходів до керування та навігації зробить ці системи більш надійними та стійкими до зовнішніх загроз.

Список використаних джерел:

1. Clavijo M, Jiménez F, Naranjo JE. The Development and Prospects of Autonomous Driving Technology. Applied Sciences. 2023; 13(9):5377. <https://doi.org/10.3390/app13095377>
2. Li W, Gu J, Liu J, Cheng B, Zhu H, Miao Y, Guo W, Jiang G, Wu H, Song W. A Review of Key Technological Developments in Autonomous Unmanned Operation Systems for Agriculture in China. AgriEngineering. 2025; 7(3):71. <https://doi.org/10.3390/agriengineering7030071>
3. T.Kadylnykova, O.Honchar, M.Dalik Ground Autonomous Platforms: Current State and Development Perspectives Vol. 2 (2024): Challenges and Issues of Modern Science <https://cims.fti.dp.ua/j/article/view/150>

УДК 656.7:044.22:044.42

ЗАСОБИ ПІДТРИМКИ ПРОЦЕДУР ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЛІТАКІВ. РОЗРОБКА ЗАХИЩЕНОЇ СЕРВЕРНОЇ ЧАСТИНИ ВЕБ ПРИКЛАДЕННЯ НА АРХІТЕКТУРИ REST API

Олександр Пшеничко, Ярослав Сандул

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Вадим Сураєв, к.т.н., доц.

Ключові слова: технічне обслуговування літаків, автоматизовані інформаційні системи, електронна пошта, серверна частина веб прикладення, REST API.

Вступ. Технічне обслуговування літаків є невід'ємною частиною роботи авіакомпанії, що забезпечує безпеку польотів та ефективність експлуатації авіатехніки. В сучасних умовах розвитку інформаційних технологій важливим аспектом забезпечення технічного обслуговування авіаційної техніки є впровадження автоматизованих інформаційних систем, які дозволяють підвищити швидкість і точність обробки даних, знизити ймовірність людських помилок та забезпечити своєчасне проведення необхідних технічних процедур та звітність. Серверна частина веб прикладення системи технічного обслуговування літаків має виконувати важливу роль в обробці запитів, зберіганні та обробці даних, а також взаємодії з іншими компонентами інформаційної системи. Вона забезпечує доступ до необхідної інформації, що стосується технічного стану літаків, обслуговування, історії ремонтів та інших важливих аспектів, що впливають на безперебійну роботу авіатехніки.

Мета. Розробка та впровадження автоматизованої та захищеної серверної частини на архітектурі REST API, що забезпечує інформацією процедури технічного обслуговування літаків авіакомпанії.

Матеріали та методи розробки

Для розробки серверної частини веб-застосунку підтримки технічного обслуговування літаків обрано мову програмування Python з фреймворком FastAPI для створення REST API. Дані пропонується зберігати у реляційній базі PostgreSQL із застосуванням бібліотек SQLAlchemy та Alembic. Використання цих бібліотек дозволить ефективно працювати з базою даних, а також надасть надійні міграції схеми бази, що буде корисно для розвитку системи у майбутньому.

Для автентифікації та авторизації можна використати JSON Web Token (JWT). Задля покращення продуктивності має бути реалізовано кешування запитів через розподілене сховище Redis, а для захисту паролів користувачів застосовано бібліотеку Passlib. Для автоматизації розгортання та тестування будуть використовуватися інструменти практики CI/CD, що забезпечують безперервну інтеграцію та розгортання нових версій. Усі компоненти мають бути ізольовані через Docker для стабільності роботи.

Має використовуватись електронна пошта для автоматичної генерації та відправлення повідомлень користувачам щодо статусу технічного обслуговування.

Висновок. Пропонується розробка захищеної серверної частини веб прикладення на архітектурі REST API, що підвищить ефективність роботи авіакомпанії шляхом мінімізації затримок у комунікації і забезпечить своєчасне виконання технічних процедур. У майбутньому можна розглядати можливість інтеграції додаткових функцій, таких як машинне навчання для аналізу та прогнозування технічного стану літаків.

Список використаних джерел:

1. Jones, M., & Hardjono, T. (2015). JSON Web Token (JWT). IETF. URL: <https://datatracker.ietf.org/doc/html/rfc7519> (Last accessed: 25.01.2025).
2. Документація по FastAPI. URL: <https://kubernetes.io/ru/docs/home/> (Last accessed: 17.02.2025).
3. Документація по SQLAlchemy. URL: <https://kubernetes.io/ru/docs/home/> (Last accessed: 17.02.2025).
4. Документація по Docker. URL: <https://docs.docker.com/> (Last accessed: 17.02.2025).
5. Державіаслужба України. (2019). Авіаційні правила України "Підтримання льотної придатності повітряних суден та авіаційних виробів, компонентів і обладнання та схвалення організацій і персоналу, залучених до виконання цих завдань" (Наказ № 286 від 06.03.2019). URL: <https://zakon.rada.gov.ua/laws/main/z0316-19>

УДК 004.77.032.26(043.2)

ОПТИМІЗАЦІЯ НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ ДЛЯ РЕАЛЬНОГО ЧАСУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ПРИСКОРЕННЯ НА GPU

Денис Рибак

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Холявкіна, к.т.н., доцент.

Ключові слова: оптимізація нейромереж, GPU-прискорення, глибоке навчання, TensorRT, CUDA.

Вступ. Використання нейромережеских моделей у задачах реального часу вимагає оптимізації їх продуктивності для забезпечення швидкого інференсу. Один із підходів до підвищення швидкодії – використання технологій прискорення на графічних процесорах. Завдяки ефективному паралельному обчисленню сучасні GPU дозволяють значно зменшити час виконання глибоких нейромережеских моделей без втрати точності.

Матеріали та методи. У дослідженні використано фреймворки TensorFlow і PyTorch для навчання моделей, а також технології прискорення NVIDIA CUDA та TensorRT для оптимізації інференсу. Було протестовано кілька популярних архітектур, зокрема ResNet-50, MobileNetV2 та EfficientNet, із застосуванням методів квантизації, усічення та компіляції для GPU. Експерименти проводилися на апаратному забезпеченні з графічним процесором NVIDIA RTX 3090.

Результати. Оптимізація нейромереж із використанням TensorRT дозволила скоротити час інференсу в середньому на 45-70% залежно від архітектури. Для моделі ResNet-50 швидкість зросла на 48%, для MobileNetV2 – на 67%, а для EfficientNet – на 72%. Аналіз показав, що найкращі результати

досягаються при зменшенні точності обчислень до FP16 та застосуванні специфічних профілів оптимізації TensorRT [1, 2, 3].

При аналізі продуктивності було помітно, що моделі з меншою кількістю параметрів, такі як MobileNetV2, демонструють значне прискорення завдяки квантизації, тоді як важчі моделі, такі як ResNet-50, отримують найбільшу вигоду від оптимізації пам'яті та паралельного обчислення. Оптимізація з використанням TensorRT дозволила зменшити затримку інференсу з 22 мс до 7 мс для MobileNetV2, що дозволяє використовувати її в реальному часі без помітної затримки для користувача. EfficientNet, завдяки своєму оптимізованому дизайну, після оптимізації TensorRT забезпечила найбільшу продуктивність у співвідношенні точності та швидкості, зменшивши час інференсу на 72% при збереженні високої точності класифікації [4, 5].

Додатково проведене тестування показало, що використання GPU-прискорення на мобільних пристроях зменшило енергоспоживання на 25-30%, що є критичним фактором для інтеграції нейромереж у вбудовані системи та пристрої Інтернету речей. Аналіз споживання ресурсів показав, що використання FP16 і усічення менш значущих шарів зменшують не лише час виконання, але й використання відеопам'яті в середньому на 40%, що дозволяє запускати потужніші моделі на менш продуктивному обладнанні [6].

Висновок. Оптимізація нейромережевих моделей із використанням GPU-прискорення значно покращує їхню продуктивність у задачах реального часу. Найефективнішими підходами виявилися квантизація, усічення та компіляція з TensorRT. Отримані результати демонструють, що оптимізація дає змогу запускати глибокі моделі на пристроях із обмеженими ресурсами без значної втрати точності. Подальші дослідження можуть бути зосереджені на автоматизованій оптимізації моделей, інтеграції технологій розподіленого обчислення та зменшенні енергоспоживання при виконанні нейромереж.

Список використаних джерел:

1. Optimizing Deep Learning Models with TensorRT. URL: <https://astconsulting.in/artificial-intelligence/ml-machine-learning/optimizing-deep-learning-models-with-tensorrt> (date of access: 14.03.2025).
2. Accelerating Inference for Deep Learning Models. URL: https://github.com/triton-inference-server/tutorials/blob/main/Conceptual_Guide/Part_4-inference_acceleration/README.md (date of access: 14.03.2025).
3. Power of GPU Acceleration in Deep Learning: Elevating Model Training Performance. URL: <https://www.linkedin.com/pulse/power-gpu-acceleration-deep-learning-elevating-model-training-sachin-1ivtc/> (date of access: 14.03.2025).
4. ResNet-50. URL: <https://infohub.delltechnologies.com/en-us/l/power-ai-with-dell-and-nvidia/resnet-50/> (date of access: 14.03.2025).
5. How we made EfficientNet more efficient. URL: <https://towardsdatascience.com/how-we-made-efficientnet-more-efficient-61e1bf3f84b3/> (date of access: 14.03.2025).
6. Real-Time Neural Network Optimization. URL: <https://www.restack.io/p/model-optimization-answer-real-time-neural-network-optimization-cat-ai> (date of access: 14.03.2025).

УДК 656.7:044.22:044.42

**ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЛОГУВАННЯ ТА ВІДНОВЛЕННЯ КРИТИЧНИХ ДАНИХ У ІТ-СИСТЕМАХ
АВІАКОМПАНІЇ****Євгеній Рудь***Державний університет "Київський авіаційний інститут", Київ**Науковий керівник – Вадим Сураєв, к.т.н., доц.*

Ключові слова: логування, відновлення, авіакомпанія, безпека, база даних.

Логування та відновлення критичних даних є невід’ємними аспектами для ІТ-систем авіакомпаній, оскільки вони безпосередньо впливають на безпеку та стабільність роботи всієї компанії. Втрата або некоректна зміна даних, що стосуються розкладів рейсів, екіпажів, обслуговування літаків та фінансових операцій, може призвести до серйозних збоїв у роботі, фінансових втрат та ризиків для пасажирів. Для запобігання таким ситуаціям авіакомпанії використовують спеціальні засоби моніторингу змін та механізми відновлення інформації.

Одним із основних підходів до забезпечення контролю за змінами є застосування тригерів та логування у базі даних. Це дозволяє фіксувати всі операції, що здійснюються над критичною інформацією, та за необхідності відновлювати попередні версії даних. У великих авіаційних ІТ-системах, таких як Amadeus, яка використовується для бронювання квитків, або AMOS, що застосовується для технічного обслуговування літаків, реалізовано багаторівневий контроль змін. Впровадження подібних рішень дає змогу оперативно реагувати на інциденти, мінімізувати ризики втрати інформації та забезпечувати безперебійну роботу авіакомпанії.

В авіакомпанії «Міжнародні авіалінії України» функціонує складна структура баз даних, яка обслуговує різні напрями діяльності – від пасажирських перевезень до управління технічним станом літаків. Забезпечення безперебійного функціонування цих систем вимагає впровадження ефективних механізмів логування змін. Це включає автоматичний запис усіх змін у спеціальні лог-таблиці, можливість перегляду історії модифікацій та функцію відновлення попередніх версій даних.

Важливим аспектом розробки такої системи є надання зручних інструментів для її адміністрування. Адміністратори повинні мати можливість вибирати критичні таблиці для моніторингу, налаштовувати параметри логування та здійснювати фільтрацію операцій за часом та користувачем. ІТ-інженери, у свою чергу, повинні мати доступ до перегляду змін, аналізу журналів змін та оцінки ефективності процесів відновлення даних.

Враховуючи специфіку авіаційної галузі, де будь-який збій може мати критичні наслідки, запропоноване рішення спрямоване на забезпечення швидкого відновлення інформації та підтримку стабільної роботи ІТ-систем. Для цього необхідно реалізувати механізми перевірки коректності відновлених даних, забезпечити захист від несанкціонованого доступу та провести комплексне тестування продуктивності системи.

Висновок. Впровадження такої системи дозволить значно підвищити надійність управління критичною інформацією, що є важливим кроком для покращення ефективності роботи авіакомпанії та забезпечення її стабільного функціонування.

Список використаних джерел:

- 1.Elmasri R., Navathe S. B. Fundamentals of Database Systems. – 7th ed. – Pearson, 2016. – 1272 p.
- 2.Connolly T., Begg C. Database Systems: A Practical Approach to Design, Implementation, and Management. – 6th ed. – Pearson, 2015. – 1440 p.

УДК 004.7 (043.2)

ПРИНЦИПИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ПАКЕТІВ АНОМАЛЬНОЇ СТРУКТУРИ**Віталій Самофалов***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Микола Проценко, к.т.н., доц.*

Ключові слова: мережевий пакет, аномалія, сигнатурне виявлення, поведінковий аналіз, машинне навчання, кібербезпека, структура пакета, трафік

Інформаційна безпека сучасних комп'ютерних мереж значною мірою залежить від здатності систем автоматично ідентифікувати та блокувати потенційно шкідливий трафік. Особливу загрозу становлять мережеві пакети аномальної структури, в яких можуть міститись кібератаки, спроби експлуатації вразливостей або обхідні маневри засобів виявлення шкідливого контенту. Такі пакети відрізняються від типових за розміром, послідовністю полів, значеннями заголовків або характером навантаження. Розпізнавання таких відхилень є важливим напрямом роботи засобів контролю трафіку, зокрема систем виявлення вторгнень (IDS), мережевих моніторів і аналізаторів пакетів.

Результати аналізу методів виявлення мережевих пакетів аномальної структури

В сучасних підходах виявлення мережевих пакетів аномальної структури ґрунтується на принципі порівняння реального трафіку із заздалегідь визначеною моделлю «нормальної» або очікуваної поведінки мережі [1].

Першим і базовим принципом є сигнатурне порівняння, яке полягає у зв'язці мережевих пакетів із набором відомих шаблонів шкідливої активності. Якщо структура пакета відповідає одному з шаблонів (наприклад, специфічне поле IP-заголовка має заборонене значення, або спостерігається нестандартна довжина TCP-сегмента), такий трафік вважається аномальним [1]. Цей метод швидкий і ефективний проти відомих загроз, але малоефективний проти нових або модифікованих атак.

Другим принципом є аналіз поведінкових відхилень. У цьому випадку система збирає статистику про звичайний стан мережевого трафіку – типові розміри пакетів, протоколи, частоту з'єднань, характер послідовностей. На основі цих даних формується поведінкова модель. Виявлення пакета аномальної структури відбувається шляхом визначення нетипових параметрів – наприклад, несподівано великого розміру ICMP-пакета, який може свідчити про атаку типу Ping of Death, або TCP-пакета без SYN-прапора на першій фазі з'єднання. Такий підхід є гнучким і дозволяє виявляти раніше невідомі форми загроз.

Третім важливим принципом є аналіз консистентності протоколу [1]. У цьому випадку система перевіряє, чи відповідає структура пакета специфікації відповідного протоколу. Наприклад, у HTTP-запиті може бути виявлено заголовок із порушенням формату або в UDP-пакеті – відсутність полів, що є обов'язковими за стандартом. Якщо протокол передбачає певну логіку заповнення заголовків або

черговість дій, будь-яке порушення цієї логіки розцінюється як аномалія. Це особливо актуально для протоколів прикладного рівня, де можливі атаки через маніпуляцію параметрами запиту.

Додатково все частіше застосовуються алгоритми машинного навчання для аналізу великих обсягів трафіку [2]. У цьому підході модель навчається на реальних прикладах «нормального» трафіку та самостійно виявляє відхилення – пакети з рідкісною структурою, незвичною частотою появи або змішаними заголовками. Такі системи є чутливими до нових форм атак, але потребують ретельного навчання та налаштування, аби уникати помилкових спрацьовувань.

Складність полягає в тому, що сам факт структурної аномалії не завжди означає атаку. У деяких випадках нестандартна структура пакета може бути спричинена нестабільністю мережі, помилками маршрутизаторів або програмним забезпеченням клієнта. Тому важливим є комбінування кількох принципів – сигнатурного, поведінкового, протокольного та евристичного, що дозволяє підвищити точність виявлення пакетів з шкідливим змістом.

Висновок. Виявлення мережевих пакетів аномальної структури є ключовим завданням систем кіберзахисту, особливо в умовах зростання складності атак та активного використання методів обходу традиційних фільтрів. Основні принципи виявлення – це сигнатурний аналіз, поведінкове моделювання, перевірка на відповідність протокольним специфікаціям та використання інтелектуальних алгоритмів. Комплексне поєднання цих методів забезпечує високий рівень виявлення загроз та формує основу для побудови адаптивних систем захисту інформаційної інфраструктури.

Список використаних джерел:

1. Методи аналізу та моделювання безпеки розподілених інформаційних систем: навч. посіб. / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. Чернігів: Чернігівський національний технологічний університет, 2023. - 254 с.
2. Johnson M., Peterson L. AI-Driven Solutions for Network Traffic Analysis. New York: Wiley, 2025. 280 p.

УДК 656.7:044.22:044.42

ЗАСОБИ ПІДТРИМКИ ПРОЦЕДУР ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЛІТАКІВ. РОЗРОБКА ВЕБ-ІНТЕРФЕЙСІВ ДЛЯ ВИКОНАВЦІВ РОБІТ ТА ЇХ КЕРІВНИКА

Ярослав Сандул, Олександр Пшеничко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Вадим Сураєв, к.т.н., доц.

Ключові слова: технічне обслуговування літаків, веб-інтерфейс, React, автоматизація, інтеграція.

Ефективне технічне обслуговування (ТО) авіаційної техніки є критичним фактором забезпечення безпеки польотів. Сучасні цифрові рішення дозволяють оптимізувати процеси ТО завдяки автоматизації збору та обробки даних. Веб-інтерфейси забезпечують оперативний доступ до інформації про стан літаків та планові технічні роботи, що сприяє підвищенню ефективності керування технічними процесами.

Метою цього проєкту є розробка та впровадження веб-інтерфейсу для виконавців ТО та їх керівників, що забезпечить автоматизоване керування технічним обслуговуванням літаків, спрощення комунікації між технічним персоналом та зменшення людського фактора при плануванні та виконанні завдань.

Процес розробки веб-інтерфейсу базується на принципах адаптивного дизайну, забезпечення зручної взаємодії користувачів із системою та швидкої обробки запитів. Для розробки інтерфейсу використовуються технології HTML, CSS/SCSS, Tailwind CSS для створення гнучкого та адаптивного дизайну, а також React для створення динамічних компонентів. Реалізація маршрутизації здійснюється за допомогою React Router, а управління станом – за допомогою Redux Toolkit. Взаємодія з бекендом відбувається через RESTful API, використовуючи асинхронні запити за допомогою Fetch API.

Під час розробки фронтенд-частини веб-інтерфейсу для підтримки процедур технічного обслуговування літаків, основна увага буде приділятися забезпеченню зручності користувацького досвіду та інтеграції з існуючим API яке буде надавати дані про технічне обслуговування літаків. Спочатку буде створено загальну структуру інтерфейсу з основними компонентами: головною панеллю, панелями навігації та інформаційними блоками. Далі здійснюватиметься підключення до API для отримання та відображення даних у форматі JSON.

Для відображення даних будуть створені інтерактивні компоненти, такі як таблиці для переліку проведених робіт, списки для запланованих технічних обслуговувань. Для покращення досвіду користувача застосовуватиметься сортування та фільтрація даних, що дозволить керівникам і виконавцям швидко знаходити необхідну інформацію за різними критеріями. Завдання, що потребують термінового виконання, будуть позначені кольорами або спеціальними іконками, що полегшить візуальне сприйняття критичних робіт.

Одним із важливих етапів буде впровадження реєстрації та авторизації, що дозволить гарантувати доступ до інтерфейсу лише для авторизованих користувачів. Це забезпечить захист персональних даних та важливої технічної інформації від несанкціонованого доступу.

На фінальному етапі відбудеться інтеграція всіх компонентів системи в єдину платформу. Проведення функціонального тестування та тестування взаємодії з API дозволить переконатися в коректній роботі всіх модулів, а також у відповідності до вимог щодо точності відображення даних і їх актуальності. Цей процес дозволить створити надійний веб-інтерфейс, який забезпечить ефективну комунікацію між виконавцями та керівниками робіт, мінімізуючи помилки при обробці даних і підвищуючи загальну ефективність процесу технічного обслуговування літаків

Висновок. Запропонований веб-інтерфейс значно покращує управління процедурами ТО авіаційної техніки. Автоматизація процесів знижує ймовірність помилок, підвищує ефективність комунікації та сприяє своєчасному виконанню технічних завдань. Розроблене рішення сприяє підвищенню ефективності технічного обслуговування авіаційної техніки та автоматизації процесів.

Список використаних джерел:

- 1.QATestLab. (2020). *Client-server architecture*. URL: <https://training.qatestlab.com/blog/technical-articles/client-server-architecture/>
- 2.W3C. (2023). *HTML5 Specification*. URL: <https://www.w3.org/TR/html5/>
- 3.React Documentation. (2023). *React: A JavaScript Library for Building User Interfaces*. URL: <https://reactjs.org/>
- 4.CSS-Tricks. (2022). *Tailwind CSS: Utility-First CSS Framework*. URL: <https://tailwindcss.com/>
- 5.Mozilla Developer Network. (2021). *Fetch API*. URL: https://developer.mozilla.org/en-US/docs/Web/API/Fetch_API

УДК 004.9:336.7

СВІТОВИЙ РИНОК ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ЯК ДРАЙВЕР ІННОВАЦІЙ У ФІНАНСОВИХ ТЕХНОЛОГІЯХ

Денис Сологуб, Ганна Скиба

Навчально-науковий Інститут управління, економіки та бізнесу, «ВНЗ «Міжрегіональна Академія управління персоналом», Київ

Науковий керівник – Ганна Скиба, к.е.н., доц.

Ключові слова: світовий ринок ІТ, фінансові технології, FinTech, штучний інтелект, блокчейн, хмарні обчислення, кібербезпека, цифрові платежі, децентралізовані фінанси (DeFi), автоматизація фінансових процесів, регуляторні виклики, криптовалюти, фінансові сервіси.

Вступ. У сучасному світі інформаційні технології (ІТ) відіграють ключову роль у розвитку різних сфер економіки, особливо у фінансовому секторі. Глобальний ринок ІТ є не лише інструментом автоматизації процесів, але й потужним драйвером інновацій, що змінює підходи до управління фінансами, кредитування, платежів і безпеки даних. Завдяки постійному вдосконаленню цифрових рішень, інтеграція новітніх технологій у фінансовий сектор дозволяє значно підвищити ефективність

операцій, знизити витрати та мінімізувати ризики. Актуальність дослідження зумовлена стрімким розвитком фінансових технологій (FinTech), які завдяки впровадженню штучного інтелекту, блокчейну, хмарних сервісів та великих даних формують нові можливості для бізнесу та споживачів.

Матеріали і методи. Дослідження базується на аналізі наукових джерел, статистичних даних та практичних кейсів впровадження інформаційних технологій у фінансовому секторі. Використані методи включають порівняльний аналіз, систематизацію та узагальнення даних, а також експертне оцінювання тенденцій розвитку фінансових технологій.

Результати та обговорення. Світовий IT-ринок охоплює апаратне й програмне забезпечення, хмарні сервіси, великі дані, кібербезпеку, блокчейн, квантові обчислення та IoT. Його розвиток зумовлений зростанням хмарних обчислень, штучного інтелекту та блокчейн-рішень у фінансових транзакціях [1, 2].

FinTech-технології вдосконалюють фінансові розрахунки, зменшують шахрайство та підвищують ефективність операцій. Штучний інтелект сприяє прогнозуванню ризиків, персоналізації послуг і покращенню обслуговування, а блокчейн забезпечує прозорість і розвиток DeFi.

Зростання цифрових платежів і криптовалют посилює потребу в кібербезпеці, що змушує фінансові установи інвестувати в біометричну автентифікацію, багаторівневу верифікацію та AI-системи моніторингу транзакцій.

Головним викликом є регуляторна невизначеність, адже законодавство не завжди встигає за технологічним прогресом. Держави активно працюють над правовими актами для цифрових фінансових операцій і захисту даних.

Попри виклики, перспективи FinTech залишаються позитивними: автоматизація, Open Banking та API-рішення сприятимуть інтеграції банківських і фінансових сервісів, що розширить можливості користувачів та зміцнить довіру до цифрових фінансових технологій [3].

Висновок. Глобальний ринок IT є ключовим драйвером FinTech, сприяючи автоматизації, підвищенню ефективності та безпеки фінансових операцій. Цифрові платформи, машинне навчання й обчислювальні потужності оптимізують процеси, скорочують витрати та персоналізують сервіси.

Однак розвиток FinTech супроводжується викликами: адаптацією регуляторного середовища, кібербезпекою та прозорістю операцій. Блокчейн знижує ризики шахрайства, потребуючи правової підтримки. Перспективи галузі пов'язані зі штучним інтелектом, блокчейном, цифровими валютами та DeFi, що змінять фінансовий ландшафт, розширюючи доступ до послуг та фінансову інклюзію.

Список використаних джерел:

1. Кондратенко, Н.Д. (2021). Трансформація ринку інформаційних послуг в умовах цифрової економіки. Бізнес інформ, 1, 112-118
2. Людвік, І.І. (2022). Інноваційний розвиток України в умовах глобалізації економічного простору. Економіка та підприємництво, 2(125), 36-40. <https://doi.org/10.32840/1814-1161/2022-2-6>
3. Крилов, Д.В. (2022). Сектор інформаційних технологій України: проблеми розвитку та значення для національної економіки. Причорноморські економічні студії, 75, 32-36. <https://doi.org/10.32843/bses.75-5>

УДК 004.5

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ТЕСТУВАННЯ API ЗАПИТІВ**Арсеній Сьох***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Юлія Вітрук, к.т.н., доц.***Ключові слова:** API, тестування, REST.

Вступ. Інтерфейси програмування додатків (API) стали невід’ємною частиною сучасних програмних рішень, забезпечуючи зв’язок між різними компонентами систем і дозволяючи створювати складні архітектури. Розвиток мікросервісів і хмарних сервісів не лише розширює їхнє застосування, а й підвищує вимоги до надійності, стабільності та швидкості API. Тема цієї роботи присвячена аналізу сучасних способів тестування API запитів, оцінці їхніх переваг і практичній застосовності в реальних умовах. Значення теми пояснюється потребою гарантувати безперебійну роботу, захищеність і високу швидкодію програм, які залежать від API, адже навіть незначні збої можуть призводити до суттєвих проблем у функціонуванні додатків.

Матеріали та методи

Аналіз проводився на базі RESTful API, що є стандартом для більшості веб-додатків. Основними інструментами обрано:

- **Postman** – для перевірки запитів вручну та написання простих автоматичних тестів;
- **JMeter** – для дослідження поведінки API під різними навантаженнями.

Перевірка охоплювала коректність відповідей сервера (коди стану, структура даних у форматі JSON), реакцію на помилкові запити та поведінку в екстремальних ситуаціях, наприклад, при надсиланні надмірної кількості запитів або невалідних параметрів, таких як неправильні типи даних чи відсутні значення. Для поглиблення аналізу вивчалися матеріали про бібліотеки автоматизації тестування, такі як RestAssured (Java), які дають змогу детально досліджувати API. Практичні приклади базувалися на відкритих API, наприклад, Swagger Petstore, яке пропонує набір ендпоінтів для управління інформацією про тварин, користувачів і транзакції, що робить його зручним для тестування різноманітних сценаріїв.

Результати. Результати тестування виявили сильні сторони кожного інструменту. Postman виявився зручним для оперативної перевірки запитів і створення базових автоматичних сценаріїв через інтеграцію з JavaScript, що дозволяє швидко адаптувати тести до потреб. Наприклад, у Swagger Petstore цей інструмент оперативно виявив невідповідність у коді відповіді при запиті неіснуючого об’єкта (отримано 400 замість 404), що вказує на потенційні слабкості в логіці обробки запитів. JMeter показав свою цінність у тестуванні продуктивності: при симуляції 1000 одночасних запитів до ендпоінту списку об’єктів середня затримка склала 150 мс, але при зростанні до 2000 запитів час відповіді збільшився до 340 мс, що сигналізує про можливі обмеження масштабування та потребу в оптимізації серверної частини.

Висновок. Ефективне тестування API запитів передбачає комбінацію ручного та автоматичного підходів, що дозволяє охопити різні аспекти їхньої роботи. Postman ідеально підходить для початкових перевірок і невеликих проєктів завдяки своїй інтуїтивності, JMeter незамінний для аналізу продуктивності в умовах реального навантаження, а RestAssured пропонує гнучкість для складних автоматичних тестів, забезпечуючи глибший контроль. Ці підходи разом формують цілісну картину можливостей API, сприяючи створенню надійніших систем.

Список використаних джерел:

1. Документація по Postman. URL: <https://learning.postman.com/docs/>
2. Документація по Apache JMeter. URL: <https://jmeter.apache.org/usermanual/>

УДК 004.738.5:339(043.2)

МОБІЛЬНИЙ ДОДАТОК ДЛЯ УПРАВЛІННІ МАЛИМ БІЗНЕСОМ

Катерина Цегер

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Холявкіна, к.т.н., доц.

Ключові слова: мобільний додаток, облік продажів, управління клієнтами, архітектура програми, хмарна синхронізація.

Малий бізнес відіграє ключову роль в економіці, створюючи робочі місця та сприяючи інноваціям. Однак підприємці часто стикаються з браком доступних інструментів для автоматизації бізнес-процесів, таких як облік продажів, управління клієнтами та контроль витрат[1].

Сучасні мобільні телефони відкривають можливості для ефективного управління бізнесом. Тому створення мобільного додатка, орієнтованого на малі підприємства, є перспективним рішенням[2]. Він має забезпечити зручний доступ до ключових функцій, оптимізувати витрати часу та ресурсів і залишатися доступним для широкого кола користувачів. Це підвищить ефективність управління, зменшить рутинні завдання та зміцнить конкурентоспроможність малого бізнесу.

Дослідження охоплює процеси автоматизації бізнес-операцій у малих підприємствах та використання мобільного додатка як інструменту оптимізації управління продажами, клієнтами та витратами. Аналіз потреб малого бізнесу здійснено шляхом опитування підприємців та вивчення наукової літератури[3]. Для визначення оптимальних рішень проведено порівняльний аналіз існуючих програм-аналогів[4].

Архітектура мобільного додатка розроблена на основі принципів розподіленої обробки даних та використання сучасних патернів програмування. Для моделювання структури застосовано UML-діаграми. Розробка ведеться з використанням кросплатформних технологій React Native або Unity, що забезпечує сумісність із різними пристроями. База даних побудована на PostgreSQL/MySQL для масштабованості та надійності збереження інформації.

Продуктивність додатка оцінюється за допомогою Firebase Performance Monitoring, а ефективність UX/UI тестується методами A/B-тестування та аналізу відгуків користувачів. Для забезпечення стабільності роботи

застосовується автоматизоване тестування API. Запропонований підхід дозволяє створити ефективний та зручний інструмент для управління малим бізнесом із урахуванням потреб зростаючої кількості користувачів і обсягу даних.

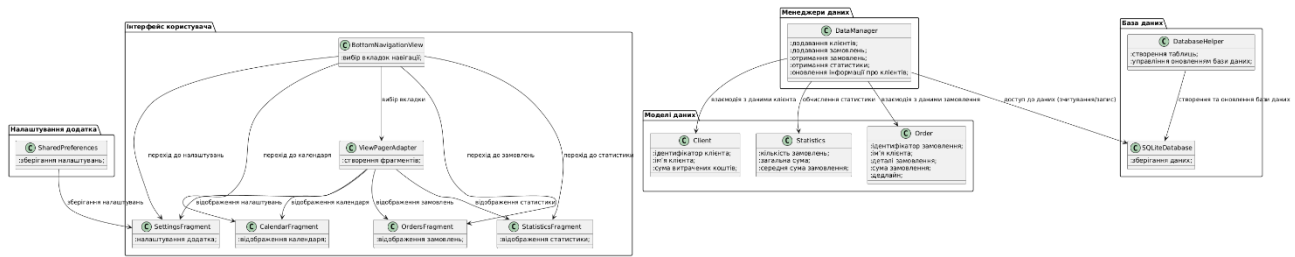


Рис.1. – Діаграма компонентів

Висновок. Розроблений мобільний додаток забезпечує ефективну автоматизацію бізнес-процесів малого підприємства, адаптуючи функціонал до специфіки різних видів діяльності завдяки використанню адаптивних алгоритмів. Він поєднує сучасні технології мобільної розробки, що гарантує кросплатформенність, масштабованість та інтеграцію з хмарними сервісами.

Функціонал додатка включає облік продажів, управління клієнтами, контроль витрат, автоматичне формування звітів та адаптивний інтерфейс, що робить його зручним та ефективним у використанні. Тестування підтвердило високу продуктивність і відповідність потребам малого бізнесу. Отримані результати можуть бути застосовані для подальшого вдосконалення цифрових інструментів управління бізнесом та розширення їхніх можливостей.

Список використаних джерел:

1. Silvia Moreira, Henrique S. Mamede, Arnaldo Santos, Business Process Automation in SMEs. Lecture Notes in Business Information Processing. In book: Information Systems (pp.426-437). 2023.
2. Laudon, K. C., & Laudon, J. P. Management Information Systems: Managing the Digital Firm. – Pearson, 2020.
3. Gartner. *Magic Quadrant for Enterprise Low-Code Application Platforms* [Електронний ресурс]. – Режим доступу: <https://www.gartner.com/en>
4. Samura, O. *Cross-Platform Mobile Development: React Native, Flutter, and Xamarin*. – Packt Publishing, 2021.

УДК 004.81:159.953.5]:811.112.2(043.2)

МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ ЕФЕКТИВНОГО ВИВЧЕННЯ НІМЕЦЬКОЇ МОВИ УКРАЇНЦЯМИ, ЯКІ ЕВАКУЮВАЛИСЯ ЧЕРЕЗ ВІЙНУ

Крістіна Шлома

Державний університет «Київський Авіаційний Інститут», Київ

Науковий керівник – Тетяна Холявкіна, к.т.н., доц.

Ключові слова: веб-застосунок, вивчення мови, адаптація, інтеграція.

Загалом, у сучасному світі, створюються нові технології та використовуються різні інновації, завдяки чому вартість технологій-попередників та їх продуктів мінімізувалися до значень широкої доступності населенню. Проте, все частіше можна зустріти випадки підвищення вартості, особливо на вторинному ринку. У чому причини такої ринкової політики?

Вступ. Через політичні обставини значна кількість українських переселенців опинилася в європейських країнах, зокрема в Німеччині. Одним із ключових викликів, що стоїть перед ними, є подолання мовного бар'єру, через який ускладнюється процес інтеграції в нове середовище, зокрема в сфері працевлаштування та й життя в цілому. Традиційні підходи до вивчення іноземних мов, як-от використання підручників або читання великих книжок, часто виявляються малоефективними через складність запам'ятовування великого обсягу інформації. Актуальність цієї теми підтверджується сучасними дослідженнями [1, 2], у яких аналізуються новітні підходи до мовної освіти із використанням цифрових технологій.

Матеріали та методи.

Під час створення веб-застосунку було задіяно HTML, CSS і JavaScript для створення функціонального інтерфейсу та інтерактивних елементів. Більша частина уваги приділялася простоті використання і зручності для користувача, що дозволяє ефективно засвоювати матеріал у зручному темпі.

Результати. Створений веб-застосунок значно полегшує процес мовної адаптації для користувачів, які перебувають у новому мовному середовищі. Основна перевага полягає у поєднанні різних методів вивчення мови в одному інструменті: читання, переклад, активне запам'ятовування та граматичний аналіз.

Під час тестування застосунку користувачами було відзначено наступні позитивні результати: **Зменшення когнітивного навантаження** завдяки роботі з короткими текстами (до 500 слів); **Покращення словникового запасу** на 30–40% вже через один регулярного використання; **Зростання мотивації до навчання**, оскільки можливість миттєвого перекладу дозволяє уникати фрустрації, пов'язаної з незрозумілими словами або фразами; **Підвищення розуміння граматичних структур**: за

результатами опитування, 75% користувачів відзначили, що інтерактивні вправи на граматику були ефективнішими за традиційні вправи у підручниках.

Користувацьке тестування охопило 10 учнів різного віку та рівня володіння німецькою мовою (від A1 до B1). За результатами анкетування, 91% користувачів заявили, що застосунок є корисним у процесі вивчення мови, а 82% висловили готовність рекомендувати його іншим переселенцям.

Ефективність використання цифрових засобів у вивченні мов підтверджується науковими дослідженнями. У роботі Саєнко та Созикиної [1] зазначено, що адаптивні технології широко використовуються в навчанні іноземних мов, зокрема для оцінювання рівнів мовної компетенції. Кузьо [2] обґрунтовує переваги веб-застосунків у формуванні навичок читання, підкреслюючи їхню доступність та інтерактивність. Крім того, у статті "Вебзастосунок для вивчення іноземних мов" [3] аналізується роль адаптивного навчання у мовній освіті, що реалізовано в даному застосунку через можливість вибору рівня складності і тематики.

Висновок. Даний веб-застосунок допомагає швидко та ефективно переселенцям, які опинилися в новому мовному середовищі, вивчати німецьку мову у зручному та доступному форматі.

Список використаних джерел:

1. Саєнко Н. В., Созикина Г. С. Переваги та недоліки адаптивного навчання іноземних мов [Електронний ресурс] // Збірник наукових праць «Scientific Collection «InterConf»». – 2022. – С. 45–50. – Режим доступу: <https://archive.interconf.center/index.php/conference-proceeding/article/download/1066/1092>. – Назва з екрана. (Дата звернення: 17.03.2025).
2. Кузьо Л. І. Актуальні проблеми навчання іноземних мов для спеціальних цілей [Електронний ресурс] // Збірник наукових статей. – Львів: ЛьвДУВС, 2023. – 131 с. – Режим доступу: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/6594/1/Актуальні%20проблеми.%20Збірник%20статей%202023.pdf> – Назва з екрана. (Дата звернення: 17.03.2025).
3. Вебзастосунок для вивчення іноземних мов [Електронний ресурс]. – Режим доступу: <https://krs.chmnu.edu.ua/jspui/bitstream/123456789/2960/1/Данкович%20Сергій%20БКР.pdf> – Назва з екрана. (Дата звернення: 17.03.2025).

УДК 004.85:519.652.3

ПОРІВНЯЛЬНИЙ АНАЛІЗ VISION TRANSFORMER ТА RESNET-50 ЯК АВТОКОДУВАЛЬНИКІВ ДЛЯ ДОСЛІДЖЕННЯ ПРОСТОРУ ПРЕДСТАВЛЕНЬ У ЗАДАЧАХ РОЗПІЗНАВАННЯ ДАНИХ З АЕРОФОТОЗЙОМКИ

Олександр Козачук

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Пилип Приставка, д.т.н., проф.

Ключові слова: автокодувальник, *Vision Transformer*, *ResNet-50*, латентний простір, розподіл даних, аерофотозйомка, комп'ютерний зір.

Метою дослідження є порівняння ефективності *Vision Transformer* та *ResNet-50* [1, 2] як автокодувальників у задачах реконструкції зображень з аерофотозйомки, а також аналіз розподілу даних

у латентному просторі з використанням набору даних "*Training set AERIAL SURVEY for Data Recognition Systems From Aerial Surveillance Cameras*" [3].

Для аналізу використано дві архітектури:

- *Vision Transformer (ViT)*: адаптовано до автокодувальника з розміром патчів 8×8 та латентним простором розмірності 256.
- *ResNet-50*: модифіковано шляхом заміни класифікаційного шару на шар стиснення до 256 вимірів, зберігаючи здатність моделі до детального аналізу локальних особливостей завдяки залишковим з'єднанням.



Рис. 1 Реконструкція ViT-AE

Порівняння якості реконструкції зображень показало, що *Vision Transformer* перевершує *ResNet-50* у відтворенні складних структур і глобальних патернів (Рис. 1). Натомість *ResNet-50* демонструє кращу точність у передачі локальних деталей (Рис. 2).

Аналіз латентного простору за допомогою *PCA* показав, що *Vision Transformer* формує більш чіткі кластери (Рис.3.) для різних класів даних порівняно з *ResNet-50* (Рис.2).



Рис. 2. Реконструкція ResNet-50-AE

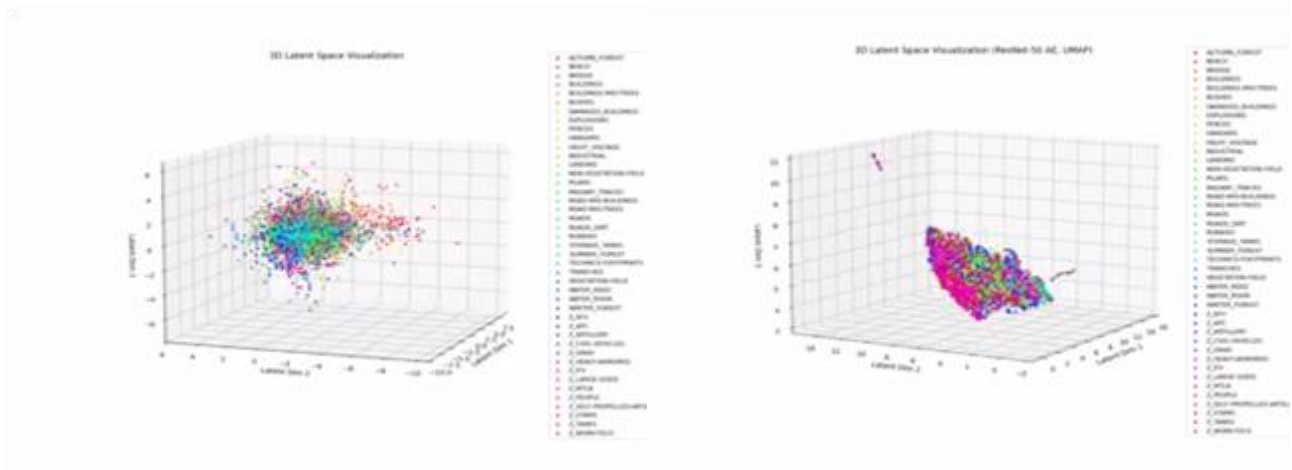


Рис 3. Зліва простір представлень ViT-AE, справа ResNet-50-AE

Висновки

ViT перевершує *ResNet-50* у реконструкції складних зображень з аерофотозйомки та організації латентного простору, демонструючи меншу середньоквадратичну похибку — 0.012 проти 0.015. Натомість *ResNet-50* краще відтворює локальні деталі, що робить його ефективним для задач, де важлива точність дрібних об'єктів.

Список використаних джерел:

1. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., Gelly, S., Usunier, N., Houlsby, N. "An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale." arXiv:2010.11929 (2020).
2. He, K., Zhang, X., Ren, S., Sun, J. "Deep Residual Learning for Image Recognition." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2016).
3. Zivakin, V., Kozachuk, O., Prystavka, P., Cholyskhina, O. "Training set AERIAL SURVEY for Data Recognition Systems From Aerial Surveillance Cameras." IT&I, 2022, pp. 246-255.

УДК 004.8

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ МОДЕЛЕЙ КЛАСИФІКАТОРІВ НА КОМП'ЮТЕРАХ ОБМЕЖЕНОЇ ПОТУЖНОСТІ

Борис Стеценко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – д-р.техн.наук проф. Приставка П. О.

Ключові слова: EfficientNetV2S, EfficientNetB7, MobileNetV2, ResNet50, ResNet101, моделі класифікаторів, класифікація зображень, час класифікації, Raspberry Pi 4 Model B.

Проведено дослідження можливості застосування моделей класифікаторів EfficientNetV2S, EfficientNetB7, MobileNetV2, ResNet50 і ResNet101, на комп'ютерах обмеженої потужності, для прикладу розглядався Raspberry Pi 4 Model B.

Суть експерименту полягала в застосуванні класифікаторів до наборів цифрових зображень різної кількості. Було згенеровано по 3000 наборів зображень, розміром 64x64, випадкової кількості, для кожної вибраної розмірності ([1; 16], [16; 32] ..., [256; 528]). Після цього результат подавався на вхід моделі нейронної мережі, що класифікувала групи зображень за один раз, а час класифікації фіксувався. Експеримент повторювався для кожної мережі.

Згідно з регресійним аналізом, застосованим до отриманих даних, можна спрогнозувати час, за який розглянуті моделі можуть класифікувати різну кількість зображень на комп'ютерах обмеженої потужності. Наприклад, за час менший за 1 секунду: EfficientNetV2S класифікує 18 картинок, EfficientNetB7 – 5, MobileNetV2 – 74, ResNet50 – 19, ResNet101 – 9.

Результати дослідження можуть бути використані при прогнозуванні часу роботи додатків, які потребують класифікації об'єктів, і при виборі моделей для таких застосунків, при застосуванні на комп'ютерах обмеженої потужності.

Список використаних джерел:

1. Keras Applications: EfficientNetV2. URL: https://keras.io/api/applications/efficientnet_v2/
2. Hugging Face: EfficientNet-B7. URL: <https://huggingface.co/google/efficientnet-b7>
3. Keras Applications: ResNet. URL: <https://keras.io/api/applications/resnet/>
4. Keras Applications: MobileNetV2. URL: <https://keras.io/api/applications/mobilenet/>

УДК 004.4'234:004.932.72'1

ВІДСТЕЖЕННЯ РУХОМИХ ОБ'ЄКТІВ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ НА ПРИСТРОЯХ З ОБМЕЖЕНИМИ ОБЧИСЛЮВАНИМИ РЕСУРСАМИ

Мозольов Олександр

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник: Пилип Олександрович ПРИСТАВКА, д-р техн. наук, проф.

Ключові слова: трекінг, відеопотік, системи з обмеженими обчислювальними ресурсами

Задача відстеження об'єктів у відеопотоці в режимі реального часу є затребуваною в багатьох сферах діяльності людини, а від мети її застосування залежить вибір засобів та шляхів реалізації. В даному матеріалі буде розглянуто питання супроводження об'єктів між кадрами відеоматеріалу для комп'ютерів з низькими обчислюваними можливостями: таких, які можуть застосовуватись на бортових системах БПЛА (безпілотних літальних апаратах) або інших автономних пристроях спостереження чи навігації.

