МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ПТІКІ'2025)

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції (зимовий форум)

ОДЕСА
2025

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 14 листопада 2025 р.

Матеріали конференції
(зимовий форум)

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings (winter forum). Odesa : International university, 2025, 96 p.

DOI https://doi.org/10.32837/11300.31326

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції (зимовий форум). Одеса : Міжнародний університет, 2025, 96 с.

Матеріали конференції представляють результати наукових досліджень у галузях інженерії програмного забезпечення, комп’ютерних наук і комп’ютерної інженерії, зокрема з питань моделювання та проєктування складних інформаційних систем, забезпечення кібербезпеки й захисту інформації, а також розвитку електронних комунікацій і радіотехнічних систем. Окрему увагу приділено сучасним освітнім технологіям та методикам навчання інформатики й інформаційних технологій. Збірник призначено для науковців, викладачів закладів вищої освіти, аспірантів і здобувачів, які здійснюють діяльність у сферах інженерії програмного забезпечення, комп’ютерних наук, комп’ютерної інженерії, кібербезпеки, електронних комунікацій і середньої освіти.

Матеріали публікуються в авторській редакції.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.
ПЕДЯШ В.В. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.
ЖИГУЛІН О.А. **–** д.е.н., проф., Міжнародний університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний університет, м.Одеса, Україна.

ISBN 978-617-554-718-2

ВІТАЛЬНЕ СЛОВО ПРЕЗИДЕНТА МІЖНАРОДНОГО УНІВЕРСИТЕТУ СЕРГІЯ ВАСИЛЬОВИЧА КІВАЛОВА

Шановні учасники Міжнародної науково-практичної конференції «Передові технології в інформаційно-комунікаційній інженерії», від імені всього колективу нашого університету щиро вітаю вас на святі науки – на святі майбутнього!

2025 рік – це рік нових викликів і нових можливостей для нашої країни. Незважаючи на випробування, які ми пройшли і ще проходимо, дух незламності та віра в світле майбутнє України залишаються незмінними. Наші захисники, яких ми глибоко шануємо, і надалі стоять на сторожі миру, щоб ми могли працювати, творити, розвиватися. Їм наша нескінченна вдячність і низький уклін.

Тема нашої конференції, як і раніше, присвячена найактуальнішим аспектам інформаційно-комунікаційної інженерії – сфері, що стала невід'ємною частиною повсякденного життя кожної людини. Ми живемо у світі, де цифрові технології визначають розвиток економіки, науки, культури та безпеки держави. Проте паралельно ростуть і загрози інформаційній безпеці, що вимагає від нас посиленої уваги до кіберзахисту та інноваційних підходів у цій сфері.

Особливо важливим для України сьогодні є застосування новітніх інформаційних технологій у процесі відбудови країни, її переходу на новий рівень технологічного і соціального розвитку. Ваша креативність, дослідницький запал і готовність впроваджувати інновації – це запорука успіху України на міжнародній арені та основа її технологічного суверенітету.

Я переконаний, що саме завдяки молоді, яка навчається і працює у Міжнародному університеті, ми здолаємо всі труднощі і разом досягнемо нових вершин у розвитку інформаційно-комунікаційної інженерії. Нехай на наших майбутніх конференціях лунатимуть не тривожні сигнали, а радісні пісні, а Україна буде вільною, сильною та процвітаючою державою!

Шановні учасники, бажаю вам плідної роботи, цікавих ідей, натхнення та наукових відкриттів! Нехай ваш внесок прискорить наш спільний шлях до Перемоги і миру. Віримо в Україну! Працюємо для Перемоги! Слава Україні!

Сергій КІВАЛОВ
Президент Міжнародного університету,
академік, доктор юридичних наук,
професор, заслужений юрист України,
Почесний громадянин міста Одеса

ВІТАЛЬНЕ СЛОВО РЕКТОРА МІЖНАРОДНОГО УНІВЕРСИТЕТУ КОСТЯНТИНА ВІКТОРОВИЧА ГРОМОВЕНКА

Шановні учасники Міжнародної науково-практичної конференції «Передові технології в інформаційно-комунікаційній інженерії»! Від імені усього колективу Міжнародного університету щиро вітаю вас у стінах нашого закладу!

Одеса завжди була центром науки і культури, і попри всі важкі випробування, які принесла нам війна, залишається таким надійним осередком знань та інновацій. Ми пишаємося тим, що у цьому році нам вдалося укласти низку важливих договорів про співпрацю з провідними підприємствами інформаційно-комунікаційної галузі. Ці партнерства відкривають для наших здобувачів і науковців широкі можливості для практичної реалізації своїх знань, проходження стажувань, участі в спільних проєктах і дослідженнях. Завдяки цим зв'язкам ми поглиблюємо зв'язок між освітою і реальним сектором економіки, створюючи міцний фундамент для розвитку інновацій та підготовки конкурентоспроможних фахівців.

Наш факультет кібербезпеки, програмної інженерії та комп'ютерних наук, створений трохи більше трьох років тому, впевнено відповідає викликам часу, задовольняючи потребу у висококваліфікованих ІТ-фахівцях. Ми пишаємося тим, що пропонуємо сучасні спеціальності на усіх рівнях вищої освіти, які користуються попитом серед молоді. Наш університет і наш факультет стали другим домом для все більшої кількості талановитих студентів та аспірантів, які вже сьогодні формують фундамент технологічного майбутнього нашої країни.

Сьогоднішня конференція є важливим майданчиком для обміну найновішими науковими здобутками в сферах комп'ютерних наук, кібербезпеки, захисту інформації та програмної інженерії, що актуально не лише для України, а й для міжнародної спільноти.

Бажаю всім учасникам плідної роботи, нових ідей і вагомих наукових результатів! Наснаги, терпіння та здоров'я вам та вашим близьким. Віримо в наших захисників, віримо у Збройні Сили України! Наближаємо Перемогу разом! Слава Україні!

Костянтин ГРОМОВЕНКО
Ректор Міжнародного університету, доктор юридичних наук, професор, заслужений юрист України

ЗМІСТ

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАТИКА

УДК 621.314
DOI: https://doi.org/10.32837/11300.31343

Русу Олександр Петрович, к.т.н.
Міжнародний університет
shurusu@ukr.net
Цуркан Леонід Леонідович
здобувач 2 курсу другого (магістерського) рівня
зі спеціальності 123 Комп'ютерна інженерія
Міжнародний університет

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗРАХУНКУ ПЕРЕТВОРЮВАЧІВ НАПРУГИ КОМП'ЮТЕРНОГО ОБЛАДНАННЯ

Анотація. *У роботі представлено підхід до створення програмного забезпечення для моделювання та розрахунку імпульсних перетворювачів напруги, що використовуються у комп'ютерних системах. Застосовано технологію динамічного зв'язку програмних модулів, яка дає змогу розробляти гнучкі програмні рішення без необхідності створення окремого інтерфейсу користувача. Розроблена бібліотека підтримує основні типи схем перетворювачів та може бути інтегрована у системи автоматизованого проєктування комп'ютерного обладнання. Показано, що запропонований підхід забезпечує мінімальні часові та фінансові витрати при збереженні точності розрахунків.*

Перетворювачі електричної енергії є ключовим елементом сучасних комп'ютерних систем, забезпечуючи живлення компонентів із різними рівнями напруги.

Для зменшення енергоспоживання та підвищення ефективності в комп'ютерному обладнанні використовуються імпульсні перетворювачі, які працюють на високих частотах комутації.

Традиційно їхній розрахунок виконується за допомогою спеціалізованих програм [1, 2], проте такі рішення часто не передбачають швидкої інтеграції з іншими середовищами автоматизованого проєктування.

Одним із можливих способів спрощення розробки є використання технології динамічного зв'язку програмних модулів (Dynamic Link Library, DLL), яка широко застосовується в операційних системах Windows.

Ця технологія забезпечує можливість багаторазового використання одного й того самого коду різними програмами без потреби дублювання ресурсів, що зменшує навантаження на оперативну пам'ять і спрощує оновлення програмних компонентів.

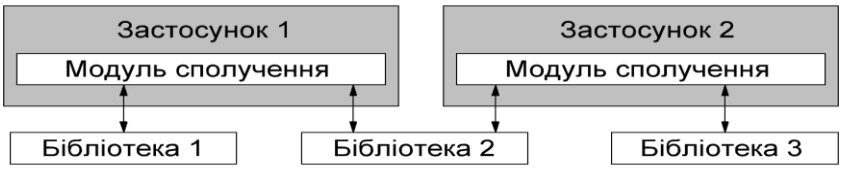


Рисунок 1 – Технологія динамічно-зв'язаних бібліотек

Розроблена динамічно-зв'язана бібліотека реалізує узагальнену математичну модель для восьми найбільш поширених схем імпульсних перетворювачів: понижувальної (рис. 2, *а*), підвищувальної (рис. 2, *б*), інвертувальної (рис. 2, *в*), схем із прямим (рис. 2, *д*) і

зворотним (рис. 2, г) увімкненням діода, півмостової (рис. 2, *ж*), мостової (рис. 2, *з*) та схеми з виводом середньої точки трансформатора (рис. 2, *е*).