Для відстеження переміщення цілі, невідомої до початку процесу (інформація або виокремлені особливості якої попередньо відсутні), використовуються алгоритми *трекінгу* об'єктів (object tracking). Тобто об'єкт визначається та виділяється його особливості під час проходження кадрів відеопотоку. Трекінг об'єктів потребує

значних обчислюваних потужностей, тому для того, щоб програма коректно слідувала за об'єктом в залежності від потреб, розробникам часто доводиться обирати між високою точністю відстеження та нижчою швидкістю зміни кадрів. Основними проблемами точності відслідковування є:

- 1) Розмиття фону та неконтрастність цілі;
- 2) Зміна вигляду, масштабу чи ракурсу об'єкта;
- 3) Оклюзії – перекриття цілі або, якщо відслідковуваних об'єктів декілька, їх злиття.

Вирішення цих проблем при збереженні швидкості обробки кадрів є ключовим завданням для роботи трекерів. Запропоновано багато підходів та типів трекінгу, які мають різну ефективність на комп'ютерах різної архітектури. Серед найбільш розповсюджених алгоритмів: “KCF”, “MIL”, “Boosting”, “TLD”, “MedianFlow”, “CSRT”, “MOSSE”, “Nano”, найшвидшим та доволі стійким при роботі на комп'ютері “Raspberry Pi 4 model B” [1] виявився тип “MOSSE”. Швидкість обробки кадрів в ньому у 2 рази більша за будь-який інший алгоритм (табл.1, №6), а точність порівняно однакова з двома іншими найшвидшими трекерами: “KCF” та “MedianFlow”, з єдиною відмінністю, що “MedianFlow” більш стійкий до змін освітлення та часткових оклюзій, а також здатен підлаштовуватись під зміну розміру об'єктів. Алгоритм “KCF” відстає від типу “MOSSE” за всіма параметрами (оскільки алгоритм “MOSSE” є значно покращеною версією методу “KCF”), та частково кращий за “MedianFlow” у швидкості роботи.

Проте попередньо наведені алгоритми сильно відстають у стійкості від типів трекінгу “Nano”, “CSRT” та “Boosting”. Час обробки кадрів у таких методах сильно вищий за попередньо наведені підходи (табл.1), але ризик втрати об'єкта більш малоімовірний. Кожен з цих трьох видів демонструють гарну якість та ефективність. Найбільш пристосованим для роботи на комп'ютерах з обмеженими обчислювальними ресурсами є трекер типу “Nano”, адже він працює частково на основі згорткових нейронних мереж, оптимізованих спеціально для роботи на мобільних та вбудованих пристроях. Він є оптимальним варіантом для використання на таких комп'ютерах, як Raspberry Pi 4, зі сторони співвідношення швидкості до точності, проте має некритично меншу якість відслідковування у порівнянні з алгоритмами “CSRT” чи “Boosting”.

№	Тип трекера	Математичне сподівання (fps)	Середнє квадратичне відхилення (fps)
1	Boosting	11,7344687	0,870200232
2	KCF	24,54556525	1,806202302
3	MedianFlow	24,72572034	1,709365948
4	CSRT	11,12048037	0,548477326
5	MIL	5,476254226	0,294518341
6	MOSSE	47,00090968	5,451185162
7	TLD	5,435944255	0,280347522
8	Nano	14,24260771	0,437068062

табл.1

Трекер типу “CSRT” є одним з найбільш зручних алгоритмів, оскільки він має високу якість відстеження: у порівнянні з типом “Nano” більш точно вказує на об'єкт, а в зіставленні з “Boosting” – менша вірогідність «дрейфу» (накопичення помилок під час оновлення положення об'єкта, що призводить до поступового зміщення та втрати

точності відстеження). Якість даного алгоритму в запобіганні оклюзій є найвищою серед існуючих популярних методах трекінгу.

Варто окремо виділити тип трекінгу “TLD”, який єдиним серед доступних алгоритмів спроможний виявити об’єкт після повного його зникнення з відеопотоку і подальшій його появі в іншій області кадрів. Це може бути корисним в багатьох випадках, проте цей метод дуже ресурсозатребуваний, а отже має дуже низьку швидкість роботи та є доволі нестійким і неточним.

УДК 519.2

АНАЛІЗ ФАКТОРІВ ВПЛИВУ НА РОЗДРІБНУ ТОРГІВЛЮ В УКРАЇНІ З ВИКОРИСТАННЯМ СТАТИСТИЧНИХ МЕТОДІВ ТА МАШИННОГО НАВЧАННЯ

Севіль Сулейманова

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Пулип Приставка, д.т.н., проф.

Ключові слова: Роздрібна торгівля, кореляційний аналіз, ансамблеві методи, Random Forest.

Роздрібна торгівля є однією з рушійних сил економіки України, виступаючи посередником між виробниками та споживачами. Вона є ключовою ланкою забезпечення населення всім необхідним у повсякденному житті та формуванні стабільних фінансових потоків наповнення бюджету країни [1]. Метою дослідження є аналіз впливу факторів на роздрібну торгівлю в Україні за допомогою статистичних методів та машинного навчання.

У дослідженні було використано дані, які були зібрані з відкритих джерел: Державної служби статистики України, Minfin, Github. До аналізу включено наступні показники: динаміка зміни цін у будівництві, середня тривалість повітряних тривог, рівень інфляції, середня заробітна плата, а також місячний роздрібний товарообіг. Для аналізу використано дані за період 2022–2024 років, що охоплюють динаміку змін у роздрібній торгівлі та вплив зовнішніх факторів на споживчу активність. Після збору дані було стандартизовано.

Для проведення аналізу були використано комбінацію статистичних – оцінка часткових коефіцієнтів кореляції [2] та ансамблевих методів, зокрема Random Forest [3]. Було розраховано часткові коефіцієнти кореляції Спірмена для кожної пари змінних: обсягу місячного роздрібногo товарообігу та кожного з описаних вище показників, після усунення впливу інших факторів.

З рис.1 видно, що найбільший позитивний вплив на роздрібний товарообіг має середня зарплата, збільшення доходів населення дозволяє споживачам більше витратити на товари та послуги. Найбільший негативний вплив на роздрібний товарообіг має зміна цін на будівництво. Зростання цін у будівельній галузі може суттєво обмежувати споживчі витрати. Інфляція та тривалість повітряних тривог також мають негативний вплив на роздрібний товарообіг, проте їх вплив менший.



Рис.1. Теплова карта часткових коефіцієнтів кореляції

Наступним кроком для визначення важливості впливу фактору на обсяги торгівлі була побудова моделі на основі дерев рішень – Random Forest та обчислення важливості кожної ознаки, результати наведено на рис.2. Середня заробітна плата має дуже високий показник важливості, тому для кращого розуміння відносної важливості інших факторів вона була виключена з розрахунків.

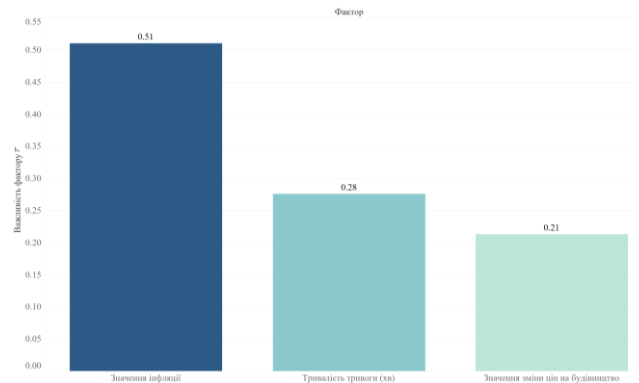


Рис.2. Значення важливості факторів

Обидва аналізи підтверджують, що інфляція має негативний вплив на роздрібну торгівлю. Однак, Random Forest показує, що цей вплив є значно сильнішим, ніж показує кореляційний аналіз. Це може бути пов'язано з тим, що Random Forest враховує складні нелінійні взаємозв'язки між факторами. Обидва аналізи підтверджують негативний вплив тривалості тривоги на роздрібну торгівлю. Зміни цін на будівництво можуть впливати на роздрібну торгівлю, але цей вплив є меншим, ніж вплив інфляції та тривалості тривоги. Однак, важливо враховувати цей фактор при аналізі роздрібною торгівлі, оскільки він може впливати на споживчі витрати та загальну економічну ситуацію.

Наступні дослідження будуть направлені на побудову прогнозової моделі, на основі відібраних факторів, що найбільше впливають на місячний роздрібний товарообіг в Україні.

Список використаних джерел:

1. Sharov V., Garafonova O., Dvornyk I. Economic challenges and financial opportunities of online retail in Ukraine during the war: alignment with global trends and innovative perspectives. Financial and credit activity problems of theory and practice. 2024. Vol. 5, no. 58. P. 331–344.
2. D'Innocenzo E., Lucas A. Dynamic partial correlation models. Journal of Econometrics. 2024. Vol. 241, no. 2. P. 105747.
3. Zhou Z., Hooker G. Unbiased Measurement of Feature Importance in Tree-Based Methods. ACM Transactions on Knowledge Discovery from Data. 2021. Vol. 15, no. 2. P. 1–21.

УДК 004.93

ВИЯВЛЕННЯ АНОМАЛІЙ В ДАНИХ ПОВІТРЯНОГО СПОСТЕРЕЖЕННЯ ЗА ДОПОМОГОЮ СПЛАЙН-МОДЕЛЕЙ

Жултинська Ангеліна

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Пилип Приставка, д.т.н., проф.*

Ключові слова: виявлення аномалій, сплайн-модель, моментні характеристики.

В умовах ведення бойових дій на території України завдання оперативного виявлення змін у зображеннях з безпілотних літальних апаратів (БПЛА) набуло особливої актуальності. У цій роботі розглянуто новий підхід до виявлення аномалій в даних повітряного спостереження з використанням моделей на основі двовимірних поліноміальних В-сплайнів.

Модель базується на представленні цифрового зображення як набору моментних характеристик [1], зокрема локального середнього значення інтенсивності $m_{v,m}$ та середньоквадратичного відхилення $\sigma_{v,m}$, розрахованих у ковзному вікні розміром $(2k+1) \times (2k+1)$. Ці параметри формують двовимірну вибірку, для якої будується функція густини розподілу за допомогою двовимірного поліноміального сплайну на основі В-сплайнів:

$$S_{2,0}(p, m, \sigma) = \sum_{i \in \mathbb{Z}} \sum_{j \in \mathbb{Z}} B_{2,h_m}(m - ih_m) B_{2,h_\sigma}(\sigma - jh_\sigma) p_{i,j},$$

де $B_{2,h}$ - базисний сплайн другого порядку, а $p_{i,j}$ - значення густини. Аномалії визначаються як малоймовірні спостереження, коли $S(f_q, m_q, \sigma_q) \leq \eta$, де η - поріг помилки, $\hat{S}(f_q, m_q, \sigma_q)$ - значення сплайну для q-го спостереження з характеристиками m_q і σ_q . Такий підхід дозволяє виявляти відхилення в текстурах, що вказують на потенційні аномалії.

Експерименти проведено на зображеннях аерофотозйомки роздільною здатністю 1920×1080 пікселів у форматі RGB. Використано ковзне вікно розміром 9×9 пікселів ($k = 4$), що забезпечило баланс між деталізацією текстур і обчислювальною ефективністю.



Рис.1. Цифрове зображення з різними текстурами

Початкове зображення лісової дороги (рис. 1) демонструє однорідну текстуру поля та відмінну текстуру дороги, що стало основою для аналізу. Модель успішно виявила ці відмінності (рис. 2а), а функція щільності розподілу (рис. 2б) показала рівномірний розподіл для лісу, чіткий розподіл для дороги та складну структуру з кількома піками для автомобіля та каменю, що відображає їхню текстурну різноманітність.

Результати аналізу (рис. 2а-2б) підтвердили здатність моделі ідентифікувати аномалії, що явно виділяються на тлі однорідних текстур. Ці зони, визначені як малоймовірні спостереження на основі низьких значень $\hat{S}(f_q, m_q, \sigma_q)$, вказують на значний інформаційний вміст.

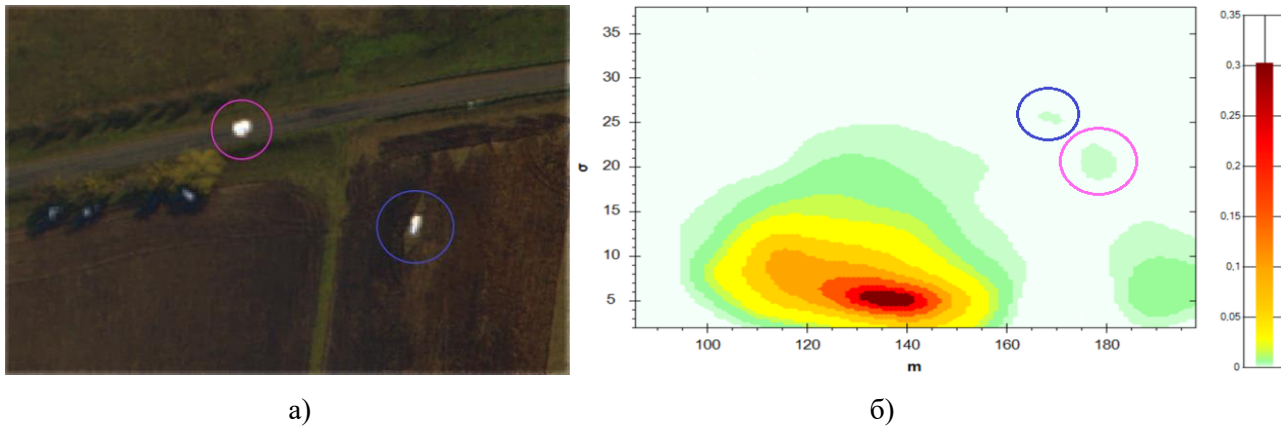


Рис.2. Побудова моделі цифрового зображення на основі статистичних характеристик та визначення аномалій:

а) сегментоване цифрове зображення; б) модель цифрового зображення

Запропонована сплайн-модель виявлення аномалій продемонструвала високу точність та ефективність завдяки адаптивності до складних текстур і стійкості до змін умов зйомки. Її здатність працювати в реальному часі робить підхід цінним для військової розвідки та цивільного моніторингу. Подальша інтеграція з методами глибокого навчання, зокрема CNN, дозволить підвищити чутливість до складних аномалій і зменшити кількість хибних спрацювань.

Список використаних джерел:

1. A. Zhultynska and P. Prystavka, " Spline model of digital images based on moment characteristics", Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024), Kyiv, Ukraine, 2024, pp. 325-333, <https://ceur-ws.org/Vol-3925/short09.pdf>

УДК 004.42

УТИЛІТА ДЛЯ ДВОСТОРОННЬОЇ КОНВЕРТАЦІЇ ДІЙСНИХ ЧИСЕЛ ІЗ ДЕСЯТКОВОГО У ДВІЙКОВЕ ПОДАННЯ

Станіслав Лізунов, Максим Тетьорко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олексій Піскунов, к.ф.-м.н., с.н.с.

Ключові слова: двійкова система числення, дійсні числа, конвертація дійсних чисел, IEEE 754

Розробка і реалізація математичних алгоритмів, які працюють у області дійсних чисел, вимагає відповідного представлення дійсних чисел у двійковій системі для можливості обчислення їх засобами електронно-

обчислювальних машин. Як показано в монографії [1], це подання є неоднозначним та при математичних обчисленнях може призводити як до занадто грубих округлень, так і до більш суттєвих помилок. Частково цю проблему вирішив міжнародний стандарт IEEE 754, що визначає формати обміну та арифметичні формати і методи для двійкової та десяткової арифметики дійсних чисел в середовищах програмного забезпечення та приділяє увагу елементарним арифметичним обчисленням. Тому від розробника та особливо тестувальника ПЗ потребується чітке розуміння значення кожного окремого біта аналізованого дійсного числа.

Необхідно розробити утиліту, що по-перше, дозволяє розробникам краще розуміти результати арифметичних обчислень та підбирати значення одинарної або подвійної точності, які потенційно призводять до помилок та грубих округлень, по-друге, використовувати її для пакетної обробки CSV-файлів.

Для реалізації використовувалась мова програмування C, вільно поширювані компілятор G++ та getopt - модуль розбору аргументів командного рядка.

Використання утиліти виконується за допомогою наступних ключів:

- d2b <double_number> - число з подвійною точністю у двійкове подання
- f2b <float_number> - число з одинарною точністю у двійкове подання
- b2d <binary_string_64> - двійкове подання 64 біт у число з подвійною точністю
- b2f <binary_string_32> - двійкове подання 32 біт у число з одинарною точністю
- 32 – одинарна точність для окремого подання знаку, експоненти і мантиси
- 64 - подвійна точність для окремого подання знаку, експоненти і мантиси
- sign <sign_bit> - окреме подання знаку
- exp <exponent_binary_string> - окреме подання експоненти у двійковому поданні
- expAlt <exponent_number> - окреме подання експоненти у десятковому поданні
- mantissa <mantissa_binary_string> - окреме подання мантиси
- csv <file_name> - конвертація стовпчика десяткових чисел у CSV-файлі
- csvb <file_name> - конвертація стовпчика двійкових чисел у CSV-файлі
- h – виклик довідки
- v – виведення додаткової інформації

Висновок

Утиліта повністю задовольняє поставлене завдання і може бути застосована при розробці функцій дійсного аргументу та для точного підбору тестових значень для перевірки коректності обчислень. Модуль getopt виявляється зручним засобом для розробки консольних додатків.

Список використаних джерел:

1. William J. Cody, William Waite Software manual for the elementary functions: монографія Englewood Cliffs: Prentice-Hall, Inc., 1980. 269 с.

УДК 519.625

ФОРМАЛЬНЕ ТЕСТУВАННЯ ФУНКЦІЙ ДІЙСНОГО АРГУМЕНТУ**Топіха Надія***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Піскунов Олексій, к.ф.-м.н., с.н.с.*

Ключові слова: формальне тестування, RAISE Specification Language, алгебраїчне проектування, функції дійсного аргументу.

У доповіді представлено застосування методів формального проектування програмного забезпечення для тестування функцій дійсного аргументу. Запропоновано використання мови формальних специфікацій RAISE Specification Language (RSL) для створення формальних специфікацій функцій обчислення довжини дуги меридіана. Виконано формулювання умов для тестування у вигляді аксіом, що дозволяє забезпечити формальну коректність програмних компонентів.

Методи формального проектування є ефективним інструментом для забезпечення надійності програмного забезпечення [1], особливо у випадках, коли йдеться про обчислення з чисельними методами. Однак їх застосування у практичній розробці досі є обмеженим. Мета дослідження – продемонструвати можливість використання формальних специфікацій у програмуванні та тестуванні математичних функцій.

Було використано чотири функції для обчислення довжини дуги меридіана [2], а також сформульовано шість умов димових тестів, що дають змогу на ранніх етапах перевіряти правильність роботи програмних компонентів. Додатково проведено тестування на порушення умов монотонності, що є важливим для забезпечення коректності математичних моделей.

Для верифікації специфікацій використано утиліту RSLTC [3], яка дозволила провести статичну перевірку коду та виділити класи еквівалентності. У ході дослідження було уточнено сім коефіцієнтів розкладу функцій у ряд Маклорена (C0, C2, C4, C6, D2, D4, D6) та розраховано два додаткові коефіцієнти (C8, D8), що дозволяє підвищити точність обчислень.

Також запропоновано техніку створення узагальненого драйвера тестів, що використовує механізм успадкування класів у .NET. Це дає змогу організувати ефективне тестування функцій ще до їхньої остаточної реалізації, підвищуючи якість розробленого програмного забезпечення.

Висновки

Результати дослідження свідчать про ефективність застосування формальних специфікацій для тестування функцій дійсного аргументу. Запропонований підхід сприяє підвищенню надійності

програмних компонентів [4] і може бути використаний у промисловій розробці програмного забезпечення.

Список використаних джерел:

1. Haxthausen A.E. Lecture Notes on The RAISE Development Method, 1999. <http://www2.imm.dtu.dk/courses/02263/E20/Files/methodnotes99.pdf>.
2. Cody W. Software Manual for the Elementary Functions/ W.Cody, W.Waite//. Prentice-Hall, Inc., USA, 1980.
3. Piskunov A.G. Формальний погляд на тестування функцій дійсного аргументу / О.Г.Піскунов, Н.П.Тупко, Н.В.Топіха // XI Міжнародна науково-технічна Internet-конференція 'Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційнотехнічними та техно-логічними комплексами' AIAT-2024, 2024.
4. Parnas D.L. Really rethinking 'formal methods'. Computer (IEEE Computer Society), 43:28–34, 01 2010.

УДК 004.424, 004.8+159.95

ДОСЛІДЖЕННЯ ОЦІНКИ ЯКОСТІ МОДЕЛЕЙ НАВЧАННЯ

Куліш Руслана

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Приставка Пилип, д.т.н., зав. каф. ПМ

Ключові слова: Машинне навчання, оцінка якості моделей.

Зі стрімким розвитком машинного навчання та його широким впровадженням у різноманітні сфери життя набуває актуальності проблема якісної оцінки для забезпечення надійності та ефективності роботи моделей у реальних застосуваннях. Зростає потреба у вдосконалених методах аналізу та порівняння результатів. Використання різних інструментів для оцінки дозволяє отримати детальнішу картину ефективності моделей, що сприяє їх подальшій оптимізації та адаптації до конкретних завдань.

Розробка та реалізація програмного забезпечення для оцінки якості моделей навчання шляхом застосування різноманітних інструментів та метрик оцінювання.

У дослідженні оцінювали якість моделей машинного навчання, використовуючи метрики, що базуються на підрахунку істинно "вірних"(TP), хибно "вірних"(FP), істинно "невірних"(TN) та хибно "невірних"(FN) значень [1, 2].

Результати проведеного дослідження наочно представлені у вигляді графіків. Основними знахідками є: графік, що відображає співвідношення істинно позитивних (TP) та хибно позитивних (FP) результатів для різних моделей; графік, який ілюструє співвідношення істинно негативних (TN) та хибно негативних (FN) значень; а також набір графіків, що візуалізують розподіл ймовірностей для кожного з розглянутих класів. Ці візуалізації дозволяють комплексно оцінити якість та особливості роботи кожної досліджуваної моделі.

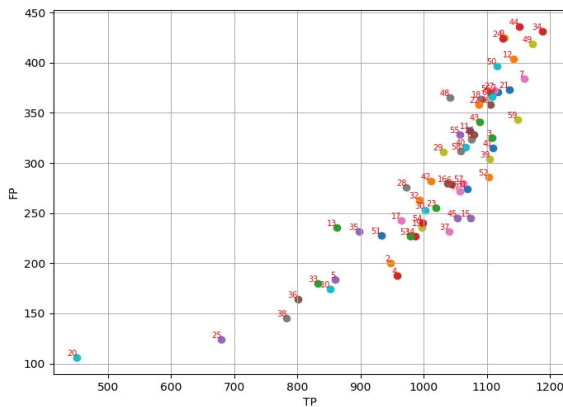


Рис. 1: Співвідношення TP та FP

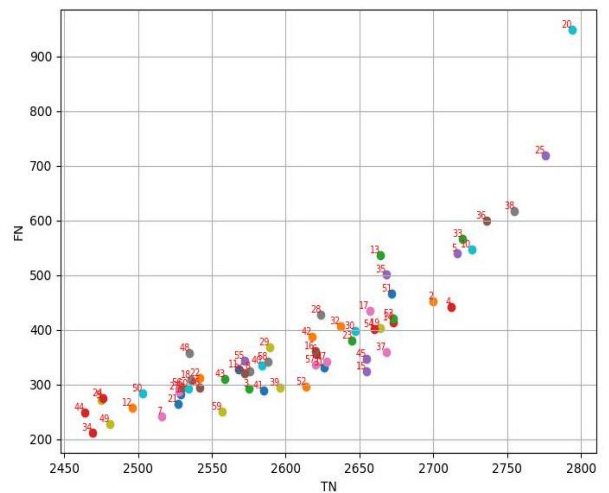


Рис. 2: Співвідношення TN та FN

Висновки

Отримані результати дозволяють оцінити ефективність моделей класифікації для кожного класу та виявити потенційні проблемні області. Проведений аналіз може бути використаний для подальшої оптимізації моделей та підвищення їхньої точності в реальних застосуваннях.

Список використаних джерел:

1. Calin, O. Deep Learning Architectures. A Mathematical Approach / Ovidiu Calin. — Cham : Springer, 2020. — 760 p.
2. Murphy, K. P. Probabilistic Machine Learning: An Introduction / Kevin P. Murphy. — Cambridge, MA : MIT Press, 2022. — 858 p.

УДК 004.424

МНОЖЕННЯ МАТРИЦЬ З ВИКОРИСТАННЯМ КЕШ-ФРЕНДЛІ КОДУ

Шапран Олег, Кротова Анастасія, Головкін Максим

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Андрій Шевченко, ст. вик. каф. ПМ

Ключові слова: множення матриць, кеш-френдлі код, ARM64, Intel x64, типи даних.

Множення матриць — це фундаментальна бінарна операція, яка утворює нову матрицю (добуток) із двох заданих матриць, і є ключовою в обчислювальній техніці, зокрема в машинному навчанні [1]. Вона широко застосовується в нейронних мережах, таких як багатошарові перцептрони (MLP), згорткові мережі (CNN), трансформери та графові нейронні мережі (GNN), де домінує в операціях згортки, механізму уваги та лінійних шарів. Однак висока обчислювальна складність множення матриць, яка сягає $O(N^3)$, потребує оптимізації для забезпечення ефективності сучасних систем. Дослідження показують, що кеш-френдлі підходи, такі як плиткове розбиття (тайлінг), значно підвищують продуктивність завдяки зменшенню промахів кешу та оптимізації доступу до пам'яті [2]. Актуальність порівняння наївного та оптимізованого методів множення матриць на різних архітектурах ЦП (ARM64 та Intel i9-13980HX) та різних типах елементів матриць.

Порівняти продуктивність «наївного» та кеш-френдлі методів множення матриць використовуючи ПК та SBC з ЦП ARM64 та Intel i9-13980HX. Додатково проаналізувати ефективність/швидкодію обчислень використавши типи даних int та float.

Досліджено множення матриць різних розмірів (512×512 , 1024×1024 , ... , 3072×3072) на архітектурах ARM64 та Intel i9-13980HX для типів int і float. Реалізовано два алгоритми: «наївний» (з потрійним циклом) та оптимізований метод (що використовує спец. техніки оптимізації).

Оптимізований метод включає п'ять ключових кроків: **тайлінг** - розбиття матриць на блоки (наприклад, 64×64) для зменшення промахів кешу та прискорення обчислень; **розгортання циклу** - внутрішній цикл множення «розгорнуто» на 8 операцій за ітерацію, для зменшення накладних витрат на організацію циклу і полегшення векторизації компілятором; **кеш-френдлі** - копіювання блоку матриці B в суцільний масив з використанням вказівників та одночасного транспонування (блоку матриці B); **використання вказівників** - застосування вказівників для послідовного доступу до елементів, що прискорює виконання та покращує вірогідність векторизації коду компілятором.

Кеш-френдлі метод із тайлінгом, розгортанням циклу, транспонуванням та іншими оптимізаціями прискорює множення матриць порівняно з наївним завдяки зменшенню промахів кешу та накладних витрат на цикли.

Таблиця 1. Прискорення множення матриць на різних платформах

Intel x64		ARM64	
Розмір матриці N	Швидкодія	Розмір матриці N	Швидкодія
Int			
512×512	2.5	512×512	13.0
...	...	...	...
3072×3072	17.0	3072×3072	39.3
Float			
512×512	2.0	512×512	3.7
...	...	...	...
3072×3072	7.4	3072×3072	9.8

ARM64 демонструє значно вище прискорення для int завдяки кращій оптимізації кешу та вищій енергоефективності, тоді як для float різниця менш виражена через обмеження векторизації.

Кеш-оптимізація множення матриць забезпечує значне підвищення продуктивності, що має цінність для високопродуктивних обчислень. Отримані результати можуть бути застосовані в задачах машинного навчання та обробки великих даних, де важлива ефективність роботи з матрицями на різних архітектурах.

Список використаних джерел:

1. Гантмахер Ф. Р. Теорія матриць. — 2025. — 757 с.(укр.)
2. Carvalho, J. Embedded Computing for High Performance: Efficient Mapping of Computations Using Customization, Code Transformations and Compilation / João M.P. Cardoso, José G.F. Coutinho, Pedro C. Diniz. — London : Morgan Kaufmann, 2017. — 161p. — URL: <https://books.google.com.ua/books?id=BaDDCQAAQBAJ> (дата звернення: 24.03.2025).
3. Skiena, Steven (2008). Sorting and Searching. The Algorithm Design Manual. (англ.)

УДК 004.42

ПРАВОВА ОХОРОНА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кулешова Анастасія

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Шевченко Андрій, ст. викл. каф. ПМ*

Ключові слова: ліцензування ІТ, патентування ІТ, інтелектуальна власність

На даний момент, у час бурхливого розвитку інформаційних технологій, актуальною є проблема ефективної правової охорони інтелектуальної власності, головним чином через ліцензування та патентування у сфері інформаційних технологій (ІТ). Дослідження в цій галузі дуже важливі, оскільки інновації стають основою для конкурентоспроможності компаній і для розвитку національної економіки.

Грамотне використання різних видів ліцензій допоможе досягти оптимального балансу між технологічною відкритістю та збереженням комерційних інтересів розробників, що є основною умовою просування інноваційного процесу. Ліцензування може здійснюватися за різними моделями – від відкритих ліцензій, наприклад, GNU General Public License (GPL), MIT License, Apache License, до комерційних варіантів.

Кожен тип має свій набір характеристик, плюсів і мінусів, тому всі вони знаходять застосування в різних сферах ІТ. Нижче представлено узагальнену таблицю, що ілюструє основні параметри аналізованих типів ліцензій:

Тип ліцензії	Переваги	Недоліки	Застосування
GNU General Public License (GPL)	Він гарантує збереження відкритості коду, стимулює співпрацю в розробці та сприяє спільноті розробників.	Не дозволяє інтегрувати його в комерційні проекти, оскільки похідний код має розповсюджуватися за тією самою ліцензією.	Продукти з відкритим кодом, проекти з колективною розробкою.
MIT License	Дуже простий і доступний для комерційного використання, сприяє швидкому впровадженню новаторських рішень.	Вимоги щодо авторських прав можуть призвести до неструктурованого використання коду без гарантій.	Стартапи, легкі та модульні проекти, які потребують адаптації коду.
Apache License	Формує міцну основу для патентних прав розробників, забезпечує юридичну визначеність, яка захищає їхні права, залишається сумісною з іншими відкритими ліцензіями.	Складне злиття з дуже складними комерційними угодами. Це вимагає ретельного аналізу умов ліцензії, щоб гарантувати їх відповідність формальностям компанії.	Широкі структури програмного забезпечення, які мають патентні міркування.
Комерційні ліцензії	Пропонують максимальний контроль над використанням програмного забезпечення, можливість отримати додатковий дохід від ліцензування.	Прописування доступу до коду може не сприяти розвитку потенціалу спільної розробки, може створювати перешкоди для інноваційної інтеграції.	Висока комерційна вартість програмних продуктів, корпоративних рішень.

У сфері ІТ патентування забезпечує правовий захист інновацій та монополію на їх використання. Однак існують проблеми з патентуванням ідей та алгоритмів, які не завжди підлягають правовій охороні. Поєднання патентного захисту та ліцензування дозволяє ефективно реалізувати інтереси розробників і підтримувати обіг знань у наукових колах.

Відкрите ліцензування сприяє інтеграції нових рішень у наявні системи, тоді як комерційні ліцензії та патенти захищають інвестиції в технології. Встановлення балансу між цими підходами є важливим завданням законодавства та корпоративної політики.

Знання особливостей ІТ-ліцензування та патентування відіграє ключову роль у правовому та фінансовому успіху інноваційних проєктів. Нові тенденції свідчать, що поєднання відкритого та комерційного ліцензування з належним патентним захистом сприятиме розвитку ІТ-індустрії, підвищенню конкурентоспроможності та ефективному використанню технологій на світовому ринку.

УДК 004.42

РОЗРОБКА КЛІЄНТ-СЕРВЕРНОЇ СИСТЕМИ УПРАВЛІННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ ІЗ СИНХРОНІЗОВАНОЮ ОБРОБКОЮ ВІДЕОПОТОКУ ТА ТЕЛЕМЕТРИЧНИХ ДАНИХ ЧЕРЕЗ MAVSDK

Єгор Пронь

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Пилип Приставка, д.т.н., проф.

Ключові слова: автономна система управління, БПЛА, клієнт-серверний додаток

Вступ. Сучасні засоби подавлення зв'язку спонукають до розвитку автономних систем управління, які нівелюють фактор втрати зв'язку з пультом керування безпілотного літального апарату (далі БПЛА). У статті [1] від Palantir розглядаються майбутні напрямки розвитку автономної навігації БПЛА, ідея полягає в тому, щоб поєднати сенсори БПЛА (гіроскоп, акселерометр і т.і.), оптичний потік (рух пікселів) і впізнавання орієнтирів по вбудованій мапі. Саме для реалізації цієї системи необхідно вміти взаємодіяти з БПЛА через протокол обміну інформації MAVLink.

Мета. Розробка та апробація клієнт-серверної системи, яка дозволяє: надсилати команди з наземної станції на БПЛА; отримувати відео з камери БПЛА на сервері; синхронізувати відео з телеметрією.

Об'єкт дослідження – управління БПЛА.

Програмне забезпечення та технології: мова програмування Python, бібліотека для написання паралельного коду asyncio; взаємодія з польотним контролером за допомогою бібліотеки MAVSDK (команди arm, disarm і т.і., отримання телеметрії); клієнт-серверна взаємодія через TCP з'єднання; симулятор польоту SITL; бібліотека передачі відео vidgear.

Методика

1. Багатопотокова (конкурентна) архітектура, у якій виділено окремі потоки на обробку телеметрії, передачу команд та обробку і передачу відео
2. Тестування клієнт-серверного додатку в симуляції

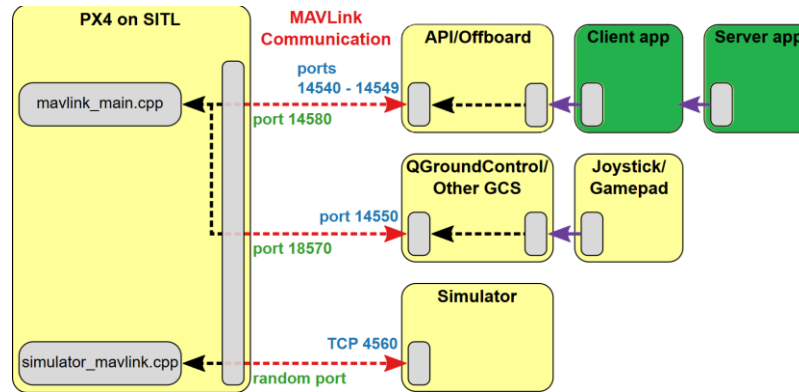


Рис. 1 Схема типового середовища симуляції SITL [2]

Результати. Перед випробуваннями на БПЛА, попереднє тестування клієнт-серверного додатку в симуляції допомогло вирішити “дитячі” проблеми додатку. Також симуляція допомогла спланувати послідовність дій в майбутньому експерименті. Перші спроби реального випробування були неуспішні через некалібровані сенсори БПЛА. Проте після калібрування, експеримент вдалося провести. Взаємодія комп’ютера компаньйона Raspberry PI 4B із польотним контролером Pixhawk 2.4.6 успішна протестована за допомогою таких дій як: зліт на певну висоту, утримання висоти, зміна вектору руху.

Передача команд і відео також була успішна, але із віддаленням БПЛА від наземної станції виникає нестабільний Wi-Fi зв’язок через вбудовані антени в пристроях Raspberry та на ноутбуці (наземна станція). Проте навіть при втраті зв’язку, компаньйон комп’ютер продовжував давати команди для виконання попередньо надісланої місії з наземної станції.

Висновки

Клієнт-серверна система продемонструвала ефективне поєднання методів передачі команд та обробки відео, що дає змогу масштабувати підхід для створення автономних безпілотних систем керування. Додаток може бути використаний у проектах, де потрібна синхронізована взаємодія між польотним контролером і компаньйоном комп’ютером.

Список використаних джерел:

1. The Future of Drone Navigation. URL: <https://blog.palantir.com/the-future-of-drone-navigation-7236075fdedf> (Published: 14.10.2024).
2. Симуляція. URL: <https://docs.px4.io/main/uk/simulation/>

УДК 004.8

ІНТЕГРАЦІЯ НЕЙРОННИХ МЕРЕЖ ТА ЕВРИСТИЧНИХ АЛГОРИТМІВ В СИСТЕМАХ ПРИЙНЯТТЯ РІШЕНЬ

Могильний Павло

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Микола Гузій, к.т.н., доц.

Ключові слова: штучний інтелект, алгоритми прийняття рішень, нейронні мережі, підкріплювальне навчання, Minimax, Монте-Карло.

Вступ. Сучасні алгоритми прийняття рішень відіграють важливу роль у багатьох галузях, включаючи автономні системи, фінансове прогнозування, робототехніку та медичну діагностику [1]. Вони потребують вдосконалення для ефективного функціонування в умовах складних обчислювальних середовищ. Класичні евристичні алгоритми (Minimax, Монте-Карло), мають значні обмеження у швидкодії та масштабованості.[2] Одним із підходів до вирішення цієї проблеми є інтеграція глибоких нейронних мереж та евристичних алгоритмів для покращення їх ефективності за рахунок оптимізації оцінки станів і пошуку рішень [3]

Попри схожість класичними з підходами, що використовуються для пошуку рішень, (наприклад в AlphaZero), це дослідження зосереджується на гібридному підході. Він передбачає використання нейромереж як допоміжного інструменту для покращення традиційних алгоритмів.

Мета. Дослідити можливості використання нейронних мереж для покращення ефективності класичних алгоритмів прийняття рішень, зокрема Minimax та Монте-Карло.

Матеріали та методи. Об'єктом дослідження є алгоритми прийняття рішень. Предметом дослідження є методи інтеграції нейронних мереж у класичні алгоритми прийняття рішень. Реалізовано модель глибокої нейронної мережі для оцінки станів, яка може використовуватися як евристична функція для Minimax або для покращення процесу вибору в Монте-Карло. Програмна реалізація виконана на базі бібліотек TensorFlow, PyTorch, NumPy та Pandas. Для оцінки ефективності алгоритмів проведено тестування в контексті шахового рушія. Порівняльний аналіз проведено за критеріями швидкодії, якості прийнятих рішень та використання обчислювальних ресурсів.

Результати. У порівнянні з класичним Minimax, використання нейромережі дозволило зменшити середній час обчислення на 12%. Це відповідає результатам, отриманим у дослідженнях Silver et al. [2], де застосування нейромереж у глибоких ігрових алгоритмах значно покращувало швидкодію. Нейромережа дозволяє швидше відкидати менш перспективні варіанти, що значно скорочувало кількість необхідних розрахунків.

При тестуванні евристичного алгоритму пошуку по дереву Монте-Карло з використанням нейромережі вдалося зменшити кількість необхідних симуляцій майже вдвічі без значної втрати точності

вибору ходів. Це підтверджує ефективність підходу, запропонованого в [3], де навчання з підкріпленням дозволяло значно покращити адаптацію алгоритму до складних ситуацій.

Оцінка продуктивності алгоритмів також включає аналіз використання обчислювальних ресурсів. Впровадження нейромережі призвело до збільшення вимог до пам'яті та часу на навчання, проте це компенсувалося покращенням швидкодії у процесі прийняття рішень.

Висновки. Інтеграція нейронних мереж та класичних евристичних алгоритмів прийняття рішень значно покращує їхню ефективність. Поєднання алгоритму Minimax з нейронною мережею дозволяє зменшити обчислювальні витрати, а навчання з підкріпленням в алгоритмі пошуку по дереву Монте-Карло дозволяє краще аналізувати можливі сценарії та обирати найбільш перспективні шляхи. Гібридний підхід показав свою ефективність у шахових рушіях, що відкриває можливості для його подальшого використання в теорії ігор, теорії прийняття рішень, дослідженні операцій.

Список використаних джерел

1. Russell S. J., Norvig P. Artificial Intelligence: A Modern Approach, Pearson EText, Global Edition. Pearson Education, Limited, 2021.
2. A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play / D. Silver et al. *Science*. 2018. Vol. 362, no. 6419. P. 1140–1144. URL: <https://doi.org/10.1126/science.aar6404> (date of access: 25.03.2025).
3. Bengio Y., Courville A., Goodfellow I. Deep Learning. MIT Press, 2016. 800 p..

УДК 004.8:004.9

ТЕХНОЛОГІЇ НЕЙРОННИХ МЕРЕЖ ДЛЯ ОБРОБКИ ВЕЛИКИХ ОБ'ЄМІВ ДАНИХ

Олександр Винник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Микола Проценко, к.т.н., доц.

Ключові слова: нейронні мережі, CNN, LSTM, глибинне навчання

Стрімкий розвиток нейронних мереж та зростання обсягу доступних даних відкривають нові можливості практичного використання технологій інтелектуального аналізу даних. Штучні нейронні мережі (НМ) – математичні моделі, побудовані за принципами подання й обробки інформації у біологічних нейронних мережах[1] Завдяки здатності до самонавчання на великих обсягах даних НМ можуть виявляти складні закономірності та приховані зв'язки, які не завжди доступні традиційним методам аналізу.

Для аналізу великих об'ємів даних із подальшим опрацюванням ознак та знаходження закономірностей найчастіше використовуються CNN та LSTM моделі нейронних мереж із застосуванням різних методів навчання, кожна із моделей має різні структурні складові та будову.

Згорткові нейронні мережі (ЗНМ, CNN, ConvNet) – клас глибоких штучних нейронних мереж прямого поширення, який застосовується до аналізу зображень. ЗНМ використовують різновид багатопарових перцептронів, архітектури спільних ваг та характеристик ЗНМ інваріантні відносно паралельного перенесення. Незалежність у конструюванні ознак від апіорних знань є великою перевагою. Приховані шари ЗНМ зазвичай складаються зі згорткових шарів, агрегувальних шарів, повноз'єднаних шарів та шарів нормалізації. Згорткові шари застосовують до входу операцію згортки, передаючи результат до наступного шару. Згортка імітує реакцію окремого нейрону на зоровий стимул. Наприклад для діагностики серцево-судинних захворювань CNN часто використовуються для класифікації ЕКГ-сигналів або зображень судин та визначати аритмії чи інші зміни.

Основна ідея LSTM полягає в тому, що вхідні послідовності по-різному впливають на результат поточної ітерації, необхідно розробити метод, який деяким елементам в контексті в минулих ітераціях буде надавати більшу вагу, тобто більший вплив, а іншим елементам – менший[2]. Структура LSTM також нагадує ланцюг, але модулі виглядають по-іншому. Замість одного шару нейронної мережі, вони містять чотири шари, які взаємодіють особливим чином (рис. 1)

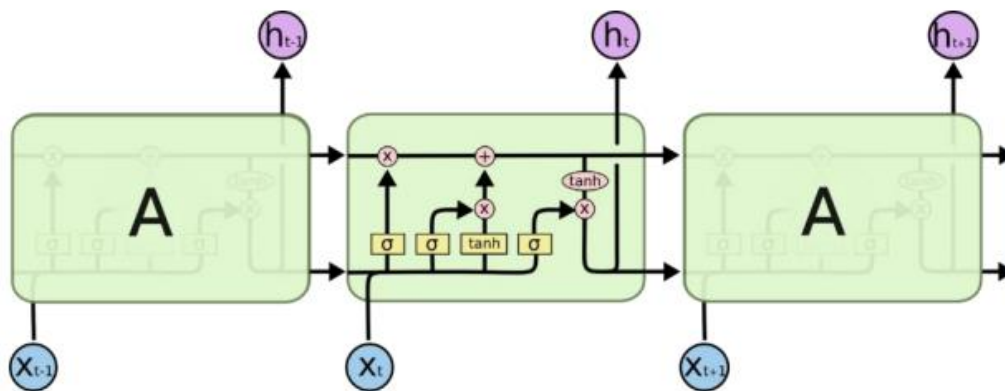


Рис.1 Чотиришарова модель LSTM [4]

Ключовий компонент LSTM – це стан комірки (cell state) – верхня горизонтальна лінія (рис.1). Дана модель має певні структури – фільтри (gates), за допомогою яких можна керувати інформацією: пропускати / не пропускати, видаляти за необхідності. Також дані фільтри дозволяють захищати та контролювати стан комірки, LSTM застосовуються для прогнозування числових рядів на основі обробки наборів даних та виявлення аномалій.

Особливої уваги заслуговують гібридні підходи. Дослідження показують, що CNN краще обробляють короткі сегменти даних або статичні зображення, тоді як LSTM ефективніші для довгих послідовностей. Однак у багатьох випадках комбінація CNN і LSTM (гібридні моделі) демонструє найкращі результати. Наприклад, CNN може витягувати просторові ознаки з ЕКГ, а LSTM — аналізувати їх у часовому контексті. У порівнянні гібридна модель досягла точності 98% у класифікації аритмій при серцево-судинних захворюваннях, перевершивши результати обробки даних CNN (95%) та LSTM (93%) [3].

Висновок. Використання згорткових нейромереж CNN для коротких сегментів даних, LSTM для довгих послідовностей та гібридних моделей для комплексного аналізу числових рядів відкриває нові можливості для підвищення точності та достовірності результатів обробки великих наборів даних (зокрема виявлення аномалій трафіка в комп'ютерній інженерії).

Список використаних джерел:

1. Добровська Л. М., Добровська І. А. Теорія та практика нейронних мереж : навч. посіб. Київ, 2015. 395 с.
2. Субботін С. О. НЕЙРОННІ МЕРЕЖІ: ТЕОРІЯ ТА ПРАКТИКА : навч. посіб. Житомир : О. О. Євенок, 2020. 184 с.
3. Sudha V. K., Kumar D. Hybrid CNN and LSTM Network For Heart Disease Prediction. 2022. 11 p.

УДК 004.8

**РОЗПІЗНАВАННЯ МІСЦЕВОСТІ ЗА ДАНИМИ ПОВІТРЯНОГО СПОСТЕРЕЖЕННЯ
НА ОСНОВІ СТРУКТУРНИХ ОЗНАК**

Кривуца Ігор

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Пулип Приставка, д.т.н., проф.

Ключові слова: інформативні ділянки, ResNet50v2, аерофотозйомка

Метою роботи є розробка альтернативного методу навігації для безпілотних літальних апаратів (БПЛА) в умовах заглушення або відсутності сигналів Global Position System (GPS), зокрема через використання методів комп'ютерного зору та машинного навчання.

У якості вхідних даних використовуються цифрові знімки місцевості, прив'язані до географічних координат та зображення з камери БПЛА. Основним методом аналізу зображень є згорткова нейронна мережа-класифікатор ResNet50v2 [1], донавчена на датасеті «Аерозйомка» [2]. Для пошуку інформативних ділянок застосовано алгоритми, що ґрунтуються на методі головних компонентів (МГК) та відстані Махаланобіса. Для порівняння гістограм використовується критерій Колмогорова–Смирнова та розбіжність Кульбака–Лейбнера.

Розроблена технологія включає два етапи: виявлення інформативних ділянок на ЦЗ та аналіз даних під час польоту. Ідентифікація особливостей здійснюється через побудову гістограми класів текстур у ковзному вікні. За результатами аналізу формується масив найбільш інформативних ділянок, з яких обираються точки для формування маршруту. Під час польоту знімки, які отримані з камери БПЛА, перевіряються на відповідність з еталонним зображенням. У разі співпадіння здійснюється уточнення місцеположення об'єкта через мінімізацію розбіжності Кульбака–Лейблера між гістограмами.

Висновки. Запропонована технологія дозволяє підвищити ефективність місій БПЛА за рахунок автоматизованого виділення ключових ділянок до польоту та визначення координат місцевості під час польоту.

Список використаних джерел:

1. He, K., Zhang, X., Ren, S., Sun, J. "Deep Residual Learning for Image Recognition." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2016).
2. Навчальний набір даних «Аерозйомка» [Електронний ресурс]: https://drive.google.com/file/d/1BAmsRbYUyCnrPYn-jpHI7l_6qsNmc9o6/view

УДК 004.8

ТЕХНОЛОГІЯ ПІДТРИМКИ ВИРІШЕННЯ НАВІГАЦІЙНИХ ЗАДАЧ НА ОСНОВІ ДАНИХ ПОВІТРЯНОГО СПОСТЕРЕЖЕННЯ ТА АЛГОРИТМІВ ПОШУКУ ОСОБЛИВИХ ТОЧОК**Прищепя Дмитро***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – д-р.техн.наук проф. Приставка П. О.*

Ключові слова: навігація, розпізнавання, SIFT, ORB, LightGlue, SuperPoint, обробка в режимі реального часу, локальні особливості зображень, автономність БПЛА.

Навігаційні технології, що забезпечують автономність борту літального апарату є актуальною задачею [1], адже вони використовуються у розвідувальних та бойових місіях за умов дій ворожих завад. Метою роботи є створення інформаційної технології, що дозволяє на основі даних з камер цільового призначення БПЛА та методів комп'ютерного зору виявити або уточнити місцеположення БПЛА. Така технологія передбачає розпізнавання об'єкту на основі методів з пошуку особливих точок, визначення приблизних координат об'єктів, що знаходяться в полі видимості камери борту БПЛА, за необхідності можливе визначення потрібного вектору руху.

У роботі розглянуто методи пошуку та зіставлення локальних особливостей зображень, досліджено їх продуктивність [2]. Тестування було здійснено на різних відео, фото та різному апаратному забезпеченні. Також застосовано операції згладжування та зміну розміру зображення. Робота може бути використана для підтримки вирішення навігаційних задач, що пов'язані зі встановленням геолокації борту БПЛА у режимі радіомовчання або за умови дій радіозавад.

Серед напрямків подальших досліджень можна виділити підбір гіперпараметрів методів, що використовувалися, підбір порогового значення для відсіювання хибних спрацювань, модифікація існуючих або створення власних методів для пошуку та порівняння локальних особливостей зображень.

Список використаних джерел:

1. Деякі питання розвитку критичних технологій у сфері виробництва озброєння та військової техніки [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/600-2017-%D1%80>
2. Karami E. Image Matching Using SIFT, SURF, BRIEF and ORB: Performance Comparison for Distorted Images / E. Karami, S. Prasad, M. Shehata. – 2015. – С.5

УДК 004.8

МОДЕЛЮВАННЯ ОСВІТНІХ ТРАЄКТОРІЙ УКРАЇНСЬКИХ СТУДЕНТІВ НА ОСНОВІ ВІДКРИТИХ ДАНИХ

Владислав Бандурін

Державний університет "Київський авіаційний інститут", м. Київ

Науковий керівник – Пилип Приставка, д-р техн. наук.

Ключові слова: освітні траєкторії, аналіз даних, вища освіта, вибір спеціальності, вступ, регіони.

Система вищої освіти в Україні зазнає значних змін, зумовлених економічними, демографічними, воєнними та соціальними факторами. Повномасштабне вторгнення Росії в Україну у 2022 році стало каталізатором істотних змін у структурі вступу до закладів вищої освіти, зокрема – у регіональному розподілі абітурієнтів та їхніх освітніх уподобаннях.

У даному дослідженні розглянуто, як змінилася географія вступу та вибір спеціальностей серед абітурієнтів України до і після початку повномасштабної війни. Метою є виявлення закономірностей у зміні освітніх траєкторій молоді в контексті переміщення населення, доступності освіти в різних регіонах, зміни умов вступу та впливу безпекових факторів.

Об'єктами дослідження є абітурієнти та їхній вибір ЗВО і спеціальностей в межах вступних кампаній 2019–2024 років. Основними характеристиками досліджуваних даних є регіон реєстрації вступника, обраний університет, спеціальність та середній бал ЗНО/НМТ. Аналізуються відкриті дані з порталу ЄДЕБО, що дозволяють відстежити динаміку вступу за роками.

Дослідження проведено за допомогою методів аналізу даних та візуалізації. Було використано:

- аналіз часових рядів для оцінки змін у розподілі вступників за регіонами;
- порівняльний аналіз спеціальностей, які стали більш або менш популярними після 2022 року;
- побудову карт вступної активності по регіонах України.

Результати дослідження показали, що після початку війни спостерігається значне зменшення вступної активності в регіонах, які зазнали бойових дій, натомість зросла кількість вступників у західних регіонах та Києві. Також помітна зміна в уподобаннях щодо спеціальностей – зростання популярності ІТ. Виявлено зменшення регіонального різноманіття у виборі ЗВО.

Отримані дані можуть бути використані для коригування освітньої політики, зокрема – планування ліцензійних обсягів, регіональної підтримки університетів та інформування абітурієнтів.

Подальші дослідження можуть включати аналіз впливу онлайн-освіти, зміни доступу до якісної освіти у різних регіонах та оцінку довгострокових наслідків для розвитку людського капіталу в країні.

Список використаних джерел:

1. Дані ЄДЕБО про вступні кампанії [Електронний ресурс] – Режим доступу: <https://vstup.edbo.gov.ua>.
2. Український центр оцінювання якості освіти (УЦОЯО). Статистичні звіти та результати ЗНО/НМТ [Електронний ресурс] – Режим доступу: <https://testportal.gov.ua>.

UDC 519.233

THE USAGE OF LOGISTIC REGRESSION MODEL FOR DETERMINING RISK OF DIABETES MELLITUS

Vlad Studennykov

State University “Kyiv Aviation Institute”, Kyiv

Supervisor – Tetiana Konrad, PhD, associate professor

Keywords: logistic regression, diabetes mellitus, statistical analysis, machine learning.

Type 2 diabetes mellitus (T2DM) is a widespread chronic disease that significantly affects global public health. Early identification of individuals at high risk of developing T2DM is crucial for implementing preventive measures and reducing healthcare burdens. Machine learning methods, particularly logistic regression, have proven to be effective in predictive modeling for medical applications. Logistic regression provides interpretable results, making it suitable for risk assessment in clinical practice. This study aims to develop and evaluate a logistic regression model for predicting the risk of T2DM based on lifestyle and health-related data.

The aim of this study is to develop a logistic regression model for predicting the risk of type 2 diabetes based on statistical analysis of lifestyle and health-related data.

In this study, the dataset containing information on individuals' lifestyle habits and their diabetes status was used. The dataset was preprocessed and analyzed using statistical methods to identify relevant features for prediction. A logistic regression model was trained using appropriate machine learning libraries, and its performance was evaluated using standard metrics such as accuracy, precision, recall, and the ROC curve. The results were analyzed to determine the model's effectiveness in assessing diabetes risk. Results of this work include the analysis of given dataset, teaching logistic regression model and analysis of its effectiveness. Detailed description of given dataset is given in [1] along with the features that would be used for model training.

Fig. 1 shows the confusion matrix of the trained logistic regression model. For the majority of cases, work of model is correct. ROC curve, shown on figure 2, shows that model performance could be considered as good as the area under curve is > 0.8 .

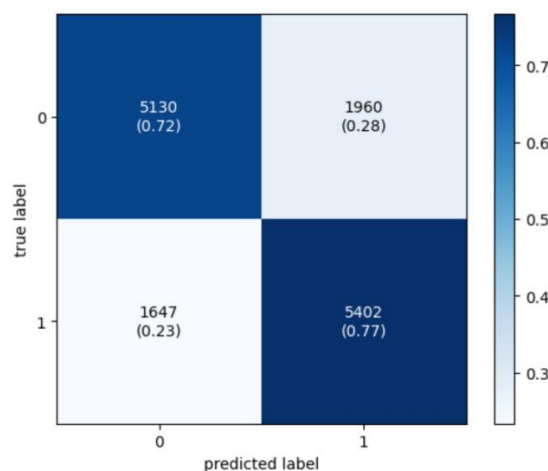


Figure 1 – confusion matrix of model performance

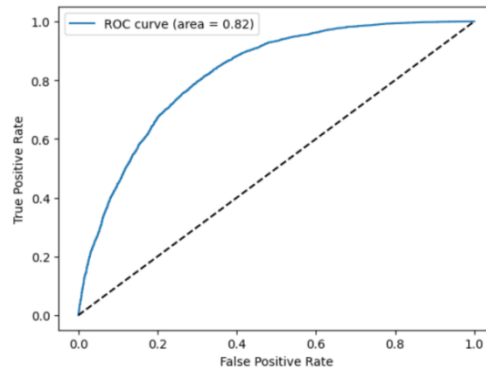


Figure 2 – ROC curve that shows acceptable model performance

Conclusion

This study demonstrated the effectiveness of logistic regression in predicting the risk of type 2 diabetes based on lifestyle and health-related data. The model provided interpretable results, allowing for the identification of key risk factors associated with diabetes. The analysis showed that machine learning techniques, combined with statistical methods, can enhance early risk assessment and support preventive healthcare strategies. Future research could focus on incorporating additional features and comparing different predictive models to improve accuracy and reliability.

References:

1. Diabetes Health Indicators Dataset. (2021, November 8). Kaggle. <https://www.kaggle.com/datasets/alexteboul/diabetes-health-indicators-dataset/data>.
2. Bishop, C. M. (n.d.). *Pattern recognition and machine learning*. Springer Verlag.

УДК 004.8/9(043.2)

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ РУХОМИХ ОБ'ЄКТІВ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Артюх Владислав

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Альберт Воронін, професор.

Ключові слова: машинне навчання, виявлення об'єктів, комп'ютерний зір, алгоритми, обробка зображень.

Виявлення рухомих об'єктів є важливим завданням у багатьох галузях, наприклад системах безпеки, безпілотних літальних апаратах і робототехніці. З розвитком машинного навчання та нейронних мереж, вдалося підвищити точність та ефективність систем виявлення об'єктів [1]. Це дослідження спрямоване на вдосконалення методів виявлення об'єктів за допомогою машинного навчання та базується на аналізі наукових матеріалів на тему комп'ютерного зору і машинного навчання.

Метою дослідження є розробка інформаційної технології виявлення рухомих об'єктів, з використанням методів машинного навчання та комп'ютерного зору для швидкої та більш точнішої обробки зображень.

Об'єктами дослідження є зображення та відео з відеокамер спостереження за використанням згорткових нейронних мереж, для аналізу відео та фотоінформації.

Застосування алгоритму згорткової нейронної мережі (R-CNN) демонструє значне покращення точності виявлення, особливо умовах складного освітлення та розмитості зображення. Дослідження показали, що з впровадженням згорткових нейронних мереж точність систем зросла на 30%[2]. Розробка моделі нейронної мережі передбачає використання великих обсягів даних, особливо зображень різних об'єктів. Системи на основі нейронних мережах, демонструють точність до 95%, перевершуючи традиційні методи [3]. Оптимізація алгоритму дозволить значно зменшити час обробки, забезпечивши високу ефективність у реальному часі [4].

В дослідженні розглядаються згорткові нейронні мережі R-CNN. R-CNN складається із згорткових шарів, які використовуються для визначення важливих ознак з вхідних даних, таких як локальні патерни, межі та текстури, організовуючи під вибірку даних. Рівень підвибірки використовується для зменшення обчислювальної складності, зберігаючи особливості зображення. Завдяки своїй здатності до автоматичного вивчення та абстрагування складних ознак, R-CNN вважається перспективними для підвищення точності виявлення і класифікації об'єктів. Це робить R-CNN важливим напрямком для подальшого вдосконалення методів аналізу зображень у різних сферах.

Висновок. Інформаційна технологія для виявлення об'єктів рухомих об'єктів на базі методів машинного навчання дає змогу суттєво поліпшити швидкість і точність визначення об'єктів. Її можна використати у різноманітних сферах, зокрема, у системах відеоспостереження й транспортних засобах, для збільшення їхньої ефективності та надійності.

Список використаних джерел:

1. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement. 2018
2. Zhang, Y., & Zhang, M. (2021). Advances in Object Detection with Convolutional Neural Networks. Journal of Machine Learning Research.
3. Li, X., & Li, J. (2020). The Impact of Deep Learning on Autonomous Vehicles. Autonomous Systems Review.
4. Wang, H., & Chen, Z. (2019). Optimization Techniques in Computer Vision: A Review. International Journal of Computer Vision.

УДК 004.8/.9(043.2)

INFORMATION TECHNOLOGY FOR DETECTING MOVING OBJECTS BASED ON MACHINE LEARNING

*State University “Kyiv Aviation Institute”, Kyiv**Thesis advisor: Albert Voronin, professor.*

Keywords: machine learning, object detection, computer vision, algorithms, image processing.

Detecting moving objects is an important task in many industries, such as security technology, drones, and robots. With the development of machine learning and neural networks, the accuracy and efficiency of object recognition systems have been improved [1]. This study aims to improve object detection methods using machine learning and is based on the analysis of scientific materials on computer vision and machine learning..

The purpose of the study is to develop information technology for detecting moving objects using machine learning and computer vision methods for faster and more accurate image processing.

The objects of the study are images and videos from surveillance cameras using convolutional neural networks to analyze video and photo information.

The application of the convolutional neural network (R-CNN) algorithm demonstrates a significant improvement in detection accuracy, especially in conditions of difficult lighting and blurred images. Studies have shown that with the introduction of convolutional neural networks, the accuracy of systems has increased by 30%[2]. The development of a neural network model involves the use of large amounts of data, especially images of various objects. Systems based on neural networks demonstrate an accuracy of up to 95%, outperforming traditional methods [3]. Optimization of the algorithm will significantly reduce processing time, ensuring high efficiency in real time[4].

This study examines convolutional neural networks (R-CNN). R-CNN consists of convolutional layers that identify important features of input data, such as local patterns, boundaries, and textures, by organizing the data into subsamples. The subsampling layers reduce the amount of computation while preserving image features. R-CNN is considered promising for improving the accuracy of object detection and classification due to its ability to automatically learn and abstract complex features. This makes R-CNNs an important direction for further improvement of image analysis methods in various fields.

Conclusion. Information technology for moving object detection based on machine learning methods can significantly improve the speed and accuracy of object detection. It can be used in various fields, including video surveillance systems and vehicles, to increase their efficiency and reliability.

References:

1. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement. 2018
2. Zhang, Y., & Zhang, M. (2021). Advances in Object Detection with Convolutional Neural Networks. Journal of Machine Learning Research.
3. Li, X., & Li, J. (2020). The Impact of Deep Learning on Autonomous Vehicles. Autonomous Systems Review.
4. Wang, H., & Chen, Z. (2019). Optimization Techniques in Computer Vision: A Review. International Journal of Computer Vision.

УДК 004.43

СИСТЕМА РОЗРОБКИ І ВИКОРИСТАННЯ СТАНДАРТІВ ОБСЛУГОВУВАННЯ СПІВРОБІТНИКІВ АВІАКОМПАНІЇ

Ярослав Бабич

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Вадим Сураєв, к.т.н., доц.

Ключові слова: авіакомпанія, стандарт обслуговування, сервіс, привілеї, HelpDesk, запит.

Ефективне управління процесами обслуговування співробітників авіакомпанії потребує впровадження чіткої системи стандартів. В авіакомпанії може бути впроваджено систему розробки та використання стандартів обслуговування, яка дозволяє оптимізувати роботу персоналу, підвищити рівень сервісу та забезпечити контроль якості надання послуг.

Стандарт обслуговування – це регламентований набір послуг, що надаються співробітникам відповідно до їхньої посади та підрозділу. Наприклад, для бортпроводників до стандартного пакета входять доступ до системи управління екіпажами, забезпечення робочої уніформи та зв'язок із диспетчерською службою. Для технічного персоналу – доступ до системи технічного обслуговування AMOS, забезпечення робочого інструменту та інші спеціалізовані сервіси.

Розмежування рівнів доступу до інформаційних систем та сервісів здійснюється через диференціацію привілеїв. Для кожного стандарту визначаються права доступу, можливості створення, редагування або видалення даних. Всі ці параметри зберігаються у відповідній базі даних.

Процес обслуговування співробітників складається з кількох етапів:

1. **Початкове налаштування (стартові послуги):** автоматичне створення запитів у системі HelpDesk при прийомі нового працівника. Відповідальний менеджер лише обирає стандарт для відповідної посади.
2. **Поточне обслуговування:** підтримка сервісів відповідно до стандарту та обробка запитів співробітників.
3. **Завершальне обслуговування (стопові послуги):** автоматичне припинення доступу до сервісів при звільненні працівника.
4. **Адаптація при зміні посади:** система аналізує зміни в стандартах та автоматично генерує необхідні запити на оновлення доступу.

Розробка та підтримка бази стандартів здійснюється підрозділом ІТ, а менеджери бізнес-підрозділів можуть вносити пропозиції щодо їхнього оновлення. Усі дані зберігаються на платформі Microsoft SQL

Server, а управління стандартами реалізоване через веб-інтерфейс на базі фреймворку Flask (Python). Доступ до цієї платформи мають менеджери, IT-фахівці та працівники відділу кадрів.

Висновок

Впровадження системи стандартів обслуговування дозволяє значно підвищити ефективність роботи всіх підрозділів авіакомпанії, забезпечити швидке налаштування робочих процесів для персоналу та знизити навантаження на IT-службу.

Список використаних джерел:

1. Матеріали XXIV Міжнародної науково-практичної конференції молодих учених і студентів «Політ. Сучасні проблеми науки» 2-5 квітня 2024 р.
2. Kittitach Keawchaoon ก. ค., Thirawat Chantuk ช. จ., & ศิริวงศ์ พ. (2018). The Developments of Components of Service Standards System for Enhancing Personal Skills Towards Excellency in Social Network System of Thai Commercial Aviation's Employee. *Dusit Thani College Journal*, 11(3), 137–150.

УДК 004.4

ОГЛЯД СУЧАСНИХ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Андрій Бех

Державний університет "Київський авіаційний інститут", Київ

Науковий керівник – Михайло Оленін, к.ф.-м.н., с.н.с., доц.

Ключові слова: розподілені системи, інформаційні системи, хмарні технології, транзакції, узгодженість даних.

Сучасні розподілені інформаційні системи, які об'єднують хмарні технології з мікросервісною архітектурою, мають найвищі рівні масштабованості, надійності та гнучкості обробки даних. Разом з тим, швидкі темпи цифрової трансформації підприємств та, насамперед, сегменту автомобільного транспорту, роблять актуальним необхідність ефективної інтеграції та управління транзакціями [1, 4].

Мета полягає в здійсненні цілісного обзору сучасних розподілених інформаційних систем з аналізом їх архітектурних особливостей, методів інтеграції даних і управління транзакціями з метою виявлення закономірностей, які забезпечують найвищий рівень доступності, надійності та узгодженості даних.

Для цього використовується сучасна наукова література та аналітичні праці, що висвітлюють теоретичні та практичні аспекти побудови систем, особливо в хмарних середовищах з використанням мікросервісної архітектури та технологій штучного інтелекту. Методологія дослідження базується на порівняльному аналізі різних підходів до інтеграції компонентів системи з використанням методів системного аналізу та статистичного моделювання, що дозволяє оцінити ефективність, гнучкість і надійність управління транзакціями.

Аналіз сучасних розподілених інформаційних систем визначає низку ключових аспектів, які впливають на їх масштабованість, інтеграцію даних та ефективність управління транзакціями. Зокрема, дослідження [1] показує, що комбіноване використання хмарних технологій зі штучним інтелектом сприяє оптимізації продуктивності, спричиненої розподіленою обробкою даних, тоді як робота [2] підкреслює переваги архітектури мікросервісів у зменшенні зв'язності між компонентами та збільшенні автономності окремих модулів, хоча занадто багато невеликих сервісів може ускладнити процес зв'язку через необхідність ретельного моделювання меж (bounded contexts). Сучасні підходи до транзакційного управління, орієнтовані на забезпечення консистентності даних за допомогою технологій ACID/BASE, як зазначено у [1] та [4], забезпечують високий рівень інтеграції та узгодженості інформації у єдиному інформаційному просторі, що є критично важливим для систем транспортного обслуговування. Додатково, організаційні та технологічні виклики, розглянуті у [2] та [3], вказують на необхідність ефективної взаємодії між командами розробників та адаптації технологічного стеку до змін ринкових умов, зокрема через впровадження принципів, передбачених Conway's law. Порівняльний аналіз показує, що підхід [1] орієнтований на використання AI для оптимізації розподілених систем, тоді як [2] зосереджується на структурних аспектах зниження зв'язності, а [3] доповнює ці підходи статистичним аналізом ринкових трендів, що дозволяє прогнозувати майбутні напрямки розвитку технологій, у той час як [4] пропонує комплексне визначення територіально-розподілених систем із інтеграцією організаційних, технічних та інформаційних аспектів, що суттєво розширює традиційні підходи до побудови сучасних інформаційних систем.

Висновок

Отримані результати свідчать про те, що сучасні розподілені інформаційні системи здатні забезпечити високий рівень масштабованості, гнучкості та узгодженості даних за рахунок використання хмарних технологій та мікросервісної архітектури. Системний аналіз дозволив встановити, що ефективне управління транзакціями в розподілених середовищах є критичним для забезпечення цілісності інформації, що особливо актуально у сферах із високими вимогами до оперативності обробки даних, зокрема в транспортному обслуговуванні. Подальші дослідження повинні зосередитись на розробці нових методів оптимізації транзакційного управління, що враховують як технологічні, так і організаційні аспекти інтеграції систем.

Список використаних джерел:

1. Zangana, H. M. та Zeebaree, S. R. M. «Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services». *International Journal of Informatics, Information System and Computer Engineering*, 5(1), 2024, с. 11–30.
2. Talaver, O. V. та Vakaliuk, T. A. «Reliable distributed systems: review of modern approaches». *Journal of Edge Computing*, 2023, 2(1), с. 84–101. DOI:10.55056/jec.586.
3. Ткаченко, О. І., Ткаченко, К. О. та Піддубченко, М. В. «Аналіз сучасних тенденцій розробки інформаційних систем». № 4 (24), 2024, с. 205–220. DOI:10.28925/2663-4023.2024.24.205220
4. Додонов, О. Г., Никифоров, О. В., Путятін, В. Г., Додонов, В. О., Куценко, С. А. та Германюк, А. П. «Територіально-розподілені інформаційні комп'ютерні системи у єдиному інформаційному просторі: базові поняття та визначення». *Реєстрація, зберігання і обробка даних*, 2024, Т. 26, № 1, с. 89–99. DOI:10.35681/1560-9189.2024.26.1.308647

УДК 371.26, 004.82

ЗАСТОСУВАННЯ АЛГОРИТМІВ ВИПАДКОВОГО ВИБОРУ ДЛЯ ФОРМУВАННЯ ТЕСТОВИХ ЗАВДАНЬ

Сніжана Білан

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Шибицька, к.т.н., доц.

Ключові слова: алгоритми випадкового вибору, тестовий контроль знань, автоматизація тестування

Вступ

Алгоритми випадкового вибору відіграють важливу роль у сучасних системах оцінювання знань. Вони автоматизують процес формування тестових завдань, забезпечуючи збалансований розподіл питань за рівнем складності[1]. Це сприяє підвищенню об'єктивності оцінювання, зменшенню ймовірності упередженості та адаптації тестів до освітніх стандартів.

Метою дослідження є аналіз ефективності алгоритмів випадкового вибору для генерації тестових завдань та оцінка їх впливу на точність і справедливість процесу оцінювання знань.

Матеріали та методи

Для реалізації випадкової генерації тестових завдань використовуються такі алгоритми[2,3]:

1. Рівномірний випадковий вибір – алгоритм, що забезпечує однакову ймовірність вибору для кожного питання із загального набору.
2. Випадковий вибір із ваговими коефіцієнтами – враховує складність питань, задаючи їм вагові коефіцієнти.
3. Стратифікований вибір – забезпечує рівномірний розподіл запитань за категоріями складності, зменшуючи ризик нерівномірного наповнення тесту.

Результати та обговорення

Для обґрунтування ефективності кожного з цих підходів проведено порівняльний аналіз груп тестів, створених із використанням зазначених методів. У табл.1 наведено ключові переваги та недоліки алгоритмів, які досліджуються.

Рівномірний випадковий вибір є найбільш простим у реалізації, однак він не враховує складність запитань, що може призвести до нерівномірного розподілу складності в тесті. Вибір із ваговими коефіцієнтами дозволяє контролювати складність тесту, коригуючи ймовірність вибору запитань, але цей метод вимагає точного визначення коефіцієнтів для кожного питання, що може бути складним. Стратифікований вибір дає змогу рівномірно розподілити запитання за категоріями складності, що значно зменшує ймовірність перенасичення тесту питаннями одного рівня складності, однак він може бути обмежений, якщо кількість категорій складності перевищує кількість запитань у тесті.

Таблиця 1. Переваги, недоліки та особливості алгоритмів випадкового вибору

Алгоритм	Особливості	Переваги	Недоліки
Рівномірний випадковий вибір	Кожне питання має однакову ймовірність бути обраним із набору запитань незалежно від його складності.	Простота реалізації, мінімізація упередженості у виборі запитань.	Неврахування рівня складності запитань, що може призводити до нерівномірності розподілу складності в тестах.
Вибір із ваговими коефіцієнтами	Використовується механізм коригування ймовірності вибору запитань на основі їхньої складності.	Дозволяє контролювати складність тесту, збалансуючи набір запитань відповідно до освітніх вимог.	Складність визначення вагових коефіцієнтів для кожного запитання, що може ускладнити процес впровадження.
Стратифікований вибір	Забезпечується рівномірний розподіл запитань за заздалегідь визначеними категоріями складності.	Гарантує збалансованість тесту, мінімізує перенасичення питаннями одного рівня складності.	Вимога точного визначення категорій складності, може бути складним при невеликій кількості запитань у тесті.

Узагальнення порівняння алгоритмів випадкового вибору демонструє їхні характерні особливості, що впливають на балансування складності тестів. Простота реалізації та відсутність упередженості є ключовими перевагами рівномірного випадкового вибору, хоча цей метод не завжди забезпечує рівномірність рівнів складності. Вибір із ваговими коефіцієнтами сприяє точному налаштуванню тесту відповідно до визначених освітніх цілей, водночас залишаючи відкритим питання щодо складності коригування коефіцієнтів. Стратифікований вибір забезпечує найбільшу збалансованість за категоріями складності, хоча його ефективність залежить від достатньої кількості запитань у кожній категорії.

Висновок

Використання алгоритмів випадкового вибору оптимізує процес створення тестових завдань, балансує їх складність і підвищує об'єктивність оцінювання знань. Найбільш ефективним є стратифікований вибір, адже він забезпечує рівномірний розподіл запитань за рівнями складності, що значно покращує збалансованість та якість тестів.

Список використаних джерел

1. М.В.Лотош, Н.М.Шибіцька, Особливості створення тестових завдань з програмування //Збірник тез VIII науково-практичної конференції "Новітні мультимедійні технології в освіті та інших сферах діяльності". - К.: НАУ, 2019. – С. 48.
2. H.Wainer, *Computerized Adaptive Testing: A Primer*. Routledge.-2015. – 362p.
3. Kim, J., & Nicewander, W. A. (2018). *Randomization Methods in Online Testing*. Journal of Educational Measurement, 55(3), 289–305.

UDC 656.7:044.22:044:42

IT SERVICE APPLICATION FOR AIRLINE EMPLOYEES POWERED BY ARTIFICIAL INTELLIGENCE

Maksym Budianskyi

State University "Kyiv Aviation Institute", Kyiv

Academic supervisor - Vadym Suraiev, Candidate of Engineering Sciences (Ph. D.)

Keywords: IT Service, Artificial Intelligence, Application Programming Interface.

Aviation faces ever-increasing requirements for the efficiency and speed of IT support for employees. Manual methods of employee support can't keep pace with technological advances, resulting in delays and lost productivity. Recent research shows that artificial intelligence has potential to create hypotheses in science, which allows the use of AI in specific tasks [1]. Working with aviation tasks is so specific, AI models can essentially improve IT service by automating routine tasks and providing quick assistance.

The purpose of the research is to conduct a comparison of the capabilities of Google Gemini and OpenAI ChatGPT models for integration in IT support application. The research is focused on fast AI models.

A comparative analysis of the functionality of Gemini and ChatGPT was realized to validate the results of the research. The study evaluated the performance, cost and availability of both platforms.

Gemini and ChatGPT provide powerful application programming interface for integrating AI in applications, which is especially relevant for a mission-critical industry such as aviation. In aviation IT support, where every minute of downtime can have serious impact, speed and accuracy of problem resolution are crucial. Gemini 2.0 Flash, with its flexible big data pricing plans [2], can be especially useful for processing a large sample of data. For example, when an error occurs across many employees, Gemini can quickly analyze thousands of requests, identify the cause of the failure, and suggest specific steps to fix it.

ChatGPT-4o, with simpler pricing structure and less processing power [3], can be effective for automating routine tasks such as processing employee requests, answering frequently asked questions and providing operating instructions. For example, an IT employee can use the application to get answers to questions about standards or instructions on troubleshooting issues. In the critical situation of a large amount of data, a price comparable OpenAI model can be overloaded and unable to handle all requests.

The Gemini API provides developer tools to integrate AI capabilities in various applications, including aviation IT support systems. Libraries are used to integrate the API into Python application. The google-genai library is a Python SDK that provides a user-friendly way to interact with Gemini generative artificial intelligence models. Providing an API key allows to interact with Gemini.

Conclusions

In the context of IT support for airline employees, Gemini has proven more suitable for scenarios requiring deep data analysis and complex queries, also processing the daily requests of IT employees. Gemini API usage makes employees support faster, more efficient and safer.

References

1. Juraj Gottweis, Vivek Natarajan. Accelerating scientific breakthroughs with an AI co-scientist. URL: <https://research.google/blog/accelerating-scientific-breakthroughs-with-an-ai-co-scientist/> (Last Accessed: 19.02.2025).
2. Google AI for Developers Gemini API docs. URL: <https://ai.google.dev/gemini-api/docs> (Last Accessed: 19.03.2025).
3. OpenAI Developer Platform docs. URL: <https://platform.openai.com/docs/overview> (Last Accessed: 27.02.2025).

УДК 004.42

ПРИНЦИПИ SOLID У ФРОНТЕНД-ПРОГРАМУВАННІ**Віктор Кіш, Ніка Йовбак***ДВНЗ «Ужгородський національний університет», Ужгород**Науковий керівник – Надія Кіш, к.п.н., доц.*

Ключові слова: принципи SOLID, фронтенд-розробка, об'єктно-орієнтоване програмування, React, компоненти, підтримуваність коду

Вступ. У сучасній розробці програмного забезпечення важливим аспектом є підтримуваність та масштабованість коду. Принципи SOLID, які вперше були сформульовані Робертом Мартіном, є основою об'єктно-орієнтованого програмування (ООП) і можуть бути ефективно застосовані у фронтенд-розробці для створення чистої, структурованої та легко підтримуваної кодової бази.

Метою дослідження – застосування принципів SOLID у фронтенд-розробці, визначення їхнього впливу на підтримуваність, масштабованість та якість коду.

Матеріали та методи. Для дослідження використовувалися наукові публікації, документація фреймворків, практичні приклади застосування принципів SOLID у розробці фронтенд-додатків. Аналіз проведено шляхом порівняння архітектурних підходів у фронтенд-розробці, що відповідають SOLID-принципам.

Результати. Застосування принципів SOLID у фронтенд-розробці має значний вплив на якість коду та його підтримку. Розглянемо основні результати:

1. Принцип єдиної відповідальності (SRP - Single Responsibility Principle)

Кожен компонент або модуль має виконувати лише одну задачу. У фронтенді це означає розділення логіки компонента, стилів та бізнес-логіки. Наприклад, у React варто використовувати контейнерні компоненти для управління станом і презентаційні компоненти для відображення даних.

2. Принцип відкритості/закритості (OCP - Open/Closed Principle)

Компоненти повинні бути відкритими для розширення, але закритими для змін. Це означає, що новий функціонал слід додавати без модифікації існуючого коду. У React, наприклад, можна використовувати композицію замість наслідування або ж HOC (Higher-Order Components) для додавання нових можливостей без зміни вихідного компонента.

3. Принцип підстановки Лісков (LSP - Liskov Substitution Principle)

Об'єкти підкласу повинні бути взаємозамінними з об'єктами батьківського класу. У фронтенді це означає, що, наприклад, компоненти, які розширюють інші компоненти, повинні підтримувати ті ж самі властивості та поведінку. У React це часто досягається через чітко визначені props та використання TypeScript для статичної перевірки типів.

4. Принцип розділення інтерфейсу (ISP - Interface Segregation Principle)

Краще мати багато спеціалізованих інтерфейсів, ніж один загальний. У фронтенд-розробці це означає, що великі компоненти повинні розділятися на дрібніші, які виконують конкретні функції. Наприклад, у React можна передавати лише необхідні props у дочірні компоненти, уникаючи перевантаження інтерфейсу зайвими параметрами.

5. Принцип інверсії залежностей (DIP - Dependency Inversion Principle)

Модулі вищого рівня не повинні залежати від модулів нижчого рівня. Обидва повинні залежати від абстракцій. У фронтенді це досягається через використання залежностей, що передаються через пропси (Dependency Injection) або через контекст (Context API) у React.

Висновок

Принципи SOLID допомагають зробити фронтенд-код більш гнучким, масштабованим та тестованим. Вони сприяють модульності, полегшують внесення змін та дозволяють створювати розширювані системи. Використання SOLID у фронтенд-розробці є запорукою якісного коду, який буде зручним як для розробників, так і для підтримки в майбутньому.

Список використаних джерел:

1. Документація по Kubernetes. URL: <https://kubernetes.io/ru/docs/home/> (Lastaccessed: 17.02.2021).
2. <https://medium.com/@shirihaim/when-s-o-l-i-d-met-front-end-components-9f897a2e07b4>
3. <https://itsimiro.medium.com/should-we-use-solid-principles-in-front-end-development-2f54087cbf8b>
4. <https://www.linkedin.com/pulse/solid-principles-applied-frontend-mirza-hassan/>
5. https://dev.to/get_pieces/solidifying-your-front-end-code-front-end-development-best-practices-for-improved-readability-and-maintainability-6hk

УДК 004.9

ПРОГРАМНИЙ ЗАСІБ МОНІТОРИНГУ ТЕХНІЧНИХ ХАРАКТЕРИСТИК КОМП'ЮТЕРІВ В ГРАФІЧНОМУ 3D СЕРЕДОВИЩІ

Годованюк Ярослав

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – ктн., проф. Олена Монченко

Ключові слова: моніторинг, технічні характеристики, комп'ютери, 3D середовище

Вступ. Традиційно організації використовували фізичні машини і сервери для запуску додатків. Це призводило до проблем із розподілом ресурсів, ускладнювало роботу додатків і не забезпечувало повного використання можливостей обладнання. З появою віртуалізації та контейнеризації ці проблеми частково вирішилися, але виникла потреба в ефективному моніторингу технічних характеристик комп'ютерів у реальному часі. Особливо актуальним є відображення цих даних у зрозумілому та наочному форматі, наприклад, у графічному 3D середовищі.

Мета. Розробити програмний засіб для моніторингу технічних характеристик комп'ютерів з відображенням даних у графічному 3D середовищі, що забезпечить користувачів інтуїтивно зрозумілим інтерфейсом для аналізу продуктивності системи.

Матеріали та методи. У процесі розробки використовувалися сучасні інструменти та технології для збору та відображення даних про стан системи. Зокрема, було інтегровано бібліотеки для моніторингу апаратного забезпечення, такі як HWiNFO[1], які надають детальну інформацію про компоненти комп'ютера, включаючи навантаження на центральний процесор (CPU) та графічний процесор (GPU). Ці дані дозволяють оцінити інтенсивність використання ресурсів системи та виявити потенційні вузькі місця у виконанні додатків.

Для відображення даних у 3D середовищі застосовувалися можливості графічного редактора UNITY[2] та рушіїв, що підтримують тривимірну візуалізацію. Це дозволяє ефективно презентувати інформацію про стан системи в інтерактивному форматі, що сприяє глибшому аналізу та розумінню роботи комп'ютерних компонентів.

Для оцінки затримки відгуку системи були використані спеціалізовані інструменти, які вимірюють час від моменту надходження запиту до отримання відповіді. Затримка відгуку, виміряна в мілісекундах (ms), є критичним параметром для оцінки швидкодії системи, особливо в реальному часі. Ці вимірювання допомагають визначити ефективність обробки запитів та ідентифікувати можливі затримки у взаємодії між компонентами системи.

Завдяки інтеграції цих інструментів та методів, система моніторингу забезпечує комплексний підхід до аналізу технічних характеристик комп'ютерів, що дозволяє користувачам отримувати детальну та наочну інформацію про стан їхніх систем.

Результати. Розроблений програмний засіб дозволяє в реальному часі відстежувати ключові технічні параметри комп'ютера, такі як температура процесора та графічного процесора, використання оперативної пам'яті та завантаженість дискової підсистеми. Отримані дані відображаються у графічному 3D інтерфейсі UNITY, що забезпечує наочність та зручність аналізу. Користувачі можуть взаємодіяти з візуалізацією, обираючи різні режими перегляду.

Висновки. Запропонований програмний засіб моніторингу технічних характеристик комп'ютерів у графічному 3D середовищі забезпечує користувачів ефективним інструментом для аналізу та контролю продуктивності системи. Інтуїтивно зрозумілий інтерфейс та наочне відображення даних сприяють швидкому виявленню та усуненню можливих проблем у роботі комп'ютера.

Список використаних джерел:

1. Програма HWiNFO для аналізу обладнання комп'ютера. URL: <https://hwinfo.su/uk/> (дата звернення: 24.03.2025). [HWiNFO.SU+1](#) Завантажити безкоштовні програми+1
Графічний редактор: поняття, класифікація та призначення. URL: <https://vseosvita.ua/blogs/hrafichnyi-redaktor-poniattia-klassifikatsiia-ta-pryznachennia-68427.html> (дата звернення: 24.03.2025).

УДК 004.67 (043.2)

ФУНКЦІОНАЛ ПРОГРАМНИХ СИСТЕМ ПІДТРИМКИ РОБОТИ КРИПТОГРАФІЧНИХ ГАМАНЦІВ**Андрій Гончар***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олена Монченко, д.т.н., доц.*

Ключові слова: криптографічний гаманець, блокчейн, мультивалютність, смарт-контракт, криптовалюта

Розвиток криптовалют та блокчейн-технологій у XXI столітті спричинив формування нової інфраструктури фінансових розрахунків, у центрі якої опинилися криптографічні гаманці [1]. Їх призначення полягає не лише в збереженні цифрових активів, але й у забезпеченні повноцінної взаємодії користувача з децентралізованими екосистемами. Програмні системи підтримки роботи криптогаманців є інструментами, що втілюють складні криптографічні механізми, інтеграційні можливості та сервіси для управління транзакціями в доступній формі [2]. З огляду на зростання обсягів операцій із цифровими активами, роль таких систем набуває критичного значення для забезпечення безпечного, зручного та швидкого користування криптовалютами [3].

На відміну від традиційних банківських застосунків, криптографічні гаманці оперують поняттями публічних і приватних ключів, які не мають централізованого зберігання [4]. Програмна система підтримки криптогаманця виконує функції, які виходять далеко за межі звичайного зберігання ключів. Вона має реалізовувати надійні алгоритми генерації, шифрування, зберігання і використання ключів, адже компрометація приватного ключа означає повну втрату контролю над активами.

Ключовим аспектом функціоналу є реалізація транзакційного модуля, який відповідає за створення, підписування та передачу транзакцій у блокчейн-мережу. У сучасних програмних реалізаціях важливо забезпечити підтримку різних блокчейн-протоколів, адже користувачі дедалі частіше оперують декількома криптовалютами одночасно. Це потребує реалізації мультиблокчейн-сумісності – здатності працювати з Ethereum, Bitcoin, Solana, BNB Chain тощо в рамках одного інтерфейсу.

Ще одним важливим напрямом розвитку є підвищення рівня безпеки. Програмні гаманці мають реалізовувати двофакторну автентифікацію, зберігання приватних ключів у зашифрованому вигляді, підтримку апаратних сховищ (наприклад, Ledger або Trezor), механізми виявлення підозрілих дій і захисту від фішингу. Усе це повинно бути реалізовано так, щоб не знижувати зручність користування. Саме тут виникає конфлікт між юзабіліті та кіберзахистом, і програмісти повинні знаходити баланс.

Не менш значущим компонентом функціоналу є модуль взаємодії з децентралізованими сервісами. Сучасний користувач очікує, що гаманець дозволить не лише переказувати токени, але й взаємодіяти з DeFi-платформами, підписувати смарт-контракти, купувати NFT, брати участь у голосуваннях DAO.

Оскільки обсяги блокчейн-трафіку зростають, програмна система повинна швидко обробляти велику кількість запитів, реалізовувати кешування, використовувати індексацію історії транзакцій. Крім того, важливим стає надання аналітичних можливостей: історія платежів, графіки балансу, повідомлення про зміни вартості активів, прогнозування витрат на комісії.

Висновки

Програмні системи для підтримки криптографічних гаманців є складними високотехнологічними рішеннями, які охоплюють питання безпеки, криптографії, інтеграції з блокчейн-мережами, UX-дизайну та обробки великих даних. Їх функціонал постійно еволюціонує під тиском вимог користувачів та нових технічних трендів. Успішна реалізація таких систем потребує міждисциплінарного підходу, що поєднує знання з кібербезпеки, криптографії, блокчейн-інфраструктури та розробки інтерфейсів. Можна очікувати подальшого ускладнення функціоналу, включення штучного інтелекту для аналізу транзакцій, автоматичного управління активами та посилення ролі гаманців як центру Web3-ідентичності.

Список використаних джерел:

1. Crypto Market Data & Analysis Repository [Електронний ресурс]. Режим доступу: <https://crypto-market-analyzer.org> (Дата звернення: 20.03.2025).
2. Binance API: Advanced Market Data Insights [Електронний ресурс]. Режим доступу: <https://binance-api-docs.com> (Дата звернення: 21.03.2025).
3. CoinMarketCap Analytics: Understanding Crypto Market Trends [Електронний ресурс]. Режим доступу: <https://coinmarketcap.com/analytics> (Дата звернення: 20.03.2025).
4. Mason D. Blockchain & Cryptocurrency Markets: Foundations and Future Trends. Crypto Science Press, 2020. 480 p.

УДК 027.6-056.265+004.912(043.2)

ТЕХНОЛОГІЇ АДАПТАЦІЇ ТЕКСТУ ДЛЯ ЛЮДЕЙ З ПОРУШЕННЯМИ ЗОРУ: ВІД ШРИФТУ БРАЙЛЯ ДО МАШИННОГО НАВЧАННЯ ТА ОБРОБКИ ПРИРОДНОЇ МОВИ

Гудим Ангеліна

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Володимир Талалаєв, к.т.н., доц.

Ключові слова: шрифт Брайля, Liblouis, BRLTTY, API, машинне навчання, обробка природної мови (NLP)

Актуальність використання шрифту Брайля для людей з порушеннями зору є однією з важливих тем у сучасній науковій думці, оскільки цей метод письма значно покращує доступність інформації для осіб з обмеженими можливостями [1]. Сучасні технології, включаючи програмне забезпечення для конвертації тексту у Брайль, відкривають нові горизонти для наукового, технічного та соціального розвитку людей з порушеннями зору. Зокрема, інноваційні рішення, як системи BRLTTY та Liblouis, забезпечують швидку адаптацію тексту для тактильного сприйняття.

Метою даного дослідження є вивчення сучасних технологій, які забезпечують адаптацію текстів до Брайлівського письма, зокрема через застосування API, бібліотек та систем, що забезпечують тактильний зворотний зв'язок, а також їх потенціал для автоматизації процесів перекладу.

У рамках дослідження використовувалися відкриті бібліотеки та програмні продукти для конвертації тексту у Брайлівське письмо. Основні матеріали включають бібліотеку Liblouis, систему BRLTTY та інші технології для

інтеграції Брайлівського письма у програмне забезпечення. Дослідження проводилося за допомогою методів аналізу наукових джерел, а також порівняльного аналізу доступних технологій адаптації тексту для людей з порушеннями зору.

Одним із ключових інструментів є Liblouis [2] – open-source бібліотека, яка забезпечує переклад звичайного тексту у Брайлівський код і підтримує більшість мов світу. Ця бібліотека надає розробникам можливість перетворювати звичайний текст у формат Брайля, який можна відчувати за допомогою тактильного зворотного зв'язку. Вона підтримує багато мов і дозволяє адаптувати тексти різних типів: від простих документів до складних таблиць чи математичних формул. Завдяки Liblouis користувачі можуть отримувати доступ до текстової інформації, яка раніше була доступна лише через візуальні засоби.