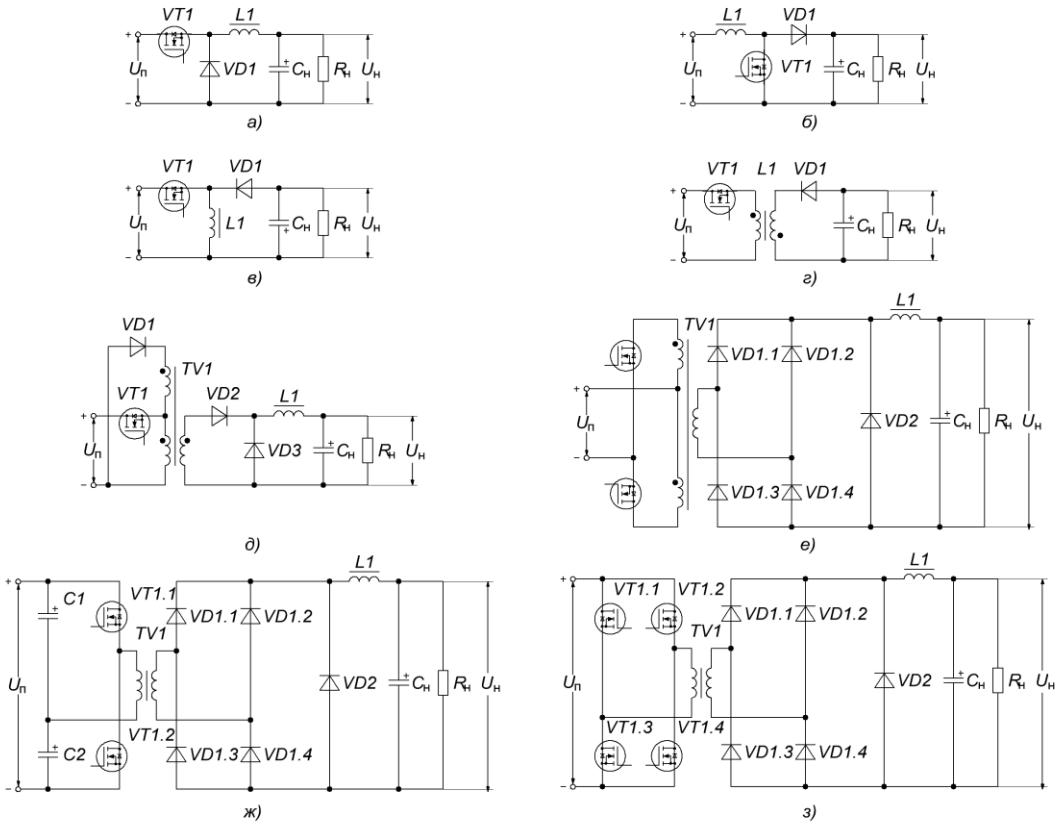


Рисунок 2 – Схеми перетворювачів

Бібліотека враховує режими безперервного та розривного струму в дроселі, що забезпечує універсальність розрахунків. Користувач може отримати дані щодо напруг, струмів, втрат потужності, ефективності та параметрів магнітних компонентів.

Основна увага під час розроблення була приділена оптимізації алгоритму обчислень. На початковому етапі проводиться перевірка коректності вхідних даних, після чого відбувається визначення режиму роботи перетворювача – стабілізації або стеження. Для кожного режиму формуються відповідні співвідношення, які описують процес накопичення та повернення енергії в магнітному колі.

Отримані результати дозволяють визначити миттєві, середні та діючі значення електричних параметрів для всіх елементів схеми. Перевагою використання бібліотеки є можливість її прямої інтеграції у середовища типу TechProjects або інші CAD-системи без розроблення додаткового інтерфейсу.

Висновки. Розроблене програмне забезпечення реалізує універсальний підхід до моделювання та розрахунку імпульсних перетворювачів напруги. Використання технології динамічного зв’язку дозволило створити гнучкий програмний інструмент, який поєднує точність розрахунків і простоту інтеграції з системами автоматизованого проєктування. Запропонована бібліотека може бути основою для подальшого розвитку інтелектуальних програмних модулів, здатних автоматично підбирати оптимальні параметри перетворювачів залежно від вимог до ефективності, габаритів та вартості.

Література:

1. Zehendner M., Ulmann M. Power Topologies Handbook. Texas Instruments, 2016. 216с.

2. Kadatskyy A.F., Rusu A.P. Determination of the necessary inductor core dimensions for switching electrical energy converters. *Наукові праці ОНАЗ ім. О.С. Попова*. 2018. №1. С.125-134.

УДК 005.33,004.8
DOI: https://doi.org/10.32837/11300.31337

Жигулін Олександр Андрійович
д.е.н., професор кафедри інформаційних технологій
Міжнародний університет, м. Одеса
zhigulin998@gmail.com
Шестаков Микола Миколайович
здобувач 2 курсу другого (магістерського) рівня
спеціальності 121 Інженерія програмного забезпечення
Міжнародний університет, м. Одеса
msestakov78@gmail.com

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЗАБЕЗПЕЧЕННІ СТАЛОГО РОЗВИТКУ БІЗНЕСУ

Анотація. *Розглянуто використання інформаційних технологій в забезпеченні сталого розвитку бізнесу. Як предмет практичного рішення запропоновано впровадження асистентів на базі штучного інтелекту. Саме цей інструмент сприяє покращенню трьох основних аспектів сталого розвитку – це економічний, соціальний та екологічний. А також важливо відмітити, що він може запроваджуватись за допомогою ноу-код/лоу-код середовищ, що робить його більш дружнім для посереднього користувача.*

Сталий розвиток бізнесу передбачає збалансоване поєднання прибутковості, екологічної відповідальності та соціальної якості [1]. В такому контексті інформаційні технології перестають бути просто інструментами, натомість, вони здатні перетворюватись на повноцінні рішення, які будуть актуальними, гнучкими та універсальними. Помічники на базі ШІ і є такими рішеннями. Це програмні агенти, які використовують штучний інтелект, обробку природної мови (NLP), машинне навчання (ML) та великі мовні моделі (LLM) [2]. Вони здатні навчатися на базі корпоративних даних, сприймати запити природною мовою, та опрацьовувати їх, брати на себе певний перелік рутинних задач та допомагають змістити фокус витрати ресурсів компанії на вирішення більш фундаментальних задач. Поєднання всього вищеперерахованого створює надійний, дружній та ефективний університет.

Згадуючи економічний аспект сталого розвитку бізнесу, можна відмітити, що впровадження ШІ-асистента створюють всі необхідні умови для звільнення часу від рутинних операцій, скорочення циклів погоджень та помилок, на які може впливати людський фактор. Також значно пришвидшуються підготовки договорів, звітів, призначення зустрічей та подібне. Це дозволяє набагато ефективніше використовувати один із найважливіших ресурсів, який необхідний для розвитку бізнесу – час.

Основною перевагою ШІ-асистента в екологічному напрямі є дематеріалізація процесів. Це пояснюється переведенням договорів, актів та іншої документації у повністю безпаперовий цикл. Також, в залежності від специфіки бізнесу віртуальні помічники можуть напряму сприяти економії енергетичних ресурсів та загального енергоспоживання [3], або ж зменшення викидів вуглекислого газу в атмосферу [4]. Використання такого рішення відкриває нові можливості для зменшення екологічну сліду компанії.

Соціальний вимір посилюється завдяки доступності такого помічника 24/7, персоналізованій комунікації практично на всіх мовах світу, підвищенні продуктивності співробітників та довіри клієнтів, партнерів та інвесторів до компанії.

Ще однією перевагою є те, що знання коду не є обов'язковою опцією для створення таких віртуальних помічників. Наразі вже можна обирати лоу-код, або навіть ноу-код середовища, які дозволяють створювати структуру агента. Варто виділити три найпопулярніших рішення, які дозволяють інтегрувати та використовувати надзвичайно різноманітну кількість сервісів, якими користується велика кількість бізнесів. Це Zapier, Make або n8n [5]. Ці середовища роблять поріг використання таких помічників дуже низьким

та дозволяють навіть керівнику компанії самостійно працювати з ними і вже автоматизовувати та оптимізовувати базові робочі процеси без залучення нових працівників. Отже це економія часу та грошей для підприємства.

Механізм дії асистента базується на кількох зв'язках. По-перше, управління знаннями: семантичний пошук у внутрішніх документах, відповіді на питання з посиланнями на джерела і шаблони, що зменшує дублювання робіт та прискорює прийняття рішень. По-друге, автоматизація процесів: погодження рахунків, формування актів, та ініціювання завдань у суміжних системах. По-третє, підтримка рішень: узагальнення даних із BI, what-if-моделювання попиту і навантаження, пояснення аномалій та ризиків. Далі це моніторинг і звітність: збір показників, виявлення прогалин у даних, генерація текстових розділів, що спрощує дотримання стандартів прозорості. Також клієнтський досвід: швидкі та релевантні відповіді, проактивні підказки й персоналізація комунікації. І ще один механізм – це розвиток персоналу: навчання, адаптивні інструкції та діагностика прогалин у компетенціях.

Впровадження асистента варто починати з чітких бізнес-кейсів. Критично важлива підготовка даних: опис джерел, правила доступу, політики приватності, механізми журналювання дій асистента та контроль якості. Архітектура повинна передбачати інтеграції з ключовими системами, централізований моніторинг роботи й можливість швидкого розширення на нові процеси. Безпека та етика — обов'язкові умови: шифрування, контроль доступів та збереження ролі людини в контурі прийняття рішень.

Можна зробити висновок, що асистенти на базі ШІ — це практичний каталізатор сталого розвитку бізнесу. Вони збалансовують економічну ефективність, екологічну відповідальність і соціальну якість сервісу, якщо будуються на якісних даних, впроваджуються з урахуванням безпеки та етики і доповнюють, а не замінюють відповідальність людей у критичних рішеннях.