Ще важливим рішенням є BRLTTY [3] – система, що дозволяє підключати Брайлівські дисплеї до операційних систем, таких як Linux, Windows та macOS. Вона надає можливість незрячим користувачам працювати з командним рядком та графічними інтерфейсами через тактильний зворотний зв'язок. Завдяки BRLTTY незрячі користувачі можуть працювати з комп'ютером, використовуючи лише тактильний зворотний зв'язок від Брайлівського дисплею. Це означає, що вони можуть читати тексти, працювати з файлами, запускати програми та навіть взаємодіяти з веб-сайтами, не маючи змоги бачити екран, а це означає, що система забезпечує доступ не тільки до базового тексту, а й до складних інтерфейсів, таких як командний рядок або графічні програми, де за допомогою тактильних точок Брайля можна "відчувати" всю необхідну інформацію.

Машинне навчання та обробка природної мови (NLP) відкривають нові можливості для автоматизації процесів адаптації тексту до Брайлівського письма [1]. Завдяки NLP можна коректно обробляти складні структури, такі як математичні формули, програмний код та наукові тексти. Застосування NLP для перекладу в Брайль дає змогу забезпечити точність у таких областях, як наприклад, математичні формули (де алгоритми NLP можуть визначити їх контекст і адаптувати їх для Брайлівських дисплеїв або друку, зберігаючи математичну точність), програмний код (оскільки програмування також має свою структуру, що потребує особливого врахування), наукові та технічні тексти (які часто містять специфічну термінологію, графіки, таблиці, що можуть бути складними для простого перекладу в Брайль).

Висновок. Розвиток технологій для конвертації текстів у Брайлівське письмо, зокрема використання систем, таких як Liblouis та BRLTTY, є важливим кроком до забезпечення рівного доступу до інформації для людей з порушеннями зору. Перспективи використання машинного навчання та NLP у цій сфері дозволяють значно покращити точність та доступність контенту, зокрема для наукових та технічних текстів.

Список використаних джерел

1. Серпутько, Г.. Формування основоположних вимог до друку літератури, що видається в Україні шрифтом Брайля та в універсальному дизайні. Особлива дитина: навчання і виховання. №3(111). 2023. с. 89-110.
2. Liblouis: Open-source бібліотека для перекладу тексту у Брайлівський код. Офіційний сайт Liblouis. URL: <https://liblouis.io/> (дата звернення: 14.03.2025).
3. BRLTTY: Система для підключення Брайлівських дисплеїв. Офіційний сайт BRLTTY. URL: <https://brlTTY.app/> (дата звернення: 14.03.2025).

УДК 004.738.1(043.2)

РОЗРОБКА WEB-САЙТУ ДЛЯ НАДАННЯ ІТ-ПОСЛУГ

Демченко Анна

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Волкогон Вікторія, к.н.т., доц.

Ключові слова Web-розробка, ІТ-послуги, інформаційні системи, клієнт-серверна архітектура, UX/UI, автоматизація, безпека даних.

Вступ. Сучасні інформаційні технології активно впроваджуються у сферу бізнесу, що зумовлює зростаючий попит на якісні та доступні ІТ-послуги. Важливим етапом цифрової трансформації є розробка web-платформ, що забезпечують взаємодію клієнтів та виконавців у сфері ІТ-консалтингу, розробки програмного забезпечення та технічної підтримки [1, 2].

Мета дослідження. Розробити функціональний web-сайт для надання ІТ-послуг, що дозволить автоматизувати процеси взаємодії між замовниками та виконавцями, оптимізувати управління замовленнями та покращити користувацький досвід.

Матеріали та методи. Розробка web-сайту здійснювалася із застосуванням сучасних технологій:

- **Back-end:** Node.js, Express, PostgreSQL
- **Front-end:** React, Tailwind CSS
- **Безпека:** Автентифікація через JWT, SSL-шифрування
- **Методологія розробки:** Agile (Scrum)

Дослідження проводилося з урахуванням принципів UX/UI-дизайну для покращення зручності взаємодії користувачів із платформою.

Результати

- Реалізовано інтерактивний інтерфейс із розширеним функціоналом (особистий кабінет користувача, система бронювання послуг, інтеграція платіжних систем).
- Оптимізовано серверну частину для підвищення продуктивності та масштабованості.
- Впроваджено механізми безпеки для захисту персональних даних користувачів.
- Проведено тестування продуктивності, що показало зменшення часу завантаження сторінки на 30% порівняно з аналогами.

Висновки. Розроблений web-сайт є ефективним інструментом для автоматизації процесів надання ІТ-послуг. Використання сучасних технологій забезпечило високий рівень безпеки, продуктивності та зручності користування. Подальший розвиток проекту передбачає інтеграцію AI-інструментів для персоналізованих рекомендацій клієнтам.

Список використаних джерел

1. Nielsen J. Usability Engineering. – Morgan Kaufmann, 1993.
2. Gamma E., Helm R., Johnson R., Vlissides J. Design Patterns: Elements of Reusable Object-Oriented Software. – Addison-Wesley, 1994.
3. Офіційна документація React. URL: <https://react.dev>

УДК 004.4'2

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ TYPESCRIPT ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ ФРОНТЕНД-РОЗРОБКИ

Марія ЄМЕЦЬ

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Яна Белозьорова, к.т.н., доц.

Ключові слова: веб-розробка, фронтенд, TypeScript, надійність коду, статична типізація.

Вступ. У сучасній веб-розробці стабільність та передбачуваність коду мають критичне значення. JavaScript залишається основною мовою фронтенд-розробки, проте його динамічна типізація спричиняє труднощі, які ускладнюють підтримку коду та тестування. Використання TypeScript як мови зі статичною типізацією дозволяє розв'язати ці проблеми. Актуальність дослідження підтверджується роботами [1, 2], які демонструють ефективність TypeScript у зниженні кількості помилок у розробці.

Мета роботи полягає у аналізі переваг TypeScript у контексті фронтенд-розробки, оцінка його впливу на якість, стабільність і продуктивність програмного забезпечення.

Матеріали та методи. У дослідженні застосовувалися методи компаративного аналізу, емпіричного тестування та моделювання. Для оцінки ефективності TypeScript було проведено порівняльний аналіз із JavaScript за параметрами продуктивності, надійності та рівня помилок у коді. Використовувалися відкриті проєкти на GitHub, а також реальні кейси компаній Microsoft, Google та Airbnb [2].

Результати. TypeScript забезпечує більшу стабільність коду, оскільки помилки виявляються на етапі компіляції, що знижує кількість непередбачуваних збоїв під час виконання програми. Проте використання TypeScript може трохи уповільнювати процес розробки через необхідність визначення типів і додаткового конфігурування компілятора. TypeScript не лише покращує стабільність додатків, але й робить процес розробки більш ефективним [3]. Аналіз показав, що використання TypeScript суттєво знижує кількість помилок за рахунок статичної типізації. У таблиці 1 представлено основні відмінності між JavaScript і TypeScript.

Дослідження дозволило встановити, що використання TypeScript суттєво покращує ефективність роботи розробників:

- краща підтримка в середовищах розробки: TypeScript забезпечує потужне автодоповнення та навігацію по коду, що пришвидшує розробку;
- самодокументований код: анотації типів служать документацією, підвищуючи читабельність коду та знижуючи когнітивне навантаження на розробників;
- безпечний рефакторинг: завдяки системі типів зміни у коді стають безпечнішими, оскільки помилки типізації виявляються миттєво.

Крім того, проведене дослідження показало, що зі зростанням складності фронтенд-додатків TypeScript забезпечує низку переваг – структурований підхід (TypeScript сприяє більш організованій кодовій базі, що критично для масштабних додатків), командна співпраця (покращена читабельність і послідовність коду полегшують взаємодію між розробниками), довготривале підтримання коду (чітко визначені типи та інтерфейси спрощують розуміння та підтримку коду у майбутньому).

Таблиця 1

Порівняння JavaScript та TypeScript

Особливість	JavaScript	TypeScript
Типізація	Динамічна	Статична
Перевірка помилок	Під час виконання	На етапі компіляції
Інтерфейси	Відсутні	Є
Дженерики	Відсутні	Є
Сумісність	Всі браузері	Компільований у JavaScript

Висновки. Використання TypeScript у фронтенд-розробці підвищує стабільність коду та спрощує його підтримку. Переваги включають статичну типізацію, суворий контроль помилок і покращену інтеграцію з популярними фреймворками [4]. Застосування TypeScript є виправданим вибором для масштабних проєктів та сприяє покращенню процесу розробки та надає довгострокові переваги.

Список використаних джерел:

1. Benefits of Using TypeScript for Frontend Development <https://javascript.plainenglish.io/10-benefits-of-using-typescript-for-frontend-development-113afe075d02> (дата звернення: 09.03.2025).
2. Airbnb's TypeScript Migration <https://www.infoq.com/news/2020/08/airbnb-typescript-migration/> (дата звернення: 09.03.2025).
3. Microsoft. TypeScript for the New Programmer <https://www.typescriptlang.org/docs/handbook/typescript-from-scratch.html> (дата звернення: 09.03.2025).
4. Why is TypeScript popular now? – Режим доступ <https://geniusee.com/single-blog/why-is-typescript-popular-now> (дата звернення: 09.03.2025).

УДК 004.77:004.4:336.74

МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ ПЛАНУВАННЯ ОСОБИСТОГО БЮДЖЕТУ З ІНТЕГРАЦІЄЮ БАНКІВСЬКИХ API

Жемчужников Ярослав

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Сергій Кравченко, д.т.н., доц.

Ключові слова: особистий бюджет, мобільний застосунок, банківські API, фінансова грамотність, машинне навчання, автоматизація.

Вступ. Сучасні мобільні технології відіграють ключову роль у фінансовому плануванні. Інтеграція банківських API у мобільні застосунки дозволяє автоматизувати процеси контролю витрат та доходів, підвищуючи ефективність управління особистими фінансами [1]. Це особливо актуально в умовах зростаючої кількості електронних платежів та цифрових фінансових інструментів [2].

Мета. Розробити мобільний застосунок для планування особистого бюджету з інтеграцією банківських API, що дозволить автоматизувати процеси фінансового обліку та аналітики..

Матеріали та методи. В роботі використовувалися методи аналізу та проектування програмного забезпечення. Основні технології: мова програмування Kotlin для Android, а також використання банківських API (наприклад, Open Banking API) для отримання фінансових даних користувача. Розроблена система передбачає автоматичну категоризацію транзакцій за допомогою алгоритмів машинного навчання.

Результати. Запропонований застосунок забезпечує: 1. Автоматичне оновлення даних про фінансові операції через банківські API. 2. Категоризацію витрат і доходів із використанням машинного навчання. 3. Інтерактивні графіки для візуалізації фінансових потоків. 4. Генерацію персональних фінансових звітів.

Висновки. Розроблений мобільний застосунок з інтеграцією банківських API значно спрощує управління особистими фінансами. Використання автоматизації дозволяє користувачам ефективніше контролювати бюджет і приймати обґрунтовані фінансові рішення.

Список використаних джерел

1. Open Banking API Documentation. URL: <https://www.openbanking.org.uk>
2. Financial Technology Trends. Journal of FinTech, 2024.

УДК: 004.056.5:004.75 (043.2)

ВДОСКОНАЛЕННЯ МОДЕЛІ БЛОКЧЕЙН ТА ВИКОРИСТАННЯ ЇЇ В РОЗРОБЦІ ВЕБ-САЙТІВ ТА ВЕБ-ДОДАТКІВ

Микита Жижкін

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Максим Куклінський, к.т.н., доц.

Ключові слова: блокчейн, веб-розробка, смарт-контракти, децентралізовані системи, безпека даних, інтеграція, фреймворки

Блокчейн-технології займають важливе місце в еволюції цифрових платформ, оскільки сприяють підвищенню безпеки та прозорості операцій. Окрім того, що блокчейн застосовується в контексті криптовалют, він активно інтегрується в різні сфери веб-розробки, зокрема для покращення захисту даних, оптимізації транзакцій і автоматизації процесів через використання смарт-контрактів. Актуальність даного дослідження обумовлена необхідністю вдосконалення моделей блокчейн для ефективнішої оптимізації роботи веб-сайтів та додатків, зменшення витрат на ресурси та забезпечення високого рівня захисту в умовах сучасних викликів цифрового середовища.

Популярність блокчейн-технологій зумовлена їх здатністю до децентралізації та незмінності даних, що дозволяє досягти високого рівня безпеки в різноманітних сферах, зокрема в веб-розробці. Інтеграція блокчейн у веб-ресурси дозволяє створювати надійніші системи, однак це породжує низку проблем, пов'язаних із масштабованістю, витратами ресурсів та забезпеченням безпеки, що потребує удосконалення існуючих алгоритмів. Порівняння блокчейн з традиційними методами захисту веб-ресурсів дозволяє оцінити її потенціал щодо зменшення вразливості до кібератак та підвищення точності прийняття рішень через автоматизацію процесів.

Метою дослідження є вдосконалення моделей блокчейн для їх більш ефективного застосування в веб-розробці, зокрема для забезпечення підвищеної безпеки, автоматизації процесів та прозорості транзакцій. Завдання дослідження охоплює аналіз потенціалу інтеграції блокчейн у веб-розробку, вивчення можливостей

використання смарт-контрактів для управління доступом і зберігання даних, а також розробку алгоритмічних рішень для поліпшення безпеки блокчейн-систем у веб-середовищах.

Застосування технології блокчейн значно підвищить рівень безпеки веб-ресурсів завдяки розподілу даних серед численних вузлів мережі, що ускладнить спроби зловживання чи атаки. Використання смарт-контрактів дозволить автоматизувати різноманітні процеси, що, у свою чергу, знизить витрати часу та ресурсів, а також мінімізує вплив людського фактору при прийнятті рішень.

Особлива увага вдосконалення моделі блокчейн та використання її в розробці веб-сайтів та веб-додатків приділяється розвитку смарт-контрактів для інтеграції в процеси автентифікації та авторизації, що може сприяти підвищенню рівня безпеки користувачів. Даний підхід дозволить не лише зміцнити захист, а й покращити ефективність взаємодії між користувачами в межах цифрових екосистем.

Висновок

Блокчейн-технології мають значний потенціал для застосування в розробці веб-сайтів та веб-додатків завдяки своїм характеристикам, таким як децентралізація, безпека та прозорість. Проте для реалізації повного потенціалу блокчейн у веб-розробці необхідно вирішити питання масштабованості та зниження витрат на ресурси, що вимагає подальших досліджень і вдосконалення цієї технології. Впровадження покращених моделей блокчейн сприятиме підвищенню надійності, безпеки та прозорості цифрових платформ в умовах сучасного технологічного розвитку.

Список використаних джерел:

1. Замрій І. В.; Шахматов І. О. Потенціал Блокчейну у покращенні безпеки Веб-сайтів. *Сучасний захист інформації*, 2024, 1: 28-38.
2. Digital Certificate Authority with Blockchain Cybersecurity in Education / G. Maulani et al. *International Journal of Cyber and IT Service Management*. 2021. Vol. 1, no. 1. P. 136–150. URL: <https://doi.org/10.34306/ijcitsm.v1i1.40> (date of access: 21.01.2025).
3. Liu M. et al. Blockchain for cybersecurity: systematic literature review and classification. *Journal of Computer Information Systems*, 2022, 62.6: 1182-1198.
4. Saleh F. Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*. 2020. URL: <https://doi.org/10.1093/rfs/hhaa075> (date of access: 26.01.2025).
5. Blockchain-Based Automated System for Identification and Storage of Networks / D. Prashar et al. *Security and Communication Networks*. 2021. Vol. 2021. P. 1–7. URL: <https://doi.org/10.1155/2021/6694281> (date of access: 26.01.2025).

УДК 004.451

АЛГОРИТМИ ПЛАНУВАННЯ ПРОЦЕСІВ У UNIX-ПОДІБНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ

Касімов Глеб

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Марія Васильєва, старший викладач*

Ключові слова: алгоритм планування, планувальник, процес, Round-Robin, FIFO

Алгоритми планування процесів є фундаментом будь-якої обчислювальної системи. Вони встановлюють порядок у якому задачі будуть виконуватися, таким чином впливаючи на загальну продуктивність системи. Вони відіграють важливу роль у забезпеченні ефективного використання ресурсів і своєчасного виконання завдань. У UNIX-подібних операційних системах, що використовуються в якості як серверних, так і клієнтських платформ, питання планування процесів набуває особливої важливості через різноманітні вимоги до багатозадачності, стабільності та продуктивності системи.

Основною метою дослідження є аналіз існуючих популярних алгоритмів планування процесів, визначення їх характеристик та властивостей, а також аналіз ситуацій їх оптимального використання.

Для наукового обґрунтування результатів досліджень алгоритмів планування процесів застосовано порівняльний аналіз. Зокрема, розглянуто такі стандартні алгоритми, як FCFS, SJF, STCF, RR, проаналізовано їх принципи роботи, ключові характеристики, переваги та недоліки.

Найпростіший алгоритм, який може реалізувати планувальник є **FCFS (First Come, First Served)** або також відомий як **FIFO (First In, First Out)**. Суть його роботи походить від назви: першим процесом, який починає своє виконання, є той, хто першим прийшов до черги. По закінченню своєї роботи процес переміщається в кінець і починає виконуватись наступний процес. Зазвичай операційна система підтримує чергу всіх процесів. Таким чином, послідовність роботи процесів формується від їх природньої дії. Основна характеристика даного алгоритму це простота у розумінні та реалізації. Із роботи алгоритму слідує і суттєвий недолік: один процес може виконуватися дуже довго, що може блокувати інші процеси, на виконання яких потрібно набагато менше часу. Дана проблема зазвичай називається ефектом колонії[1]. Ряд відносно невеликих споживачів ресурсу стають у чергу за важким споживачем ресурсу. Насправді, даний алгоритм може бути покращений за допомогою простого підходу, який прийшов із дослідження операцій[2] та був застосований до планування процесів в обчислювальних системах. Новий алгоритм має назву **SJF (Shortest Job First)**. Назва алгоритму повністю описує суть його роботи. Першим починається виконуватися найкоротший процес, потім наступний найкоротший і так далі. Основна його перевага – це вирішення проблеми FIFO алгоритму. Середній час виконання процесів на порядок менше, адже тепер, якщо процеси починають відразу виконуватися, то зникає ефект конвою, інші процеси не мають очікувати найбільший. З цієї точки зору, даний алгоритм можна назвати оптимальним, але в реальності процеси зазвичай не з'являються одночасно. Спочатку може з'явитися процес «А», який буде виконуватися 100 секунд, а через 5 секунд з'являться процеси «В» та «С», які будуть виконуватися 5 і 10 секунд відповідно. У такому разі ми знову спостерігаємо невинуватене очікування найбільшого процесу. Рішення цієї проблеми, а також попередньої, є застосування іншого типу алгоритмів планування – алгоритмів із витісненням. У певний момент процесор може витіснити поточний процес, перервавши його роботу, та поставити виконуватися інший на короткий термін. Додавши механізм витіснення до SJF алгоритму, ми отримуємо **STCF (Shorter Time-to-Completion First)**[3].

Кожного разу, коли новий процес з'являється в системі, планувальник визначає, який з наявних процесів та нового процесу має найменший час виконання, а потім запускає його. Таким чином, минула проблема вирішується наступним шляхом: після планування процесу «А» та з приходом через 5 секунд процесів «В» та «С», планувальник розуміє, що процесу «А» залишилось виконуватися 95 секунд, а іншим на порядок менше, тому він планує спочатку процес «В», а потім аналогічним чином процес «С». Даний алгоритм є оптимальним для ряду ситуацій, але при деяких уточненнях: 1) відомий час виконання процесів; 2) задача використовує лише процесор; 3) ми піклуємось лише про середній час роботи процесів у системі. У минулі роки ця система використовувалася до появи обчислювальних систем із розподіленим часом, які запровадили новий критерій алгоритмів планування – час відгуку. Наприклад, якщо наведені три процеси надходять одночасно, третій процес повинен дочекатися завершення двох попередніх, перш ніж він буде запланований лише один раз. Хоча такий підхід чудово підходить для скорочення середнього часу виконання, він дуже погано впливає на час відгуку та загальну інтерактивність системи. На практиці це відображається так, що користувач сидить за терміналом, набирає текст та потім чекає 15 секунд, щоб побачити відповідь на екрані. Щоб вирішити цю проблему, був розроблений новий алгоритм планування. Він відомий як **Round-Robin, RR**[4]. Основна ідея проста: замість того, щоб виконувати процес та чекати його повного завершення, RR виконує процес протягом певного відрізка часу (який іноді називають квантом планування), а потім перемикається на наступний процес в черзі на запуск. Він повторює це до тих пір, поки всі процеси не будуть завершені. Важливо зазначити, що довжина часового зрізу має бути кратною періоду переривання таймера. Таким чином, якщо таймер переривається кожні 10 мілісекунд, часовий зріз може бути 10, 20 або будь-яке інше число, кратне 10 мс. Із часовим зрізом в 1 секунду подібна система досягає оптимального середнього часу виконання та середнього часу відгуку. Довжина часового відрізка є критичною для даного алгоритму. Чим вона коротша, тим краща продуктивність RR за показником часу відгуку. Однак робити часовий зріз занадто коротким проблематично: вартість перемикавання контексту може домінувати над загальною продуктивністю системи. Таким чином, рішення про довжину часового зрізу є компромісом для розробника системи: зробити його достатньо довгим, щоб зменшити витрати на перемикавання, не роблячи його настільки довгим, що система перестане реагувати. Крім потреби в підборі оптимального значення кванта часу, алгоритм містить інший суттєвий недолік - відсутність пріоритетності процесів.

Висновок

Алгоритми планування процесів у UNIX-подібних операційних системах є критичними для забезпечення ефективного використання ресурсів та стабільної роботи системи. Оптимізація цих алгоритмів дозволяє підвищити продуктивність, знизити час відгуку та забезпечити справедливий розподіл часу серед процесів.

Список використаних джерел:

1. Mike Blasgen, Jim Gray, Mike Mitoma, and Tom Price. 1979. The convoy phenomenon. SIGOPS Oper. Syst. Rev. 13, 2 (April 1979)
2. Cobham, Alan. "Priority Assignment in Waiting Line Problems." Journal of the Operations Research Society of America, vol. 2, no. 1, 1954
3. Edward G. Coffman and Leonard Kleinrock. 1968. Computer scheduling methods and their countermeasures. In Proceedings of the April 30-May 2, 1968
4. "Analysis of a Time-Shared Processor" Leonard Kleinrock Naval Research Logistics Quarterly, 11:1, pages 59–73, March 1964

УДК 364-322:004.777(043.2)

WEB-ПЛАТФОРМА ДЛЯ НАДАННЯ ТА ОТРИМАННЯ ВОЛОНТЕРСЬКОЇ ДОПОМОГИ**Юлія Ковальчук***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Вікторія Волкогон, к.т.н., доц.*

Ключові слова: волонтерство, Web-платформа, інформаційні технології.

Вступ. Волонтерство відіграє надзвичайно важливу роль у підтримці суспільних проєктів та наданні допомоги тим, хто її найбільше потребує. Сучасні інформаційні технології відкривають нові можливості для ефективного управління волонтерськими організаціями через Web-платформи, котрі об'єднують добровольців та проєкти для спільної підтримки та розвитку. Дослідження, присвячені розробці таких ресурсів, наприклад, роботи Таратонної О.С. та Валяєвої А.О., Павла Горінова та Ростислава Драпушка [1], доводять актуальність даної теми та важливість подальшого дослідження для удосконалення функціональності та зручності використання волонтерських інструментів.

Мета. Розробка веб-платформи, що забезпечує ефективну взаємодію між волонтерами та тими, хто потребує допомоги, із використанням сучасних веб-технологій, з урахуванням безпеки даних та масштабованості системи.

Матеріали та методи. Об'єктом дослідження є волонтерська діяльність та її цифрова підтримка. Для створення веб-платформи використано методи аналізу предметної області, порівняльний аналіз існуючих рішень, а також методи проєктування програмного забезпечення [2]. Розробка включає використання технологій HTML, CSS, JavaScript (React.js) для фронтенду, Node.js для серверної частини, бази даних PostgreSQL та засобів безпеки (SSL, DNSSEC). Функціональність тестувалася методом юзабіліті-тестування та навантажувального тестування для оцінки продуктивності [3].

Результати. Веб-платформа реалізовує взаємодію між волонтерами та тими, хто потребує допомоги, через зручний інтерфейс. Функціонал включає реєстрацію користувачів, визначення ролі (волонтер чи отримувач допомоги), створення і опрацювання запитів, а також відстеження активності через адміністративну панель. Двофакторна аутентифікація та шифрування SSL підвищують захист платформи. Запити користувачів організовані в базі даних PostgreSQL з можливістю пошуку за певними параметрами: геолокація, вид допомоги, терміновість. Використання React.js на клієнтській стороні покращує швидкодію та скорочує час відгуку системи. Інтеграція сервісу карт дозволяє оперативно знаходити волонтерів поруч.

Тестування навантаження продемонструвало, що система без зайвих проблем обробляє 1000 одночасних запитів, не втрачаючи продуктивність. Порівняльний аналіз з іншими платформами показав вищий рівень персоналізації запитів та покращену адаптивність для мобільних пристроїв.

Висновки. Розроблена веб-система суттєво покращує комунікацію між волонтерами та тими, хто потребує допомоги. Вона відкриває можливості для розширення та поєднання з іншими громадськими проєктами. Напрацювання можуть бути застосовані для покращення цифрових інструментів у полі волонтерської діяльності.

Список використаних джерел

1. Горінов П., Драпушко Р. Волонтерська діяльність в Україні: соціально-правове дослідження: монографія. Київ: Державний інститут сімейної та молодіжної політики, 2022. 240 с.
2. Smith J., Brown K. "Digital Volunteering Platforms: Trends and Challenges". Journal of Information Systems, 2023.
3. Ivanov P. "Optimization of Web-Based Volunteer Matching Systems". Software Engineering Review, 2022.

УДК 004.93

ПОРІВНЯННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМАЛЬНОГО ВИЯВЛЕННЯ ТА СУПРОВОДЖЕННЯ ОБ'ЄКТІВ ЧЕРЕЗ ВІЗУАЛЬНІ КАНАЛИ ДЛЯ ПОДАЛЬШОГО ВПРОВАДЖЕННЯ НА БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТАХ

Колесник Денис, Джебраїлов Роман

«Інститут інформаційних технологій та систем НАН України», Київ

Науковий керівник – Бондар Сергій, д-р. філ.

Ключові слова: безпілотні літальні апарати, нейронні мережі, розпізнавання об'єктів, супроводження об'єктів.

Вступ. Застосування штучного інтелекту для операцій виявлення та супроводження об'єктів є дуже актуальною, а особливо під час повномасштабного вторгнення країни-агресора на територію України. Виявлення найкращої технології яка забезпечить швидку та ресурсоефективну обробку зображень з відеоряду є однією з першочергових задач і її вирішення дозволить адаптацію програмних рішень до впровадження на БПЛА з максимальною користю.

Мета. Проведення практичних досліджень процедур виявлення та супроводження на відеофайлах, порівняльний аналіз ефективності технологій штучного інтелекту SAM2 [1] та YOLO [2] для виконання задач розпізнавання та супроводження об'єктів.

Матеріали та методи. Для виконання досліджень був розроблений Web-інтерфейс та програмний код (система обробки зображень та відео). Система написана мовою Python, з використанням бібліотек: FastAPI, Pydantic, Pytest, PIL, Numpy, OpenCV, Torch, Supervision, Sam2, Inference_sdk. Для обробки система використовує вже наявні моделі нейронних мереж.

Нейронна мережа (CNN) SAM2 (Segment Anything Model 2) від компанії Meta AI.

Моделі SAM2 не можуть самостійно виявляти об'єкти на зображеннях, не підтримують класифікацію об'єктів, покадрову обробку наданих даних, а працюють тільки з масивами. Головною перевагою моделей SAM2 є супровід об'єктів на відео.

Нейронна мережа (CNN) YOLO (You Only Look Once). Поширюється під відкритою ліцензією.

Моделі YOLO самостійно визначають розташування об'єкта на зображенні (одночасно може визначити багато схожих об'єктів), а також підтримують класифікацію об'єктів (одна модель YOLO може розпізнавати різні типи об'єктів).

Результати. Дослідження були проведені на фото/відео низької та високої якості з одним та з багатьма об'єктами (таб.1). Під час оцінки швидкості обробки зображення YOLO слід враховувати, що запит оброблявся на серверах інших країн, що впливає на швидкість обробки одного кадру.

Таб.1. Порівняння технологій YOLO та SAM2 за ключовими параметрами.

CNN	Розпізнавання	Ефективність виявлення	Вплив кількості об'єктів
YOLO	так	75-100%	низький
SAM2	ні	100%	суттєвий
CNN	Виявлення	Швидкість обробки 1 кадру, с	Вплив якості зображення
YOLO	так	3,83	середній
SAM2	так	8.52	не виявлено

1. Поєднання цих двох моделей забезпечує високу точність виявлення та супроводження. Їх комбінація забезпечить виявлення та супровід декількох об'єктів одночасно.
2. Великим недоліком цього підходу, є швидкість обробки одного кадру, яка буде залежати від якості відео, а також від кількості об'єктів для супроводу. Обробка одного кадру може тривати від 3.43 до 17,39 і більше секунд.
3. Швидкодія цих технологій прямо залежить від обчислювальних потужностей обладнання на якому виконується, що може бути істотною перешкодою в разі використання такої системи на окремому екземплярі БПЛА.

Висновок. Не зважаючи на те, що 100% виявлення будь-якого об'єкта на кадрі навіть з проміжком в 30 кадрів є безперечною перевагою моделей SAM2, але тривалість обробки одного кадру стає суттєвою перешкодою для цієї нейронної мережі. Також вагомим недоліком є неможливість точного розпізнавання об'єктів, а тільки супровід їх за заздалегідь отриманими характеристиками.

На відміну від SAM2 нейронна мережа YOLO виглядає дуже перспективною. Приблизний середній час обробки може складати від 1 до 2 секунд, що є прийнятним для впровадження до системи виявлення та супроводження об'єктів. Моделі YOLO підтримують класифікацію об'єктів, це забезпечить точне визначення виду одиниці об'єкта. Перспективним є заміна SAM2 на трекери машинного зору в поєднанні з моделями YOLO, що забезпечить швидшу обробку кадру, а також стабільність в процесі виявлення та супроводження об'єктів через візуальні канали.

Список використаних джерел:

1. Офіційний опис, документація SAM2. URL: <https://github.com/facebookresearch/segment-anything>
2. Офіційна документація YOLO від Ultralytics. URL: <https://github.com/ultralytics/yolov5>

УДК 004.8

ВИКОРИСТАННЯ ІНСТРУМЕНТУ ШТУЧНОГО ІНТЕЛЕКТУ TABNINE ДЛЯ АВТОМАТИЗАЦІЇ КОДУВАННЯ

Анастасія Кудря

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Наталія Шибицька, к.т.н., доц.*

Ключові слова: програмне забезпечення, штучний інтелект, автозаповнення коду, Tabnine.

Вступ

Технології на основі штучного інтелекту (ШІ) вже стали загальноприйнятими в багатьох галузях, зумовлюючи значне підвищення продуктивності праці, виникнення нових продуктів, зменшення кількості повторюваних, рутинних завдань тощо [1]. Особливо помітний вплив ШІ спостерігається в інтеграції розробки програмних забезпечень (ПЗ). Одним із таких інструментів є Tabnine — система автоматичного доповнення коду, яка використовує алгоритми ШІ для аналізу та передбачення коду, що вводиться. Однак питання ефективності таких інструментів у реальних умовах залишається відкритим. Метою дослідження є оцінка ефективності використання Tabnine для оптимізації процесу кодування та визначення його впливу на продуктивність розробників, зокрема на час, витрачений на написання коду.

Матеріали і методи

Методика дослідження передбачає використання інструменту ШІ Tabnine у середовищі VS Code для аналізу його впливу на швидкість та ефективність написання коду мовою програмування JavaScript. Основна увага приділяється зменшенню часу на написання коду завдяки автоматичному доповненню. Стрімкий розвиток програмної індустрії у світі обумовлює також більш жорсткі вимоги до якості програмних продуктів [2]. Це робить необхідним застосування інструментів, здатних підвищити продуктивність та якість процесу розробки ПЗ.

Результати

Сучасні технології ШІ, зокрема такі, як машинне навчання та нейромережі, відіграють велику роль на процес написання коду. Використання таких інструментів ШІ значно покращують ефективність розробки, автоматизуючи багато рутинних завдань і дозволяючи розробникам зосередитися на складніших аспектах програмування. Завдяки такому підходу процес створення ПЗ стає швидшим, точнішим і менш схильним до помилок. Щоб кількісно оцінити ефективність використання Tabnine, було проведено дослідження, у якому порівнювався час, витрачений на написання функції для перевірки парності числа в JavaScript, з використанням автозаповнення та без його використання. Результати цього дослідження наведені в Табл. 1.

Табл.1 Порівняння часу витраченого на написання коду

Висновок	Без автозаповнення	З автозаповненням Tabnine
Час на написання функції	20 секунд	5 секунд
Часова економія	-	15 секунд

При написанні коду вручну без автозаповнення, програміст витрачає значну кількість часу на введення та перевірку кожної частини функції. Середній час на написання такої функції складає 15-20 секунд.

При використанні автозаповнення Tabnine, після введення лише першої частини функції, інструмент пропонує готове доповнення. В результаті, час на написання функції з автозаповненням складає в середньому 5 секунд.

Порівняння коду для перевірки парності числа без автозаповнення та з автозаповненням Tabnine наведені в Табл. 2.

Табл.2 Порівняння коду без автозаповнення та з автозаповненням

Код без автозаповнення	Код з автозаповненням Tabnine
<pre>function checkEven(num) { if (num % 2 === 0) { return true; } else { return false; } }</pre>	<pre>function checkEvenNumber(num) { return num % 2 === 0; }</pre>

Висновок

Результати дослідження показали, що використання Tabnine для автоматизації кодування значно підвищує продуктивність розробників та скорочує час написання коду, що дозволяє програмісту зосередитись на більш складних завданнях.

Список використаних джерел:

1. Піжук, О. І. (2019). Штучний інтелект як один із ключових драйверів цифрової трансформації економіки. Економіка, управління та адміністрування, (3(89), 41–46. [https://doi.org/10.26642/ema-2019-3\(89\)-41-46](https://doi.org/10.26642/ema-2019-3(89)-41-46)
2. Шибицька Н.М., Кочеткова О.В. Інтеграційне тестування та контроль якості програмного забезпечення// Proceedings 1st international scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2024)", March 6, 2024 - K.: FIT TSNUK, 2024.- С.366-369

УДК

SOFTWARE FOR AERIAL TERRAIN PHOTOGRAPHY WITH A DJI QUADCOPTER**Маршалок Дмитро***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олексій Глазок, к.т.н.*

Ключові слова: DJI drones, Flight scripts, Image processing, Mapping.

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. Thanks to its balance of price and quality, the company enjoys high ratings and strong sales. 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. Additionally, some applications, such as Pix4D and DroneDeploy, use Ground Control Points (GCP), but this feature is impractical for operation in hazardous or hard-to-reach areas.

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. It is a free cross-platform library for real-time image processing, which has become the de facto standard tool for everything related to computer vision [3].

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. Additionally, support was added for controlling other DJI drones (excluding Tello). 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 [4].

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.

The developed software for DJI drones allows users to create static flight routes for terrain photography without relying on GPS signals. It also enables the merging of captured images into a unified map. The use of the OpenCV library for image processing and the DJITelloPy library for drone control greatly simplifies programming and allows for efficient drone operation.

Список використаних джерел:

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. Learning Image Processing with OpenCV / [G. G. Bueno, O. S. Deniz, J. A. Luis Espinosa et al.]. – Packt, Birmingham, 2015. – 208 с.
4. 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 004.65:656.022(043.2)

ІНФОЛОГІЧНА МОДЕЛЬ ФАКТОРІВ, ПОКАЗНИКІВ ТА КРИТЕРІЇВ ОПТИМАЛЬНОСТІ МАРШРУТІВ ПЕРЕВЕЗЕНЬ НА ГРАФОВИХ БАЗАХ ДАНИХ

Назар Мельник

*Національний технічний університет України «Київський політехнічний інститут імені Ігоря
Сікорського», Київ*

Науковий керівник – Олександр Корочкін, к.т.н., доц., доц. кафедри ОТ ФІОТ

Ключові слова: багатокритеріальність, оптимальність, критерій, графові бази даних, транспортні перевезення.

У сучасних умовах військового стану розподіл торговельних транспортних засобів зазнав суттєвих змін: повітряні перевезення повністю припинилися через заборону польотів цивільної авіації, обсяги залізничних перевезень скоротилися на 65,3% через обмежену пропускну спроможність на прикордонних пунктах, значне скорочення водних перевезень через окупацію значної частини морських портів [1]. Зважаючи на ці обмеження, ринок транспортних послуг переорієнтувався на автомобільний транспорт, надаючи йому пріоритет для здійснення вантажних перевезень.

Традиційні реляційні бази даних мають суттєві обмеження у моделюванні складних зв'язків між об'єктами транспортної мережі, особливо при роботі з ієрархічними та графоподібними структурами. У той же час графові бази даних пропонують ефективні рішення для моделювання та аналізу складних багатозв'язних структур [2].

Метою роботи є розробка інфологічної моделі факторів, показників та критеріїв оптимальності маршрутів перевезень з використанням графової бази даних.

Розв'язування задачі включало: формальне представлення розглянутих транспортних маршрутів на графі (рис. 1) та візуалізацію маршрутів на мапі (рис. 2); обробку та збереження в графі даних, отриманих через публічний API; розробку інфологічної моделі факторів, показників та критеріїв оптимальності маршрутів перевезень (таблиця 1), розглядаючи ефективність маршруту як відношення позитивного ефекту до витрат визначення оптимального маршруту за допомогою нелінійної схеми компромісів професора Вороніна А.М., виходячи із доведених переваг цієї схеми агрегації [3, 4].

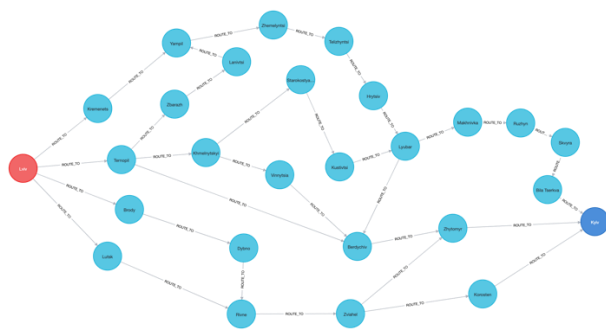


Рис. 1

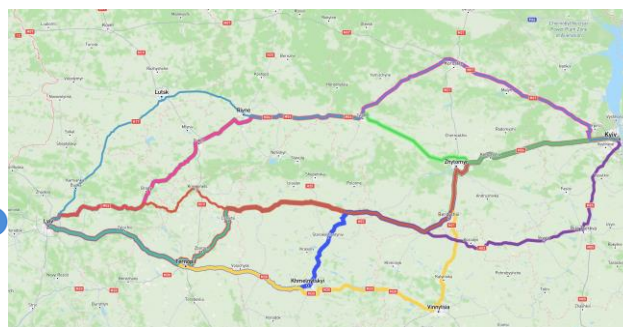


Рис. 2

Таблиця 1. Інфологічна модель факторів, показників та критеріїв ефективності

Критерій	Категорія
Відстань	Витрати
Кількість залізничних переїздів	Витрати
Час у дорозі	Витрати
Кількість перехресть/світлофорів	Витрати
Кількість проміжних населених пунктів	Витрати
Кількість мостів та тунелів	Витрати
Індекс якості дорожнього покриття	Позитивний ефект
Середня швидкість	Позитивний ефект
Кількість АЗС	Позитивний ефект
Індекс безпеки	Позитивний ефект

Було розглянуто множину альтернативних маршрутів з Львова до Києва (рис. 1) та для кожного визначено значення показників відповідно до інфологічної моделі (таблиця 1). Використовуючи нелінійну схему компромісів професора Вороніна А.М. отримано інтегровану оцінку оптимальності для кожного маршруту та після їх нормування та розподілу згідно з лінгвістичними категоріями, де певному значенню інтегрованої оцінки (від 0 до 1) відповідає певна лінгвістична категорія від (незадовільної до високої), визначено пріоритетність маршрутів та оптимальний маршрут.

Висновок

Наукова новизна дослідження полягає у впровадженні багаторівневої моделі оцінювання ефективності транспортних маршрутів, реалізованої в середовищі графової бази даних. Практичне значення отриманих результатів полягає у можливості впровадження розробленої моделі в системи логістичного планування для оптимізації вантажних перевезень, зокрема в умовах обмеженого доступу до інфраструктури під час воєнного стану.

Список використаних джерел:

1. О. В. Малєєва, Д. А. Набокін, Ю. А. Малєєва (2024). Вибір найбільш ефективного маршруту перевезень з урахуванням індексів небезпечності територій в умовах воєнного часу. Системи управління, навігації та зв'язку. Збірник наукових праць. 3. 141-145. 10.26906/SUNZ.2024.3.141.
2. Liu, X., Cats, O., & Van Nes, R. (2018). Exploring the use of time-varying graphs for modelling transit networks. *Public Transport*, 10(1), 183–210. DOI: 10.1007/s12469-018-0178-5.
3. Воронін А. М. Нелінійна схема компромісів у багатокритеріальних задачах оцінювання та оптимізації/ А.М. Воронін // Кібернетика та системний аналіз. - 2009. - Т. 45, № 4. - С. 106- 114
4. Харченко В. П. Нелінійне та багатокритеріальне моделювання процесів у системах керування рухом: моногр. / В. П. Харченко, О. О. Писарчук. – К.: Ін-т обдарованої дитини, 2015. – 248 с.

УДК 004.4

GIT ЯК ІНСТРУМЕНТ УДОСКОНАЛЕННЯ ПРОЦЕСІВ КОМАНДНОЇ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тарас Мельник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Яна Белозьорова, к.т.н., доц.

Ключові слова: Git, версія, розробка, система, дані, інформація, система контролю версій.

Вступ

У зв'язку зі зростанням обсягів та ускладненням програмних систем дедалі більшого значення набуває злагоджена робота команд розробників. Однією з відповідей на виклики колективної розробки стали системи контролю версій (Version Control Systems, VCS), які дозволяють відстежувати зміни у коді, організовувати спільну роботу та зберігати повну історію редагувань. Серед них особливе місце посідає Git – розподілена система, яка стала де-факто стандартом у сучасній розробці програмного забезпечення [1].

Матеріали і методи

У рамках дослідження було розглянуто етапи розвитку систем версійного контролю: від простих локальних інструментів до централізованих платформ, а згодом – до розподілених рішень. Акцент зроблено на Git як на прикладі системи, що поєднує стабільність, масштабованість і можливість одночасної роботи великої кількості учасників.

Для ілюстрації застосування Git розглянуто ситуації з колективною розробкою навчальних проєктів. Проаналізовано основні механізми роботи Git, зокрема створення гілок, комітів та злиттів. Висвітлено переваги, що відрізняють Git від попередників, зокрема автономність роботи, надійне зберігання копій та зручність у використанні.

Мабуть кожний стикався із ситуацією, коли необхідно виправляти якийсь файл, наприклад, дипломну роботу, але при цьому треба про всяк випадок зберегти попередні зміни. Потім ще дещо потрібно виправити і так далі. На виході отримуємо купу файлів дипломної роботи, які за своїм змістом є майже ідентичними. Вже на даному етапі виникає необхідність створення системи версій даного файлу. У розглянутому випадку контроль над версіями бере на себе людина, при цьому всі версії зберігаються у неї локально на комп'ютері. Це приклад використання локальної системи керування версій.

А якщо дипломна робота має колективний характер і над нею одночасно працюють декілька студентів? Виникає необхідність передавання та синхронізування інформації. Для вирішення даної проблеми були створені централізовані системи керування версій: всі дані, з якими відбувається взаємодія, зберігаються на централізованому сервері, а користувачі, у свою чергу, під'єднуються до нього для роботи із файлами. Проте така система має один суттєвий недолік – якщо щось станеться із сервером, то будуть втрачені усі дані.

Дану проблему було вирішено у розподілених системах контролю версій: для роботи із даними, що зберігаються на сервері, користувачі повинні завантажити усі ці дані собі на комп'ютер, створивши тим самим

локальну копію всієї інформації. Тепер, якщо щось станеться із центральним сервером, можна буде взяти версію когось із користувачів і відновити дані. Саме до таких систем відноситься Git.

Результати

Git надає гнучкий та водночас швидкий функціонал [2,3]. Робота із файлами відбувається у репозиторії – директорії, дані якої підлягають версіонуванню. У ньому можна створювати гілки – різні відгалуження програми, – в яких відбувається розробка. При внесенні змін можна створити коміт – так званий «знімок» поточного стану гілки репозиторія, в якій ведеться робота. Такі «знімки» можна комбінувати між гілками, переміщати в різні місця, іншими словами, – маніпулювати версіями програмного продукту. І все це може незалежно виконувати кожна людина, що залучена до розробки даного програмного забезпечення. Всі ці, а також багато інших особливостей, роблять Git дуже потужним інструментом командної розробки.

У роботі зібрано і описано, як сьогодні використовують Git під час командної розробки програм; виділено основні технічні переваги Git, які роблять його зручним і корисним для програмістів; розглянуто історичний процес розвитку систем керування версій, вершиною якого на даний момент являється Git.

Висновки

Git значно трансформував підхід до спільної розробки програмного забезпечення. Здатність підтримувати автономну роботу, гнучке керування версіями та високий рівень відмовостійкості робить цей інструмент критично важливим для сучасних ІТ-процесів. Git не лише оптимізовує технічні аспекти розробки, а й сприяє кращій організації командної співпраці, що обумовлює його актуальність у подальших наукових дослідженнях.

Список використаних джерел

1. Git. URL: <https://git-scm.com>.
2. The Benefits of Working with Git. URL: <https://medium.com/@niklongstone/the-benefits-of-working-with-git-e948a147763c>.
3. What is Version Control and What Are Its Benefits? URL: <https://www.simplilearn.com/tutorials/devops-tutorial/version-control>.

УДК

ДОСЛІДЖЕННЯ АКТУАЛЬНОСТІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Артем Моргун

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Андрій Гізун, к.т.н., доц.

Ключові слова: Мікросервісна архітектура, Моноліт, SOA, ШІ

Вступ. Традиційним підходом до проєктування програмного забезпечення є монолітна архітектура (далі – моноліт), що характеризується наявністю єдиного компоненту й розгортається та функціонує як одне ціле. Хоч даний підхід є виправданим, для відносно простих систем або стартапу, з розширенням функціоналу виникають типові, як для моноліту, проблеми: складність підтримки модульності коду та його тестування; ускладнена взаємодія команд розробників при роботі з єдиною кодовою базою; розгортання додаткової інфраструктури для реагування на підвищення навантаження тощо.

Мета. Дослідити причини виникнення мікросервісної архітектури (далі - MSA), підтвердити або спростувати обґрунтування її актуальності для застосування у сучасних програмних рішеннях і напрямки її розвитку.

Об'єктом дослідження є архітектура програмного забезпечення та процеси розробки програмних систем та рішень, а предметом дослідження є MSA. Були застосовані методи аналізу наукової літератури з подальшим їх синтезом.

Матеріали та методи. Для вирішення проблем моноліту було запропонований сервісно-орієнтований підхід (SOA), основною задачею якого є розбиття моноліту на окремі сервіси, які взаємодіють між собою за допомогою синхронних методів (SOAP, WSDL та ін.) [1]. Однак, незважаючи на мету та ідею SOA, реалізація мала цілу низку викликів, оскільки у розробників було відсутнє єдине розуміння SOA та як його застосовувати на практиці, що призводило до архітектури розподілених монолітів [2]. Додатково, технічні можливості (такі як відсутність хмарного середовища) й вартість складових серверів (пам'ять, розмір сховищ) у першій декаді 2000 року не сприяли створенню розподілених систем [3].

Результати. Термін MSA було офіційно представлено у 2011 році [4] й MSA можна розглядати як вдалу імплементацію SOA, де досягається розподілення функціональності системи на окремі компоненти, які мають ряд характеристик: незалежне розгортання компонентів, чітко визначені задачі для кожного конкретного сервісу, зберігання свого стану у власному сховищі, гнучкість [2].

Забезпеченню переваг MSA сприяє стрімкий розвиток хмарних технологій (найпопулярнішими провайдерами є AWS, Google Cloud, Microsoft Azure), де задача розгортання окремих сервісів та методів їх взаємодії значно спрощується. Наприклад - SaaS рішення як Serverless пропонують розробникам фокусуватися винятково на вирішенні бізнес проблем з мінімальним конфігуруванням інфраструктури.

Завдяки вказаним властивостям, MSA системи набули широкого застосування у різноманітних сферах бізнесу: сервіси відтворення відео та кіно YouTube, Netflix; соціальні мережі Facebook, Instagram; служби таксі Uber, Bolt; сервіси доставки їжі JustEatTakeaway.com, Glovo, Deliveroo; виробники газованих напоїв Coca-Cola та ін. Використання MSA даними компаніями дозволяє їм додавати новий функціонал швидше та реагувати на збільшення навантаження шляхом швидкого розгортання нової інфраструктури.

З активним розвитком технологій штучного інтелекту (ШІ) набуває актуальності розгляд їх використання у MSA як для її проектування так і для виділення окремих ШІ сервісів. ШІ може бути використане для автоматизації генерування моделей сервісів на основі існуючого моноліту. Як окремі сервіси, ШІ можуть виконувати наступні функції: генерація персоналізованого контенту для користувачів, виявлення аномалій, адаптації інфраструктури MSA до навантаження тощо [5].

Висновки. Результати дослідження показали, що виникнення MSA є результатом проблем моноліту та спроб застосування принципів SOA. Офіційно отримавши назву MSA у 2011 році, даний тип

архітектури активно впроваджується різноманітними компаніями для адаптації до умов високого навантаження й бізнес конкуренції. Додатковим фактором розвитку MSA є виникнення та удосконалення хмарних середовищ. З появою та активним розвитком III технологій виникає інтерес до впровадження даних технологій у MSA як для її проєктування, так і для використання в окремих сервісах. Таким чином, застосування MSA як одного з найбільш перспективних підходів щодо розробки ефективних програмних систем є безсумнівним.

Список використаних джерел:

8. Papazoglou M. P., van den Heuvel W.-J. Service oriented architectures: approaches, technologies and research issues. The VLDB Journal. 2007. Vol. 16, no. 3. P. 389–415.
9. Newman S. Building microservices: Designing fine-grained systems. O'Reilly, 2021. 612 p.
10. Jonas J. Reactive Microservices Architecture. O'Reilly, 2016. 54 p.
11. Design, monitoring, and testing of microservices systems: The practitioners' perspective / M. Waseem et al. Journal of Systems and Software. 2021. Vol. 182. P. 111061
12. Katal A., Prasanna P., Birla R., Kunal. Evolution from Monolithic to Microservices Architecture: A New Era in Software Architecture // Advancements in Optimization and Nature-Inspired Computing for Solutions in Contemporary Engineering Challenges / ред. K. Srinivas, S. K. Sharma, S. Chaudhary. Singapore: Springer, 2025. С. 235–279

УДК 656.70:44.220:44.42

ЗАСОБИ УПРАВЛІННЯ СЕРТИФІКАЦІЄЮ ПРАЦІВНИКІВ АВІАКОМПАНІЇ

Віталій Пелех

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Вадим Сураєв, к.т.н., доц.

Ключові слова: Flask, SQL, авіакомпанія, штучний інтелект, API

Управління сертифікацією працівників є важливою складовою діяльності будь-якої авіакомпанії.

Мета дослідження — розробити засіб, використовуючи доступні технології для того, щоб спростити процес управління сертифікацією відповідних спеціалістів в авіакомпанії.

В результаті досліджень було розпочато розробку веб-додатка мовою програмування Python за допомогою мікрофреймворка Flask. Також для розробки веб-додатка було використано MS SQL Server, де була створена база даних.

Веб-додаток має включати такі основні функції: авторизація користувачів з різними рівнями доступу, що забезпечує безпеку даних та персоналізований доступ до функціоналу системи; управління інформацією про працівників, включаючи їх департаменти, посади та статус сертифікації; внесення та редагування інформації про сертифікацію, що містить дату закінчення навчання, список необхідних навичок, графік занять. Крім цього, реалізовано механізм призначення викладачів для проведення сертифікаційних курсів, а також контроль термінів дії сертифікатів.

Система передбачає доступ до штучного інтелекту ChatGPT через API, що дозволяє користувачам отримувати відповіді на запитання щодо сертифікаційних вимог та процедур, спрощуючи роботу з платформою. Гнучка система керування дозволяє адміністраторам легко оновлювати дані, вносити зміни до розкладу занять, призначати відповідальних осіб та відстежувати ефективність навчального процесу. Це робить веб-додаток корисним інструментом для авіакомпаній, що прагнуть оптимізувати процес сертифікації працівників.

Висновки

Розроблений веб-додаток є ефективним інструментом для управління сертифікацією працівників авіакомпанії. Він дозволяє оптимізувати облік навчання таких категорій співробітників, як пілоти, стюардеси, техніки, зменшити адміністративне навантаження та покращити контроль за сертифікаційними процесами. Інтеграція з ChatGPT підвищує зручність використання, забезпечуючи оперативний доступ до необхідної інформації через API.

Список використаних джерел:

1. Документація по фреймворку Flask (3.1.x) URL: <https://flask.palletsprojects.com/en/stable/> (Last accessed: 18.03.2025).
2. Документація по OpenAI API URL: <https://platform.openai.com/docs/api-reference/introduction> (Last accessed: 18.03.2025).

УДК 005.922.52:004.932(043.2)

ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ПРИВЕДЕННЯ СТРУКТУРОВАНИХ ДОКУМЕНТІВ ДО КАНОНІЧНОЇ ФОРМИ

Дмитро Сирейщіков

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Михайло Оленін, к.ф.-м.н., с.н.с.

Ключові слова: XML, канонічна форма, машинне навчання, цифрова безпека, стандарти W3C.

У сучасному цифровому світі XML-документи відіграють ключову роль у функціонуванні різних інформаційних систем, зокрема вебсервісів, наукових баз даних, бібліометричних API та банківських платформ. Однак спосіб їхньої серіалізації може суттєво відрізнятися, що створює труднощі з порівнянням, збереженням та верифікацією таких документів. Для розв'язання цієї проблеми застосовують методи канонізації XML, які дозволяють уніфікувати структуру документа, не змінюючи його змісту [1–3].

У межах цього дослідження розглянуто сучасні методи канонізації XML-документів з метою визначення найбільш ефективного підходу. Оптимальне рішення має забезпечити точніше порівняння XML-структур, ефективну обробку великих обсягів даних та надійний захист інформації. Аналіз останніх наукових праць показує, що більшість існуючих методів базуються на стандартах W3C, однак досі не включають технології машинного навчання. Це певним чином суперечить загальним тенденціям у сфері автоматизованої обробки даних [4].

На сьогодні основні підходи до канонізації XML мають свої обмеження:

- Синтаксичні методи не враховують семантичного змісту документа.
- Семантичні алгоритми дають точніші результати, але вимагають значних обчислювальних ресурсів.
- Евристичні підходи забезпечують гнучкість, проте можуть бути нестабільними.
- Методи, орієнтовані на безпеку, не вирішують проблеми форматування XML.

Останні розробки у сфері машинного навчання відкривають нові можливості для автоматизації процесу нормалізації XML. Моделі на основі глибокого навчання, зокрема BERT та LayoutLM, демонструють здатність аналізувати структуру XML та коректно відображати теги, що особливо актуально для великих динамічних XML-систем. Водночас ці методи вимагають значних обчислювальних ресурсів та ретельного навчання моделей [5–6].

Висновок

Враховуючи недоліки окремих підходів, перспективним напрямом є розробка гібридного методу, що поєднує синтаксичну нормалізацію, семантичний аналіз, евристичні алгоритми, методи машинного навчання та механізми безпеки. Такий комплексний підхід дозволить усунути як форматні, так і змістові відмінності XML-документів, що, у свою чергу, підвищить точність їхнього порівняння, спростить обробку великих масивів XML-даних та забезпечить надійний захист інформації в критичних системах.

Список використаних джерел:

1. Song, E., & Haw, S.-C. (2020). XML-REG: Transforming XML into relational using hybrid-based mapping approach. URL: <https://ieeexplore.ieee.org/document/9204703> (Last accessed: 13.03.2025)
2. Ali, M., Khan, M. A., & Rasool, R. U. (2024). A hybrid machine learning model for efficient XML parsing. URL: <https://ieeexplore.ieee.org/document/10810393> (Last accessed: 13.03.2025)
3. Li, S., & Rigger, M. (2024). Finding XPath bugs in XML document processors via differential testing. *Proceedings of the 2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE)* URL: <https://ieeexplore.ieee.org/document/10549336> (Last accessed: 13.03.2025)
4. Achachlouei, M. A., Patil, O., Joshi, T., & Nair, V. N. (2024). Document automation architectures: Updated survey in light of large language models. URL: <https://doi.org/10.48550/arXiv.2308.09341> (Last accessed: 13.03.2025)
5. Marouaa, B., & Pappa, A. (2021). WebT-IDC: A web tool for intelligent dataset creation – A use case for forums and blogs. *Procedia Computer Science*, 192, 1051–1060. URL: <https://doi.org/10.1016/j.procs.2021.08.108> (Last accessed: 13.03.2025)
6. Wang, Z., & Shang, J. (2023). Towards zero-shot relation extraction in web mining: A multimodal approach with relative XML path. URL: <https://arxiv.org/abs/2305.13805> (Last accessed: 13.03.2025)

УДК 004.4

ПОНЯТТЯ ДИСТИЛЯЦІЇ ЗНАНЬ ДЛЯ СТИСНЕННЯ МОДЕЛЕЙ НЕЙРОННИХ МЕРЕЖ

Суховий Олександр

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олена Грінченко, к.т.н., доц.

Ключові слова: дистиліяція знань, нейронна мережа, глибока нейронна мережа, штучний інтелект, машинне навчання, стиснення моделей нейронних мереж.

Відповідно до опитування [1] у 2024-му році 78% компаній стверджували що використовують штучний інтелект. Відповідно до [2] найпопулярнішим рішенням що базується на штучному інтелекті є чат-бот ChatGPT що використовує технологію глибоких нейронних мереж [3].

Рішення що базуються на штучному інтелекті потребують значних обчислювальних ресурсів як в процесі навчання так і в процесі експлуатації уже навченої моделі – згідно звіту [4] витрати на

інфраструктуру для роботи штучного інтелекту перевищать 200 мільярдів доларів США до 2028-го року. Для зменшення потреби в значних обчислювальних ресурсах в процесі експлуатації моделі глибоких нейронних мереж піддають стисненню. Стиснення моделі нейронної мережі – це процес отримання нової нейронної мережі що містить меншу кількість шарів, нейронів та зв'язків між ними на базі існуючої нейронної мережі зі збереженням функції початкової нейромережі. До таких методів відносять квантування, обрізку, апроксимацію низького рангу та дистиляцію знань та інші [5].

Метод дистиляції знань викликає особливий інтерес так як даний метод оперує на більш абстрактному рівні ніж інші методи. На відміну від інших методів дистиляція знань не оперує внутрішньою структурою моделі нейронної мережі. Дистиляція знань переносить знання з одної нейронної мережі в іншу за допомогою алгоритмів машинного навчання. При цьому нейронну мережу що є джерелом знань прийнято називати вчителем а нейронну мережу що навчається – учнем. Стиснення досягається за рахунок того що модель учня менша ніж модель учителя. Суть даного методу полягає у використанні результатів роботи уже навченої нейронної мережі у якості очікуваних результатів при навчанні іншої нейромережі. Тобто, очікувані результати роботи учня для кожного екземпляру навчальних даних формуються як результат роботи учителя на даному екземплярі навчальних даних [6].

Даний метод успішно застосовується для навчання моделей нейронних мереж до яких ставляться вимоги запуску на обладнанні з обмеженими обчислювальними ресурсами такими як пристрої інтернету речей [7].

Варто зазначити що дистиляцію знань можна використовувати не лише для стиснення моделей нейронних мереж але і для перенесення даних з одної моделі нейромережі в іншу незалежно від розмірів мережі вчителя і студента. Такий підхід є малодослідженим.

Висновок

Метод дистиляції знань добре зарекомендував себе в якості рішення для стиснення моделей нейронних мереж однак використання даного методу для вирішення інших задач машинного навчання залишається малодослідженим.

Список використаних джерел:

1. The state of AI: How organizations are rewiring to capture value / A. Singla та ін. *McKinsey & Company*. 12.03.2025. URL: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai> (дата звернення: 26.03.2025).
2. Most Popular AI Tools. *Aitools.xyz*. URL: <https://aitools.xyz/popular-ai-tools/2025/january> (дата звернення: 26.03.2025).
3. GPT-4 Technical Report. *OpenAI*. URL: <https://cdn.openai.com/papers/gpt-4.pdf> (дата звернення: 26.03.2025).
4. Artificial Intelligence Infrastructure Spending to Surpass the \$200Bn USD Mark in the Next 5 years, According to IDC. *International Data Corporation*. 18.02.2025. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS52758624> (дата звернення: 26.03.2025).
5. Song H., Huizi M., William J. D. Deep compression: Compressing deep neural networks with pruning, trained quantization and Huffman coding. *4th International Conference on Learning Representations, ICLR 2016*, San Juan, 2–4 трав. 2016.
6. Knowledge Distillation: A Survey / G. Jianping та ін. *International Journal of Computer Vision*. 2021. вип. 129. С. 1789–1819. ISSN 09205691. URL: <https://doi.org/10.1007/s11263-021-01453-z>.
7. Compacting Deep Neural Networks for Internet of Things: Methods and Applications / Z. Ke та ін. *IEEE Internet of Things Journal*. 2021. Т. 8. С. 11935–11959. ISSN 23274662. URL: <https://10.1109/IIOT.2021.3063497>.

УДК 004.77:004.8:371.3

ПРОГРАМНИЙ ЗАСІБ МОНІТОРИНГУ НАВЧАЛЬНОЇ АКТИВНОСТІ В ЗАКЛАДАХ ОСВІТИ

Торський Андрій

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Сергій Кравченко ч. к.х.н., доц.

Ключові слова: програмний засіб, моніторинг навчальної активності, масиви даних, аналіз даних

Вступ. Сучасні заклади освіти активно впроваджують цифрові технології для підвищення ефективності навчального процесу, важливим застосуванням яких є моніторинг навчальної активності учнів для виявлення проблемних аспектів та підвищення ефективності методів викладання. Існують різні підходи до автоматизованого збору та аналізу даних про активність учнів у навчальному середовищі [1, 2], однак, існуючі рішення мають певні обмеження відносно гнучкості та адаптивності до потреб навчальних закладів [3]. Потреба в програмних засобах для моніторингу навчальної активності учнів, як ефективного інструменту у сфері освіти залишається актуальною.

Мета. Розробка програмного засобу моніторингу навчальної активності учнів у закладах освіти для автоматизації збору та аналізу даних, що стосуються щодо рівня залучення учнів до навчального процесу..

Матеріали та методи. Виконується збір даних про активність учнів на платформі навчання для їх автоматичної обробки з подальшим створенням звітів для вчителів. Обробка даних здійснюється з використанням методів статистичного аналізу та машинного навчання для прогнозування подальшої навчальної активності на основі історичних даних.

Результати. Додаток аналізує навчальну активність учнів на основі даних про їхню взаємодію з електронними освітніми ресурсами, основним показником яких є частота входів у систему, час виконання завдань, рівень взаємодії з навчальними матеріалами та результати тестувань. Методи машинного навчання дозволяють прогнозувати ймовірності рівня успішності на основі історичних даних.

Висновки. Програмний додаток автоматизує моніторинг навчальної активності учнів, що підвищує ефективність аналізу успішності та своєчасного виявлення проблем у навчальному процесі та може бути використаний в закладах освіти для персоналізованого підходу до підвищення ефективності навчання.

Список використаних джерел:

1. Зварич І. "Моніторинг навчально-пізнавальної активності учнів як показник якості освітніх послуг" // Вісник післядипломної освіти, 2020. umo.edu.ua.
2. Шегда А. "Моніторинг розвитку навчальної діяльності учнів" // Інститут модернізації змісту освіти, 2023. imso.zippo.net.ua.
3. Gao N., Shao W., Rahaman M.S., Salim F.D. "n-Gage: Predicting in-class Emotional, Behavioural and Cognitive Engagement in the Wild" // arXiv preprint arXiv:2007.04831, 2020.

УДК 004.62:004.63(043)

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ 24-БІТНИХ ЗСУВІВ В АЛГОРИТМІ СТИСНЕННЯ ДАНИХ LZSS

Назар Федоренко

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник — Вовк Володимир Григорович, к. т. н., доцент*

Ключові слова: стиснення даних, стиснення без втрат, LZ77, LZSS, 24-бітні зсуви.

Об'єми електронних носіїв даних постійно збільшуються, але разом з ними також збільшуються і обсяги інформації, а тому завжди існувала потреба у компактному кодуванні цих даних. Для цього були створені алгоритми LZ77 та його покращений варіант LZSS [1]. Популярні реалізації цих алгоритмів (LZ4, ZLIB та ін.) можуть використовувати максимум 16- і 15-бітні [2, 3] зсуви відповідно, що обмежує можливість кращого стиснення даних.

Метою роботи є дослідження використання 24-бітних зсувів в алгоритмі LZSS для досягнення кращих коефіцієнтів стиснення даних.

Алгоритм стиснення даних без втрат LZ77 замінює повторювані сегменти даних на вказівник на позицію попереднього такого самого сегменту у поданому наборі даних. Вказівник складається із зсуву (кількості символів від початку повтору) та довжини сегменту. LZSS відрізняється тим, що якщо повторюваний сегмент є меншим або дорівнює довжині вказівника, то він не замінюється цим вказівником [1].

У реалізаціях цих алгоритмів зсув має обмеження, яке визначається максимальною кількістю бітів, якими він кодується. В LZ4 зсуви можуть мати максимум 16 біт (макс. зсув — 65535) [2], а в Deflate — 15 біт (макс. зсув — 32768) [3]. Це зумовлено тим, що вони розраховані на прийнятну швидкість стиснення/розтиснення, а Deflate розроблявся у часи, коли комп'ютери мали відносно малу кількість оперативної пам'яті (4-8 МБ). 24-бітний зсув розширює дистанцію до 16777215 символів, що може збільшити коефіцієнт стиснення.

Для наукового обґрунтування результатів досліджень використано експериментальний та статистичний метод, а саме створено програмну реалізацію LZSS з використанням 24-бітних зсувів та порівняно її з іншими популярними компресорами.

Компресор Kitten є реалізацією цього методу мовою C. Він орієнтований на швидке розтиснення та більші коефіцієнти стиснення, ніж інші швидкі компресори (LZ4 та ін.). Він зможе конкурувати з Deflate або подібними, якщо додати ентропійне кодування [3]. Його було інтегровано у бенчмарк lzbenc 1.8 та протестовано на двох датасетах: Silesia та enwik8. Для компіляції бенчмарку використовувався компілятор LLVM Clang x86_64 15.0.7, ПК із ЦП AMD Ryzen 7 5800H, 16 ГБ ОП та ОС Windows 11 23H2.

Таб. 1. Тест на Silesia Corpus

Компресор	Швидкість стиснення	Швидкість розтиснення	Розмір стиснених даних (байт)	Співвідношення стиснених даних (%)
kitten 1.0 -9	0.31 МБ/с	3398 МБ/с	74225715	35.02
kitten 1.0 -12	0.17 МБ/с	3252 МБ/с	73057265	34.47
kitten 1.0 -15	0.13 МБ/с	3005 МБ/с	72400016	34.16
kitten 1.0 -22	0.31 МБ/с	2528 МБ/с	71745154	33.85
LZ4 1.9.3	786 МБ/с	4391 МБ/с	100880833	47.6
LZ4HC 1.9.3 -12	14 МБ/с	4329 МБ/с	77262717	36.45

Таб. 2. Тест на enwik8

Компресор	Швидкість стиснення	Швидкість розтиснення	Розмір стиснених даних (байт)	Співвідношення стиснених даних (%)
kitten 1.0 -12	0.3 МБ/с	2834 МБ/с	36021480	36.02
kitten 1.0 -15	0.19 МБ/с	2237 МБ/с	34976775	34.98
kitten 1.0 -22	0.1 МБ/с	1360 МБ/с	33610190	33.61
LZ4 1.9.3	570 МБ/с	3940 МБ/с	57262281	57.26
LZ4HC 1.9.3 -12	20.5 МБ/с	3430 МБ/с	41913140	41.91
ZLIB 1.2.11 -9	22.2 МБ/с	372 МБ/с	36475792	36.48

Висновок

Завдяки використанню 24-бітних зсувів компресор Kitten має краще стиснення, ніж інші швидкі компресори, а з ентропійним кодуванням він може досягнути іще кращого коефіцієнту стиснення. Але він є дуже асиметричним: він має низьку швидкість стиснення та може використовуватися для даних, які стискатимуться раз, а розтискатимуться багато разів.

Список використаних джерел:

1. Khalid S. Introduction to Data Compression : 6th Edition. Elsevier, 2018. 765 p.
2. LZ4 explained. *Fast Compression* : вебсайт. URL: <https://fastcompression.blogspot.com/2011/05/lz4-explained.html> (дата звернення: 08.03.2025).
3. RFC 1951. DEFLATE Compressed Data Format Specification version 1.3. IETF, 1996.

УДК 004.418

АНАЛІЗ ДОЦІЛЬНОСТІ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ «ВЕБ-СИСТЕМИ УПРАВЛІННЯ СТУДМІСТЕЧКОМ КАІ»

Валерія Харіна

Державний університет "Київський авіаційний інститут"

Науковий керівник – Тетяна Конрад, к.т.н.

Ключові слова: програмне забезпечення, автоматизація, веб-система, цифрова трансформація, Студмістечко, гуртожиток, КАІ.

Заклади вищої освіти України активно залучають цифрові технології для автоматизації виробничих процесів. Державний університет "Київський авіаційний інститут" (КАІ) не є винятком, тому для підтримки потреб навчального процесу і внутрішнього електронного документообігу запроваджено систему Digital University, яка є багатофункціональною для реалізації виробничих потреб викладачів, адміністративних працівників і здобувачів освіти, зокрема дозволяє студентам переглядати семестрові бали та розклад навчання. Однак, процеси управління гуртожитками університету все ще залишаються без змін і потребують осучаснення за рахунок цифровізації. Впровадження «Веб-системи управління Студмістечком КАІ» дозволить знизити навантаження на адміністрацію гуртожитку, автоматизує рутинні завдання, а також забезпечить студентам більш ефективну взаємодію з керівництвом, зменшивши час, витрачений на бюрократичні процедури.

Управління гуртожитками є важливою складовою частиною адміністративної роботи університету. Основні нормативно-правові документи, що регулюють роботу Студмістечка КАІ: «Положення про Студентське містечко Національного авіаційного університету», що регламентує функціонування гуртожитків [1]; «Положення про

оплату за проживання в гуртожитках Студентського містечка Національного авіаційного університету», яке регламентує оплату за проживання [2]; «Положення про користування гуртожитком Національного авіаційного університету», визначає механізм забезпечення гуртожитками здобувачів вищої освіти [3]; «Положення про гуртожитки Студентського містечка НАУ», що регламентує правила проживання в Студмістечку [4]; «Правила внутрішнього розпорядку в студентських гуртожитках», встановлює внутрішній розпорядок діяльності гуртожитку [5]; «Положення про поселення та проживання в студентських гуртожитках», яке регламентує процес поселення та виселення [6]; «Положення про експлуатаційний відділ Студентського містечка Національного авіаційного університету», регламентує функціонування експлуатаційного відділу [7].

Ключові процеси, що здійснюються в Студентському містечку КАІ: організація поселення та виселення; контроль дотримання правил проживання; облік та управління; технічне обслуговування, рис. 1.



Рис. 1. Ключові процеси Студмістечка КАІ

Порівняємо існуючі рішення у сфері управління Студентськими містечками для визначення актуальних функцій та оцінку потенційної ефективності впровадження. Розглянемо функціонал закордонних аналогів: StarRez та ResLife Portal.

StarRez – це провідна глобальна платформа для автоматизації житлових процесів не лише у студентських гуртожитках, а й у інших житлових комплексах.

ResLife Portal – це сучасна платформа для управління студентським житловим фондом заснована в 2007 році в Сан-Дієго, Каліфорнія, США.

В таблиці 1 наведено проаналізований функціонал кожної системи, «+» позначено наявний функціонал, «-» відсутність функції.

Таблиця 1

Порівняння існуючих програм-аналогів

Функції / Назва системи	Онлайн поселення	Дотримання правил проживання	Облік та управління	Технічне обслуговування	Фінансові функції	Бронювання кімнат	Підбір сусідів по кімнаті	Комунікація з адміністрацією
ResLife Portal	+	+	+	+	+	+	-	+
StarRez	+	+	+	+	+	+	+	+

З таблиці видно, що обидві платформи надають схожий функціонал, проте їх впровадження може бути занадто дорогим для державних закладів України. Наприклад, для використання ResLife Portal необхідно заплатити 470\$ на місяць, а для підключення додаткових функцій від 120\$ до 450\$. Окрім високої вартості, існують й інші обмеження: складність впровадження та інтеграції з уже існуючими інформаційними системами університету, відсутність української локалізації інтерфейсу, що потребуватиме додаткових витрат на переклад, а також необхідність навчання персоналу для роботи із середовищем.

Створення та впровадження «Веб-системи управління Студмістечком КАІ» дозволить спростити та процеси організації поселення та виселення студентів. Студентам будуть доступні функції онлайн подачі документів, вибору

кімнати, запису до електронної черги та ін. Для студентів передбачено електронний кабінет, в якому вони зможуть переглядати необхідну інформацію та подавати заяви на технічне обслуговування. Для адміністрації автоматизація направлена на облік та управління житловим фондом, зменшення паперової роботи та переведення її в цифрову площину. Кожна з розроблених функцій допоможе заощадити час усіх користувачів інформаційної системи.

Висновки

Розробка та впровадження «Веб-системи управління Студмістечком КАІ» є актуальним кроком у цифровій трансформації інфраструктури Державного університету "Київський авіаційний інститут", що дозволить підвищити ефективність адміністративних процесів, покращить комунікацію між студентами та адміністрацією, зменшить час виконання рутинних завдань.

Аналіз закордонних аналогів, таких як StarRez та ResLife Portal показав, що хоч вони мають широкий функціонал, їх недоліки, виявлені під час аналізу, роблять програмні рішення майже не придатними для використання у державних закладах України. Веб-система управління Студмістечком КАІ» враховує всі негативні аспекти, виявлені під час аналізу іноземних продуктів, та стане доступним, зручним та ефективним рішенням, яке відповідатиме потребам університету.

Список використаних джерел:

1. ПОЛОЖЕННЯ про Студентське містечко Національного авіаційного університету СМЯ НАУ П 06.32 (01) - 02 – 2023.
2. Положення про оплату за проживання в гуртожитках Студентського містечка Національного авіаційного університету СМЯ НАУ П 06.04.06(02) – 02 – 2023.
3. ПОЛОЖЕННЯ про користування гуртожитком Національного авіаційного університету СМЯ НАУ П-06.32(01) – 01- 2020.
4. ПОЛОЖЕННЯ про гуртожитки Студентського містечка НАУ СМЯ НАУ П – 06.32(03) – 01 – 2014.
5. ПРАВИЛА внутрішнього розпорядку в студентських гуртожитках СМЯ НАУ П – 06.32 – 04 – 2014
6. ПОЛОЖЕННЯ про поселення та проживання в студентських гуртожитках СМЯ НАУ П – 06.32(02) – 02 – 2014.
7. ПОЛОЖЕННЯ про експлуатаційний відділ Студентського містечка Національного авіаційного університету СМЯ НАУ П 06.32.04 (01) – 01 – 2023.
8. ResLife Portal URL: <https://www.reslifeportal.com/> (дата звернення 06.03.2025)
9. StarRez | A Cloud Based Residential Community Management Software Platform URL: <https://www.starrez.com/> (дата звернення 06.03.2025).

УДК 656.7:044.22:044:42

СИСТЕМА АВТОМАТИЧНОГО ІНФОРМАЦІЙНОГО ОПОВІЩЕННЯ ПІДРОЗДІЛІВ АВІАКОМПАНІЇ

Чичкань Вячеслав

Державний університет "Київський авіаційний інститут"

Науковий керівник – Вадим Сураєв, к.т.н., доц.

Ключові слова: автоматичне оповіщення, авіаційні інформаційні системи, оперативне інформування, технології сповіщення.

Вступ. Своєчасне інформування підрозділів авіакомпанії про зміни у рейсах та надзвичайні ситуації є критично важливим для стабільної роботи перевізника. Затримки в комунікації спричиняють перебої, додаткові витрати та ризики. Багато авіакомпаній, зокрема Delta Airlines, впроваджують централізовані системи оповіщення, що покращують координацію та скорочують затримки. Пасажири також очікують миттєвих повідомлень [1]. Автоматизація комунікації підвищує ефективність управління, зменшує вплив людського чинника та забезпечує оперативне реагування [2, 3].

Мета. Розробка та впровадження автоматизованої системи інформаційного оповіщення, що забезпечує швидке багатоканальне доведення повідомлень до співробітників авіакомпанії з метою підвищення ефективності управління операціями.

Матеріали та методи. У дослідженні проведено аналіз сучасних систем автоматичного оповіщення авіакомпаній. Визначено ключові канали комунікації: SMS, email, push-сповіщення, месенджери (Telegram, WhatsApp), голосові повідомлення та корпоративні платформи (MS Teams, Slack) [4]. Для реалізації системи обрано архітектуру клієнт-сервер з використанням Python (Django), бази даних PostgreSQL та API для інтеграції з сервісами Twilio (SMS/голосові сповіщення) і SendGrid (email) [5]. Запроваджено базу знань для динамічного керування правилами розсилки. Методи дослідження включають моделювання інформаційних потоків, тестування продуктивності та аналіз ефективності оповіщень у реальних сценаріях роботи авіакомпанії.

Результати. Ведеться розробка системи для автоматичного багатоканального оповіщення про критичні події в авіакомпанії. Передбачається, що повідомлення про затримку чи скасування рейсу надсилатимуться пасажиром і підрозділам (диспетчерам, реєстраторам, техперсоналу) протягом 5–10 секунд через SMS, email, push-нотифікації та месенджери, що має замінити ручне інформування, яке займало до 1–2 хвилин.

Система матиме багатоканальну структуру з персоналізацією повідомлень за ролями. Тестування підтвердило здатність обробляти понад 1000 повідомлень на годину без затримок. Реалізується механізм фільтрації оповіщень за типом подій (метео, технічні збої, зміни гейту) для уникнення інформаційного перевантаження [6].

Також створюється адміністративний інтерфейс для моніторингу розсилок, перегляду журналу подій і оцінки часу реакції. Очікується покращення координації підрозділів і зростання пунктуальності рейсів на 25–30% відповідно до галузевого досвіду.

Висновок

Розробляю систему автоматичного оповіщення підвищуючу ефективність роботи авіакомпанії шляхом мінімізації затримок у комунікації між підрозділами. Використання багатоканальних технологій дозволяє адаптувати систему до потреб конкретного перевізника.

Список використаних джерел:

1. Wise, J.A., Hopkin, V.D., & Smith, M.L. (Eds.). (1991). *Automation and Systems Issues in Air Traffic Control*. Springer-Verlag. URL: <https://link.springer.com/book/10.1007/978-3-642-76556-8> (Last accessed: 18.03.2025).
2. Hedskog, A. (2017). Digital crisis management in aviation: A more digital, flexible and mobile approach. *International Airport Review*. URL: <https://www.internationalairportreview.com/article/37049/airport-crisis-management-digital-flexible-mobile-approach/> (Last accessed: 18.03.2025).
3. Baselt, D., Schmitt, C., & Schaefer, G. (2022). Security issues in aviation satellite communication systems. *Security in Digital Aeronautical Communications: A Comprehensive Survey*, 23-45. URL: <https://www.sciencedirect.com/science/article/pii/S187454822200035X> (Last accessed: 18.03.2025).
4. Khan, M.A., & Rehman, A.U. (2021). Cyber security challenges in aviation communication, navigation, and surveillance systems. *Computers & Security*, 102516. URL: <https://www.sciencedirect.com/science/article/pii/S0167404821003400> (Last accessed: 18.03.2025).
5. Zhang, Y., Wan, X., & Zhang, Y. (2023). Applications of artificial intelligence in air operations: A systematic review. *Journal of Air Transport Management*, 105, 102356. URL: <https://www.sciencedirect.com/science/article/pii/S096969972400156X> (Last accessed: 18.03.2025).
6. Vaughn College of Aeronautics and Technology. (2024). The impact of AI on air traffic control. URL: <https://www.vaughn.edu/blog/ai-driven-technology-takes-air-traffic-control-to-the-next-level/> (Last accessed: 18.03.2025).

Звіт про класифікацію:				
	precision	recall	f1-score	support
0	0.70	0.99	0.82	60593
1	1.00	0.90	0.95	250436
accuracy			0.92	311029
macro avg	0.85	0.94	0.88	311029
weighted avg	0.94	0.92	0.92	311029
Точність моделі: 0.92				
До тесту: normal: 60593/311029, anomaly: 250436/311029				
Після тесту: normal: 85363/311029, anomaly: 225666/311029				

Рис. 2. Звіт про класифікацію моделі

Висновок

Виявлені вразливості дозволили оцінити ефективність існуючих протоколів захисту та запропонувати рекомендації щодо їх удосконалення. Оцінка ефективності розробленої моделі ШІ продемонструвала високу ефективність виявлення аномалій у мережевому трафіку, модель забезпечує ефективне розпізнавання атак різних типів.

Завдяки здатності до безперервного навчання та адаптації до нових умов, ШІ-системи можуть забезпечити виявлення атак нового типу у реальному часі і підвищити загальний рівень захисту інформаційних систем.

Список використаних джерел:

1. Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки 6.050101 «Комп'ютерні науки» / Уклад. : А.С. Савченко, О. О. Синельников. – К. : НАУ, 2017. – 190 с.
2. <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>

УДК 004.65

БЕЗСЕРВЕРНІ ТЕХНОЛОГІЇ ВЕБ-РОЗРОБКИ

Молодоженя Назар

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Микола Проценко, к.т.н., доц.

Ключові слова: безсерверні технології, безсерверні обчислення, безсерверні бази даних, веб-розробка, мікросервісна архітектура.

Вступ. Сучасна веб-розробка все частіше звертається до безсерверних обчислень (serverless computing) та безсерверних баз даних (serverless databases) через їхню здатність забезпечувати високу масштабованість, ефективність витрат та спрощення управління інфраструктурою. Актуальність цієї теми підкреслюється зростанням популярності хмарних обчислень та необхідністю швидкого адаптування до мінливих потреб користувачів [1,2]. Безсерверні технології дозволяють розробникам зосередитися на створенні функціональності

додатків, не турбуючись про підтримку серверів чи масштабування. Метою даного дослідження є порівняльний аналіз технологій безсерверних обчислень та баз даних у контексті веб-розробки.

Матеріали та методи

Безсерверні обчислення (serverless computing) — це модель хмарних обчислень, де платформа автоматично керує виділенням та масштабуванням ресурсів для виконання коду. Основна одиниця коду — функція, яка виконується у тимчасових контейнерах, що створюються та знищуються після завершення задачі. Користувачі не керують серверами, а платять лише за час виконання коду.

Безсерверні бази даних (serverless databases) — це бази даних, які розширюють модель безсерверних обчислень до рівня зберігання та обробки даних. Вони автоматично масштабуються, керують ресурсами та забезпечують високу доступність без необхідності адміністрування з боку користувача. Користувачі платять лише за фактичне використання ресурсів (наприклад, за обсяг даних або кількість операцій).

Для визначення переваг та недоліків безсерверних обчислень і баз даних у веб-розробці використано комплекс методів, які дозволяють оцінити їхню ефективність, масштабованість та економічну доцільність.

Аналіз продуктивності: вимірювання часу відгуку безсерверних функцій (AWS Lambda) у різних умовах та бази даних (Amazon Aurora Serverless) для операцій читання, запису та обробки запитів.

Економічний аналіз: розрахунок вартості використання безсерверних технологій у порівнянні з традиційними серверами. Враховувались такі фактори, як оплата за використання (pay-as-you-go), вартість пам'яті, обчислювальних ресурсів та мережових операцій.

Аналіз сценаріїв застосування безсерверних технологій у веб-розробці на основі вивчення реальних кейсів (наприклад, Netflix, Coca-Cola), аналізу документації хмарних провайдерів (AWS, Google Cloud, Azure) та огляду наукових статей та технічних звітів.

Результати. Використано метрики CloudWatch для автоматичного збору даних про час виконання Lambda-функцій та Apache JMeter – програма з відкритим вихідним кодом, призначена для завантаження веб-додатків та перевірки їхньої продуктивності.

Переваги: безсерверні технології є ефективними для додатків з мінливим навантаженням, забезпечують автоматичне масштабування, економію витрат та спрощення управління інфраструктурою.

Недоліки: затримки під час холодного старту, обмежений контроль над інфраструктурою та потенційно висока вартість при постійно високому навантаженні.

Висновок. Безсерверні технології відкривають нові можливості для веб-розробки, пропонуючи гнучкість, автоматичне масштабування та економію ресурсів.. Існує велика кількість сценаріїв успішної реалізації цих технологій, таких як API Backend, обробка подій, рендеринг на стороні сервера та інтеграція з третіми сервісами. Однак при виборі безсерверних технологій важливо орієнтуватися на конкретні цілі проекту, враховуючи його навантаження, бюджет та вимоги до продуктивності. Ці технології мають великий потенціал для впровадження в різних галузях, де ефективність та масштабованість є ключовими факторами.

Список використаних джерел:

1. **Amazon Web Services.** AWS Lambda Documentation : [електронний ресурс]. – 2023. – URL: <https://docs.aws.amazon.com/lambda/> (дата звернення: 22.03.2025).
2. **Google Cloud.** Google Cloud Functions Documentation : [електронний ресурс]. – 2023. – URL: <https://cloud.google.com/functions/docs> (дата звернення: 21.03.2025).
3. **Microsoft Azure.** Azure Functions Documentation : [електронний ресурс]. – 2023. – URL: <https://docs.microsoft.com/en-us/azure/azure-functions/> (дата звернення: 21.03.2025).

УДК 004.94.05-028.27(043.2)

ДОСВІД ВИКОРИСТАННЯ СИСТЕМИ МОДЕЛЮВАННЯ QUCS В НАВЧАЛЬНОМУ ПРОЦЕСІ

Максим Галушка

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олександр Андреев, к.т.н., доц.

Ключові слова: моделювання, система автоматичного проектування, програмне забезпечення

На сьогоднішній день моделювання на персональному комп'ютері за допомогою різноманітного програмного забезпечення (ПЗ) широко розповсюджено в навчальному процесі при вивченні багатьох дисциплін. Особливе місце серед ПЗ, яке використовується в навчальному процесі займають системи автоматичного проектування для електроніки (САПР, або EDA), до яких відносяться системи моделювання електронних схем та компонентів, таких як Multisim та MicroCAP, ліцензія на використання яких коштує досить дорого. Останнім часом актуальним є питання ліцензійної чистоти ПЗ, яке використовується в навчальному процесі. Доцільним було б використання ПЗ, включаючи і операційну систему (ОС), які розповсюджувались би по ліцензії GPL з відкритим вихідним кодом (open-source software), що дозволяє їх вільне та безоплатне використання. В якості такої ОС може виступати Linux. Однією з таких програм є QUCS [1], що призначена для моделювання електронних схем і компонентів, що розповсюджується по ліцензії GPL. Саме використання цієї моделюючої системи, або стимулятора, разом з ОС Linux Ubuntu [2] в навчальному процесі було реалізовано на кафедрі Комп'ютерних систем та мереж.

QUCS (від англ. Quite Universal Circuit Simulator, майже універсальний симулятор електронних ланцюгів), що розповсюджується по ліцензії GPL з відкритим вихідним кодом, та представляє собою симулятор електронних схем і компонентів, який має графічний інтерфейс, та здатен здійснювати всі види моделювання електричних кіл, таких як аналогове та цифрове моделювання, моделювання на постійному DC та змінному струмі AC, моделювання S-параметрів, перехідних процесів, шуму та гармонічного балансу. Цей стимулятор має версії для найбільш поширених на сьогоднішній день операційних систем: Windows, Linux, та MacOS. Для того, щоб в симуляторі QUCS стало доступним цифрове моделювання, треба встановити пакет FreeHDL [3].

Робота в QUCS має свої особливості: для електронної схеми треба вказати тип моделювання, яке буде відбуватись: DC analysis (на постійному струмі), AC analysis (на змінному струмі) та Digital simulation (цифрове моделювання). Якщо треба отримати графіки – наприклад, часові діаграми, або амплітудно-частотні, чи фазо-частотні характеристики, то треба вказати, що буде відбуватися моделювання перехідного процесу – Transient analysis, а потім побудувати відповідні графіки на екрані, які можуть бути як в 2D, так і в 3D вигляді, та полярних координатах.

Для того, щоб встановити пакети програмного забезпечення QUCS в ОС Linux Ubuntu, треба через термінал системи виконати наступну послідовність команд, яку треба виконати, як адміністратор:

```
sudo apt-add-repository ppa:qucs/qucs  
sudo apt-get update  
sudo apt-get install qucs
```

Для того, щоб встановити пакет FreeHDL через термінал, як було показано вище:

```
sudo apt-get update
```

```
sudo apt-get install freehdl
```

Лабораторні роботи на основі стимулятора QUCS були створені на кафедрі комп'ютерних систем та мереж для таких навчальних дисциплін, як «Комп'ютерна електроніка» та «Комп'ютерна мікроелектроніка». Серед цих лабораторних робіт є наступні:

- Дослідження діодів та стабілітронів.
- Дослідження біполярних транзисторів в статичному та динамічному режимі.
- Дослідження біполярних транзисторів в ключовому режимі.
- Дослідження автоколивальних та загальмованих мультівібраторів.
- Дослідження багатокаскадних транзисторних підсилювачів.
- Дослідження зворотних зв'язків в підсилювачах.
- Дослідження операційних підсилювачів.

Таким чином, практичний досвід доводить можливість та доцільність використання вільного ПЗ на базі ОС Linux та цю ОС в навчальному процесі, зокрема для моделювання електронних схем і компонентів за допомогою моделюючої системи QUCS при виконанні лабораторних робіт для таких навчальних дисциплін, як «Комп'ютерна електроніка» та «Комп'ютерна мікроелектроніка», зберігаючи при цьому ліцензійну чистоту та дозволяючи заощаджувати кошти, при цьому розширюючи кругозір студентів.

Список використаних джерел:

1. QUCS Quite Universal Circuit Simulator URL: <https://qucs.sourceforge.net/> (Last accessed: 19.09.2023).
2. Горбань Г.В. Операційна система Linux : навчаль-ний посібник / Г.В. Горбань, І.О. Кандиба. – Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2019. – 276 с.
3. FreeHDL Project URL: <http://www.freehdl.seul.org/> (Last accessed: 20.10.2021).

УДК 004.9

ПРОГРАМНИЙ МОДУЛЬ ДЛЯ ПІДТРИМКИ МЕНТАЛЬНОГО ЗДОРОВ'Я З ПЕРСОНАЛІЗОВАНИМИ РЕКОМЕНДАЦІЯМИ

Ангеліна Отеченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник - Світлана Кашкевич, ст. викладач

Ключові слова: ментальне здоров'я, персоналізовані рекомендації, машинне навчання, когнітивно-поведінкова терапія.

Вступ: В умовах війни ментальне здоров'я українців зазнає безпрецедентного тиску через постійну тривогу, стрес та емоційне виснаження. Багато людей уникають психологічної допомоги через страх осуду або стереотипи. Однак технології надають можливість отримати підтримку онлайн або через анонімний чат. Мобільні додатки, штучний інтелект і когнітивно-поведінкова терапія відкривають

доступ до психологічної допомоги без бар'єрів і страху. Завдяки технологіям психологічна підтримка більше не обмежується кабінетом терапевта.