Література:

1. Чому сталий розвиток важливий для бізнесу? URL: https://tms.ua/blog/chomu-stalyj-rozvytok-vazhlyvyj-dlia-biznesu/

2. ШІ-асистенти: що це таке, як працюють, чому стають популярними. URL: https://mmr.ua/longreads/digital/shi-asystenty-shho-cze-take-yak-praczyuyut-i-chomu-stayut-populyarnymy/

3. DeepMind AI reduces energy used for cooling Google data centers by 40%. URL: https://blog.google/outreach-initiatives/environment/deepmind-ai-reduces-energy-used-for/?utm_source=chatgpt.com

4. AI Case Study. URL: https://www.bestpractice.ai/ai-case-study-best-practice/ups_saves_over_10_million_gallons_of_fuel_and_up_to_%24400m_in_costs_annually_with_advanced_telematics_and_analysis?utm_source=chatgpt.com

5. Порівняння Zapier, Make і n8n. URL: https://dou.ua/forums/topic/52030/

УДК 004.89:004.912
DOI: https://doi.org/10.32837/11300.31327

Азовський А. І., студент,
Педяш В.В., к.т.н., доцент,
Міжнародний університет,
zlokva@gmail.com

ПРОГРАМНА РЕАЛІЗАЦІЯ НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ ДЛЯ АВТОМАТИЗОВАНОГО АНАЛІЗУ ТЕКСТОВИХ ДАНИХ

Анотація. *Робота присвячена розробці та дослідженню нейромережевих моделей для класифікації емоцій у текстових повідомленнях. Запропоновано архітектуру на основі двонаправленої LSTM з механізмами регуляризації. Проведено експериментальне дослідження на збалансованому датасеті з шести класів емоцій. Досягнуто високу точність класифікації 95,18%, що підтверджує ефективність запропонованого підходу для задач автоматизованого аналізу тональності тексту.*

Автоматизований аналіз текстових даних є одним з найважливіших напрямків сучасного штучного інтелекту та обробки природної мови. Розпізнавання емоцій у текстових повідомленнях знаходить застосування в численних галузях, включаючи аналіз соціальних мереж, обробку відгуків клієнтів, моніторинг психологічного стану користувачів та створення інтелектуальних діалогових систем [1, 2]. В останні роки глибокі нейронні мережі продемонстрували вражаючі результати в задачах обробки природної мови, значно перевершуючи традиційні методи машинного навчання. Рекурентні нейронні мережі, зокрема архітектури на основі LSTM (довга короткочасна пам’ять), показали високу ефективність у моделюванні послідовностей та захопленні контекстуальних залежностей у текстових даних [3]. Особливою перевагою LSTM є здатність до збереження довготривалих залежностей завдяки механізму воріт, що дозволяє мережі вибірково запам’ятовувати або забувати інформацію залежно від її релевантності для конкретної задачі. Актуальність дослідження зумовлена зростаючою потребою в автоматизованих системах аналізу емоційного забарвлення текстів для моніторингу громадської думки, підтримки клієнтів та аналізу поведінки користувачів онлайн-платформ.

Метою даної роботи є розробка та проведення експериментального аналізу продуктивності ефективної архітектури нейронної мережі для класифікації емоцій у текстових повідомленнях англійською мовою на збалансованому датасеті.

Для вирішення поставленої задачі використовувався збалансований датасет emotion-balanced, що містить 17952 текстових повідомлення, рівномірно розподілені між шістьма класами емоцій: сум (sadness), радість (joy), кохання (love), гнів (anger), страх (fear) та здивування (surprise). Кожен клас представлений 2992 записами, що становить 16,67% від загальної кількості даних. Така збалансованість датасету є критично важливою для навчання об’єктивної моделі, що не має схильності до переважного розпізнавання певних класів. Статистичний аналіз показав, що середня довжина текстових повідомлень становить 16,9 слів, при цьому довжина варіюється від 2 до 48 слів, що характерно для коротких повідомлень у соціальних мережах та чатах. Медіанне значення довжини тексту становить 16 слів, що свідчить про відсутність значних викидів у розподілі довжин повідомлень. Аналіз лексичного різноманіття датасету виявив широкий спектр емоційно забарвлених слів та виразів, що дозволяє моделі навчитися розпізнавати різноманітні способи вираження емоцій.

Запропонована архітектура нейронної мережі базується на поєднанні шару вбудовування, двонаправленої LSTM та механізмів регуляризації. На першому етапі обробки текст токенізується з побудовою словника обсягом до 10000 найчастіших слів, після чого послідовності вирівнюються до максимальної довжини 100 токенів. Використання обмеженого словника дозволяє зменшити розмірність простору ознак та зосередитися на

найбільш частотних та інформативних словах, при цьому рідкісні слова замінюються спеціальним токеном поза словником. Шар вбудовування розмірністю 128 перетворює кожне слово на щільний вектор, що дозволяє мережі вивчати семантичні залежності між словами та групувати семантично близькі слова в багатовимірному просторі. Ключовим компонентом архітектури є двонаправлений LSTM шар з 64 нейронами, який обробляє послідовність у обох напрямках, що дозволяє враховувати як попередній, так і наступний контекст для кожного слова [4]. Двонаправленість є критично важливою для розуміння емоційного контексту, оскільки емоційне значення слова часто залежить як від попередніх, так і від наступних слів у реченні.

Після LSTM шару застосовується операція глобального максимального об'єднання для виділення найбільш значущих ознак з усієї послідовності, що дозволяє зменшити розмірність представлення та зосередитися на ключових емоційних маркерах у тексті. Для запобігання перенавчанню використовується відключення з коефіцієнтом 0,5 після LSTM шару та додаткове відключення перед вихідним шаром, що випадково відключає половину нейронів під час навчання та змушує мережу навчатися більш надійним та узагальненим ознакам. Після шару об'єднання додається повнозв'язний шар з 64 нейронами та функцією активації ReLU, що дозволяє моделі вивчати нелінійні комбінації виділених ознак. Вихідний шар містить 6 нейронів з функцією активації softmax для багатокласової класифікації, що забезпечує ймовірнісну інтерпретацію результатів класифікації. Загальна архітектура реалізує ієрархічний підхід до вивчення текстових представлень: від окремих слів через контекстуалізовані представлення послідовностей до агрегованих ознак документа.

Навчання моделі проводилося з використанням оптимізатора Адам та функції втрат категоріальної перехресноїентропії. Датасет було розділено на навчальну (80%) та тестову (20%) вибірки зі збереженням стратифікації по класах, що забезпечує однаковий розподіл емоцій у обох вибірках. Застосовувались механізми раннього зупинення з терпимістю 5 епох та динамічного зменшення швидкості навчання для оптимізації процесу навчання. Раннє зупинення моніторить функцію втрат на валідаційній вибірці та зупиняє навчання, якщо не спостерігається покращення протягом 5 послідовних епох, при цьому відновлюються ваги моделі з найкращими показниками. Динамічне зменшення швидкості навчання зменшує швидкість навчання вдвічі, якщо валідаційні втрати не покращуються протягом 3 епох, що дозволяє моделі більш точно налаштовуватися при наближенні до оптимуму. Розмір пакета становив 32 записи, максимальна кількість епох навчання була обмежена 50, проте завдяки ранньому зупиненню фактичне навчання завершилось після 8 епох. Графік динаміки навчання, представлений на рисунку 1, демонструє стабільне зростання точності на навчальній вибірці з початкових 86% до 96% та на валідаційній вибірці з 94,5% до 95%, що свідчить про ефективне навчання без ознак значного перенавчання.

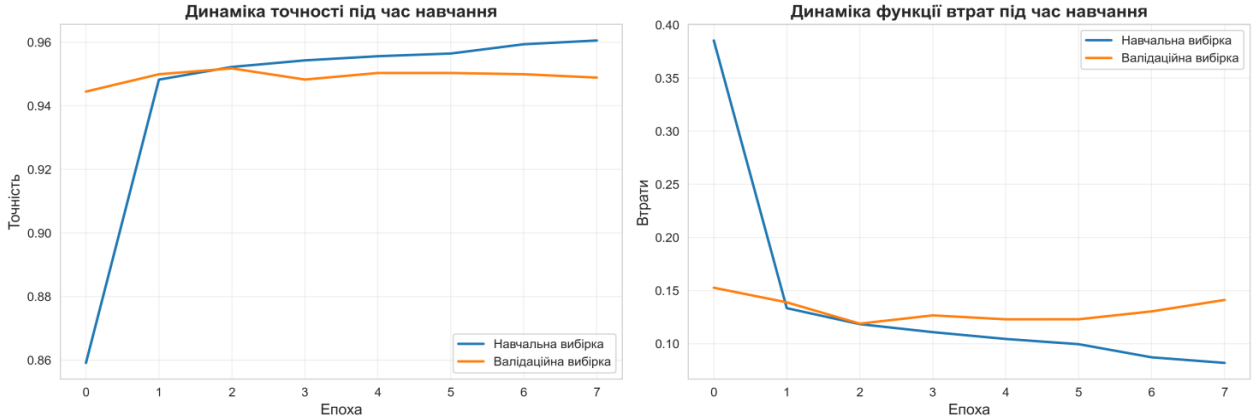


Рисунок 1 – Динаміка точності та функції втрат під час навчання моделі

Після завершення навчання модель була оцінена на тестовій вибірці обсягом 3591 запис. Результати оцінки продуктивності моделі представлені в таблиці 1. Загальна точність

класифікації становить 0,9518 (95,18%), що є високим показником для задачі багатокласової класифікації емоцій. Зважені метрики точності (0,9536), повноти (0,9518) та F1-міри (0,9515) також демонструють збалансовану продуктивність моделі без значного дисбалансу між типами помилок. Висока збалансованість між точністю та повнотою свідчить про те, що модель однаково добре виявляє істинні випадки кожної емоції та уникає хибно-позитивних класифікацій. Аналіз метрик за окремими класами показує, що найкраще розпізнаються емоції суму (F1=0,9730) та кохання (F1=0,9640), що пояснюється їх чіткими лексичними маркерами та відносно однорідним способом вираження в тексті.