Мета: Розробка програмного модуля, що аналізує стан користувача за допомогою тестів, забезпечує безперервний зв'язок із фахівцями та надає персоналізовані базові рекомендації для покращення ментального здоров'я.

Матеріали та методи: Дослідження зосереджене на інтеграції методів машинного навчання, аналізу даних та когнітивно-поведінкової терапії для оцінки психоемоційного стану користувачів та надання персоналізованої підтримки ментального здоров'я. Джерелами даних є відповіді користувачів на спеціалізовані опитування, а також сенсорні дані про режим сну та рівень фізичної активності. Основним завданням є збирання та обробка даних для створення репрезентативної вибірки, застосування алгоритмів класифікації для визначення психоемоційного стану користувача, а також розробка персоналізованих рекомендацій, що базуються на принципах когнітивно-поведінкової терапії. Програмний модуль буде реалізовано у вигляді веб-сторінки або додатку, що забезпечить зручний доступ користувачів до психологічної підтримки.

Результати: Розроблений програмний модуль забезпечує ідентифікацію емоційного стану користувача та генерацію рекомендацій, орієнтованих на його індивідуальні характеристики. Автоматизує визначення рівня стресу та тривожності шляхом аналізу зібраних даних після чого обирає та пропонує релаксаційні техніки і медитативні практики, що відповідають поточному стану користувача. Нагадує про необхідність проведення перерв для відновлення психоемоційного балансу та профілактики перевантаження. Моніторить динаміку змін психоемоційного стану з можливістю адаптації рекомендацій відповідно до отриманих даних, що дозволяє коригувати підхід до користувача в режимі реального часу. Наявна кнопка SOS, що дозволяє користувачу за необхідності миттєво звернутися за допомогою до фахівця або екстрених служб. Нотатник, в якому зберігаються важливі ментальні зміни та емоційні переживання користувача, що дозволяє відслідковувати зміни стану та коригувати рекомендації на основі цієї інформації.

Висновки: Впровадження розробленого програмного модуля дозволить покращити доступність психологічної підтримки для осіб, які переживають наслідки війни. Модуль сприятиме зниженню рівня стресу та тривожності через персоналізовані рекомендації та моніторинг емоційного стану. Подальші дослідження будуть спрямовані на підвищення точності аналізу та розширення функціоналу рекомендаційної системи для ефективнішої підтримки користувачів.

Список використаних джерел

1. Smith J., Brown K. "AI in Mental Health: Opportunities and Challenges." *Psychological Review*, 2022.
2. James R. "Cognitive Behavioral Therapy for Anxiety and Depression." *Journal of Psychology*, 2020.
3. Психологічне здоров'я в Україні під час війни та після: системний підхід до прогнозу непередбачуваних змін // *Health Ukraine*, 2024.

ЕФЕКТИВНІСТЬ ІТЕРАЦІЙНИХ МЕТОДІВ РОЗВ'ЯЗАННЯ СЛАР У ФОРМАТІ POSIT**Віталій Воронцов***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Вікторія Лукашенко, д.т.н., доц.*

Ключові слова: posit, FPGA, інструкції визначені користувачем, асемблер, СЛАР, процесор.

Вступ. Системи лінійних алгебраїчних рівнянь є базовим класом завдань багатьох наукових і технічних застосувань, включаючи аеродинамічні розрахунки та оптимізаційні проблеми, пов'язані з машинним навчанням. Сучасні дослідження цього класу задач ведуться ітераційними методами розв'язання систем лінійних алгебраїчних рівнянь з розрідженими матрицями, що надає можливість наблизитись до оптимальної складності обробки великих розріджених матриць. Прикладом важливих задач є розв'язання нестационарних задач обтікання в авіації та обчислення СЛАР при оптимізації другого порядку у машинному навчанні. У цьому дослідженні проведено аналіз ефективності ітераційних методів у контексті обчислень з обмеженою точністю, зокрема з використанням арифметики posit16.

Мета. Провести аналіз ітераційних методів розв'язання СЛАР та обґрунтувати вибір методу обчислення для застосування в нестационарних задачах обтікання в авіації та оптимізації другого порядку в машинному навчанні. Дослідження проводиться в межах дисертаційної роботи на здобуття наукового ступеня доктора філософії. Обраний метод буде реалізовано на апаратному рівні мовами опису апаратури у вигляді інструкцій процесора MIPS.

Матеріали та методи. Дослідження базується на аналізі ітераційних методів чисельного рішення окремих систем лінійних рівнянь, включаючи методи Якобі, Гаусса-Зейделя, Бі-Спряжених градієнтів та метод спряжених градієнтів. Для моделювання використано обчислення з 16-бітною арифметикою Posit, що реалізована за допомогою бібліотеки SoftPosit. Експерименти проводилися на тестових наборах матриць.

Результати. Метод спряжених градієнтів показав найкраще співвідношення точності та швидкодії серед розглянутих методів у форматі posit16. На відміну від методів Якобі та Гаусса-Зейделя, які мають низьку швидкість збіжності, метод спряжених градієнтів демонструє значне прискорення при розв'язанні розріджених симетричних додатньо визначених СЛАР. У порівнянні з методом Бі-Спряжених градієнтів, метод спряжених градієнтів має менші вимоги до обчислень і споживаної пам'яті, що є важливим для вбудованих систем та енергозбереження.

Метод спряжених градієнтів демонструє досягнення збіжності за меншу кількість ітерацій у порівнянні з методом Якобі. Використання posit16 призводить до збільшення похибки до 15% для метод спряжених градієнтів та до 40% для методу Якобі у порівнянні з аналогічними розрахунками на float32.

Величина похибки залежить від обраного формату числового представлення та особливостей тестової вибірки. Використання posit16 при програмній реалізації не доречно з точки зору швидкодії, оскільки відбувається перетворення формату числення у відомий для центрального процесора формат. Однак при апаратній реалізації posit16 реалізація може збільшити швидкодію та зменшити об'єм пам'яті для вирішення задачі.

Висновки. Метод спряжених градієнтів є оптимальним для розв'язання симетричних додатньо визначених СЛАР у форматі posit16 завдяки швидкій збіжності та стійкості до похибок. Його використання забезпечує відносно високу точність при обмеженій розрядності формату числення. Ефективне використання формату подання чисел posit16 досягається виключно за умови його повної апаратної реалізації, що обумовлено специфікою архітектури та необхідністю мінімізації обчислювальних накладних витрат, властивих програмовим емуляціям.

Список використаних джерел:

1. Posit Standard Documentation. URL: https://posithub.org/docs/posit_standard.pdf (Last accessed: 24.03.2025).
2. Golub, G. H., Van Loan, C. F. A comprehensive treatment of numerical linear algebra from the standpoint of both theory and practice. URL: <https://books.google.com.ua/books?id=X5YfsuCWpxMC> (Last accessed: 24.03.2025).

УДК 004.942

РОЛЬ СИМУЛЯЦІЇ ІОТ-ПРИСТРОЇВ У РОЗРОБЦІ ЕФЕКТИВНИХ СИСТЕМ УПРАВЛІННЯ МІСЬКИМ ПАРКУВАННЯМ

Артем Чинник

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Голего, старший викладач

Ключові слова: Інтернет речей (IoT), симуляція, розумне паркування, Cooja, Contiki OS, моделювання, управління паркінгом, міська інфраструктура, Smart City, сенсорна мережа, передача даних, паркомісця, тестування, мережеві втрати, цифровізація, проектування IoT-систем.

Із кожним роком кількість автомобілів у містах України зростає, що створює нові виклики для організації дорожнього руху та ефективного використання паркувального простору. Проблема нестачі паркомісць, нераціонального їх розміщення та відсутності оперативної інформації про завантаженість паркінгів є типовими для багатьох населених пунктів. Традиційні підходи, що базуються на ручному обліку або розміщенні табличок, не можуть задовольнити потреби сучасного динамічного міста [1]. У зв'язку з цим виникає необхідність у впровадженні розумних технологій, які дозволяють автоматизувати процес управління паркуванням і підвищити комфорт для водіїв. Одним із перспективних напрямів є застосування систем на основі Інтернету речей (IoT), які забезпечують онлайн-моніторинг і контроль за станом паркувального простору [2].

Повноцінне розгортання IoT-систем потребує значних фінансових ресурсів, часу та людських зусиль. Зазвичай, проблеми та помилки виявляються вже на стадії впровадження, що призводить до

додаткових витрат і затримок [3]. Складність полягає також у необхідності передбачення різноманітних сценаріїв поведінки системи в реальному середовищі. Тестування в польових умовах, особливо у великому місті, може бути технічно неможливим або надто дорогим. Через це симуляція — тобто віртуальне моделювання поведінки IoT-пристроїв і їхньої взаємодії — стає вкрай актуальною [6].

Ця робота спрямована на обґрунтування доцільності використання симуляцій IoT-пристроїв на етапі проєктування систем управління паркуванням, а також аналіз їхніх переваг порівняно з традиційними методами розробки та впровадження таких рішень [3].

Для моделювання роботи систем управління паркінгом на основі IoT можуть використовуватись такі симуляційні середовища, як Cooja, NS-3, OMNeT++ [4; 5]. Вони дозволяють змодельовати мережеву взаємодію сенсорів, передачу та втрату даних, різні топології розміщення пристроїв та навіть вплив зовнішніх чинників. У симуляціях можна перевірити, як система реагує на зміну трафіку, втрату зв'язку, збільшення кількості користувачів, перевірити алгоритми прийняття рішень контролером та протестувати поведінку серверної частини.

Для перевірки функціонування системи управління паркуванням була змодельована базова IoT-мережа з використанням симуляційного середовища Cooja, що входить до складу операційної системи Contiki OS [4]. Модель відтворює умовну ділянку міста з 10 паркувальними місцями, кожне з яких обладнане віртуальним сенсором наявності автомобіля. Сенсори періодично передають дані про статус паркомісця (вільне/зайняте) до центрального вузла (gateway), який, у свою чергу, надсилає агреговану інформацію на сервер управління.

У моделі реалізовано:

Топологію мережі типу «зірка», де всі сенсори безпосередньо з'єднані з головним вузлом.

Затримки передачі даних, типові для міського середовища (100–300 мс).

Втрату пакетів у 5–10% випадків для перевірки стійкості системи.

Зміни статусу паркомісць у випадковому порядку з інтервалом 20–60 секунд (імітація прибуття та від'їзду автомобілів).

Формат передачі даних у вигляді простих JSON-повідомлень, які можна легко адаптувати до реальної серверної інфраструктури.

Модель дозволила виявити потенційні проблеми синхронізації даних, перевірити швидкість оновлення інформації на сервері та визначити оптимальний інтервал між сеансами зв'язку сенсорів і центрального вузла, щоб зменшити навантаження на мережу [3].

Використання симуляції дає змогу виявити помилки в логіці ще до початку фізичної реалізації. Наприклад, в моделюванні можна з'ясувати, що пристрої неефективно розподіляють навантаження між собою, або що дані передаються із запізненням, що може спричинити некоректну роботу паркінгового контролера. Крім того, симуляція дозволяє дослідити оптимальне розміщення сенсорів, протестувати кілька варіантів конфігурації без витрат на фізичне обладнання [3]. У навчальному процесі симуляція є

чудовим інструментом для ознайомлення студентів із принципами роботи IoT-систем, а для інженерів — способом швидкої перевірки ідей без ризиків [2].

Висновок

Симуляція IoT-пристроїв — це не просто зручний інструмент, а необхідний етап сучасного проєктування «розумних» міських систем, зокрема систем управління паркінгом. Вона дозволяє зменшити витрати, уникнути помилок на ранніх етапах, підвищити надійність і масштабованість майбутнього рішення. У світлі розвитку концепції Smart City та цифровізації міської інфраструктури, симуляція є важливим кроком до впровадження ефективних, доступних та технологічно досконалих рішень у сфері міського управління [6].

Список використаних джерел:

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. <https://doi.org/10.1109/COMST.2015.2444095>
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions*. Future Generation Computer Systems, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
3. Shah, R., & Kumar, R. (2022). *Simulation Tools for IoT-Based Smart Parking Systems: A Review*. <https://www.researchgate.net/publication/361497319>
4. Cooja Simulator - Contiki OS Wiki. <https://github.com/contiki-os/contiki/wiki/Cooja-Simulator>
5. OMNeT++ Network Simulator. <https://omnetpp.org/>
6. Bandyopadhyay, D., & Sen, J. (2011). *Internet of Things: Applications and Challenges in Technology and Standardization*. Wireless Personal Communications, 58, 49–69. <https://doi.org/10.1007/s11277-011-0288-5>

УДК 004.75:378

ТЕЛЕГРАМ-БОТ ДЛЯ ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ ТА РОЗКЛАДУ ЗАНЯТЬ

Жаданов Даніель

ДУ «Київський авіаційний інститут», Київ

Науковий керівник – Наталія Пащенко, ст. викладач

Ключові слова: Телеграм-бот, Python, API Telegram.

Вступ. У сучасному світі автоматизація навчального процесу набуває все більшого значення. Використання інформаційних технологій у сфері освіти сприяє підвищенню ефективності навчання, спрощенню адміністративних процесів і покращенню комунікації між студентами та викладачами. З розвитком онлайн-освіти та дистанційного навчання зростає потреба в інструментах, які допомагають організовувати освітній процес. Один з ефективних способів оптимізації організації курсів з програмування – створення чат-бота, який дозволяє автоматично інформувати студентів про розклад занять, нагадувати про дедлайни, забезпечувати інтерактивну взаємодію з викладачем, а також надавати додаткові навчальні матеріали та тести для самоперевірки.

Телеграм-бот є спеціалізованим різновидом чат-бота, інтегрованим у платформу Telegram, що забезпечує автоматизоване виконання завдань, надання інформації та підтримку користувачів через

текстові команди та сценарії. Телеграм-боти мають низку переваг перед іншими засобами комунікації, такими як email-розсилки або веб-портали: вони швидко надсилають повідомлення, підтримують інтерактивні команди, легко інтегруються з іншими сервісами (Google Calendar, електронні таблиці, бази даних), а також доступні на різних пристроях. Завдяки цим перевагам Телеграм-боти стають ефективним інструментом для автоматизації освітніх процесів.

Матеріали та методи. Для аналізу ефективності чат-ботів у навчальному процесі було проведено емпіричне дослідження серед студентів вищих навчальних закладів. Використовувалися такі методи збору даних, як анкетування, спостереження та аналіз статистичних даних. Опитування охоплювало питання щодо зручності використання чат-ботів, рівня їхньої корисності та впливу на навчальну мотивацію. Результати опитування наведені на рис.1. Більше 50% опитаних респондентів зазначили, що використовують чат-боти для отримання новин, отримання автоматичних нагадувань про завдання чи події, а також для організації групових чатів та взаємодії з навчальними матеріалами. Крім того, боти використовують для автоматизації рутинних завдань, таких як перевірка розкладу чи отримання консультацій.

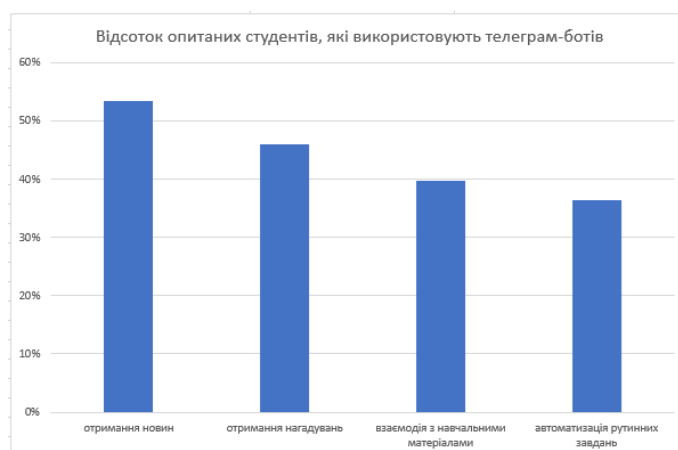


Рис. 1. Результати дослідження щодо використання студентами телеграм-ботів

Результати. Основні технології реалізації Телеграм-бота включають в себе мову програмування (Python), бібліотеку для роботи з Telegram API (aiogram), базу даних (SQLite, PostgreSQL). Бот працює як серверний додаток, який отримує запити від користувачів через Telegram, обробляє їх і повертає відповідь у вигляді повідомлень, кнопок або інтерактивних меню. Для безперервної роботи бота використовується хостинг на серверах, таких як Heroku або AWS Lambda. Docker-контейнери можуть використовуватися для спрощення розгортання та підтримки стабільної роботи. Для автоматичного додавання занять у календар, зберігання списку студентів і їхніх результатів тестування телеграм-боти мають підтримувати інтеграцію з іншими сервісами - Google Calendar API, Google Sheets API, ChatGPT API та ін.

Телеграм-боти також стикаються з певними загрозами з боку злоумисників. Для забезпечення безпеки бота та захисту даних важливо застосовувати комплексний підхід, який включає **оновлення**

програмного забезпечення, налаштування брандмауера, використання протоколу HTTPS, шифрування даних, контроль доступу.

Висновок. Використання Телеграм-бота для автоматизації навчального процесу є перспективним напрямком розвитку освітніх технологій. Розроблений бот дозволяє спростити адміністративні завдання, підвищити рівень організації студентів та забезпечити зручний доступ до розкладу занять і навчальних матеріалів. Подальший розвиток такого інструменту може включати додавання підтримки голосових команд, інтеграцію з іншими освітніми платформами та впровадження елементів штучного інтелекту для персоналізованого навчання.

Список використаних джерел:

1. Telegram API Documentation. URL: <https://core.telegram.org/bots/api>.
2. Telegram bots for Education: A Comprehensive Study (2021). DOI: 10.1007/s12345-2021-98765.

UDC 004.738.5.056.52(043.2)

**COMPUTER SYSTEM FOR CONTROLLING ACCESS OF
THE ENTERPRISE USERS TO THE INTERNET**

Hedz Viktoriia

State university «Kyiv Aviation Institute», Kyiv

Supervisor – Hataliia Fomina, Senior Lecturer.

Key words: system, access, security, Internet, enterprise.

As businesses become more reliant on digital tools, the need for strong and effective access control systems has grown a lot. These systems play a crucial role in protecting data, optimizing resource use, and ensuring compliance with regulations. Without proper control over internet access, businesses risk facing productivity loss, inflated costs, and serious security vulnerabilities. These risks can have severe consequences for any enterprise. The focus of this research is to study a computer-based system to manage and control user access, specifically addressing the challenges faced by modern organizations. Recent research emphasizes the importance of adaptive, secure, and scalable access control solutions tailored to each business's unique needs. [1, 2].

Building an effective access control system starts with a thorough analysis of the organization's structure. By identifying the various user roles and their respective responsibilities, we can lay the groundwork for a role-based access control framework. This framework helps categorize users and assign the appropriate permissions. [2]. To further strengthen security and efficiency, predefined access rules and policies are incorporated, ensuring that permissions align with job responsibilities and minimizing the risk of unauthorized access. Additionally, monitoring tools are put in place to track internet usage and detect any breaches of the established protocols. This system ensures consistent security over time by maintaining a secure, well-structured framework.

Encryption protocols are also integrated to protect the integrity of data as it's transmitted, further bolstering the system's security.

Such an access control system offers significant benefits to enterprises. By reducing the chances of unauthorized access, it helps protect sensitive data from potential threats and leakage of confidential company information. Limiting internet use to tasks specific to each role also prevents misuse of bandwidth, improving overall productivity. The system's monitoring features ensure that it can adapt to changes within the organization, maintaining its effectiveness as the business evolves. Furthermore, the system helps save costs by improving resource management and minimizing IT-related risks, ultimately lowering operational expenses. Its scalability ensures it can grow alongside the organization, accommodating changes in workforce size and business complexity.

Conclusions. This research underscores the importance of implementing computer-based access control systems to ensure both security and efficiency within modern enterprises. The proposed system's aim is a valuable tool in tackling the challenges of managing internet resources, providing a customizable and scalable solution that aligns with the specific needs of each organization. By offering a robust framework for monitoring and controlling user access, it not only enhances security but also supports the efficient allocation of resources across the enterprise. Furthermore, this approach addresses the evolving demands of modern businesses, where digital environments are increasingly complex and dynamic. As organizations continue to grow and adapt, the ability of access control systems to scale and evolve with them becomes critical. The integration of real-time monitoring and automated security measures ensures that the system remains effective even as the enterprise expands or shifts focus.

References

1. Kuinam J.Kim, "On Automated Role-Based Access Control Assessment in Enterprise Systems",
2. URL: <https://link.springer.com/book/10.1007/978-981-15-1465-4> (Last accessed: 23.03.2025).
3. Huawei Agile Controller-Campus,
4. URL: <https://www.scribd.com/document/378803816/> (Last accessed: 23.03.2025)

УДК 04.07+04.08+04.25+04.33

ДОСЛІДЖЕННЯ ВПЛИВУ ОСОБЛИВОСТЕЙ ТОПОЛОГІЙ МАТЕРИНСЬКИХ ПЛАТ НА ФУНКЦІОНУВАННЯ ОПЕРАТИВНО-ЗАПАМ'ЯТОВУЮЧИХ ПРИСТРОЇВ

Тихон Целованський

Державний університет інформаційно комунікаційних технологій, м. Київ

Науковий керівник — Олена Шидула, д.ф.-м.н., проф.

Ключові слова: топологія материнських плат, затримки сигналів в комп'ютерній техніці, DDR, Daisy Chain, T-Topology

Вступ. Сучасні комп'ютерні системи, зокрема серверні платформи, обчислювальні кластери та ігрові ПК, потребують максимізації продуктивності оперативної пам'яті (ОЗП). Важливим фактором, що

впливає на її ефективність, є топологія розподілу сигнальних ліній на материнській платі [1, 3]. Дослідження останніх років [2, 4] доводять, що конфігурація електричних зв'язків між слотами ОЗП та контролером пам'яті суттєво впливає на затримки, пропускну здатність і стабільність. Зазначається, що неоптимальна топологія збільшує затримки на 15–25%, що є критичним для систем обробки даних у реальному часі. Актуальність дослідження полягає у визначенні оптимальних топологій для мінімізації компромісів між швидкістю та надійністю на базі сучасних апаратних компонентів.

Мета. Дослідити вплив типів топологій материнських плат (Daisy Chain, T-Topology, гібридної) на показники швидкодії та стабільності оперативної пам'яті DDR4 у системі з процесором Intel Core i9-10900, а також сформулювати рекомендації щодо їх застосування.

Матеріали та методи. Дослідження проводилось на материнських платах, що є представниками різних топологій: ASUS ROG Maximus XII Hero (Daisy Chain), послідовне підключення модулів ОЗП (в теорії характерно кращою стабільністю роботи з 2 модулями пам'яті), MSI MEG Z490 GODLIKE (T-Topology), симетричний розподіл трас у формі літери Т (в теорії характерна краща стабільність роботи як з 2 так й з 4 модулями, але вищі затримки). GIGABYTE Z490 AORUS Xtreme (гібридна), комбінація Daisy Chain для адресних ліній та T-Topology для шини даних. Материнські плати працювали з однаковим набором обладнання, Intel Core i9-10900, та ОЗП G.Skill Trident Z DDR4-3600 (4 модулі по 16 ГБ). AIDA64 Extreme — вимірювання латентності (затримок) та пропускну здатності (методика Cache & Memory Benchmark). MemTest86 Pro — тестування стабільності протягом 24 годин. Розрахунок відхилень та похибок проходив з використанням Python з бібліотеками Pandas (агрегація даних) та SciPy (t-тест для оцінки значущості результатів). Кожен тест повторювався 10 разів. Похибка вимірювань не перевищувала 2%.

Результати. Під час тестування були визначені затримки та особливості кожної з топологій. Топологія Daisy Chain має затримки на рівні 48–52 нс (найнижчі серед досліджуваних). Відхилення швидкості обміну даними $\pm 6\%$ при навантаженні $>85\%$. Останній модуль у ланцюгу (четвертий) має на 18% вищу латентність через імпедансні спотворення. Топологія T-Topology має затримки 62–65 нс (збільшені через довжину трас ≈ 20 см). Відхилення швидкості обміну даними складають $\pm 2.5\%$ навіть при 95% навантаженні. До переваг можна віднести рівномірний розподіл сигналу між усіма слотами. Гібридна топологія має затримки: 55–58 нс. Відхилення швидкості обміну даними $\pm 2\%$. В гібридних платах характерно використання Daisy Chain для адресних ліній (мінімізація затримок) та T-Topology для шини даних (підвищення стабільності).

Висновки. Daisy Chain забезпечує найкращу швидкодію для систем з 1–2 модулями ОЗП, але її не рекомендовано для серверних рішень через знижену стабільність показників при модифікації таймінгів, та залежності від рівня навантаження. T-Topology є оптимальною для високонавантажених систем (рендеринг, розрахунки, віртуалізація), де стабільність показників більш важлива ніж рівень затримок. Гібридна топологія демонструє збалансовані результати і підходить для ігрових ПК та робочих

станцій, де потрібний усереднений результат в будь-яких задачах. Використання DDR4-3600 з процесором Intel i9-10900 підтвердило залежність продуктивності від топології, та важливість правильного підбору материнської плати, згідно до задач [2, 4].

Список використаних джерел:

1. Smith, J. High-Speed PCB Design. IEEE Transactions on Electromagnetic Compatibility, 2020.
2. Lee, H. Memory Architecture in Modern Motherboards. Elsevier, 2022. DOI: 10.1016/j.memarc.2022.100345.
3. ASUS. DDR4 Routing Guidelines for Daisy Chain Topology. Technical White Paper, 2021.
4. Intel. 10th Gen Intel® Core™ i9 Processors: Memory Optimization. 2023. URL: <https://www.intel.com> (дата звернення: 15.03.2025).
5. MemTest86. Official Documentation. 2023. URL: <https://www.memtest86.com> (дата звернення: 9.02.2025).

УДК 004.38:629.7.014-519(043.2)

СПОСІБ ІНІЦІАЛІЗАЦІЇ ПАРАМЕТРІВ НЕЙРОКОМП'ЮТЕРА ДЛЯ ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ

Сіренко Максим

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Печурін Микола, д.т.н., професор.

Ключові слова: нейрокомп'ютер, безпілотні літальні апарати, нейронні мережі, електромагнітне випромінювання.

В умовах активного розвитку комплексів безпілотних літальних апаратів (БПЛА), які функціонують у складі взаємодіючих груп (роїв), виникає потреба у вирішенні завдання оптимізації енергоспоживання. Особливо гостро ця задача постає для надлегкого класу БПЛА, де накладаються суттєві обмеження на нормовані енерговитрати. Одним з перспективних підходів вирішення окресленої проблеми є впровадження нейрокомп'ютерних систем для адаптивного керування потужністю приймально-передавального обладнання, що дозволяє мінімізувати енерговитрати зі збереженням достатнього ступеня інтегрованості між елементами комплексу.

Метою роботи є розробка методу початкового налаштування параметрів нейрокомп'ютера для адаптивного керування потужністю передавачів у складі рою БПЛА, за критерієм мінімізації енергоспоживання.

Для вирішення поставленого завдання було запроваджено припущення щодо характеру згасання сигналу в середовищі зв'язку, а також взаємозалежність енерговитрат з потужністю приймально-передавального обладнання складових нейрокомп'ютерної системи.

Первинними даними для визначення початкових параметрів моделі є інформація про актуальне просторове розміщення кожного з m елементів нейромережі, що розподілені на взаємодіючих БПЛА у тривимірному середовищі.

Суть запропонованого методу полягає у знаходженні для кожного вузла рою БПЛА мінімально необхідного значення потужності приймально-передавального обладнання P за умови забезпечення належного рівня інтегрованості комплексу. Математична модель, що описує поставлену задачу, має наступний вигляд:

$$P_i = \left(\frac{L_{ij}}{k}\right)^3, i = \overline{(1, m)}, j = \overline{(1, m)},$$

де L_{ij} – відстань між взаємодіючими вузлами;

k – коефіцієнт, що описує характеристики комунікаційного простору (ступінь згасання сигналу).

Аналіз розробленої моделі був здійснений з використанням інструментарію мови програмування *Python*. Результати проведеного моделювання дозволили отримати чисельні значення початкових параметрів налаштування нейрокомп'ютера залежно від розташування вузлів рою БПЛА, частина отриманих результатів наведена у таблиці 1.

Таблиця 1

Розрахунок початкових значень параметрів нейрокомп'ютера

№ вузла, i	L_{ij}	k	P_i
1	72.45	128	0.1813
2	65.26	128	0.1325
3	51.94	128	0.0668
4	103.76	128	0.5327
5	121.53	128	0.8558
...	...	...	...

Висновок

Запропонований спосіб початкового налаштування нейрокомп'ютерної системи дозволяє визначити оптимальні рівні потужності приймально-передавального обладнання кожного вузла в рої БПЛА з метою мінімізації сумарного енергоспоживання комплексу. Застосування цього методу забезпечує необхідну інтеграцію вузлів у рої та дозволяє ефективніше використовувати енергетичні ресурси, що особливо важливо для надлегкого класу БПЛА.

Список використаних джерел

1. Pal, O. K., Shovon, M. S. H., Mridha, M. F., & Shin, J. (2024). In-depth review of AI-enabled unmanned aerial vehicles: trends, vision, and challenges. *Discover Artificial Intelligence*, 4(1). <https://doi.org/10.1007/s44163-024-00209-1>.
2. Czachórski, T., Gelenbe, E., Kuaban, G. S., & Marek, D. (2022b). Optimizing energy usage for an electric drone. *Communications in computer and information science* (pp. 61–75). https://doi.org/10.1007/978-3-031-09357-9_6.
3. Jin, H., Jin, X., Zhou, Y., Guo, P., Ren, J., Yao, J., & Zhang, S. (2023b). A survey of energy efficient methods for UAV communication. *Vehicular Communications*, 41, 100594. <https://doi.org/10.1016/j.vehcom.2023.100594>.

УДК 004.7

ДОСЛІДЖЕННЯ І ОПТИМІЗАЦІЯ ХМАРНИХ ТА BACKEND-ТЕХНОЛОГІЙ У КОНТЕКСТІ РОЗРОБКИ СИСТЕМ УПРАВЛІННЯ ЗАМОВЛЕННЯМИ МАЛОГО БІЗНЕСУ

Ульянич Олександр

Державний університет "Київський авіаційний інститут", Київ

Науковий керівник – Наталія Пащенко, ст.викладач

Ключові слова: хмарні технології, AWS, бази даних, e-commerce, serverless-архітектура.

Вступ. Сучасні системи управління замовленнями відіграють ключову роль у цифровій трансформації малих підприємств, сприяють оптимізації бізнес-процесів, зменшенню операційних витрат та забезпечують високий рівень задоволеності клієнтів.

У даній роботі представлено аналіз сучасних хмарних платформ та фреймворків для backend-розробки, які можуть бути корисними для малого бізнесу. Основна увага приділяється не лише технічним характеристикам, а й економічній доцільності їх використання.

Матеріали та методи. Дослідження зосереджено на аналізі хмарних сервісів та backend-фреймворків, які застосовуються для створення систем управління замовленнями, їх впливу на такі параметри систем, як швидкодія, здатність до масштабування, стійкість до високих навантажень та рівень захищеності. Для наукового обґрунтування результатів дослідження використані методи збирання, обробки та аналізу даних

Результати. Було проведено порівняння функціональних можливостей провідних хмарних платформ, таких як Amazon Web Services, Google Cloud Platform та Microsoft Azure, у поєднанні з популярними фреймворками, серед яких Node.js, Django та Spring Boot.

У результаті дослідження було виявлено кілька важливих аспектів, які слід враховувати при виборі технологій для систем управління замовленнями:

- Вплив хмарних сервісів на продуктивність: AWS Lambda та Google Cloud Functions забезпечують високу гнучкість завдяки serverless-архітектурі, що дозволяє значно знизити витрати на інфраструктуру. Microsoft Azure, у свою чергу, виділяється простотою інтеграції з корпоративними системами. Дослідження також показало, що AWS має перевагу у швидкості обробки запитів порівняно з іншими платформами, що робить її привабливим вибором для систем, де важлива мінімальна затримка.

- Ефективність backend-фреймворків: Node.js показав себе як найкращий інструмент для обробки асинхронних запитів під високим навантаженням, що є ключовим для e-commerce платформ. Django та Spring Boot, з іншого боку, пропонують потужні інструменти для забезпечення безпеки та підтримки складних бізнес-процесів, що робить їх ідеальними для транзакційних систем. Також було досліджено інтеграцію з базами даних, де PostgreSQL виявився оптимальним рішенням завдяки поєднанню швидкості, гнучкості та надійності.

- Безпека та інтеграція: Використання OAuth 2.0 для аутентифікації та TLS-шифрування для захисту даних значно підвищує стійкість системи до зовнішніх загроз. Інтеграція з платіжними шлюзами та CRM-системами є важливим елементом для забезпечення конкурентоспроможності. Також було проаналізовано методи захисту backend-інфраструктури, такі як впровадження Web Application Firewall (WAF) та використання багаторівневої авторизації (MFA), що дозволяє ефективно протистояти атакам.

- Економічна доцільність: Аналіз витрат на використання хмарних технологій порівняно з локальними рішеннями показав, що довгострокові витрати на підтримку власних серверів значно вищі. Хмарні рішення, завдяки можливості гнучкого масштабування, пропонують малому бізнесу значні переваги, зокрема зниження операційних витрат та підвищення ефективності.

На основі проведеного аналізу сформовані рекомендації використання AWS у поєднанні з Node.js та PostgreSQL для досягнення оптимального балансу між продуктивністю, безпекою та економічною ефективністю. Для бізнесів із складними процесами обробки замовлень варто розглянути Django або Spring Boot разом із Google Cloud Platform, що забезпечить додатковий рівень захисту та гнучкості.

Висновок. Дослідження підтвердило, що використання хмарних технологій разом із правильно підібраними backend-інструментами значно покращує ефективність систем управління замовленнями, особливо для малого бізнесу. Вибір технологій варто базувати на таких факторах, як розмір бізнесу, вимоги до захисту даних та необхідність інтеграції з іншими платформами. У майбутньому доцільно провести тестування обраної архітектури в реальних умовах бізнесу, щоб виявити можливі недоліки та вдосконалити систему. Також варто дослідити можливість застосування машинного навчання для прогнозування попиту та покращення логістичних процесів у рамках систем управління замовленнями.

Список використаних джерел:

1. Google Cloud. (2023). Cloud Functions vs. Kubernetes: A comparative study. URL: <https://cloud.google.com/blog/products/serverless>
2. Armbrust, M., Fox, A., Griffith, R., et al. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.

UDC 629.39

INTEGRATION OF COMPUTER NAVIGATION SYSTEMS WITH AUTONOMOUS VEHICLE SYSTEMS

Nazarii Semeniak

State university "Kyiv aviation institute", Kyiv

Scientific advisor – Nataliia Fomina, senior lecturer

Keywords: autonomous vehicles, navigation systems, GPS, SLAM, system integration.

Introduction. Autonomous vehicle systems require precise and reliable navigation solutions to ensure safe and efficient operation. Integrating computer navigation technologies such as GPS, IMU, and SLAM [1, 2] is essential for achieving robust navigation. The growing implementation of autonomous transportation in logistics, urban mobility, and defence highlights the importance of integrated navigation approaches [1, 2].

Purpose. This research explores how GPS, IMU, and SLAM integration enhances navigation accuracy, positioning reliability, and operational efficiency in complex environments. A novel approach to adaptive sensor weighting is introduced, dynamically adjusting navigation component reliability based on environmental conditions. Additionally, deep learning-based anomaly detection is incorporated to improve navigation stability and data processing efficiency.

Materials and Methods. The study examines the integration of GPS, IMU, and SLAM within autonomous vehicle systems. GPS provides absolute positioning using satellite signals but is often unreliable in obstructed environments such as tunnels or urban canyons. To mitigate this, IMUs measure acceleration and angular velocity, allowing vehicles to maintain accurate positioning even when GPS signals are weak or lost.

SLAM enhances localization by simultaneously mapping the surroundings and determining the vehicle's position within it. Using data from LiDAR, cameras, and radar, SLAM generates real-time environmental models, making it particularly valuable in GPS-denied environments.

Machine learning techniques [2, 3] refine navigation accuracy through neural networks and advanced filtering algorithms, such as Kalman and particle filters, which process sensor data to predict motion and compensate for errors. This research introduces an adaptive sensor weighting method where machine learning dynamically prioritizes GPS, IMU, and SLAM data based on real-time environmental conditions, improving overall accuracy and system responsiveness.

Simulations conducted in MATLAB and Python assessed the effectiveness of different integration methods under real-world conditions, including GPS signal loss and sensor fusion challenges. Key performance metrics, such as positioning accuracy, system latency, and computational efficiency, were analysed [3], demonstrating the benefits of deep learning-based anomaly detection in improving system robustness and reliability.

Results. The integration of GPS, IMU, and SLAM [1, 2] significantly improves navigation accuracy, even in complex environments such as urban canyons and tunnels. Machine learning algorithms contribute to minimizing data processing errors and increasing system robustness against external disturbances. The introduction of an adaptive sensor weighting methodology improves the system's ability to dynamically adjust to changing conditions, leading to more reliable autonomous navigation. Additionally, the integration of deep learning-based anomaly detection enables the system to identify and correct sensor errors in real time, further enhancing navigation stability and accuracy.

Conclusions. The integration of computer navigation systems with autonomous vehicle technologies enhances accuracy and reliability. The proposed adaptive sensor weighting and deep learning-based anomaly detection provide significant improvements in real-time navigation, making autonomous systems more robust and efficient. These findings contribute to the advancement of next-generation autonomous vehicle navigation technologies.

References

1. Li, Z., Wang, H., & Chen, Y. (2021). Advances in SLAM for autonomous driving: Current trends and future perspectives. *IEEE Transactions on Intelligent Transportation Systems*, 22(5), 2456-2472.
2. Zhang, T., Li, J., & Xu, Y. (2022). Machine learning approaches for enhancing GNSS-IMU integration in autonomous vehicles. *Journal of Navigation*, 75(3), 678-695.
3. Smith, R., & Lee, K. (2023). Real-time sensor fusion for autonomous vehicle navigation. *Autonomous Systems Journal*, 14(2), 112-128.

УДК 519.644.2

ОБЧИСЛЕННЯ ВИЗНАЧЕНИХ ІНТЕГРАЛІВ ФУНКЦІЙ З ПРИХОВАНИМИ СИМЕТРИЧНИМИ ВЛАСТИВОСТЯМИ

Дар'я Михайлова

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Віктор Репета, к.ф.-м.н., доц.*

Ключові слова: визначений інтеграл, непарна функція, симетричні властивості

Вступ. Однією із основних задач інтегрального числення функцій однієї змінної є задача обчислення визначених інтегралів. Skorистatisia formuloiu Nyutona-Leybnitsa mozhna lishe dlia neznačnoi kіlʹkosti інтегровних функцій. Rozglianemo geometrichnii metod obchislennia viznacheniakh інтегралів від функцій спеціального вигляду, які володіють певними симетричними властивостями.

Результати.

1. Розглянемо спочатку задачу обчислення визначеного інтеграла вигляду

$$\int_{-a}^a \frac{dx}{1+b^{f(x)}}, \quad (1)$$

де неперервна на відрізку $[-a; a]$ функція $f(x)$ є непарною: $f(-x) = -f(x)$; $0 < b \neq 1$ – стала.

Скористаємося ідеєю, реалізованою в [1]. Позначимо $h(x) = \frac{1}{1+b^{f(x)}}$ й виконаємо перетворення

$$\frac{h(x)+h(-x)}{2} = \frac{1}{2} \left(\frac{1}{1+b^{f(x)}} + \frac{1}{1+b^{-f(x)}} \right) = \frac{1}{2} \left(\frac{1}{1+b^{f(x)}} + \frac{b^{f(x)}}{b^{f(x)}+1} \right) = \frac{1}{2} = h(0).$$

Отже, точка $(0; 0,5)$ є серединою відрізка, що сполучає точки $(-x; h(-x))$ та $(x; h(x))$.

Доходимо висновку, що функція $h(x) - 0,5$ є непарною, відповідно отримуємо

$$\int_{-a}^a h(x) dx = \int_{-a}^a (h(x) - 0,5) dx + \int_{-a}^a 0,5 dx = 0 + a = a.$$

Геометрично $\int_{-a}^a h(x) dx$ чисельно дорівнює площі прямокутника $AKPD$ (див. рис.1).

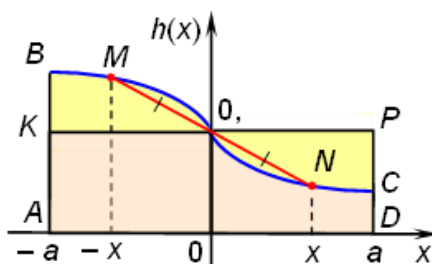


Рис.1. Геометричний сенс інтеграла (1)

Приклад.

$$\int_0^{2\pi} \frac{dt}{1+e^{\sin t}} = \left| \begin{matrix} t = \pi - x \\ dt = -dx \end{matrix} \right| = - \int_{\pi}^{-\pi} \frac{dx}{1+e^{\sin(\pi-x)}} = \int_{-\pi}^{\pi} \frac{dx}{1+e^{\sin x}}.$$

Позначимо $h(x) = \frac{1}{1+e^{\sin x}}$. Маємо $h(0) = \frac{1}{1+e^0} = \frac{1}{2}$,

$$h(x) - h(0) = \frac{1}{1+e^{\sin x}} - \frac{1}{2} = \frac{2-1-e^{\sin x}}{2(1+e^{\sin x})} = \frac{1}{2} \cdot \frac{1-e^{\sin x}}{1+e^{\sin x}} -$$

непарна функція. Тоді

$$\int_{-\pi}^{\pi} \frac{dx}{1+e^{\sin x}} = \frac{1}{2} \int_{-\pi}^{\pi} \frac{1-e^{\sin x}}{1+e^{\sin x}} dx + \int_{-\pi}^{\pi} \frac{1}{2} dx = 0 + \frac{1}{2}(\pi - (-\pi)) = \pi.$$

Наведені результати природно узагальнити.

2. Якщо функція $f(x)$ на відрізку $[-a; a]$ є непарною: $f(-x) = -f(x)$, а $g(x)$ – парною й додатною: $g(-x) = g(x)$; $g(x) > 0$, тоді

$$\int_{-a}^a \frac{dx}{1+g(x)^{f(x)}} = a.$$

Приклад. $\int_{-1}^1 \frac{dx}{1+(1+x^2)^{x \cos x}} = 1.$

3. Якщо функція $f(x) - \lambda$ на відрізку $[-a; a]$ є непарною, то

$$\int_{-a}^a f(x) dx = 2\lambda a.$$

Приклад. $\int_{-1}^1 \arctg e^x dx = \int_{-1}^1 \left(\arctg e^x - \frac{\pi}{4} \right) dx + \int_{-1}^1 \frac{\pi}{4} dx = \int_{-1}^1 \underbrace{\arctg \frac{e^x - 1}{e^x + 1}}_{\text{непарна}} dx + \int_{-1}^1 \frac{\pi}{4} dx = \frac{\pi}{2}.$

Висновок

Запропонований геометричний метод дозволяє обчислювати визначені інтеграли функцій, що володіють певними симетричними властивостями, особливо у випадках, коли неможливо визначити первісну підінтегральної функції й безпосередньо застосувати формулу Ньютона-Лейбніца.

Список використаних джерел:

1. Nelsen R.B. Symmetry and integration. In: *Cameos for Calculus: Visualization in the First-Year Course*. Classroom Resource Materials. Mathematical Association of America; 2015:57-60.

УДК 51-77

МАТЕМАТИЧНІ ПІДХОДИ ДО АНАЛІЗУ ЕФЕКТИВНОСТІ ПРОМО-АКЦІЙ

Вікторія Сосна

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ірина Шевченко, к.е.н., доцент

Ключові слова: промо-акція, маркетинг, ефективність, диференціальне числення функцій, оптимізація промо-акцій.

Промо-акції є невід'ємною складовою маркетингових стратегій сучасних компаній. Вони спрямовані на стимулювання попиту, підвищення обсягів продажу та залучення нових клієнтів. Для досягнення бажаних результатів необхідно ретельно аналізувати ефективність проведених заходів, використовуючи як якісні, так і кількісні методи оцінки.

Актуальність дослідження питання оцінки ефективності промо-акцій зумовлена необхідністю оптимізації маркетингових витрат, підвищення конкурентоспроможності компаній та адаптації до змін у поведінці споживачів.

Етапами аналізу ефективності промо-акцій є:

1. Постановка цілей. Аналіз ефективності починається ще до проведення акції. Насамперед необхідно встановити цілі, яких ми плануємо досягти, проводячи промо-акцію. У подальшому аналіз таких цілей дозволить оцінити рівень успішності проведеної акції, її результативність.
2. Використання ключових розрахункових показників. Для оцінки ефективності промо-акцій використовуються наступні ключові показники (табл. 1):

Таблиця 1

Показник	Формула	Взаємозв'язок з іншими показниками
Приріст обсягу продажів (ΔS)	$\Delta S = S_{\text{після}} - S_{\text{до}}$, $S_{\text{після}}$ - обсяг продажів після акції, $S_{\text{до}}$ - обсяг продажів до акції	Впливає на ΔVP та ROI , оскільки збільшення продажів збільшує прибуток та рентабельність інвестицій
Рентабельність інвестицій (ROI)	$ROI = \frac{\Delta VP}{\text{Витрати на акцію}} \cdot 100\%$	Залежить від ΔVP та витрат на акцію, визначає фінансову ефективність кампанії
Коефіцієнт залучення клієнтів (CAC)	$CAC = \frac{\text{Витрати на акцію}}{\text{Кількість нових клієнтів}}$	Чим вищий ΔS і ΔVP , тим менший CAC , якщо зростає кількість нових клієнтів.
Зміна валового прибутку (ΔVP)	$\Delta VP = \Delta S \cdot (\text{Середня маржа}) - \text{Витрати на акцію}$	Визначає загальну прибутковість акції

3. Використання диференціального числення функцій, зокрема похідної, для оптимізації промо-акцій. Похідна функції дозволяє знайти оптимальні значення параметрів для максимізації прибутку або мінімізації витрат.

Наприклад, розглянемо функціональну залежність обсягів продажу від витрат на рекламу – $S(x)$. Тоді функція валового прибутку має вигляд:

$$VP(x) = (S(x) \cdot (\text{ціна-собівартість})) - x.$$

За похідною функції $VP(x)$ отримуємо маржинальний валовий прибуток. При відомих значеннях ціни та собівартості товару розв'яжемо рівняння $(VP(x))' = 0$ і отримаємо оптимальні мінімальні витрати на рекламу.