Таблиця 1 – Результати оцінки продуктивності моделі класифікації емоцій

Клас	Точність	Повнота	F1-міра
sadness	0,9965	0,9505	0,9730
joy	0,9906	0,9191	0,9535
love	0,9328	0,9973	0,9640
anger	0,9351	0,9726	0,9535
fear	0,9543	0,8723	0,9115
surprise	0,9121	0,9987	0,9534

Дещо нижчі показники для класу страху (F1=0,9115) пов’язані з нижчим значенням повноти (0,8723), що вказує на труднощі моделі у виявленні всіх випадків цієї емоції, можливо, через її змішування з іншими негативними емоціями. Детальний аналіз помилково класифікованих випадків страху показав, що 12,77% випадків страху були помилково розпізнані як інші емоції, причому найчастіше як здивування (8,76%) та гнів (3,68%), що узгоджується з психологічними дослідженнями про близькість цих емоційних станів у рамках моделі негативних емоцій високої активації. Матриця помилок показує, що найбільша точність досягається для класу кохання (99,73% правильно класифікованих випадків) та здивування (99,87%), тоді як найбільше плутанини спостерігається між емоційно близькими станами, зокрема між радістю та коханням (6,82% випадків радості класифіковано як кохання), а також між страхом та здивуванням (8,76% випадків страху класифіковано як здивування). Це узгоджується з психологічними дослідженнями про близькість цих емоційних станів [5].

Особливо цікавими є показники для емоції кохання, яка демонструє найвищу повноту (0,9973), що означає практично повне виявлення всіх випадків цієї емоції, хоча точність дещо нижча (0,9328) через деяку кількість хибно-позитивних класифікацій. Аналіз показав, що 0,27% випадків радості та 0,33% випадків гніву були помилково класифіковані як кохання, що може бути пов’язано з використанням схожих інтенсивних емоційних виразів у текстах. Для емоції здивування спостерігається найвища повнота (0,9987), але дещо нижча точність (0,9121), що вказує на тенденцію моделі класифікувати деякі інші емоції як здивування, особливо ті випадки, що містять вигукові конструкції або незвичайні словосполучення.

Аналіз динаміки функції втрат демонструє швидку збіжність алгоритму навчання. На навчальній вибірці функція втрат знизилась з початкових 0,38 до 0,08 за 8 епох, при цьому на валідаційній вибірці спостерігається стабільна поведінка в діапазоні 0,12-0,14 після перших епох. Невелика різниця між навчальними та валідаційними втратами свідчить про хорошу узагальнюючу здатність моделі та ефективність застосованих методів регуляризації через відключення. Найбільше зменшення втрат відбувається протягом першої епохи, коли модель швидко навчається основним закономірностям у даних, після чого процес навчання уповільнюється та модель починає налаштовуватися на більш тонкі патерни. Загальна кількість параметрів моделі становить близько 1,4 мільйона, що є прийнятним для сучасних обчислювальних платформ та дозволяє проводити як навчання, так і висновування на стандартному обладнанні без необхідності використання спеціалізованих графічних процесорів. Час навчання однієї епохи складав приблизно 45 секунд на процесорі Intel Core

i7, а час класифікації одного повідомлення в режимі висновування становить менше 10 мілісекунд, що дозволяє використовувати модель у реальному часі.

Порівняння з базовими підходами показує значну перевагу запропонованої архітектури. Традиційні методи на основі мішка слів з класифікаторами методу опорних векторів або наївним Байєсом зазвичай досягають точності 75-82% на подібних задачах, тоді як проста рекурентна мережа без двонаправленості та відключення показує точність близько 88-90%. Використання двонаправленої LSTM підвищило точність на 3-4% порівняно з однонаправленою версією, а застосування механізмів регуляризації додало ще 1-2% точності, запобігаючи перенавчанню. Порівняння розподілу помилок між класами виявило, що модель демонструє більш рівномірну продуктивність порівняно з базовими підходами, які часто мають значну варіативність точності між різними класами емоцій.

Проведене дослідження продемонструвало високу ефективність архітектури на основі двонаправленої LSTM для задачі класифікації емоцій у текстових повідомленнях. Досягнута точність 95,18% перевищує результати багатьох базових підходів та підтверджує доцільність використання рекурентних архітектур для моделювання послідовних залежностей у тексті. Збалансованість метрик точності та повноти свідчить про відсутність значного зміщення моделі до певних класів. Використання механізмів регуляризації та раннього зупинення забезпечило стабільне навчання без перенавчання, що критично важливо для практичного застосування моделі на нових даних. Запропонована архітектура може бути адаптована для інших задач аналізу тональності та емоцій у текстах різними мовами.

Перспективними напрямками подальших досліджень є експериментування з більш сучасними архітектурами на основі трансформерів, такими як BERT та GPT, які показують ще вищі результати в задачах обробки природної мови завдяки механізмам самоуваги та попередньому навчанню на великих корпусах текстів, а також розширення датасету для включення більш складних емоційних станів та багатомовних текстів. Додатково планується розробка механізмів пояснюваності рішень моделі через методи уваги та візуалізації активацій, що підвищить довіру до системи при її впровадженні в реальні застосування. Також доцільним є дослідження ефективності моделі на незбалансованих датасетах та в умовах наявності шуму в даних, що відповідає реальним сценаріям використання. Перспективним напрямком є також розробка багатозадачних моделей, які одночасно визначають емоцію та її інтенсивність, а також виділяють ключові слова та фрази, що найбільше впливають на емоційне забарвлення тексту.

Література:

1. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding / J. Devlin, M.-W. Chang, K. Lee, K. Toutanova // Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. – Vol. 1 (Long and Short Papers). – Minneapolis, MN, USA : Association for Computational Linguistics, 2019. – P. 4171-4186.

2. Liu B. Sentiment Analysis and Opinion Mining. – San Rafael : Morgan & Claypool Publishers, 2012. – 167 p.

3. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge, MA : MIT Press, 2016. – 800 p.

4. Hochreiter S., Schmidhuber J. Long Short-Term Memory / S. Hochreiter, J. Schmidhuber // Neural Computation. – 1997. – Vol. 9, No. 8. – P. 1735-1780.

5. Ekman P. An Argument for Basic Emotions / P. Ekman // Cognition & Emotion. – 1992. – Vol. 6, No. 3-4. – P. 169-200.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

УДК 519.688:004
DOI: https://doi.org/10.32837/11300.31346

Стрелковська І.В., д.т.н., професор;
Салоїд В.О., магістр 2 курсу навчання зі спеціальності
121 Інженерія програмного забезпечення
Міжнародний університет
i.strelkovskaya@mgu.edu.ua,
viacheslavsaloid@gmail.com

СПЛАЙН-АПРОКСИМАЦІЯ РОЗПІЗНАВАННЯ ЖЕСТІВ РУК НА БАЗІ OPENCV

Анотація. *Розглянуто основні методи розпізнавання жестів рук та проведено аналіз їхніх можливостей щодо виявлення та класифікації конфігурацій жестів рук. Запропоновано використання комп'ютерного зору на базі бібліотеки OpenCV мови Python для розпізнавання конфігурацій жестів рук. Для підвищення точності розпізнавання контурів жестів рук використано сплайн-апроксимацію з кубічними сплайн-функціями. Отримані результати можуть бути використані для інтерфейсів людино-машинної взаємодії, систем жестового управління та застосуваннях доповненої та віртуальної реальності.*

У сучасних умовах розвитку комп'ютерного зору та штучного інтелекту все більшої уваги набувають системи, здатні розпізнавати жести рук людини. Такі системи мають широке застосування від інтерфейсів безконтактного керування та інтерактивних мультимедійних рішень до допоміжних технологій для людей з обмеженими можливостями.

Розпізнавання жестів рук – це задача, яка направлена на визначення, який саме жест виконує людина, на основі візуальних даних. Класифікація жестів технічними засобами – це ключова технологія в таких областях, як інтерфейси людина-комп'ютер, віртуальна реальність та робототехніка. Серед основних методів розпізнавання жестів рук можна виділити метод сенсорних пристроїв [1], що використовує рукавички з вбудованими датчиками, які фіксують положення, рухи пальців рук та формують дані для подальшої обробки. Використання інфрачервоних камер [1], які фіксують жести рук у тривимірному просторі, дозволяють отримувати тривимірні моделі жестів рук, але такий підхід також потребує спеціального обладнання та може бути досить витратним. Використання систем розпізнавання образів на базі комп'ютерного зору, дозволяють розв'язувати різні задачі інтерпретації зображень та відео з метою отримання необхідної інформації, при цьому, без необхідності додаткових сенсорів та обладнання.

Серед найпопулярніших бібліотек, що використовуються для розробки систем розпізнавання жестів використовуються OpenCV, MediaPipe, TensorFlow [2-4]. Використання бібліотеки комп'ютерного зору OpenCV (Open Source Computer Vision Library) [2] для розпізнавання жестів рук забезпечує широкий набір інструментів для обробки зображень та відео, включаючи детектування контурів, відстеження об'єктів і аналіз жестів.

Однак, ефективність вищерозглянутих систем розпізнавання жестів значною мірою залежить від точності апроксимації форми та руху руки, що потребує використання гнучких математичних методів обробки контурів та траєкторій руху.

В якості математичного методу для обробки візуальних даних розпізнавання жестів запропоновано використання сплайн-апроксимації [5], яка дозволить за допомогою лінійних та кубічних сплайн-функцій виконати відтворення жестів, при цьому зменшить

обсяг обчислень та підвищити точність та стійкість до шумів під час розпізнавання жестів.