Висновок

Аналіз ефективності промо-акцій є критично важливим для оптимізації маркетингових витрат та підвищення прибутковості компанії. Використання ключових показників – ΔS , ROI , CAC та ΔVP дозволяє кількісно оцінити результативність проведених заходів. Крім того, застосування математичних методів, зокрема **диференціального числення функцій**, дає можливість оптимізувати параметри промо-акцій для досягнення максимальної ефективності при мінімізації витрат. Регулярний та комплексний аналіз промо-акцій допомагає компаніям приймати обґрунтовані рішення та підвищувати свою конкурентоспроможність.

Список використаних джерел:

- 1.Книшов Д. С. Економіко-математичне моделювання оцінки ефективності рекламних заходів на підприємстві: магістерська робота. Харків : Харківський національний університет радіоелектроніки, 2021. 98 с.
- 2.Забаштанський М., Забаштанська Т., Герасімчук М. Застосування промоакційного маркетингу підприємствами в умовах цифровізації .*Науковий вісник Полісся*. 2023. № 2(25). С. 222-239.
- 3.Герасімчук В. Маркетингові дослідження. Львів: Світ, 2022. 340 с.
- 4.PlanoHero. Промоакції та знижки: Як збільшити продажі в магазині
URL: <https://planohero.com/uk/blog/retail-discounting/> (дата звернення: 17.03.2025)

UDC 519.2(075.8)

ANALYZING WEBSITE TRAFFIC PATTERNS USING THE POISSON DISTRIBUTION

Mychailo Lokatsiun

State University “Kyiv Aviation Institute”, Kyiv

Scientific Adviser – Kaveh Eftekharinasab, Ph.D., Assoc.Prof.

Keywords: Poisson distribution, website traffic analysis, anomaly detection, probability modeling, Python simulation

Website traffic analysis is critical for optimizing user experience and server performance. This project models visitor arrivals over a 24-hour period using the Poisson distribution [1] by simulating minute-by-minute traffic, estimating probabilities, and detecting anomalies, this study provides actionable insights into traffic patterns.

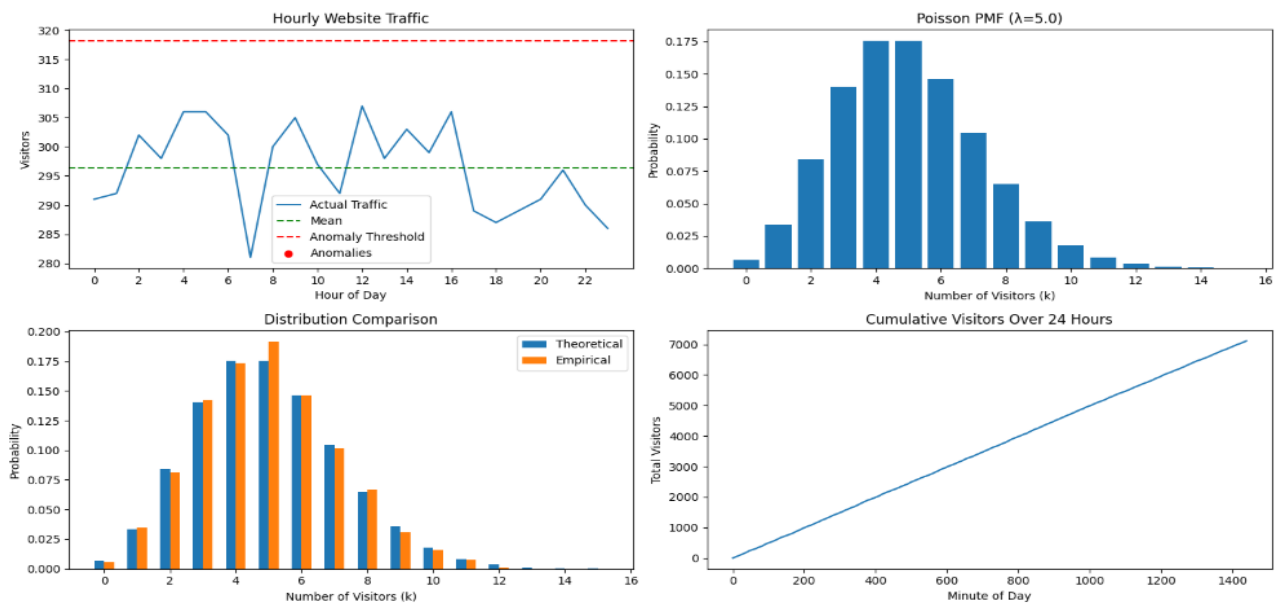
Python Implementation: Results and Visualization

We implemented the project using Python [2]. Below is the output of the results when the number of visitors per minuet is $\lambda=5$.

Total visitors in 24 hours: 7113; Average visitors per hour: 296.38

Standard deviation (hourly): 7.29; Anomaly threshold: 318.25 visitors/hour

Number of anomalous hours: 0; $P(X=5) = 0.1755$



The description of each of the graphs is given respectively as follows:

1. **Hourly Website Traffic with Anomalies**
 - Shows the number of visitors per hour.
 - Green dashed line: average visitors per hour.
 - Red dashed line: anomaly threshold (mean + 3σ).
 - Red points: anomalous hours with unusually high traffic.
2. **Poisson Probability Mass Function (PMF)**
 - Displays the theoretical probability of having a specific number of visitors per minute.
 - Demonstrates that most values cluster around the average (λ).
3. **Empirical vs. Theoretical Distribution**
 - Compares actual traffic data with the expected Poisson distribution.
 - Significant deviations may indicate unexpected traffic patterns.
4. **Cumulative Visitors Over 24 Hours**
 - Shows total visitor count growing throughout the day.
 - Helps identify peak traffic periods and trends.

References:

1. Ross, S. M. (2014). *Introduction to Probability Models* (11th ed.). Academic Press.
2. Saha, Amit (2015). *Doing Math with Python* (1st ed.). No Strach Press.

UDC 621.923.42:623.746

GRAPHICAL ANALYSIS OF TREND LINE CONSTRUCTION IN ASSESSING THE WEAR OF AVIATION TIRES

Stepan Mnatsakanov

State University "Kyiv Aviation Institute", Kyiv.

Scientific supervisor – Iryna Klius, PhD in Physics and Mathematics, Associate Professor

Keywords: mathematical model, trend line, air vehicle, tires, wear.

Introduction. One of the **essential** aspects of maintaining the airworthiness of aircraft (AC) is the development and control of the maintenance program for the AC. The airworthiness of AC is ensured both during their design phases and through the implementation of measures to maintain airworthiness, as well as the confirmation that the AC is in a condition suitable for flight. One of the most critical components of AC for ensuring flight safety is aviation tires, which provide cushioning during landing and ensure safe movement on the runway [1]. Even though the takeoff and landing of AC occupy only a tiny portion of the total duration of a flight, this leads to a decrease in the operational performance indicators of tire quality. For effective tire operation, it is necessary to analyze the causes of damage, prevent their occurrence, and be able to identify types of wear and tire failures.

The aim of this work is to define a mathematical function for assessing the impact of temperature on the surface of an aviation tire during landing, about the thermal degradation of the tire material at depth, by selecting the optimal trend line.

Materials and Methods. An assessment of the change in surface temperature of aviation tires based on the aircraft landing scenario was conducted, and the depth of thermal degradation of the tire material was analyzed in relation to the surface temperature. The analysis of these patterns was performed using Microsoft Excel, a spreadsheet application for working with numerical information and databases. When there is a nonlinear influence of a variable on the studied process, the analysis of the overall pattern of change in this process is often complicated on graphs. Trend lines allow for the evaluation of the main trend represented by the graph. A trend line visually filters out deviations in the graph, making the pattern of influence of the studied factor more comprehensible. A trend line is a geometric representation of the average values of the analyzed indicators, obtained using any mathematical function. The choice of function for constructing the trend line is usually determined by the nature of data changes over time. The quality of approximation was assessed using the coefficient of determination R^2 .

Results. Aircraft tires must withstand an extremely wide range of temperatures, varying from minus 60 °C at an altitude of 10,000 meters to extremely high temperatures during landing. During landing, the tires are subjected to high loads. For example, the Boeing 737 Max 9 has a maximum landing weight of approximately 74 tons and lands at speeds exceeding 210 km/h. After touchdown, the tires initially do not roll but slide, meaning the aircraft compresses them against the runway and drags them until the rotational speed of the wheels on the landing gear matches the speed of the aircraft itself. Aviation tires mounted on the main landing gear typically endure between 300 and 500 landings on average. This range is attributed to varying levels of wear on different runways. Figure 1 illustrates the relationship between the surface temperature of the tread and the amount of material undergoing thermal degradation beneath the surface.

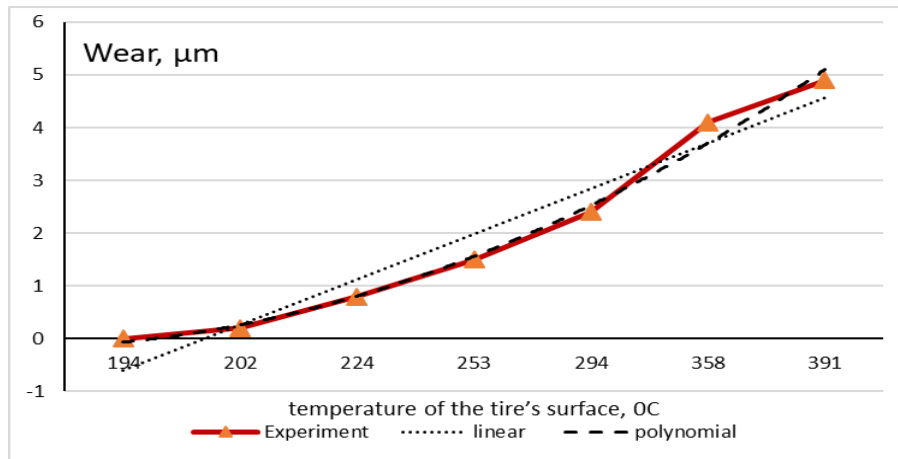


Figure 1. The impact of landing temperature on the wear of aviation tires.

By formulas:

$$y = 0.106x^2 + 0.0131x - 0.1857 \quad (1)$$

$$y = 0.8607x - 1.4571 \quad (2)$$

it has been determined that a polynomial trend line (formula (1), $R^2 = 0.9898$) allows for a more accurate assessment of the patterns of tread wear compared to a linear trend line (formula (2), $R^2 = 0.9468$).

Conclusion

The influence of surface temperature of aviation tires during aircraft landing on tread wear depth has been analyzed, and an improvement in the quality of approximation using a polynomial trend line has been determined through a graphical analysis of the dependent variable.

References:

1. Кульба П., Чередніков О., Бояров В., Єрошенко А. Дослідження температурного стану авіаційних шин іноземного виробництва. *Технічні науки та технології*. 2022. №3(29). С. 59-66. [https://doi.org/10.25140/2411-5363-2022-3\(29\)-59-66](https://doi.org/10.25140/2411-5363-2022-3(29)-59-66)
2. Li, Y., Wang, W. Thermal Penetration of Aircraft Tyre Tread at Touchdown. *International Journal of Aeronautical and Space Sciences*. 2024. 25. P.1194–1202. <https://doi.org/10.1007/s42405-024-00723-7>

УДК 517.521

ЩЕ ОДНЕ ПРЕДСТАВЛЕННЯ ЧИСЛА ЕЙЛЕРА

Дарина Гедзюра, Варвара Кольц

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Віктор Репета, к.ф.-м.н., доц.

Ключові слова: число Ейлера, факторіал, границя послідовності, інтегральна сума

Вступ. Число Ейлера (традиційно позначають буквою e) є однією з найвідоміших математичних констант, яка широко використовується в різних сферах: математиці, економіці, фізиці, біології тощо. Це число відкрив наприкінці XVII ст. Якоб Бернуллі під час розгляду фінансових задач на складні відсотки.

За означенням число e є границею послідовності $\left\{ \left(1 + \frac{1}{n} \right)^n \right\}$, коли $n \rightarrow \infty$, тобто

$$\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n} \right)^n = e \quad (1)$$

Результати. Розглянемо ще одне представлення числа e як границі іншої числової послідовності.

Твердження.
$$\lim_{n \rightarrow \infty} \frac{n}{\sqrt[n]{n!}} = e. \quad (2)$$

Ця границя безпосередньо впливає з формули Стірлінга

$$n! \sim \sqrt{2\pi n} \cdot \left(\frac{n}{e} \right)^n,$$

за якою можна обчислювати наближені значення факторіалів великих чисел з достатньо високою точністю.

Доведемо граничну рівність (2), використовуючи математичну візуалізацію. Для доведення рівності (2)

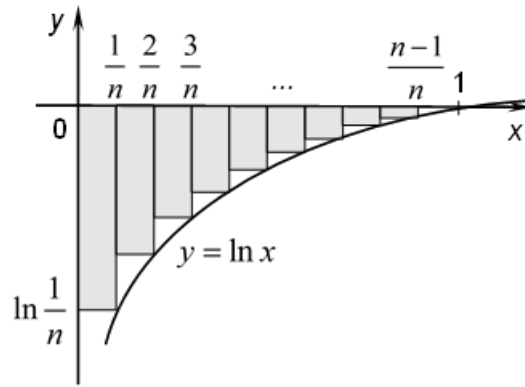
достатньо довести, що $\lim_{n \rightarrow \infty} \ln \frac{\sqrt[n]{n!}}{n} = -1$, яка рівносильна границі (2).

Виконаємо перетворення

$$\begin{aligned} \ln \frac{\sqrt[n]{n!}}{n} &= \ln \sqrt[n]{n!} - \ln n = \frac{1}{n} (\ln 1 + \ln 2 + \ln 3 + \dots + \ln k + \dots + \ln(n-1) + \ln n) - \\ &- \frac{1}{n} \left(\underbrace{\ln n + \ln n + \ln n + \dots + \ln n}_n \right) = \frac{1}{n} ((\ln 1 - \ln n) + \dots + (\ln k - \ln n) + \dots + (\ln n - \ln n)) = \\ &= \frac{1}{n} \ln \frac{1}{n} + \frac{1}{n} \ln \frac{2}{n} + \dots + \frac{1}{n} \ln \frac{k}{n} + \dots + \frac{1}{n} \ln \frac{n-1}{n} + \frac{1}{n} \ln \frac{n}{n} = \sum_{k=1}^n \frac{1}{n} \ln \frac{k}{n}. \end{aligned}$$

Геометрично сума $\sum_{k=1}^n \frac{1}{n} \ln \frac{k}{n} = \ln \frac{\sqrt[n]{n!}}{n}$ визначає площу ступінчастої фігури (див. рис.1), узятую із знаком

мінус. Цю суму можна розглядати як наближення за методом прямокутників інтеграла $\int_0^1 \ln x dx$.

Рис. 1. Ілюстрація інтегральної суми функції $y = \ln x$

Робимо висновок, що

$$\lim_{n \rightarrow \infty} \ln \frac{\sqrt[n]{n!}}{n} = \int_0^1 \ln x dx = \lim_{\varepsilon \rightarrow 0} \int_{\varepsilon}^1 \ln x dx = \lim_{\varepsilon \rightarrow 0} (x \ln x - x) \Big|_{\varepsilon}^1 = -1 - \lim_{\varepsilon \rightarrow 0} (\varepsilon \ln \varepsilon - \varepsilon) = -1.$$

Звідси випливає, що $\lim_{n \rightarrow \infty} \ln \frac{n}{\sqrt[n]{n!}} = 1$ й відповідно $\lim_{n \rightarrow \infty} \frac{n}{\sqrt[n]{n!}} = e$.

Порівняємо значення заданих послідовностей за різних значень n (див. таблицю 1).

Таблиця 1

Наближені значення числа Ейлера

n	10	100	1000	10000	100000
$\frac{n}{\sqrt[n]{n!}}$	2,2081	2,6321	2,7064	2,7168	2,7181
$\left(1 + \frac{1}{n}\right)^n$	2,5937	2,7048	2,7169	2,7182	2,71827

Висновок

Застосування для доведення математичних тверджень візуалізації дає змогу унаочнити процес доведення, що значно покращує розуміння сенсу самого твердження. Такий підхід має перспективу застосувань під час вивчення математики як у середній школі, так і в закладах вищої освіти.

Список використаних джерел:

1. Nelsen R.B. Symmetry and integration. In: *Cameos for Calculus: Visualization in the First-Year Course*. Classroom Resource Materials. Mathematical Association of America; 2015.

УДК 519.852

МЕТОДИ ОПТИМІЗАЦІЇ МАРШРУТІВ У ЗАДАЧАХ ТРАНСПОРТНОЇ ЛОГІСТИКИ

Анастасія Тімохіна, Аліна Химченко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ірина Шевченко, к.е.н, доц.

Ключові слова: транспортна логістика, алгоритм, модель, транспортні маршрути в умовах невизначеності

У сучасному світі транспортна логістика відіграє ключову роль у забезпеченні ефективного функціонування економіки. Зростання обсягів перевезень та підвищення вимог до якості послуг спонукають логістичні компанії впроваджувати ефективні методи управління маршрутами. Основною проблемою в транспортній логістиці є необхідність визначення оптимальних маршрутів для доставки вантажів з урахуванням різних обмежень, таких як вантажомісткість транспортних засобів, часові вікна для доставки, стан доріг та інші фактори.

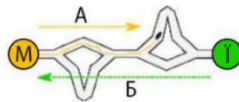
Оптимізація транспортних маршрутів дозволяє зменшити витрати, скоротити час доставки та підвищити задоволеність клієнтів. Отже, застосування методів оптимізації маршрутів надзвичайно актуально в наш час. Для вирішення задач оптимізації маршрутів у транспортній логістиці розглянемо деякі математичні методи та алгоритми.

Одним з методів розв'язання задачі маршрутизації є метод Кларка-Райта, який дозволяє оптимізувати маршрути на основі обчислення економії від об'єднання різних маршрутів у єдиний ланцюг. Економію визначають як різницю між сумою відстаней окремих маршрутів та об'єданого маршруту. Формально економія S_{ij} для об'єднання маршрутів до точок i та j обчислюється за формулою:

$$S_{ij} = dO_i = dO_j - d_{ij},$$

де dO_i і dO_j – відстань від складу до точок i та j відповідно; d_{ij} – відстань між точками i та j .

Розглянемо ще один метод розв'язання задачі маршрутизації – мурашиний алгоритм, який створений на «розумній» та цікавій поведінці мурах у природі: під час пошуку шляхів до їжі мурахи використовують певні особливості. Ідея алгоритму полягає в тому, що мураха прямує від мурашника (M) у випадковому напрямку – шлях А (рис. 1). Якщо вона знаходить їжу ($\tilde{I}$), то повертається до мурашника – шлях Б, та залишає по собі слід з феромону.

Рис. 1. Маршрут мурахи від мурашника (M) до джерела їжі ($\tilde{I}$)

Залишені феромони приваблюють інших мурах, що знаходяться поруч і, найімовірніше, вони рушають тим самим маршрутом. Повертаючись до мурашника, мурахи також залишають свій феромон й тим самим укріплюють доріжку (рис. 2). Якщо існує два маршрути, то за однаковий час коротким маршрутом встигне пройти більше мурах ніж довгим, і короткий маршрут стане вигіднішим. Довгі доріжки повільно зникають внаслідок випаровування феромонів (рис. 3).

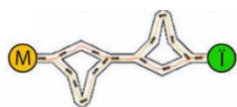


Рис. 2. Маршрут мурах слідами залишеного феромону

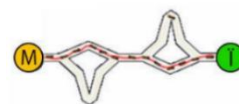


Рис. 3. Короткий та довгий маршрути мурах

За алгоритмом навколишнє середовище для мурах представлено неорієнтованим графом. Кожне ребро має вагу, яка позначається як відстань між двома вершинами. Мураха може подорожувати по грані в будь-якому напрямку. Ймовірність включення ребра в маршрут окремої мурахи пропорційна до кількості феромонів на цьому ребрі, а кількість відкладеного феромону пропорційне до довжини маршруту. Чим коротший маршрут, тим більше феромону буде відкладено на його ребрах, отже, більша кількість мурах буде включати його у власні маршрути. Ймовірність переходів визначається за формулою:

$$P_{ij}(t) = \frac{I_{ij}^q \cdot f_{ij}^p(t)}{\sum_{k=0}^N I_{kj}^q \cdot f_{kj}^p(t)},$$

де I_{ij} – величина, обернена до довжини ребра між вершиною i та вершиною j , її можна позначити: $I_{ij} = \frac{1}{d_{ij}}$; $f_{ij}(t)$

– кількість феромонів в ребрі ij під час кроку ітерації t ; N – множина ребер, що доступні на даний момент мураші; p і q – константні величини (ймовірності), які визначаються перед початком алгоритму, $p + q = 1$.

Після проходження всіх ребер до знаходження розв'язку йде оновлення феромону, чим довший шлях тим менше феромону відкладається.

Висновок

Застосування математичних методів та сучасних інформаційних технологій для оптимізації маршрутів у транспортній логістиці дозволяє значно підвищити ефективність перевезень. Використання методів оптимізації сприяє зменшенню витрат, скороченню часу доставки та підвищенню якості обслуговування клієнтів.

Список використаних джерел:

1. Хейло І.С., Колесник Л.В. Дослідження методів оптимізації маршрутів для доставки вантажів логістичної компанії // Матеріали конференції КІТ-2024, Харків, ХНАДУ, 20.11.2024.
2. А. П. Мироненко. «Застосування модифікованого алгоритму Кларка Райта для оптимізації транспортних мереж» // Вісник Національного технічного університету України «КПІ», т. 4, с. 33-38, 2019.
3. Заграй В.В. Система управління логістикою транспортною компанією з доставкою замовлення.
[URL:https://ela.kpi.ua/server/api/core/bitstreams/3d759794-9a04-4167-a25a-d07255fb9d75/content](https://ela.kpi.ua/server/api/core/bitstreams/3d759794-9a04-4167-a25a-d07255fb9d75/content)

УДК 519.6:629.7+519.873

АЕРОДИНАМІЧНІ МОДЕЛІ ТУРБУЛЕНТНОГО ПОТОКУ: МАТЕМАТИЧНІ ПІДХОДИ ДО МОДЕЛЮВАННЯ ТА ЇХ ЗНАЧЕННЯ ДЛЯ АВІАЦІЇ

Дарія Бойко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Тетяна Левковська, ст.викладач

Ключові слова: моделі турбулентності, аеродинамічне моделювання, рівняння Нав'є-Стокса.

Аеродинамічні моделі турбулентного потоку важливі для аналізу та оптимізації характеристик літальних апаратів, оскільки турбулентні потоки є частиною реальних умов польоту. Турбулентність впливає на аеродинамічні сили, стійкість, маневреність і паливну ефективність. Однак, через складність таких потоків, їх моделювання залишається складною задачею. Розробка точніших моделей турбулентності необхідна для покращення прогнозів аеродинамічних характеристик і підвищення ефективності авіаційних технологій.

Метою цієї роботи є аналіз сучасних математичних моделей турбулентних потоків, їх застосування для вирішення аеродинамічних задач, а також визначення їх значення для оптимізації конструкцій літальних апаратів та підвищення безпеки польотів.

Аеродинамічне моделювання — це створення математичних моделей і комп'ютерних симуляцій для прогнозування властивостей об'єктів, що взаємодіють з повітряним потоком. Методи проектування аеродинамічних форм транспортних засобів можна поділити на кілька етапів: інженерні наближені методи, моделювання за методами особливостей та підходи, що базуються на інтеграції рівнянь Нав'є-Стокса [1,2].

Для наукового обґрунтування результатів досліджень аеродинамічної моделі турбулентного потоку використовують метод великомасштабного усереднення (LES) та усереднене рівняння Рейнольдса (RANS). Перевагою рівнянь RANS є те, що вони описують усереднені характеристики потоку, що важливо для аеродинаміки, і дозволяють уникнути складних розрахунків турбулентних потоків. Однак вони є незамкнутими через невідомий тензор рейнольдсової напруги та тепловий потік, що вимагає емпіричних співвідношень.

Метод усереднення Рейнольдса полягає в тому, щоб замінити змінні (швидкість, тиск та ін.) на їх усереднені значення, (тобто на середні значення, що відображають статистичні характеристики турбулентного потоку). Це допомагає звести складні рівняння до більш керованої форми. Нехай $\vec{u}(\vec{x}, t)$ - це змінна швидкості в точці $\vec{x}$ і в момент часу t . У методі усереднення вводять середню швидкість $\bar{u}(\vec{x}, t)$ яка є середнім значенням швидкості на певному просторі або часі: $\vec{u}(\vec{x}, t) = \bar{u}(\vec{x}, t) + \vec{u}'(\vec{x}, t)$, де $\bar{u}(\vec{x}, t)$ - середнє значення швидкості, $\vec{u}'(\vec{x}, t)$ - флуктуація швидкості, яка відображає відхилення від середнього значення. Рівняння Нав'є-Стокса у усередненні вигляді для випадку стаціонарного потоку набирає вигляду $\frac{\partial \bar{u}}{\partial t} + \bar{u} \cdot \nabla \bar{u} = -\frac{1}{\rho} \nabla \bar{p} + \nu \nabla^2 \bar{u} - \nabla \cdot \bar{\tau} + \bar{f}$, де $\bar{u}$ - середня швидкість потоку, p - середній тиск, ν — кінематична в'язкість, ρ — густина потоку, f — зовнішні сили (гравітаційне поле або інші навантаження), τ — турбулентний тензор напружень (описує вплив турбулентних флуктуацій), ∇ — оператор градієнта. Турбулентний тензор напружень $\bar{\tau}_{ij}$ є ключовим терміном у рівнянні Нав'є-Стокса. Цей термін описує додаткові сили, які виникають через турбулентні флуктуації. Він залежить від швидкості флуктуацій $\vec{u}'$ і має вигляд: $\bar{\tau}_{ij} = \rho \overline{u'_i \cdot u'_j}$, де $\overline{u'_i \cdot u'_j}$ - це середня величина добутку компонент флуктуацій швидкості, що має фізичний зміст турбулентних напружень [1,3].

Оскільки рівняння Нав'є-Стокса складні і не мають аналітичних розв'язків, метод усереднення Рейнольдса спрощує задачу, моделюючи середні характеристики потоку. Це дозволяє отримувати прогнози аеродинамічних характеристик, таких як підйомна сила, опір і стійкість літальних апаратів. Метод великомасштабного усереднення (LES) зосереджується на усередненні великих масштабів потоку,

зберігаючи дрібномасштабні коливання. LES точніший за RANS, оскільки усереднює тільки великі турбулентні структури, залишаючи малі флуктуації непорушеними.

Замість цього вводиться модель, що описує вплив малих масштабів на великий потік через турбулентні напруження, коригуючи ефект малих вихорів [3].

Висновок

Математичні моделі турбулентних потоків є основою для прогнозування аеродинамічних характеристик літальних апаратів, що допомагає вдосконалювати їх конструкцію та покращувати ефективність і безпеку. Врахування турбулентності в моделях має вирішальне значення для зниження витрат пального в авіаційних технологіях.

Список використаних джерел:

1. Сушак, М.Б., Кушніренко, О.В., Сиворахша, Д.В., & Дудник, Т.Г. (2019). *Моделювання аеродинамічної інтерференції при створенні перспективних літаків*. Збірник наукових праць ДНДІ ВС ОБТ, 4(14).
2. Durbin, P. A., & Reuther, J. (2021). *Numerical methods for turbulent flow simulation using Reynolds-averaged Navier-Stokes equations (RANS) in aerodynamics*. Journal of Aircraft, 58(2), 486-503.
3. Nguyen, C. P., & Liao, K. H. (2020). *Turbulence modeling using large eddy simulation (LES) and Reynolds-averaged Navier-Stokes (RANS) in low-Reynolds-number flows*. International Journal of Heat and Fluid Flow, 88, 108726

УДК 517.9

ПРАКТИЧНЕ ЗАСТОСУВАННЯ ПОХІДНОЇ ДО РОЗВ'ЯЗАННЯ ПРИКЛАДНИХ ЗАДАЧ

Аліна Кайденко, Ніка Зембіцька

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Валентина Петрусенко, к.т.н., доц.

Ключові слова: похідна, екстремум, функція, графік, критична точка

Вступ. Похідна функції відіграє важливу роль у природничо-наукових та інженерно-технічних дослідженнях. Актуальність застосування похідної при вирішенні прикладних задач пояснюється її здатністю описувати зміну величин та визначати екстремальні значення функцій у різних сферах науки, техніки, економіки тощо.

Мета. Метою роботи є дослідження застосування похідної для розв'язання практичних задач у різних галузях, визначення значимості математичного аналізу в оптимізації процесів і прийнятті ефективних рішень.

Матеріали та методи. Застосування похідної для розв'язання прикладних задач охоплює кілька основних етапів. На першому етапі відбувається побудова математичної моделі, цей етап потребує ґрунтовних знань суміжних дисциплін або дисциплін, у мові яких виникає прикладна задача. На другому етапі відбувається дослідження математичної моделі, тобто розв'язування отриманої математичної задачі, цей етап дає змогу передбачити розвиток процесу, розрахувати його характеристики. На третьому

етапі відбувається інтерпретація одержаних на другому етапі результатів, тобто переклад розв'язку математичної задачі з мови математики на мову тієї галузі, де вона виникла.

Результати. Задача 1. Між якими точками необхідно провести канал (AB), що з'єднає річку з водоводом так, щоб його довжина була найменшою? Знайти довжину цього каналу.

На карті (рис.1) русло річки має форму параболи $y = x^2$, а водовід – прямої $y = x - 5$. Довжина одиничного відрізка – 1 км. Кутовий коефіцієнт прямої $k = -1$. Враховуючи, що значення похідної функції в заданій точці дорівнює кутовому коефіцієнту дотичної до графіка, проведеної в цій точці, знайдемо абсцису точки параболи, в якій дотична до неї буде паралельна прямій $y = -x - 5$: $k = \operatorname{tg} \alpha = (x^2)' = 2x = -1$, $x = -0,5$, $y(-0,5) = 0,25$.

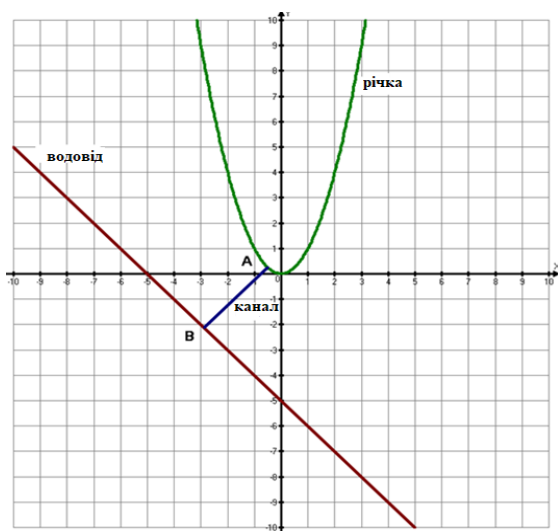


Рис.1. Графічне зображення задачі 1

Канал повинен проходити через точку $A(-0,5; 0,25)$ перпендикулярно до прямої $y = -x - 5$, яка визначає водовід. Умова перпендикулярності прямих $k_1 = -\frac{1}{k_2}$. Таким чином, кутовий коефіцієнт прямої, що містить відрізок AB , $k_2 = 1$. Рівняння прямої, що проходить через точку $A(-0,5; 0,25)$ і має кутовий коефіцієнт $k_2 = 1$: $y = x + 0,75$. Розв'язавши систему двох рівнянь знаходимо координати точки перетину каналу і водовода (точка B).

Отже, $B(-2,875; -2,125)$, а $AB = \sqrt{(-2,875 - (-0,5))^2 + (-2,125 - 0,25)^2} \approx 3,36$ км

Задача 2. Готову продукцію зі складу (точка K), що знаходиться на відстані 12 км від точки A шосе, потрібно доставити у супермаркет B , що також знаходиться на шосе. Відстань $AB=20$ км. Швидкість транспорту ґрунтовою дорогою 40 км/год, а шосе – 50 км/год. В яку точку (C) шосе потрібно прокласти ґрунтову дорогу, щоб доставляти продукцію в найкоротші терміни?

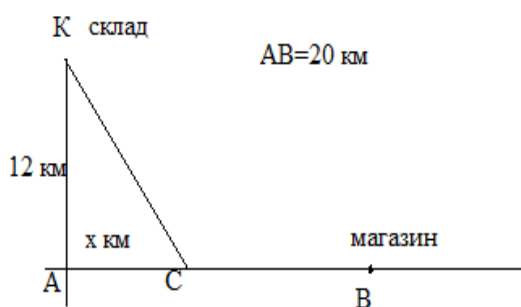


Рис.2. Графічне зображення задачі 2

Час, витрачений на шлях від K до B можна знайти за формулою: $t = t_{KC} + t_{CB} = \frac{KC}{v_{KC}} + \frac{CB}{v_{CB}} = \frac{\sqrt{144+x^2}}{40} + \frac{20-x}{50}$. Знаходимо похідну отриманої функції: $t' = \frac{x}{40\sqrt{144+x^2}} - \frac{1}{50}$. Розв'язавши рівняння $\frac{x}{40\sqrt{144+x^2}} - \frac{1}{50} = 0$, отримаємо значення критичної точки: $x = 16$ км ($0 < x < 20$).

Висновок. У навколишньому світі багато процесів можна описати за допомогою функціональних залежностей. Причому функція в деяких умовах набуває екстремального значення. Розв'язання задач на оптимізацію дає змогу витратити мінімальну кількість часу і матеріальних засобів для досягнення необхідного результату.

Список використаних джерел:

1. Погребний В. Узагальнення поняття похідної // Фізико-математична освіта: науковий журнал, 2017. Випуск 2(12), С.124-129.

UDC 51(075.8)

MATHEMATICAL MODELING OF DRUG ABSORPTION AND ELIMINATION: A CASE STUDY OF PARACETAMOL

Iryna Pavlenko

State University "Kyiv Aviation Institute", Kyiv

Scientific Adviser – Kaveh Eftekharinasab, Ph.D., Assoc.Prof.

Keywords: Pharmacokinetics, differential equations, superposition principle, paracetamol.

Predicting drug concentration over time is critical for optimizing therapeutic efficacy and minimizing toxicity. This study employs differential equations and integral calculus to model the pharmacokinetics of paracetamol, a drug with a 2-hour half-life. The objective is to demonstrate how mathematical tools elucidate drug behavior, focusing on absorption, elimination, and multi-dose dynamics.

Mathematical Framework

The process is governed by the differential equation:

$$\frac{dC}{dt} = A(t) - kC$$

where $C(t)$ is concentration, $A(t)$ is absorption rate, and k is the elimination constant ($k \approx 0.3466 \text{ h}^{-1}$). For an instantaneous 500 mg dose, the Dirac delta function $A(t) = 500\delta(t)$ models rapid absorption. Solving the equation yields exponential decay:

$$C(t) = 500e^{-0.3466t} \text{ mg/L}$$

Single-Dose Kinetics

The concentration halves every 2 hours (half-life), dropping to 250 mg/L at $t=2h$ and 15.63 mg/L after 10 hours. This aligns with the integral-derived solution, emphasizing the role of k in determining elimination speed.

Multiple Doses and Superposition

For repeated doses (500 mg every 4 hours), the superposition principle applies:

$$C(t) = 500 \sum_{n=0}^N e^{-0.3466(T-4n)} H(t-4n)$$

where $H(t)$ is the Heaviside function. Steady-state concentrations emerge when drug input equals elimination, underscoring the need to balance dosing intervals and half-life to maintain therapeutic levels.

Clinical Relevance: AUC and Applications

The area under the curve (AUC), calculated as $AUC = \int_0^{\infty} C(t)dt$, quantifies total drug exposure. Clinically, AUC

informs bioavailability, clearance, and dosing regimens to avoid subtherapeutic or toxic outcomes.

Conclusions

Integral-based models provide a robust framework for predicting drug kinetics. Key insights include exponential decay in single doses, superposition for multi-dose regimens, and AUC-driven clinical decisions. These tools enhance personalized medicine by optimizing dosing strategies and ensuring patient safety.

References:

1. Shargel, L., Wu-Pong, S., & Yu, A. B. C. (2012). Applied Biopharmaceutics & Pharmacokinetics. McGraw-Hill Education.
2. Rowland, M., & Tozer, T. N. (2011). Clinical Pharmacokinetics and Pharmacodynamics: Concepts and Applications. Lippincott Williams & Wilkins.

УДК 512

ОБЧИСЛЕННЯ ВИЗНАЧНИКІВ ЗА ДОПОМОГОЮ ТОТОЖНОСТІ СІЛЬВЕСТРА

Артем Устименко

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ганна Тугай, ст.викладач

Ключові слова: визначник, мінор, обвідний мінор, детермінантна тотожність Сільвестра

Для обчислення визначників вищих порядків використовують методи, що зводяться до обчислення визначників нижчого порядку. Розглянемо метод, що ґрунтується на детермінантній тотожності Сільвестра [1].

Нехай задано матрицю $A = (a_{ij})_{i,j=1}^n$. Позначимо $A \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ j_1 & j_2 & \dots & j_k \end{pmatrix}$ – мінор матриці A , складений з

елементів на перетині $i_1, i_2, \dots, i_k$ -го рядків та $j_1, j_2, \dots, j_k$ -го стовпців, $1 \leq i_1, i_2, \dots, i_k \leq n$, $1 \leq j_1, j_2, \dots, j_k \leq n$.

Тоді визначник матриці A можна обчислити за формулою:

$$|A| = \frac{A \begin{pmatrix} 1 & 2 & \dots & n-1 \\ 1 & 2 & \dots & n-1 \end{pmatrix} A \begin{pmatrix} 2 & 3 & \dots & n \\ 2 & 3 & \dots & n \end{pmatrix} - A \begin{pmatrix} 1 & 2 & \dots & n-1 \\ 2 & 3 & \dots & n \end{pmatrix} A \begin{pmatrix} 2 & 3 & \dots & n \\ 1 & 2 & \dots & n-1 \end{pmatrix}}{A \begin{pmatrix} 2 & 3 & \dots & n-1 \\ 2 & 3 & \dots & n-1 \end{pmatrix}}.$$

Наприклад, $\begin{vmatrix} 1 & -2 & 3 \\ 3 & 4 & -2 \\ 0 & 1 & 2 \end{vmatrix} = \frac{1}{4} \cdot \left[\begin{vmatrix} 1 & -2 \\ 3 & 4 \end{vmatrix} \cdot \begin{vmatrix} 4 & -2 \\ 1 & 2 \end{vmatrix} - \begin{vmatrix} 3 & 4 \\ 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} -2 & 3 \\ 4 & -2 \end{vmatrix} \right] = \frac{1}{4} (10 \cdot 10 - 3 \cdot (-8)) = 31.$

$$\begin{vmatrix} 1 & -2 & 3 & 3 \\ 3 & 4 & -2 & 1 \\ 0 & 1 & 2 & 2 \\ 1 & -1 & 0 & 4 \end{vmatrix} = \frac{1}{\begin{vmatrix} 4 & -2 \\ 1 & 2 \end{vmatrix}} \cdot \left[\begin{vmatrix} 1 & -2 & 3 \\ 3 & 4 & -2 \\ 0 & 1 & 2 \end{vmatrix} \cdot \begin{vmatrix} 4 & -2 & 1 \\ 1 & 2 & 2 \end{vmatrix} - \begin{vmatrix} 3 & 4 & -2 \\ 0 & 1 & 2 \\ 1 & -1 & 0 \end{vmatrix} \cdot \begin{vmatrix} -2 & 3 & 3 \\ 4 & -2 & 1 \end{vmatrix} \right] =$$

$$= \frac{1}{10} (31 \cdot 46 - 16 \cdot 21) = 109.$$

Висновок

Обчислення визначника n -го порядку зводиться до обчислення чотирьох визначників $(n-1)$ -го порядку та визначника $(n-2)$ -го порядку, що за великих n зручніше ніж розклад визначника за рядком або стовпцем, де обчислюється n визначників $(n-1)$ -го порядку.

Список використаних джерел:

1. Гантмахер Ф.Р. Теорія матриць. <https://nebayduzhi-math.azurewebsites.net/>

УДК 519.3

ЗАСТОСУВАННЯ ПАКЕТУ МАТНСАД ДЛЯ РОЗВ'ЯЗАННЯ ДЕЯКИХ ЗАДАЧ МАТЕМАТИЧНОЇ СТАТИСТИКИ

Ірина Тернова

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Анатолій Богатирчук, к.ф.-м.н., доц.

Ключові слова: інтервальний розподіл, кумулята, mathcad.

Графічна ілюстрація статистичних даних надає їм наочності і часто приводить до спрощення їх аналізу. Нехай задано інтервальний розподіл частот (Табл. 1). Потрібно побудувати кумулятивну криву (кумуляту).

Таблиця 1.

$x_{i-1} - x_i$	2-6	6-10	10-14	14-18	18-22	22-26
n_i	24	6	12	10	32	16

Виконаємо цю побудову засобами Mathcad в такій послідовності:

1. Подаємо цей розподіл в вигляді матриці (в першому стовпці — початки інтервалів, в другому — кінці інтервалів, в третьому — відповідні частоти).
2. За допомогою функції *stack(.)* для наочності графіка доповнюємо зверху і знизу допоміжні рядки матриці (інтервали з 0-вою частотою).
3. Знаходимо суму частот $n = \sum_i n_i$, а також величини відносних частот $w_i = \frac{n_i}{n}$.
4. Знаходимо накопичені відносні частоти.

Для побудови кумуляти на осі абсцис відкладається значення ознаки, а на осі ординат—накопичені відносні частоти (див. рис. 1).

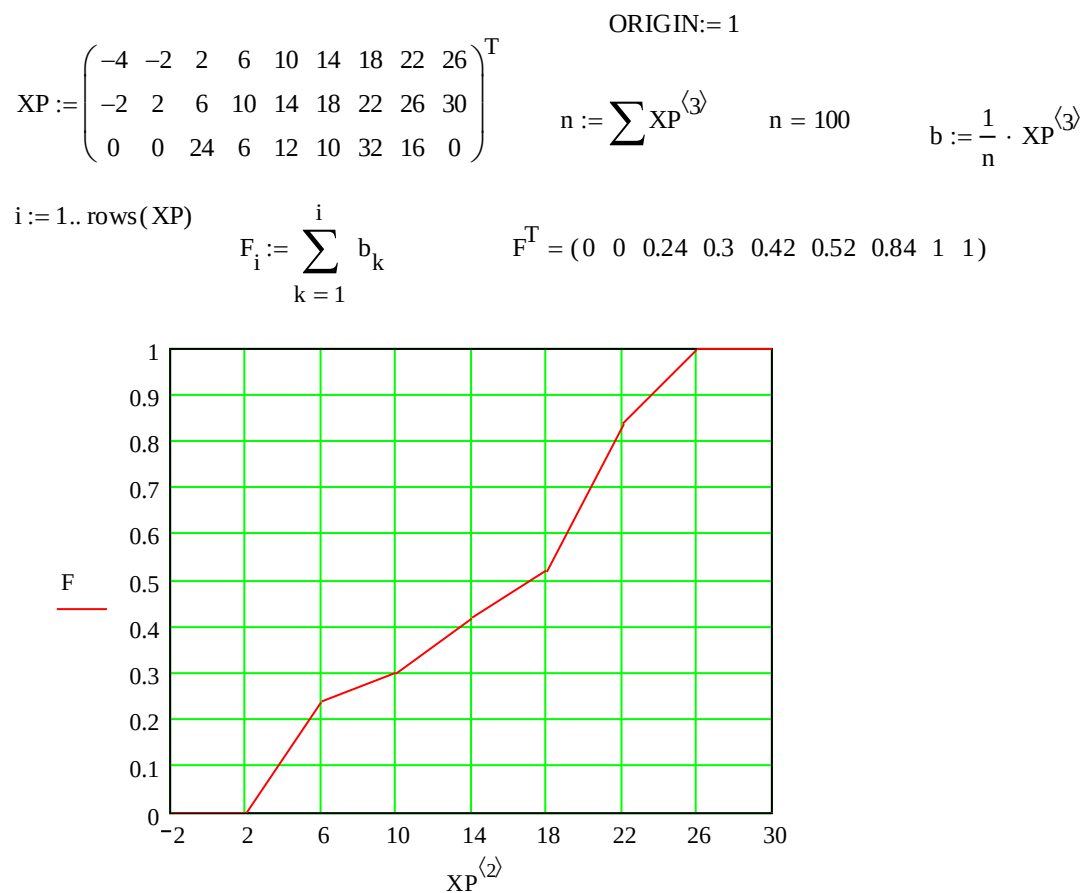


Рис.1. Документ mathcad

Висновок

Запропонований метод побудови кумулятивної кривої може бути використаний в конкретних статистичних дослідженнях, а також в навчальному процесі.

Список використаних джерел:

1. Кундрат А. М., Кундрат М. М. Науково-технічні обчислення засобами MathCAD та MS Excel.—Рівне: НУВГП, 2014.—252с.
2. Сеньо П. С. Теорія ймовірностей та математична статистика: підручник. - Київ: Знання, 2007. - 556 с.

УДК 005.334:519.866:336.7

ЗАСТОСУВАННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ ДЛЯ ОЦІНКИ ФІНАНСОВОЇ СТІЙКОСТІ БЛАГОДІЙНИХ ФОНДІВ

Олексій Юдкевич

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Ірина Степанівна Ключ, кандидат ф.-м. н., доцент*

Ключові слова: математична модель, фінансова стійкість, благодійні організації

Вступ. Протягом останніх років відсутність стабільності в Україні спонукала значному зростанню кількості волонтерських організацій, а з початком повномасштабного вторгнення запит на діяльність неформальних інституцій суттєво зріс. Такого роду соціальні практики є ефективними по відношенню до функціонування формальних державних інститутів [1]. В роботі проаналізовано фінансову стійкість благодійного фонду за допомогою дослідження функціонування відповідної математичної моделі.

Мета. Метою дослідження є застосування математичних методів аналізу для вивчення фінансової стійкості неформальних інститутів, зокрема, шляхом аналізу їхньої фінансової діяльності та статистичної обробки даних, що сприятиме кращому розумінню параметрів стійкості таких організацій. Відтак ми ставимо два головних завдання: проаналізувати фінансову статистику обраної організації та виявити закономірності, які впливають на фінансову стійкість та побудувати на основі цих закономірностей фінансовий прогноз [2].