Метою даної роботи є використання сплайн-апроксимації на базі кубічних сплайнів та комп'ютерного зору на базі бібліотеки OpenCV мови Python для підвищення точності розпізнавання жестів рук.

Розглянемо використання бібліотеки комп'ютерного зору OpenCV мови Python для розпізнавання контуру руки та подальшої апроксимації жесту руки за допомогою розробленого алгоритму, показаного на рис. 1.

Рисунок 1 - Розроблений алгоритм розпізнавання жестів рук за допомогою бібліотеки комп'ютерного зору OpenCV

Використовуючи бібліотеку комп'ютерного зору OpenCV розроблено код OpenCV на Python для функціонування алгоритму розпізнавання жестів рук, показаного на рис. 1, а саме фрагменту визначення контуру руки та апроксимації цього контуру.

В даному випадку, фрагмент коду OpenCV для розпізнавання жестів рук має наступний вигляд [2]:

```
import cv2
import numpy as np
from scipy.interpolate import CubicSpline
# Uploading images
image = cv2.imread('hand.jpg')
# Converting images to grey scale
gray = cv2.cvtColor(image, cv2.COLOR_RGB2GRAY)
# Image binarisation
_, thresh = cv2.threshold(gray, 100, 255, cv2.THRESH_BINARY)
# Find contours in an image
contours, _ = cv2.findContours(thresh, cv2.RETR_EXTERNAL, cv2.CHAIN_APPROX_SIMPLE)
# Contours shown in green
contour_image = image.copy()
cv2.drawContours(contour_image, contours, -1, (0, 0, 255), 2)
```

Даний фрагмент коду OpenCV виконує, згідно алгоритму, показаному на рис. 1, перший етап алгоритму виконує завантаження зображення та його перетворення у градації сірого Color Space Conversion cv2.cvtColor(image, cv2.COLOR_RGB2GRAY) та бінаризація зображення Image Thresholding cv2.threshold(gray, 100, 255, cv2.THRESH_BINARY). Наступним

етапом є визначення контурів на бінаризованому зображенні cv2.findContours(thresh, cv2.RETR_EXTERNAL, cv2.CHAIN_APPROX_SIMPLE).

Результат визначення контуру показано на рис. 2.

Неважко бачити, що визначений контур не описує жест руки та має значні похибки, які можуть бути зменшені за рахунок використання сплайн-апроксимації на базі лінійної або кубічної сплайн-функції.

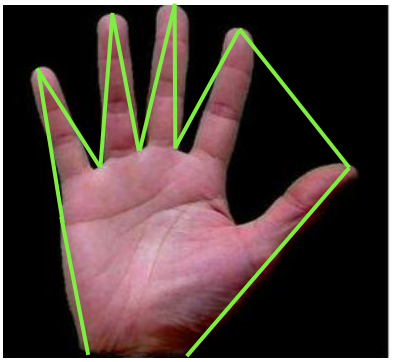


Рисунок 2 − Результат визначення контуру зображення

Розглянемо сплайн-апроксимацію контуру зображення на базі кубічного сплайну.

Кубічний сплайн на проміжку [0;T]] є кусково-неперервною функцію, яка визначає кубічний сплайн. Нехай на відрізку [0;T] задані значення пікселів зображення жесту руки $f(x)$. Розіб'ємо цей відрізок [0;T] точками Δ: $0 = x_0 < x_1 < ... < x_N = T$ на проміжки $[x_i; x_{i+1}]$, $i = \overline{0, N-1}$, на кожному з яких побудуємо кубічний сплайн $S_3(f;x)$, який задовольняє умовам [6-7]

$$S_3(f;x_i) = f_i,\ i = 0,\ 1\ \ ...\ \ N,\ \ S''(f;0) = f''(0),\ S''(f;T) = f''(T). \qquad (1)$$

Згідно [6-7], інтерполяційний кубічний сплайн $S_3(f; x)$ відповідає умовам:

$$S_3(x_i) = S_i,\ S_3(x_{i+1}) = S_{i+1},\ i = \overline{0, N-1}, \qquad (2)$$

де на кожному з відрізків $[x_i; x_{i+1}]$, $i = \overline{0, N-1}$ є многочленом третього ступеня, причому на відрізку [0;T] $S_3(f; x)$ має неперервність других похідних. Позначимо $S_3''(x_i) = M_i,\ S_3''(x_{i+1}) = M_{i+1},\ S_3''(x_0) = M_0,\ S_3''(x_1) = M_1$.

Тоді кубічний сплайн $S_3(f; x)$ має вигляд [6-7]:

$$S_3(f;x) = f_i(1-t) + f_{i+1}t - \frac{h_i^2}{6}t(1-t)[(2-t)M_i + (1+t)M_{i+1}],\ x \in [x_i, x_{i+1}],\ i = \overline{0, N-1}, \qquad (3)$$

де $h_i = x_{i+1} - x_i,\ t = (x - x_i)/h_i$.

Даний фрагмент коду OpenCV виконує, згідно алгоритму, показаному на рис. 1, сплайн-апроксимацію контуру зображення.

```
# Cubic spline approximation function
def cubic_spline_approximation(contour):
contour = contour.squeeze()
x = contour[:, 0]
 y = contour[:, 1]
cs_x = CubicSpline(np.arange(len(x)), x)
cs_y = CubicSpline(np.arange(len(y)), y)
t = np.linspace(0, len(x) - 1, num=75)
```

```
x_new = cs_x(t)
y_new = cs_y(t)
return np.column_stack((x_new, y_new))
# Approximation of each contour with a cubic spline
approx_contours = []
for contour in contours:
approx = cubic_spline_approximation(contour)
approx_contours.append(approx)
# Image of approximated contours
approx_image = contour_image.copy()
for approx in approx_contours:
approx = np.int32(approx)
cv2.polylines(approx_image, [approx], isClosed=True, color=(0, 255, 0), thickness=2)
```

Отриманий результат сплайн-апроксимації контуру зображення в процесі розпізнавання жестів рук показано на рис. 3. Неважко бачити, що використання сплйн-апроксимації на базі кубічного сплайну (рис. 3) дозволяє значно підвищити точність розпізнавання жесту руку, дозволяючи можливість використання в реальному масштабі часу.

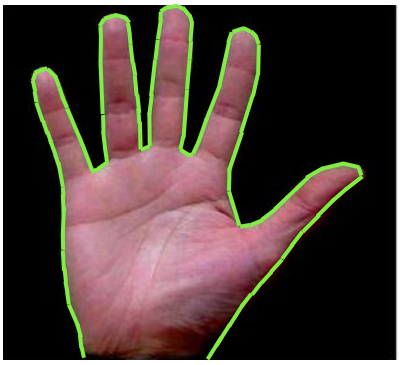


Рисунок 3 – Результат апроксимації контуру жесту руки з використанням сплайн-апроксимації на базі кубічного сплайну

Висновки:

1. Розглянуто основні методи розпізнавання жестів рук та проведено аналіз їхніх можливостей щодо виявлення та класифікації конфігурацій жестів рук. Встановлено, що доцільним є використання систем розпізнавання на базі комп'ютерного зору.

2. Запропоновано використання комп'ютерного зору на базі бібліотеки OpenCV з мовою Python для розпізнавання конфігурацій жестів рук. Розроблено алгоритм розпізнавання за допомогою бібліотеки комп'ютерного зору OpenCV та код мовою Python для розпізнавання жестів рук.

3. З метою підвищення точності розпізнавання контурів жестів рук використано сплайн-апроксимацію на базі кубічних сплайн-функцій.

4. Отримані результати можуть бути використані для інтерфейсів людино-машинної взаємодії, систем жестового управління та застосуваннях доповненої та віртуальної реальності.

Література:

1. Balas, VE, Kuriqi, A., & Murtaza, M. (eds.). Hands-on ML Projects with OpenCV: Master Computer Vision and Machine Learning using OpenCV and Python. Packt Publishing, 2022. 524 с.

2. OpenCV Documentation. OpenCV: Source Computer Vision Library [Електронний ресурс]. Режим доступу: https://docs.opencv.org

3. Козлов І.В. Практичні проекти машинного навчання з OpenCV. - Київ: MagicBook, 2021. 312 с.

4. Писаренко Д. В. Комп'ютерний зір у Python із використанням бібліотеки OpenCV. - Львів: Видавництво Львівської Політехніки, 2020. - 256 с.
5. Стрелковська І.В. Застосування дійсних та комплексних сплайнів в задачах інфокомунікацій / І.В. Стрелковська, І.М. Соловська, Ю.О. Стрелковська // Проблеми телекомунікацій. – 2021. – № 01 (28). – С. 3-19.
6. Ahlberg J.H. The Theory of Splines and Their Applications / J.H. Ahlberg, E.N. Nilson, J.L. Walsh // Academic Press, New York, 1967.
7. Larry L. Spline Functions: Basic Theory / L. Larry, S. Schumaker // Cambridge University Press, New York, 2007.

УДК 004.738.5:004.75
DOI: https://doi.org/10.32837/11300.31248

Стрелковська І.В., д.т.н., професор;
Стоянов І.А., магістр 2 року навчання
спеціальності 172 Електронні комунікації та радіотехніка
Міжнародний університет
i.strelkovskaya@mgu.edu.ua,
flagmr040@gmail.com

ДОСЛІДЖЕННЯ МЕРЕЖЕВОГО ТРАФІКУ ХМАРНИХ СЕРВІСІВ ТА CDN-ПЛАТФОРМ

Анотація. *Розглянуто обслуговування трафіку Cloud-центрами обробки даних та CDN- платформами, визначено основні особливості, що впливають на затримку, пропускну здатність і кешування. Проведено моделювання фрагменту мережі Cloud/CDN у середовищі MATLAB, що дозволило отримати характеристики трафіку запитів на сервери RPS. Встановлено, що значення характеристик якості обслуговування трафіку залежать від години найбільшої інтенсивності трафіку; при піковому навантаженні ефективність CDN значно перевершує доступ до Cloud-центрів обробки даних. Отримані результати дозволяють надати практичні рекомендації щодо обслуговування трафіку та планування інфраструктури CDN-платформи.*

Стрімкий розвиток хмарних сервісів (Google Drive, Microsoft OneDrive, Zoom, Dropbox, AWS, Google Cloud Platform) забезпечує суттєве зростання навантаження на мережеву інфраструктуру за рахунок великого обсягу мультимедійного контенту, відеосервісів, онлайн-конференцій та сервісів зберігання даних. Одним із ключових рішень цієї проблеми є використання платформ доставки вмісту CDN (Content Delivery Networks), таких як, Cloudflare, Akamai, Amazon CloudFront, Google Cloud CDN, Microsoft Azure CDN, що забезпечують розподілену масштабовану мережну інфраструктуру для розміщення вебдодатків з метою прискорення доставки контенту користувачам з найближчих серверів, розвантаження основних серверів та захисту від DDoS-атак [1-4]. У поєднанні з хмарними сервісами такі системи формують складну і динамічну систему розподілу трафіку, характеристики якої значною мірою відрізняються від класичних.

CDN-платформа доставки контенту є географічно розподілена мережева інфраструктура, яка використовується для швидкої, надійної та безпечної доставки контенту (вебсторінок, відео, зображень, скриптів тощо) користувачам. Архітектура CDN-платформи (рис. 1) побудована на базі основного серверу, який є вебсервером або сховищем даних

та периферійних CDN Edge серверів, розташованих географічно в різних країнах чи регіонах, які зберігають кешований контент, для балансування трафіку між серверами використовується Load balancer [1-4].

Серед ключових особливостей трафіку Cloud-центрів обробки даних слід зазначити його нерівномірність та наявність пікових значень інтенсивності, велику кількість API-запитів та трафіку міжсервісної взаємодії. Трафік CDN-платформи у відповідності до функціональності характеризується кешуванням та зменшенням обсягу трафіку на основний сервер, великою інтенсивністю трафіку відео та зображень. Тому важливим питанням при обслуговуванні трафіку Cloud-центрів обробки даних та CDN-платформ є визначення характеристик трафіку та характеристик якості обслуговування з метою подальшого перерозподілу трафіку на мережні вузли інфраструктури.

До основних характеристик трафіку хмарної інфраструктури слід віднести – піковий трафік з годинами найбільшої інтенсивності трафіку (19.00-22.00), частота запитів на сервери RPS (Requests Per Second) становить 500-3000 запитів. Для трафіка CDN-платформи характерним є постійний трафік із частими піками, частота запитів на сервери становить 10000-100000 RPS та кешування пакетів за протоколом TTL (Time to Live) [5].

Особливості характеристик трафіку Cloud-центрів обробки даних та CDN-платформ показані в табл. 1 [1-4].

CDN Edge 2
CDN Edge 1
CDN Edge 5
CDN Edge 3
CDN Edge 4

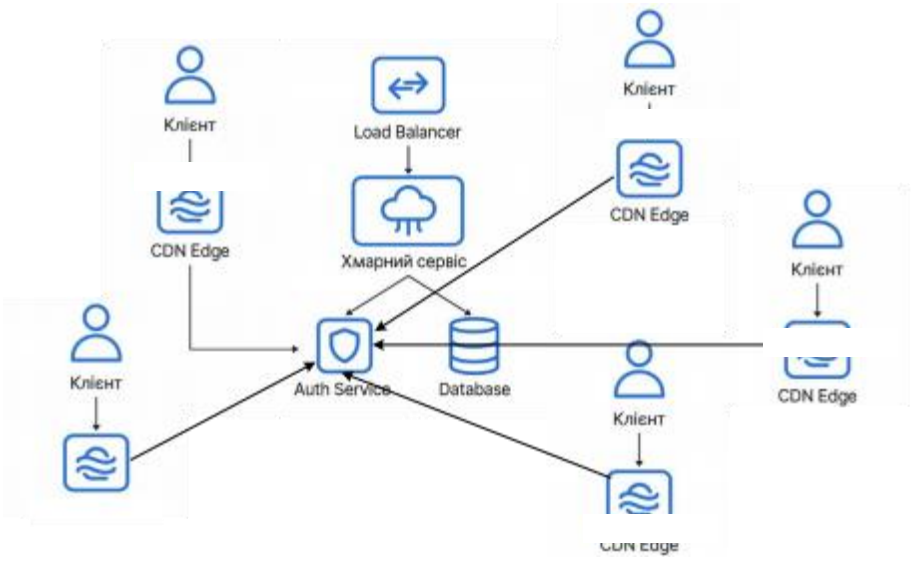


Рисунок 1 - Архітектура CDN-платформи

Таблиця 1 - Особливості характеристик трафіку Cloud-центрів обробки даних та CDN-платформ

Тип сервісу	Принципи формування трафіку	Протоколи	Особливості трафіку
Стрімінговий сервіс (YouTube, Netflix, Megogo)	Потокова передача відеотрафіку через CDN-платформу з адаптивною якістю (DASH/HLS)	HTTP/HTTPS, MPEG-DASH, HLS	Високошвидкісний трафік, який має вимоги до мінімальної затримки, джитера, втрат пакетів, пропускної спроможності
Хмарне зберігання (Google Drive, Dropbox, OneDrive)	Короткі передачі трафіку, завантаження та збереження файлів користувачами	HTTPS	Трафік формується частими та короткими сплесками трафіку
Веб-сервіси (SaaS, API, Google Docs, Zoom, Microsoft Teams, REST API)	Інтенсивний обмін даними між клієнтом і сервером, запити та відповіді в реальному часі	HTTPS, JSON, XML, WebSockets	Трафік формується короткими та частими запитами, які чутливі до затримок
Інтерактивні сервіси (Хмарні ігри (NVIDIA GeForce NOW, Xbox Cloud), AR/VR)	Інтенсивний обмін даними в реальному часі	UDP, QUIC, WebRTC	Висока частота передавання даних в реальному часі, вкрай чутливі до затримки < 20 мс, джиттера
AI-сервіси (AWS SageMaker, Google AI Platform)	Пакетне завантаження та обробка даних	HTTPS, gRPC, REST, MQTT	Нерегулярний трафік, помірна чутливість до затримок

Аналіз характеристик мережевого трафіку Cloud-центрів обробки даних та CDN-платформ показує значну різноманітність у типах трафіку, обсягах переданих даних . Найвищі вимоги до часу затримки й пропускної спроможності спостерігаються у стрімінгових та інтерактивних сервісах, тоді як сервіси зберігання даних і контентні платформи мають сплескоподібний трафік.

Трафік CDN-платформ це трафік HTTP/HTTPS запитів, REST API, WebSockets та протоколу QUIC, що ускладнює аналіз такого трафіку Особливо важливим є дослідження особливостей обслуговування та розподілу трафіку, інтенсивностей пікових навантажень, трафіку кешування з метою підвищення характеристик якості обслуговування трафіку [5].

Метою даної роботи є дослідження характеристик мережевого трафіку Cloud-центрів обробки даних та CDN-платформ з метою підвищення характеристик якості обслуговування трафіку.

Дослідження характеристик трафіку традиційно виконують за допомогою Wireshark/tcpdump, які дозволяють виконувати аналіз відомих сесій HTTPS/CDN, CDN- monitoring tools (наприклад, Cedexis, Cloudflare Analytics), що виконують аналіз сесій географічних затримок, а також Load testing (JMeter, Locust), який дозволяє моделювати реальних користувачів хмарних сервісів [4].

В даній роботі для дослідження характеристик трафіку Cloud-центрів обробки даних та CDN-платформи використано імітаційне моделювання у середовищі MATLAB, що дозволяє [6]:

- візуально змоделювати потоки трафіку запитів RPS (Requests Per Second) на сервери хмарного сервісу з CDN-платформою, включно із кешуванням,
- виконати моделювання пікової інтенсивності трафіку до хмарного сервісу та CDN-платформи.

В якості вихідних даних для моделювання задано:

- кількість запитів RPS (Requests Per Second) NRPS = 20000,
- ймовірність обслуговування вхідних запитів на сервери RPS за допомогою CDN-платформи становить PCDN = 0,8;
- ймовірність обслуговування вхідних запитів на сервери RPS за допомогою Cloud-центрів обробки даних становить PCloud = 0,2;
- інтенсивність надходження запитів на сервери RPS моделюється як змінна функція часу, 0-20 с - нормальна інтенсивність трафіку, λ = 80 запитів/с, 20-40 с - пікова інтенсивність трафіку,
λ = 240 запитів/с, 40-60 с - знижена інтенсивність трафіку, λ = 100 запитів/с.