Матеріали та методи. У дослідженні використано дані з відкритих джерел, що стосуються питання фінансової звітності волонтерських організацій і розглянуто фінансову діяльність громадської організації "Згряя".

Також ми аналізуємо фінансовий звіт за попередній рік і за допомогою методу середнього темпу змін (Average Rate of Change Method) який є фундаментальним при вивченні фінансового звіту, будуємо прогноз на майбутній рік.

Результати. Діяльність громадської організації "Згряя" полягає у наданні безкоштовної медичної допомоги населенню прифронтових міст. Проаналізувавши всі надходження і витрати громадської організації ми обчислили відносну зміну цих витрат та надходжень за формулою

$$r_t = \frac{E_t - E_{t-1}}{E_t},$$

де E_t - статистичне значення надходжень протягом місяця.

Середнє значення всіх r_t (середній темп змін) обчислено за формулою

$$r_{avr} = \frac{1}{N} \sum_{t=2}^N r_t .$$

Таким чином, встановлено що коефіцієнт змін для надходжень дорівнює 3,65%, а коефіцієнт змін для витрат дорівнює 3,56%. Ці значення ми використали для побудови прогнозу, скориставшись формулами:

$$E_{1t} = E_{t-1} \times (1 - 0,0365), \quad E_{2t} = E_{t-1} \times (1 + 0,0356).$$

Результати прогнозують що громадська організація може зіштовхнутися з дефіцитом бюджету у розмірі 756, 081 грн. в кінці року. Тому для забезпечення фінансової стійкості потрібно зосередити увагу на змінах фінансової стратегії для досягнення бажаного результату.

Висновки

Вивчення фінансової стійкості волонтерських організацій та благодійних фондів за допомогою математичних методів моделювання є перспективним напрямом економічних та математичних досліджень. Потенційна користь застосування математичних методів аналізу призведе до значного зростання стабільності неформальних інститутів і як наслідок збільшенню їх соціальної та економічної значущості.

Список використаних джерел:

1. Волонтерство та псевдоволонтерство в Україні: новий погляд крізь призму неформальних інститутів URL: <https://doi.org/10.53317/2786-4774-2024-1-2>
2. Роль економетричних моделей в прогнозуванні економічних показників URL: <https://ir.vtei.edu.ua/g.php?fname=25665.pdf> (Last accessed: 20.03.2025).

УДК 519.21

РОЗРАХУНОК ЙМОВІРНОСТІ УРАЖЕННЯ ЦІЛ СИСТЕМОЮ ПРОТИПОВІТРЯНОЇ ОБОРОНИ

Поривай Валерія, Соколенко Діана

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Ірина Шевченко, к.е.н., доц.

Ключові слова: ймовірність, нормальний розподіл випадкової величини, протиповітряна оборона, ціль ураження.

Під час повномасштабного вторгнення в Україну системи протиповітряної оборони (ППО) відіграють ключову роль у захисті військових об'єктів, критичної та цивільної інфраструктури. Ймовірність влучення систем ППО у цілі має безпосередній вплив на ефективність планування та застосування захисних заходів. Дослідження у цій сфері сприятимуть підвищенню надійності систем ППО, знижуючи ризики для цивільного населення та збереження критичних об'єктів.

Три роки поспіль серйозною проблемою для сил оборони ЗСУ є ударні безпілотні літальні апарати (БПЛА) типу «Shahed-136», що здатні виконувати бойові та розвідувальні завдання противника. Вони не можуть змінити тактичну ситуацію в зоні бойових дій, але дійсно мають серйозну загрозу для ЗСУ, критичної інфраструктури та цивільного населення, оскільки «Shahed-136» має серйозну бойову частину, і в цьому його головна загроза [1].

За словами речника ПС в Україні більшість ворожих БПЛА збивають мобільні вогневі групи з зенітних установок різних типів та великокаліберних кулеметів [2]. Для ефективної бойової роботи мобільних груп важливо підвищити ймовірність ураження цілі, враховуючи багато факторів, зокрема технічні характеристики БПЛА і систем ППО, рельєфність місцевості, кваліфікацію бійців, погодні умови тощо.

Для проведення розрахунків ймовірності ураження цілі системами ППО, зокрема, зенітними установками, розглянемо деякі тактико-технічні характеристики БПЛА типу «Shahed-136» (табл. 1) і гармати зенітної системи ППО Skyranger 30 HEL (табл. 2) [3, 4].

Таблиця 1

Тактико-технічні характеристики БПЛА типу «Shahed-136»

Дальність польоту	до 1500 км
Висота польоту (h)	від 60 до 4000 м
Швидкість польоту (V_b)	близько 180 км/год (50м/с)

Таблиця 2

Тактико-технічні характеристики гармати зенітної системи ППО Skyranger 30 HEL

Номінальна скорострільність	1200 постр/хв.
Швидкострільність одиночного пострілу	200 постр/хв.
Середня початкова швидкість V_c	1075 м/с
Радіус ураження або розкид попадань (r)	200 м

Припустимо, що промах або похибка наведення мають нормальний розподіл $N(0, \sigma^2)$, тоді ймовірність влучання в ціль залежить від того, яка частина нормального розподілу припадає на радіус ефективного ураження снаряда r – зона, в якій вибух снаряда може вивести ціль з ладу. Якщо БПЛА не маневрує активно, то ймовірність влучання дорівнює:

$$P = \Phi\left(\frac{r}{\sigma}\right) - \Phi\left(\frac{-r}{\sigma}\right), \text{ де } \Phi(x) - \text{функція Лапласа.}$$

Для заданих характеристик радіус ураження осколками 200 м, а можливий промах через похибку наведення також прийемо за 200 м, і ймовірність влучення в ціль або ймовірність того, що безпілотник потрапить в зону ураження:

$$P = \Phi\left(\frac{200}{200}\right) - \Phi\left(\frac{-200}{200}\right) = \Phi(1) + \Phi(1) = 2\Phi(1) = 2 \cdot 0,3413 = 0,6826.$$

З урахуванням випадкового розподілу похибки наведення ймовірність ураження становить приблизно 68,3%. Якщо безпілотник маневрує (змінює швидкість чи напрямок), то при розрахунку ймовірності влучення в нього потрібно врахувати переміщення БПЛА за час польоту снаряда, що ускладнює розрахунок, і, зрозуміло, ймовірність влучання зменшиться.

Висновок

У тезах розглянуто проблему підвищення надійності систем ППО, наведено основні параметри, що впливають на ймовірність ураження повітряних цілей засобами протиповітряної оборони. Отримані результати засвідчують, що розрахунок ймовірності ураження є ключовим елементом у забезпеченні ефективності

функціонування систем ППО в умовах сучасного збройного конфлікту. Врахування таких параметрів, як швидкість, висота польоту, маса та конструкційні особливості цілі, дозволяє підвищити точність ураження та зменшити ризики для військової та цивільної інфраструктури. Представлений аналіз має прикладне значення для удосконалення алгоритмів бойового застосування засобів протиповітряної оборони.

Список використаних джерел:

1. Чим небезпечні Shahed-136 на фронті та які цілі не здатні уразити. URL: [https:// fakty.com.ua/ua/ukraine/20221016-chym-nebezpechni-shahed-136-na-fronti-ta-yaki-czili-ne-zdatni-urazyty/](https://fakty.com.ua/ua/ukraine/20221016-chym-nebezpechni-shahed-136-na-fronti-ta-yaki-czili-ne-zdatni-urazyty/)
2. Як Україна збиває "Шахеди": Ігнат описав ефективну роботу мобільних вогневих груп. URL: <https://tsn.ua/ato/yak-ukrayina-zbivaye-shahedi-ignat-opisav-efektivnu-robotu-mobilnih-vognevih-grup-2476567.html>
3. Рекомендації підрозділам щодо боротьби з безпілотними літальними апаратами "КАМІКАДЗЕ" "SHAHED-136" ("ГЕРАНЬ-2"). URL: https://sprotyvg7.com.ua/lesson/_ rekomendacii-pidrozdilam-shhodo-borotbi-z-bezpilotnimi-litalnimi-aparatami-kamikadze-shahed-136-geran-2
4. Зенітна система ППО Skyranger 30 HEL: німецький небесний рейнджер, що полює за повітряними цілями. URL: <https://armyinform.com.ua/2023/03/08/zenitna-systema-ppo-skyranger-30-hel-nimeczkyj-nebesnyj-rejndzher-shho-polyuye-za-povitryanymy-czilyamy/>

УДК 656.7.052

АНАЛІЗ МОДЕЛЕЙ ПРИЙНЯТТЯ РІШЕНЬ ЛЮДИНОЮ-ОПЕРАТОРОМ АЕРОНАВІГАЦІЙНОЇ СИСТЕМИ

Руслан Мурадов

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник - Тетяна Левковська, ст.викладач

Ключові слова: аеронавігаційна система, людина, оператор, модель, прийняття рішень.

В сучасному світі авіаційної техніки та технологій, ефективність та безпека польотів значною мірою залежать від якості прийняття рішень операторами аеронавігаційних систем та чітко визначених алгоритмах дій, які викладено в нормативних та регулюючих документах. Ці алгоритми служать основою для моделювання дій людини-оператора, особливо у випадках виникнення особливих випадків у польоті [1]. Для формалізації поведінкової діяльності Л-О АНС в позаштатних ситуаціях та моделювання відповідного розвитку польотної ситуації зручними є моделі у вигляді стохастичної мережі типу GERT, які дозволяють моделювати розвиток польотної ситуації в бік ускладнення і навпаки [2].

В умовах стохастичної невизначеності, коли кожна альтернатива A_i пов'язана з множиною можливих наслідків u_j , причому кожному наслідку відповідає ймовірність виникнення p_j , послідовність дій оператора доцільно відображати з позицій системного підходу у вигляді дерева рішень [3]. Ризик у випадку сумісного ПР операторами АНС в ОВП знаходиться за формулою:

$$R_m = F_m(t_m; \{A\}; \{a\}; \{u\}; \{p\}) = t_m \sum_{k=1}^n (p_k u_k + a_k),$$
 де $R_m < R_{m-1}$ або $R_m > R_{m-1}$, t – час етапу ПР; A – вимушена

посадка з прямим/зворотним курсом; a – зсув ризику розвитку ОВП відповідно до етапу ПР; p –

ймовірність впливу несприятливих факторів; u – збиток при вимушеній посадці з прямим/зворотним курсом [3].

Розроблений алгоритм застосування системи GERT для стохастичного мережевого аналізу розвитку польотної ситуації від нормальної до катастрофічної і навпаки, за допомогою якого визначаються наступні параметри: математичне очікування часу t_{ij} розвитку ситуації; дисперсія часу t_{ij} розвитку ситуації; ймовірність p_{ij} розвитку до однієї з польотних ситуацій при виникненні ОБП. Крім перехідних ймовірностей розвитку польотної ситуації p_{ij} визначені ймовірності виникнення станів польотної ситуації: нормальної $p(G_1)$, ускладненої $p(G_2)$, складної $p(G_3)$, аварійної $p(G_4)$, катастрофічної $p(G_5)$. Представимо перехід від однієї польотної ситуації до іншої у вигляді марковського процесу загибелі і розмноження. Щоб визначити ймовірності стану системи в будь-який моменту часу, скористуємося математичними моделями марковських процесів з безперервним часом (рис. 1). Методика моделювання марковського процесу розвитку польотної ситуації базується на виконанні таких завдань: визначення стану системи (G_1-G_5); визначення коефіцієнтів інтенсивності (пропускання) (i, j) дуги в прямому і зворотному напрямках; побудова графа розвитку польотної ситуації; визначення початкових умов і розв'язання системи диференціальних рівнянь Колмогорова для марковського процесу розвитку польотної ситуації; визначення граничних ймовірностей польотної ситуації: у бік парирування польотної ситуації $p_{ij}(B) = \frac{\prod_{\{G_i\}} W_{ij}(B)}{\prod_{\{G_i\}} W_{ij}(A)} p_{ij}(A)$, у бік погіршення польотної

ситуації $p_{ij}(A) = \frac{\prod_{\{G_i\}} W_{ij}(A)}{\prod_{\{G_i\}} W_{ij}(B)} p_{ij}(B)$. Система розвитку польотної ситуації на рис. 1 описується нестационарними процесами. Це значить, що якщо система потрапить в стан G_5 , то вона не зможе перейти в інший будь-який стан. Тому для проведення розрахунків в систему введено фіктивну дугу (5-4) з параметрами $W_{54}(A)$, $p_{54}(A)$ [3]. При спробі розробити оптимальний план дій для людини-оператора, ми стикаємося з взаємодією "людина та природа", де під "природою" маються на увазі явища або фактори, які мають вплив на результати дій людини.

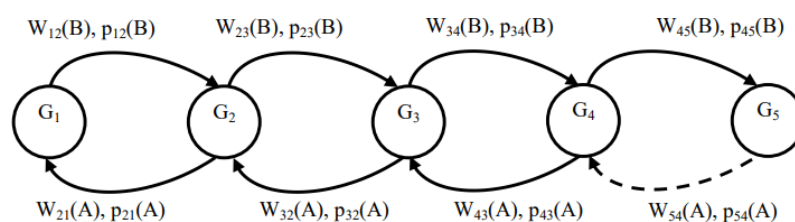


Рис. 1.

Серед критеріїв знаходження оптимальної стратегії використовується критерій Лапласа – метод прийняття рішень в умовах невизначеності, який базується на тому, що всі можливі стани природи мають однакову ймовірність [1].

Висновок

Таким чином, вибір моделі для прийняття рішення в аеронавігаційній системі залежить від багатьох факторів, серед яких основними є аналіз технології роботи, діагностика та передбачення можливих дій Л-О при виникненні польотних ситуацій в очікуваних і неочікуваних умовах експлуатації ПК.

Список використаних джерел:

1. Мар'єнков І.С., Інтелектуальна СППР. Спільні прийняття рішень в аварійній ситуації «Відмова шасі», URL: <https://er.nau.edu.ua/items/bce04773-56e9-4097-9603-64c959ccce09>
2. Шмельова Т. Ф. Моделі розвитку польотної ситуації при прийнятті рішення людиною-оператором аеронавігаційної системи, URL: http://nbuv.gov.ua/UJRN/soi_2013_8_28
3. Шмельова Т. Ф. Детерміновані та недетерміновані моделі сумісного прийняття рішень операторами аеронавігаційної системи, URL: http://nbuv.gov.ua/UJRN/Nitps_2020_1_13

УДК 517.99

ЗАСТОСУВАННЯ ІНТЕГРАЛІВ В БІОЛОГІЇ І МЕДИЦИНІ

Дар'я Євстаф'єва

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Наталя Бабкова, ст. викл.

Ключові слова: інтеграл, інтегральна швидкість, популяція, залежність від часу, гемодинаміка.

Інтеграл – це математичний об'єкт, який виник історично на основі потреби вирішення різних прикладних завдань фізики та техніки. Ті фізичні величини, що визначаються за допомогою інтегралу як правило, називаються інтегральними, а ті величини, через які виражаються інтегральні величини – диференціальними.

Інтегральне числення є важливим розділом сучасної математики. Воно має безліч зв'язків із різними науками, зокрема:

- в астрономії (інтеграли енергії та площ; рух зірок);
- медицині (комп'ютерна томографія);
- біології (встановлюють приріст чисельності популяцій; біомасу популяцій і середню довжину шляху (польоту) при проходженні деякої фіксованої ділянки) і т.д.

Розглянемо детальніше використання інтегралів у біології.

Кількість особин, постійно змінюється. За сприятливих умов вона набуватиме додатних значень, тобто народжуваність буде перевищувати смертність. У цьому випадку чисельність популяції поступово зростатиме з певною швидкістю. Позначимо цю швидкість як $v = v(t)$.

За значеннями швидкості зростання популяції біологи можуть аналізувати вік популяції загалом і активність її взаємовідносин з іншими популяціями і рівень впливу антропогенних чинників на її розвиток. Наприклад, у популяції, що складається в основному з дорослих і старих особин, швидкість v прямуватиме до нуля, проте відносно "молодої" популяції ця швидкість може значно коливатися.

Якщо ми знатимемо швидкість v , то неважко буде і розрахувати приріст чисельності популяції за певний проміжок часу від t_1 до t_2 . Функція $v(t)$ є похідною від чисельності популяції $S(t)$ (оскільки фізичний зміст похідної полягає в тому, що швидкість – це похідна від відстані, об'єму або, як у нашому випадку, чисельності популяції) [1,2,3].

Тому:

$$S(t_2) = S(t_1) + \int_{t_1}^{t_2} v(\tau) d\tau,$$

де $t_2 > t_1$.

Також вивчення інтегралів допомогло у розвитку медицини. На сьогодні неможливо вивчення гемодинаміки - руху крові по судинах без застосування інтегралів. Протягом тривалого часу катетеризація правих відділів серця була єдиним методом дослідження, що дозволяло оцінювати стан правих відділів серця та легеневої артерії [5].

За допомогою інтегралів у медицині обчислюють інтегральну швидкість для цілої судини (артерії чи вени), знаючи лінійну швидкість кровотоку; також розраховується ударний об'єм (об'єм крові) і внутрішньовенний тиск [3].

Судина (артерія чи вена) має форму близьку до циліндричної. Тому якщо потрібно знайти в порожнистому циліндрі розподіл тиску, який описується звичайним рівнянням параболічного типу за таких початкових і граничних умов: тиски на внутрішній та зовнішній поверхнях порожнистого циліндра можна вважати сталими, рівним деякому значенню ρ ; на торцевих поверхнях задано або постійні тиски різних знаків, або швидкості надходження крові; початковий розподіл тиску вважається сталим. Де r – внутрішній радіус судини, h – товщина судинної стінки, t – температура, l – довжина циліндра. Слід зауважити, що крайові умови вибирають так за умов збереження балансових рівнянь. Оскільки торцеві умови є ненульовими, то розв'язок доцільно шукати у вигляді [1,4].

$$\rho(r, h, t) = \sum_{n=0}^{\infty} \rho_n(r, t) \cos \frac{n\pi h}{l}, \quad \rho(r, t) = \frac{1}{l} \int_0^l \rho_n(r, h, t) \cos \frac{n\pi h}{l} dh$$

Висновок

Представлені вище факти демонструють широке застосування інтегралів у різних наукових галузях, що доводить невід'ємну важливість інтегралів у нашому житті. Застосування певного інтеграла багато в чому полегшує розв'язання прикладних задач з біології, медицини, геометрії, фізики та інших наук.

Список використаних джерел:

1. http://4ua.co.ua/medicine/sa3bd78b5d53a89521306c27_0.html
2. <https://core.ac.uk/download/pdf/144954141.pdf>
3. https://biology.univ.kiev.ua/images/stories/Studentam_ta_aspirantam/Zagalna_informaciya/Medichna_fisika/5_Osnovy_bioreologii_ta_hemodinamiki.pdf
4. <https://repository.ldufk.edu.ua/server/api/core/bitstreams/6511eb28-c23a-42bd-a1c6-be78f2f84b38/content>
5. А. Сем'янків. Медицина доказова і не дуже. – К.: Віхола, 2021, 446 с

УДК 519.175.4 + 681.142

ПРО ЙМОВІРНІСТЬ ЗВ'ЯЗНОСТІ ПОДВІЙНОГО ЦИКЛА**Станіслав Чистяков***Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Олександр Глухов, к.ф.-м.н, доц.*

Ключові слова: складна дискретна система, граф, зв'язність, квазівипадковий граф.

Розглядається наступна загальна задача: знайти ймовірність $P(G_n, k)$ зв'язності даного графа G_n на n вершинах при видаленні з нього k ребер [1]. В цій роботі дана загальна задача буде розглянута для графа простої структури, який називається подвійним циклом. Подвійний цикл $Z_n^{(2)}$ це граф з вершинами $\{1, 2, \dots, n\}$, в якому пари вершини $(k, k+1), k \in \{1, 2, \dots, n-1\}, (n, 1)$ з'єднані парою паралельних ребер; таким чином, граф $Z_n^{(2)}$ має n вершин і $2n$ ребер. Очевидно, що звичайна реберна зв'язність подвійного цикла дорівнює 4. Нижче будуть отримані оцінки ймовірності зв'язності подвійного цикла (рис.1).

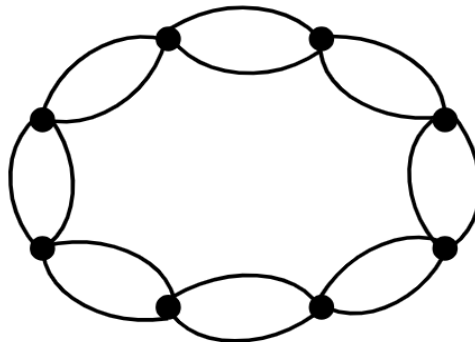


Рис.1

Загальне число варіантів видалення k ребер дорівнює $\binom{2n}{k}$, а число «сприятливих» варіантів видалення k ребер, коли граф залишається зв'язним можна порахувати як

$$\binom{n}{k} \times 2^k + n \times \binom{n-1}{k-2} \times 2^{k-2}.$$

$$\text{Таким чином, } P(Z_n^{(2)}, k) = 2^k \binom{n}{k} \times \binom{2n}{k}^{-1} \times \left(1 + \frac{k(k-1)}{4(n-k+1)(n-k+2)}\right).$$

Враховуючи, що $k < n$, а також відому нерівність $1 - x < \exp(-x)$ отримаємо, що

$$P(Z_n^{(2)}, k) = \exp\left(-\frac{k^2}{4n}\right) \times \left(1 + O\left(\frac{k^2}{n^2}\right)\right).$$

Розглянемо тепер альтернативний підхід до оцінки величини $P(Z_n^{(2)}, k)$, який базується на результатах роботи [2]. Нехай $G_n(p)$ - квазівипадковий граф на базі графа $Z_n^{(2)}$, де $p = 1 - \frac{k}{2n}$.

Нагадаємо, що квазівипадковим графом на основі зв'язного графа G називається граф $G(p)$ з множиною $(G(p))^0 = G^0$ вершин і з випадковою множиною $E = (G(p))^1$ ребер для якої виконуються умови:

$$\text{Prob}(u \in E) = p, u \in G^1, \text{Prob}(u \in E) = 0, u \notin G^1.$$

Фактично це означає, що кожне ребро графа $Z_n^{(2)}$ випадковим чином розривається з ймовірністю $q = \frac{k}{2n}$. Позначимо через P ймовірність зв'язності графа $G_n(p)$ і оцінимо величину $Q = 1 - P$.

Розглянемо наступний мультикаркас графа $G_n(p)$: $M = \{M_j\}_1^n, M_j = \{u_j, u'_j\}$, де u_j, u'_j пара паралельних ребер з кінцями в вершинах $j, j+1$. Згідно з теоремою 1 [2] має місце нерівність:

$$Q \leq nq^2 = \frac{k^2}{4n},$$

Звідки одразу випливає, що $P = 1 - \frac{k^2}{4n}$, що добре узгоджується з попередньою оцінкою.

Висновок

На підставі отриманих оцінок ймовірності зв'язності подвійного циклу на n вершинах, можна зробити висновок, що він з великою ймовірністю залишається зв'язним, якщо з нього видалені $k = o(\sqrt{n})$ ребер.

Список використаних джерел:

1. Глухов А.Д. Квазислучайные графы и структурная устойчивость сложных дискретных систем. - Электронное моделирование, т. 38, №5, 2016, с.35-41.
2. Glukhov O.D. On the connectivity of quasi-random graphs. - Електронне моделювання, т. 46, №6, 2024, с.3 -7.

УДК 656.6.517

ПРО ОДНУ ЗАДАЧУ КРИВЫХ ДРУГОГО ПОРЯДКУ

Пуршев Владислав

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Олександр Давидов, к.ф.-м.н., доц.

Ключові слова: парабола, канонічне рівняння параболі, параметр параболі, рівняння кола.

Вступ. Для опису багатьох процесів використовують квадратичні функції. Графіком квадратичної функції є парабола, канонічне рівняння якої у прямокутній декартовій системі координат має вигляд

$$y^2 = 2px,$$

де p – параметр параболі.

Цікавими є також теоретичні задачі, пов'язані з кривими другого порядку.

Результати. Розглянемо дві параболи $y^2 = 2p_1(x + a)$ та $x^2 = 2p_2(y + b)$ із взаємно перпендикулярними осями, напрямленими уздовж осей координат Ox та Oy відповідно, які перетинаються у чотирьох точках M_1, M_2, M_3 та M_4 (див. рис. 1). Доведемо що ці чотири точки лежать на одному колі [1].

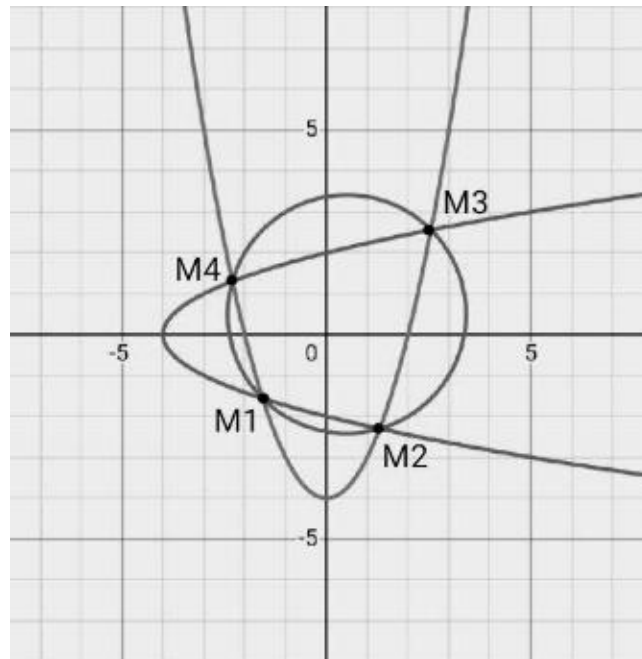


Рис.1. Графічна інтерпретація задачі.

Доведення. Оскільки точки належать кожній параболі, то справджується система

$$\begin{cases} y^2 = 2p_1(x + a), \\ x^2 = 2p_2(y + b). \end{cases}$$

Додамо перше рівняння системи до другого та виконаємо перетворення:

$$\begin{aligned} x^2 + y^2 &= 2p_1(x + a) + 2p_2(y + b), \\ x^2 + y^2 &= 2p_1x + 2p_1a + 2p_2y + 2p_2b, \\ x^2 - 2p_1x + p_1^2 - p_1^2 + y^2 + 2p_2y + p_2^2 - p_2^2 &= 2p_1a + 2p_2b, \\ (x - p_1)^2 - p_1^2 + (y - p_2)^2 - p_2^2 &= 2p_1a + 2p_2b, \\ (x - p_1)^2 + (y - p_2)^2 &= 2p_1a + 2p_2b + p_1^2 + p_2^2, \\ (x - p_1)^2 + (y - p_2)^2 &= R^2 \end{aligned} \tag{1}$$

Отримане рівняння (1) є рівнянням кола з центром в точці $O(p_1, p_2)$, радіуса R , де $R = \sqrt{2p_1a + 2p_2b + p_1^2 + p_2^2}$, що й завершує доведення.

Висновок. Запропонований підхід для доведення розглянутої задачі може бути ефективно використаний в різних задачах, пов'язаних з кривими другого порядку.

Список використаних джерел:

1. В.П. Білоусова. Аналітична геометрія / В.П. Білоусова, І.Г. Ільїн, О.П. Сергунова, В.М. Котлова. – К. : Вища шк., 1973.

УДК 517.5

ЗАСТОСУВАННЯ ВИЗНАЧЕНОГО ІНТЕГРАЛА ДЛЯ ЗНАХОДЖЕННЯ ТИСКУ ВОДИ НА СТІНКУ ГРЕБЛІ

Назар Шиков

*Державний університет «Київський авіаційний інститут», Київ**Науковий керівник – Роксолана Ткаченко, асист.*

Ключові слова: визначений інтеграл, інтегральна сума, тиск, гребля.

Історія інтеграла сягає ще давнього Єгипту, аж до 1800 р. до н. е.. Першим відомим способом для розрахунку інтегралів став метод вичерпування Евдокса (десь 370 до н. е.) [1]. Цей метод розвивав і Архімед в давній Греції, використовуючи його для знаходження площі параболічної фігури і наближеного значення площі круга. Паралельно і незалежно в Китаї у 3-му столітті н. е. Лю Хуей застосовував схожі методи для обчислення площі круга, а Цзу Чунчжи для розрахунку об'єму сфери. В 17-му столітті відбулося відкриття фундаментальної теореми інтегрального числення – відомої як формула Ньютона — Лейбніца [2]. Ця формула встановлює зв'язок між визначним та невизначеним інтегралами. Зараз визначений інтеграл застосовується дуже широко, зокрема, у геометрії, архітектурі, фізиці, хімії, економіці тощо, зокрема й під час проектування греблі.

Гребля – це основний тип водопідпірних споруд, які перегороджують його потік та долину для підйому рівня води, зосередження потужного напору води та створення водосховищ. Під час проектування греблі одним із основних параметрів є гідростатичний тиск на її стінку.

Постановка задачі. Визначити модуль гідростатичного тиску на стінку греблі, нахиленої до поверхні рідини під кутом φ . Верхня сторона $AO = a$ розташована горизонтально на поверхні води. Напірна грань $AB = b$ (див. рис. 1).

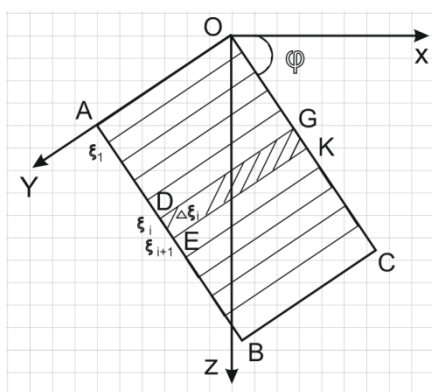


Рис.1. Схематичне зображення поверхні стінки греблі

Розв'язання. Із гідростатики відомо що модуль тиску визначають за формулою

$$P = Sh\gamma, \quad (1)$$

де S – площа стінки, γ питома вага рідини, h – відстань до вільної поверхні рідини.

Ця формула є правильною лише для горизонтального положення поверхні прикладання сили. Отже, для нашого випадку не підходить. Побудуємо прямокутну систему координат. Тут $OABC$ положення поверхні стінки греблі. Розділимо відрізок AB на n довільних частин і побудуємо прямокутники, як показано на рис.1. Площа

прямокутника $DEGK$ дорівнюватиме $a\Delta\xi_i$. Щоб визначити наближено величину тиску на цей прямокутник повернемо його навколо сторони DG так, щоб він набув горизонтального положення. Тоді до цієї площини можна застосувати формулу (1). Величина тиску рідини на прямокутник $DEGK$ приблизно дорівнюватиме $a\Delta\xi_i \cdot \gamma\xi_i \sin \alpha$. Тоді модуль тиску на стінку греблі буде наближено визначатися інтегральною сумою

$$P \approx a\gamma \sum_{i=0}^{n-1} \xi_i \sin \alpha \Delta\xi_i.$$

Для знаходження значення модуля тиску перейдемо до границі, за $\max \Delta\xi_i \rightarrow 0$, $n \rightarrow \infty$. Тоді

$$P = a\gamma \lim_{\substack{\max \Delta\xi_i \rightarrow 0 \\ n \rightarrow \infty}} \sum_{i=0}^{n-1} \xi_i \sin \alpha \Delta\xi_i \text{ й отримаємо}$$

$$P = a\gamma \int_0^b \xi \sin \alpha d\xi = \frac{a\gamma \sin \alpha}{2} \xi^2 \Big|_0^b = \frac{a\gamma \sin \alpha}{2} b^2.$$

Приклад. Визначимо гідростатичний тиск води на стінку гравітаційної бетонної греблі Гранд Діксенс у Швейцарії. Ширина її становить 700 м, а найбільша висота під'йому води – 284 м ($a = 700$, $b = 284$), кут $\varphi = \pi/2$, питому вагу води візьмемо $\gamma = 9800 \text{ Н/м}^3$. Отже,

$$P = \frac{a\gamma \sin \alpha}{2} b^2 = \frac{700 \cdot 9800}{2} \cdot 284^2 \sin \frac{\pi}{2} = 276650080000 \text{ Н} \approx 2,77 \cdot 10^8 \text{ кН}.$$

Висновок

За допомогою визначеного інтеграла виведено формулу для розрахунку значення модуля гідростатичного тиску води на стінку греблі.

Список використаних джерел:

- 1.Бевз В. Історія математики у фаховій підготовці майбутніх учителів: Монографія/ В.Г. Бевз. – К. НПУ імені Драгоманова, 2005. – 360 с.
- 2.Ластівка І.О. Вища математика: Навч. посібник / І.О. Ластівка, О.І. Безверхий, І.П. Кудзіновська. - К.: НАУ, 2018. - 452 с.

UDC: 338.47:656.7.025

APPLICATION OF LINEAR REGRESSION FOR ANALYSIS AND FORECASTING OF CARGO FLOWS IN UKRAINE

Shutishina Anastasia, Bezpalkiv Kornelia, Chernousova Anna

State University "Kyiv Aviation Institute", Kyiv

Scientific advisor Y.Liashenko,

PhD in Physics and Mathematics, Associate Professor

Key words: linear regressions, cargo flows, correlation coefficients.

Over the past decade, freight transportation in Ukraine has undergone significant changes due to economic shifts, infrastructure development, and geopolitical factors. To analyze and predict cargo flows effectively, regression analysis, particularly linear regression models, plays a crucial role. These models help identify key trends, assess influencing factors,

and generate reliable forecasts for decision-making in logistics and transportation planning. Accurate freight flow predictions are essential for optimizing transportation networks and reducing costs [1].

Regression represents the functional dependence, on average, of one random variable on another. The main task of regression analysis is to study the dependence between the resultant variable Y and the explanatory variable X, as well as to estimate the regression function [2]. The correlation coefficient r in statistics measures the strength of the relationship between X and Y. When these variables are related by a linear dependence, linear regression models can effectively analyze trends and make predictions [3].

Table 1

Year	Cargo Type	Volume (mln tons)	Transport	Main Region
2015	Grain	45	Railway	Odessa region
2016	Metal	30	Maritime	Mykolaiv region
2017	Oil	25	Road	Kyiv region
2018	Building Materials	50	Railway	Dnipropetrovsk region
2019	Machinery	10	Air	Kharkiv region
2020	Grain	55	Maritime	Odessa region
2021	Metal	35	Road	Zaporizhzhya region
2022	Oil	20	Railway	Kyiv region
2023	Building Materials	60	Maritime	Odessa region
2024	Machinery	15	Air	Lviv region

The table 1 contains data on cargo flows in Ukraine for the period from 2015 to 2024 [3]. The main parameters of cargo flows include year, type of cargo, volume in millions of tons, mode of transport, and main region.

Using the least squares method [1], the following equation has been obtained

$$y = 13.79x - 27552.33 \quad (1)$$

where: y is the cargo turnover (million tons), x is the year.

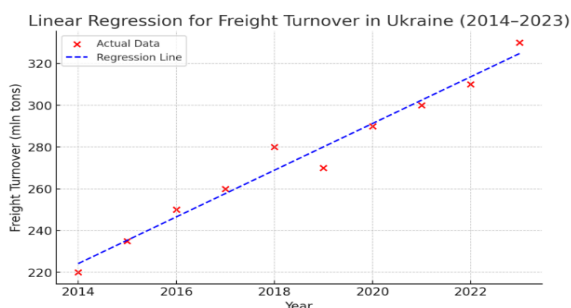


Fig 1. Graph of regression line

According to the equation of the straight line (1) a regression graph has been constructed and represented in Fig. 1.

Substituting $x=2025$ to the equation (1): $y_{2025} = 368.12$ we can make forecast for 2025.

Thus, the projected cargo turnover for 2025 is 368.1 million tons.

Similarly, substituting $x=2020$ to (1): $y_{2020} = 299.18$ we

can compare with cargo flows in 2020. Now, finding the difference: $\Delta y = y_{2025} - y_{2020} = 368.12 - 299.18 = 68.94$.

So, by 2025, the cargo turnover will have increased by 68.9 million tons compared to 2020.

Also, the year when cargo turnover exceeds 400 million tons can be found. We need to find $y > 400$: $400 = 13.79x - 27552.33$. Solving for x : $x = \frac{400 + 27552.33}{13.79} \approx 2027.31$.

Since x represents a year, we round up, meaning the cargo turnover will exceed 400 million tons in 2027.

This investigation used linear regression to analyze cargo flows in Ukraine, revealing a steady increase in freight turnover. Projections represent 368.1 million tons in 2025, surpassing 400 million tons by 2027. These insights aid logistics planning and infrastructure development.

References:

1. <https://science.lpnu.ua/uk/smeu/vsi-vypusky/vypusk-2-nomer-2-2020/logistychna-regresiya-yak-instrument-analizuvannya-vplyvu>
2. Higher Mathematics: manual. Theory of Probability and Elements of Mathematical Statistics / V.P. Denisiuk, V.M. Bobkov, L.A. Grishina – K.: NAU, 2013. 210-216 pages.
3. https://developers.google.com/machine-learning/crash-course/linear-regression?hl=uk&utm_source=chatgpt.com
4. https://robotdreams.cc/uk/blog/437-shcho-take-liniyna-regresiya?utm_source=chatgpt.com
5. https://www.easterneurope-ebm.in.ua/journal/19_2019/66.pdf

УДК 519.2

ЗАСТОСУВАННЯ БАЙЄСІВСЬКИХ ПІДХОДІВ ДЛЯ АНАЛІЗУ ДАНИХ

Северин Дар'я

Державний університет «Київський авіаційний інститут», Київ

Науковий керівник – Руслана Горідько, ст. викл.

Ключові слова: байєсівські аналізи даних, невизначеність, обмеження інформації, апіорні дані.

Успішне виконання сучасних досліджень вимагає застосування різноманітних методів, які можуть бути використані для розв'язання задач в умовах невизначеностей, відсутності необхідних об'ємів історичних даних стосовно розвитку досліджуваних процесів і т. ін. [1]. Зокрема, це стосується аналізу фінансових та інших типів ризиків, які зустрічаються практично в усіх галузях діяльності людини [2].

Байєсівські аналізи даних (БАД), засновані на теоремі Байєса, дозволяють оновлювати ймовірності подій на основі нової інформації, тобто передбачає її повторне використання при появі нових вимірів, фактів та експертних оцінок, дають можливість використовувати всю наявну інформацію з методом уточнення відомої апіорної інформації та оцінювання апостеріорних розподілів. БАД активно застосовуються в умовах невизначеності та змінних даних, можуть ґрунтуватись на коротких вибірках, на окремих фактах, експертних оцінках, окремих вимірах та ін. Більше того, методи БАД, як і більшість методів ймовірнісно-статистичної обробки даних, можуть бути успішно використані для адаптування структури і параметрів моделей до нових даних з метою підвищення адекватності моделей, що будуються. Коло задач, які можна розв'язувати байєсівськими методами, надзвичайно широке: задачі менеджменту ризиків різної природи, медичної, технічної та економічної діагностики в умовах наявності обмеженої інформації про досліджувані процеси та врахування в обчислювальних процедурах можливих невизначеностей, тобто факторів негативного впливу на досліджувані процеси та відповідні дані. Методи БАД, разом з нечіткою логікою, дають можливість враховувати невизначеності ймовірнісного та амплітудного типів і тим самим автоматично сприяють підвищенню якості рішень. Наприклад, у медицині байєсівські моделі допомагають діагностувати захворювання з огляду на результати нових аналізів, симптомів та історії пацієнта. У маркетингу вони допомагають передбачити поведінку клієнтів на основі попередніх покупок,

у страхуванні використовуються ймовірнісні моделі з метою оцінки ймовірності настання страхового випадку, в банках — для аналізу кредитних ризиків, також у прогнозуванні макроекономічних показників, таких як інфляція чи ВВП, в управлінні ризиками.

Байєсівські аналізи даних вимагають складних обчислень та спеціалізованого програмного забезпечення, що може ускладнити їх застосування, також фактор якості вихідних даних не завжди точний: якщо дані містять помилки або викиди, тобто, такі значення в наборі даних, які суттєво відрізняються від інших спостережень, тоді результати можуть бути ненадійними. Байєсівські моделі також можуть давати помилкові прогнози, якщо апіорні дані неточні.

Висновок

Сучасні аналітичні методи часто використовують байєсівські підходи, що дозволяє оновлювати апіорні ймовірності у міру надходження нової інформації.

Список використаних джерел:

1. Cooper G. F. The computational complexity of probabilistic inference using Bayesian belief networks // Artificial Intelligence. 1990. – 42, (2-3). – pp. 393-405
2. Застосування байєсівських мереж в системах аналізу даних / П.І. Бідюк, О.М. Трофимчук, О.І. Савенков // Екологічна безпека та природокористування: Зб. наук. пр. — К., 2011. — Вип. 8. — С. 191-212

УДК 528.8:528.7:528.4:528.06

ЗАСТОСУВАННЯ АПАРАТУ ТЕОРІЇ СВІДЧЕНЬ ДЕМПСТЕРА-ШЕЙФЕРА ДЛЯ ІНТЕГРУВАННЯ НЕПОВНИХ ТА НЕТОЧНИХ ДАНИХ

Софія Альперт

Державний університет «Київський авіаційний інститут», Київ

Ключові слова: теорія свідчень Демпстера-Шейфера, правило комбінації Демпстера, неточні дані, базові ймовірності

Вступ. На даний час відомі різні математичні та статистичні методи обробки даних для вирішення задач радіолокаційного спостереження та дистанційного зондування Землі (ДЗЗ), а саме: підвищення точності класифікування гіперспектральних супутникових зображень та комплексне оцінювання координат об'єктів. Дані методи детально проаналізовані у роботах Чанга С., Ерліха Р., Олсона К., Фулла В. та ін. [1-2]. Але методи інтегрування неповних, неточних та суперечливих даних, отриманих від різних датчиків чи експертів ще потребують подальшого вдосконалення. **Метою** роботи є дослідження можливостей застосування теорії свідчень Демпстера-Шейфера для вирішення завдань ДЗЗ та радіолокаційних задач.

Матеріали та методи. Теорія свідчень Демпстера-Шейфера є узагальненням теорії ймовірностей, використовується для об'єднання інформації, отриманої із різних джерел за наявності неточних вхідних даних. Тому методику Демпстера-Шейфера доцільно використовувати для класифікування гіперспектральних зображень, які містять багато спектральних каналів. Дана методика надає комплексну оцінку приналежності кожного пікселя супутникового зображення конкретному класу, інтегруючи інформацію з усіх спектральних каналів. Основним поняттям теорії свідчень є базова ймовірність (базова маса) [2]. Базова ймовірність може описати незнання та дає змогу розрізнити відсутність довіри та

недовіри. Також даний метод може бути використаний для побудови комплексної оцінки координат об'єкта для вирішення радіолокаційних задач, об'єднуючи інформацію, отриману із різних радіолокаційних станцій.

Результати. Проведений порівняльний аналіз класичної теорії ймовірностей та теорії свідчень. У теорії свідчень вводиться поняття основи аналізу Ω – це сукупність вихідних вичерпних та взаємно виключних гіпотез відносно стану об'єкта та всіх їх можливих сполучень. Ω містить 2^Q підмножин, де Q – число гіпотез. Базова

ймовірність (базова маса) задовольняє наступним умовам:

$$\begin{cases} m(\emptyset) = 0, \\ \sum_{A_i \subseteq A_0} m(A_i) = 1, \quad (i = 0, 1, 2, \dots), \end{cases} \quad (1)$$

де A_i ($i = 1, 2, \dots$) – підмножини множини A_0 , A_0 – обмежена множина. Для базової маси є необов'язковим, щоб $m(\Omega)$ дорівнювала “1”, а для класичної ймовірності: $p(\Omega) = 1$. Для базової ймовірності справедливе твердження: якщо $A \subset B$, то не обов'язково: $m(A) \leq m(B)$, а для класичної ймовірності обов'язково виконується умова: якщо $A \subset B$, то $p(A) \leq p(B)$. Для базової ймовірності не вимагається взаємозв'язок між $m(A)$ та $m(\bar{A})$, де $\bar{A}$ – доповнення до A . Для класичної ймовірності є обов'язковою умова: $p(A) + p(\bar{A}) = 1$. Частотний метод знаходження базових мас заснований на статистичному аналізі частот подій, що спостерігаються: $m(A) = \frac{N(A)}{N}$, (2)

A – підмножина гіпотез, що підтримуються спостереженням; N – загальна кількість спостережень; $N(A)$ – кількість разів, коли спостереження підтримували гіпотезу $A \subseteq \Omega$.

Нехай P – кількість незалежних джерел даних гіпотез; p – те джерело надає оцінку ймовірності гіпотези A_n у вигляді базової маси $m_p(A_n)$ або оцінку ймовірності сполучення гіпотез X у вигляді $m_p(X)$. Тоді правило комбінації Демпстера задає нову комбіновану базову ймовірність:

$$m_D(X) = \frac{1}{1-C} \sum_{\substack{X_1 \cap \dots \cap X_P = X \\ \forall (X \neq \emptyset) \in 2^Q}} \prod_{1 \leq p \leq P} m_p(X_p), \quad (3)$$

де коефіцієнт конфліктності $C \in [0, 1]$ та розраховується наступним чином:

$$C = \sum_{\substack{X_1 \cap \dots \cap X_P = \emptyset \\ \forall (X \neq \emptyset) \in 2^Q}} \prod_{1 \leq p \leq P} m_p(X_p). \quad (4)$$

Висновок

Проведено аналіз можливостей практичного застосування теорії свідчень Демпстера-Шейфера для вирішення задач обробки, зокрема, класифікування супутникових зображень та для вирішення задач у сфері радіолокації, а саме, побудови комплексної оцінки координат об'єкта.

Список використаних джерел:

1. Chang, C. I. (2013). Hyperspectral data processing: Algorithm design and analysis. Hoboken, N J: John Wiley and Sons, 1164 p.
2. Alpert, S. (2020). A new approach to applying the discount rule in hyperspectral satellite image classification. *Management of Development of Complex Systems*, 43, 76 – 82. [dx.doi.org/10.32347/2412-9933.2020.43.76-82](https://doi.org/10.32347/2412-9933.2020.43.76-82).