За результатами проведеного експерименту у середовищі MATLAB отримані наступні значення (рис. 2):

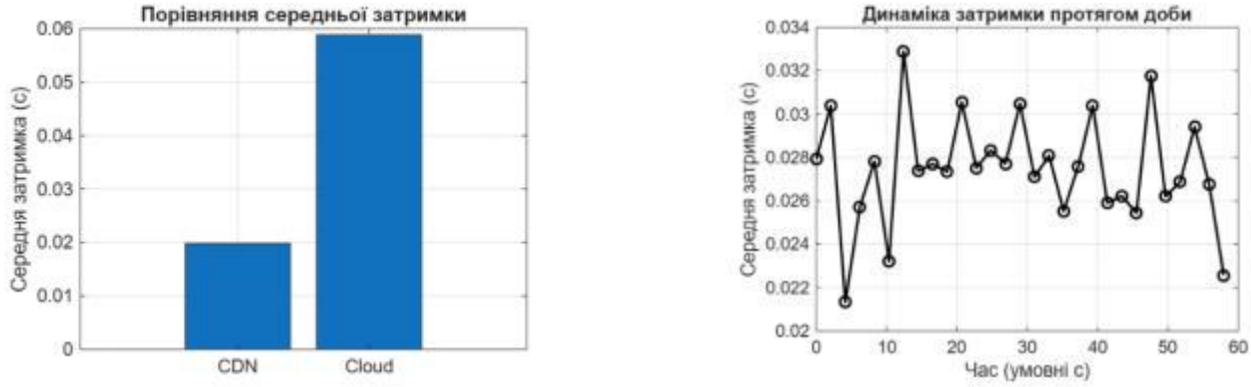


Рисунок 2 - Порівняння часу затримки та зміна часу затримки протягом доби при обслуговуванні вхідних запитів на сервери RPS за допомогою CDN-платформи та допомогою Cloud-центрів обробки даних

- час затримки обслуговування вхідних запитів на сервери RPS за допомогою CDN-платформи становить tзатр CDN = 0,02 с;
- час затримки обслуговування вхідних запитів на сервери RPS за допомогою Cloud-центрів обробки даних становить tзатр Cloud = 0,06 с.

Тоді, можливо зробити наступні висновки, у період 20-40 с пікової інтенсивності трафіку середня затримка системи зростає приблизно на 25–30%, але CDN-платформа утримує стабільний рівень обслуговування, рівень затримки становить tзатр CDN = 0,02 с, тоді як затримка Cloud-центрів обробки даних збільшується у 2 рази і становить tзатр Cloud = 0,06 с.

Зміна значення середнього часу затримки протягом доби при обслуговуванні трафіку за допомогою CDN-платформи та допомогою Cloud-центрів обробки даних пов'язана насамперед зі зміною інтенсивності надходження запитів та сплесками інтенсивностей під час годин найбільшої інтенсивності трафіку [7].

Висновки:

1. Проведено дослідження характеристик мережевого трафіку Cloud-центрів обробки даних та CDN-платформ, які обслуговують потоки трафіку запитів RPS на сервери.
2. Проведено моделювання характеристик фрагменту мережі Cloud/CDN у середовищі MATLAB, що дозволило отримати значення часу затримки обслуговування запитів на сервери RPS за допомогою Cloud-центрів обробки даних та CDN-платформи. Встановлено, що використання CDN-платформи дозволяє стабілізувати час затримки навіть при піковій інтенсивності трафіку завдяки розподілу навантаження між кеш-вузлами CDN Edge серверів.

3. Отримані значення середнього часу затримки дозволяють стверджувати про перевагу використання CDN-платформи, яка навіть при піковому збільшенні навантаження забезпечує середній час затримки tзатр CDN = 0,02 с, тоді як час затримки затримки Cloud-центрів збільшується і становить tзатр Cloud = 0,06 с.

4. Запропонована модель дозволяє виконувати імітаційне моделювання в середовищі MATLAB для різних сценаріїв обслуговування трафіку, особливо в години найбільшого навантаження (денний, вечірній, піковий) та використовувати отримані результати для планування інфраструктури CDN-платформи.

Література:

1. Редько, Д., Десятко, А., Бісарінов, Б., & Бісаріанова, А. (2024). Огляд методів аналізу трафіку компанії на основі ансамблевої кластеризації. інформаційні технології та суспільство, (4 (15), 115-124.https://doi.org/10.32689/maup.it.2024.4.18

2. Кузьменко О. В., Шевченка І. В. Хмарні обчислення та розподілені системи. - Харків: ХНУРЕ, 2020.

3. Patterson D., Hennessy J. Computer Organization and Design: The Hardware/Software Interface. - Elsevier, 2021.

4. Li, X., Zhang, J. (2023). "Performance Modeling of Cloud and CDN Hybrid Systems", Computer Networks Journal, Elsevier.

5. Statista. “Global CDN Market Size 2018–2025”, 2024. https://www.statista.com/topics/3094/content-delivery-networks/

6. MATLAB & SimEvents Documentation (R2025b) - MathWorks, 2025. https://www.mathworks.com/help/simevents

7. Li,F., Wang, J. (2024). "Analysis of Edge Computing and CDN Integration", ACM Computing Surveys , vol. 56(3).

DOI: https://doi.org/10.32837/11300.31329

Баранюк Едуард Олегович
Здобувач, Міжнародний університет
eduard.baraniuk@gmail.com
Науковий керівник: Лебедєва Олена Юріївна
Кандидат технічних наук, доцент

РОЗРОБКА ІГРОВОГО ЗАСТОСУНКУ В ЖАНРІ CITY BUILDER

Анотація. *В роботі проведено аналіз сучасного стану жанру градобудівних симуляторів (city builder) на мобільних платформах. Визначено ключові критерії для аналізу, такі як основний ігровий цикл, системи управління ресурсами та моделі монетизації. Розглянуто декілька ключових представників жанру (напр., SimCity BuildIt, Township). Виявлено домінуючі патерни проектування та монетизаційні стратегії, що використовуються розробниками для залучення та утримання аудиторії.*

Жанр city builder залишається одним із найстабільніших та найприбутковіших на ринку мобільних ігор. Його успіх обумовлений поєднанням механік довгострокового планування, менеджменту ресурсів та творчої самореалізації гравця. Проте, висока конкуренція вимагає від розробників постійного вдосконалення ігрових циклів та моделей монетизації.

Метою даної роботи є аналіз та систематизація ключових ігрових механік, що застосовуються в сучасних мобільних градобудівних симуляторах, для виявлення успішних патернів проектування.

Аналіз ключових аспектів жанру.

Для аналізу було обрано декілька репрезентативних ігор, таких як SimCity BuildIt (Electronic Arts) та Township (Playrix), які демонструють різні підходи до жанру. Аналіз проводився за наступними критеріями:

Основний ігровий цикл (Core Gameplay Loop). В SimCity BuildIt цикл базується на "крафті": гравці виробляють базові матеріали, які комбінуються у складніші товари для покращення житлових зон. Township використовує гібридний цикл "ферми" та "міста", де гравець вирощує сировину, переробляє її та виконує замовлення мешканців.

Управління ресурсами. В обох іграх ключовим обмежуючим фактором є час (таймери виробництва) та обмежена місткість складських приміщень. Це створює основний "конфлікт" для гравця і є базою для монетизації.

Моделі монетизації. Домінуючою механікою є "прискорення" (Speed-up), що дозволяє за преміальну валюту миттєво завершити будь-яке виробництво чи будівництво. Також поширеною є пряма покупка відсутніх ресурсів або предметів для розширення території.

Висновки.

Проведений аналіз показує, що сучасні мобільні ігри в жанрі city builder еволюціонували від класичних "пісочниць" до чітко прорахованих free-to-play систем. Успіх у цьому жанрі значною мірою залежить не від складності симуляції (як у ПК-версіях), а від вдало спроектованого циклу "виробництво-очікування-винагорода" та глибоко інтегрованих механік монетизації. Основними патернами є використання таймерів для всіх дій та обмеження інвентарю для стимулювання внутрішньоігрових покупок.

Література:

1. Rollings, A., Adams, E. (2020). Fundamentals of Game Design. New Riders.
2. Alha, K. (2019). The Rise of Free-to-Play: How the Revenue Model Changed Games. Proceedings of the 2019 DiGRA International Conference.
3. SimCity BuildIt [Електронний ресурс]. Electronic Arts. Режим доступу: https://www.ea.com/games/simcity/simcity-buildit.
4. Township [Електронний ресурс]. Playrix. Режим доступу: https://playrix.com/township.

DOI: https://doi.org/10.32837/11300.31331

Беседа Олексій Дмитрович
Здобувач 2-го курсу магістратури
Заочної форми навчання
Спеціальність 121 Інженерія програмного забезпечення
Міжнародний університет
e-mail: beseda.odessa@gmail.com
Науковий керівник: д.т.н., проф. Мірошник М.А.
maryna.miroshnyk1@gmail.com

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ МОБІЛЬНОЇ ПЛАТФОРМИ З ФУНКЦІЄЮ ВІДСТЕЖЕННЯ ОБ'ЄКТІВ

Анотація. *У роботі представлено концепцію та основні етапи створення інтелектуальної мобільної платформи, яка забезпечує автоматичне відстеження об'єктів у реальному часі за допомогою методів машинного навчання, комп'ютерного зору та геолокаційних технологій. Розроблена архітектура поєднує можливості мобільних пристроїв із хмарними обчисленнями, що дозволяє ефективно обробляти відеопотоки, виявляти та класифікувати об'єкти, а також відображати їх переміщення на інтерактивній карті. Проведено аналіз існуючих технологій, обґрунтовано вибір*

інструментів та запропоновано алгоритмічні рішення для підвищення точності та швидкодії системи.

Сучасні мобільні системи набувають дедалі більшого поширення у сферах безпеки, транспорту, логістики, роздрібної торгівлі та «розумного міста». Відстеження об’єктів у реальному часі є одним із найважливіших завдань таких систем, адже воно забезпечує збір аналітичних даних, контроль за переміщенням людей і транспортних засобів, а також оптимізацію бізнес-процесів.

Основною метою проєкту є створення універсальної мобільної платформи, здатної розпізнавати об’єкти на основі відеопотоку, визначати їх координати та відображати динаміку руху на карті. На відміну від традиційних систем відеоспостереження, запропоноване рішення не потребує складної серверної інфраструктури, оскільки частина обчислень переноситься безпосередньо на мобільний пристрій.

Програмна архітектура системи має модульну структуру, що складається з таких компонентів:

1. Модуль обробки відео, який виконує детекцію та класифікацію об’єктів за допомогою нейронних мереж типу *YOLOv8*, *MobileNetV3* або *EfficientDet*.
Модуль геолокації, який визначає поточні координати користувача або відстежуваного об’єкта за допомогою *GPS* або *Wi-Fi positioning*.
Серверний модуль аналітики, що працює на основі хмарних сервісів (*Firebase*, *AWS IoT Core*, *Google Cloud Vision*), забезпечуючи централізований збір, зберігання та аналіз даних.
Інтерфейс користувача, який дозволяє переглядати відеопотік у реальному часі, відображати карту з маршрутами та формувати звіти про пересування.
Для обробки зображень використовується бібліотека OpenCV, а для реалізації алгоритмів машинного навчання — TensorFlow Lite, адаптований для мобільних пристроїв з обмеженими ресурсами. Передача даних між клієнтом і сервером здійснюється за допомогою REST API та протоколу *MQTT*, що забезпечує швидку синхронізацію.

Особливу увагу приділено питанням енергоефективності та оптимізації продуктивності, оскільки постійна робота камери і GPS призводить до швидкого розряду батареї. Для цього впроваджено механізм динамічного регулювання частоти оновлення кадрів та активації геолокації лише при виявленні руху.

Проведене експериментальне тестування на пристроях Android показало, що запропонований підхід дозволяє забезпечити точність визначення координат об’єкта до 5 метрів, а середній час виявлення об’єкта в кадрі не перевищує 100 мс. Платформа здатна відстежувати одночасно до 10 рухомих об’єктів без значного зниження продуктивності.

Крім того, система підтримує аналітику в реальному часі, що дозволяє відстежувати тенденції переміщення, прогнозувати траєкторію руху та виявляти аномальні події. У майбутньому передбачається впровадження модулів доповненої реальності (AR), які дадуть змогу візуалізувати відстежувані об’єкти безпосередньо у полі зору користувача.

Висновки.

Запропонована інтелектуальна мобільна платформа демонструє високий потенціал для використання у сфері моніторингу, логістики, безпеки та «розумного міста». Вона забезпечує поєднання мобільності, автономності та точності розпізнавання об’єктів. Подальші дослідження спрямовані на підвищення рівня автоматизації системи, розширення можливостей машинного навчання, а також інтеграцію з інтернетом речей (IoT) та аналітичними панелями.

Література:

1. Мірошник М. А., Васильченко Д. О. Комп’ютерна модель системи керування рухомими об’єктами типа БПЛА. Комп’ютерне моделювання в наукоємних технологіях: Збірник наукових праць X міжнародної науково-технічної конференції (м. Харків, 27-29 листопада 2024 року) – Харків: ХНУ ім. В.Н. Каразіна, 2024. – с. 133-136. csd.karazin.ua/wp-content/uploads/2025/05/ csd.karazin.ua-maket-kmnt-2024.pdf

2. Мірошник М. А., Прокоф’єв С.В. Визначення способу організації та реалізації паралельної обробки даних на основі ПЛІС для ефективного моніторингу об’єктів критичного застосування. Комп’ютерне моделювання в наукоємних технологіях: Збірник наукових праць X міжнародної науково-технічної конференції (м. Харків, 23-25 жовтня 2023 року) – Харків: ХНУ ім. В.Н. Каразіна, 2023. – с. 146-149. csd.karazin.ua/wp-content/uploads/2023/09/ csd.karazin.ua-ix-25-27-2023-programa-kmnt-2023-f.pdf

3. Мірошник А.М., Ситнік Б. Т. Структурно-параметрична індексна ідентифікація в адаптивних системах управління рухомими об'єктами. Інформаційно-керуючі системи на залізничному транспорті, 2023, №4, С.64-70. DOI: 10.18664/ikszt.v0i4.178719 (Б) (Наказ МОН № 886 від 02.07.2020) URL: http://jiks.kart.edu.ua/

4. Redmon J., Farhadi A. YOLOv8: Real-Time Object Detection. – 2023. – [Online]. – Available: https://yolov8.com/

5. Sandler M., Howard A., Zhu M. et al. MobileNetV3: Efficient Neural Network for Mobile Vision Applications. – 2019. Available: https://arxiv.org/abs/1704.04861

6. Google Firebase Documentation. – [Online]. – Available: https://firebase.google.com/docs
AWS IoT Core Overview. – [Online]. – Available: https://aws.amazon.com/iot-core

7. Bradski G. The OpenCV Library. – *Dr. Dobb's Journal of Software Tools*, 2000. - Available: https://ftp.math.utah.edu/pub/tex/bib/toc/dr-dobbs-2000.html

УДК 004.93
DOI: https://doi.org/10.32837/11300.31333

Дудко І.А., здобувач
Міжнародний Університет
igordudko1973@gmail.com

ДОСЛІДЖЕННЯ СИСТЕМИ РОЗПІЗНАВАННЯ ЖЕСТІВ З ВИКОРИСТАННЯМ MOBILENET ДЛЯ ЗАДАЧ КОМП’ЮТЕРНОГО ЗОРУ

Анотація. *Робота присвячена розробці та дослідженню інтелектуальної системи розпізнавання жестів американської жестової мови на основі згорткових нейронних мереж. Особлива увага приділяється використанню легковагової архітектури MobileNetV2 з технікою transfer learning для ефективного розпізнавання статичних зображень жестів. Проводиться експериментальне дослідження навчання моделі на датасеті ASL Alphabet з детальним аналізом точності класифікації, динаміки навчання та обчислювальних характеристик. На основі отриманих результатів надано оцінку ефективності створеної системи та рекомендації щодо практичного застосування.*

Розпізнавання жестів є актуальною задачею комп’ютерного зору, що має важливе значення для покращення комунікації людей з вадами слуху та створення природних інтерфейсів взаємодії людини з комп’ютером. Американська жестова мова (ASL) використовується мільйонами людей, проте комунікаційний бар’єр між глухими та людьми, які не знають жестової мови, залишається значною проблемою [1]. Автоматизовані системи розпізнавання жестів можуть стати ефективним інструментом для подолання цього бар’єру та підвищення доступності цифрових технологій.

В останні роки глибокі згорткові нейронні мережі продемонстрували вражаючі результати в задачах комп’ютерного зору, включаючи розпізнавання образів та класифікацію зображень [2]. Однак впровадження таких систем на пристроях з обмеженими ресурсами залишається викликом, що потребує використання оптимізованих архітектур нейронних мереж з балансом між точністю та обчислювальною ефективністю.

Метою даної роботи є розробка та експериментальне дослідження компактної системи розпізнавання жестів американської жестової мови на основі легковагової архітектури MobileNetV2 з можливістю розгортання на мобільних пристроях та вбудованих системах.

Для розв'язання поставленої задачі було обрано архітектуру MobileNetV2, яка використовує depthwise separable convolutions для зменшення кількості параметрів та обчислювальної складності [3]. Ключовою особливістю MobileNetV2 є використання inverted residual blocks з лінійними bottleneck шарами, що дозволяє ефективно навчати мережу при збереженні високої точності класифікації. Застосування підходу transfer learning з попередньо навченими на ImageNet вагами дозволяє швидко адаптувати модель до задачі розпізнавання жестів навіть з обмеженою кількістю тренувальних даних.

Реалізація системи здійснена мовою програмування Python з використанням фреймворку TensorFlow та високорівневого API Keras [4]. Програмне забезпечення організовано за об'єктно-орієнтованим підходом з чітким розділенням функціональності між спеціалізованими класами: Config для управління конфігураційними параметрами, DatasetManager для завантаження та підготовки датасету, DataPreparation для препроцесингу та аугментації зображень, ModelBuilder для створення архітектури нейронної мережі, ModelTrainer для організації процесу навчання з використанням callbacks, та ModelEvaluator для всебічної оцінки якості моделі та візуалізації результатів.

Експериментальне дослідження проводилось на датасеті ASL Alphabet, який містить зображення жестів для 26 літер англійського алфавіту та додаткові класи для спеціальних символів (del, nothing, space), що в сумі складає 29 категорій жестів. Для прискорення експериментів використовувалося 10% датасету зі збереженням збалансованого представлення кожного класу. Основні конфігураційні параметри системи наведено у таблиці 1.

Таблиця 1 – Конфігураційні параметри системи

Параметр	Значення	Опис
DATASET_PERCENTAGE	10%	Відсоток датасету для використання
IMG_SIZE	224	Розмір зображень у пікселях
BATCH_SIZE	32	Розмір батчу для навчання
EPOCHS	50	Максимальна кількість епох
LEARNING_RATE	0.001	Початкова швидкість навчання
VALIDATION_SPLIT	0.2	Частка даних для валідації
MODEL_TYPE	mobilenet_v2	Тип базової моделі
USE_AUGMENTATION	True	Використання аугментації даних
RANDOM_SEED	42	Seed для відтворюваності

Архітектура створеної моделі складається з базової мережі MobileNetV2 з замороженими вагами, що виступає в ролі feature extractor, та додаткових класифікаційних шарів: GlobalAveragePooling2D для перетворення двовимірних карт ознак у одновимірний вектор, Dropout шарів з коефіцієнтами 0,2 та 0,3 для регуляризації та запобігання перенавчанню, повнозв'язного шару з 512 нейронами та функцією активації ReLU для вивчення нелінійних комбінацій ознак, та завершального Dense шару з 29 нейронами та softmax активацією для багатокласової класифікації.

Для підвищення узагальнюючої здатності моделі застосовувалась комплексна аугментація тренувальних даних, що включала випадкові повороти зображень в діапазоні до 20 градусів, зсуви по горизонталі та вертикалі до 20% від розміру зображення, операції shear transformation для моделювання перспективних спотворень, випадкове масштабування та горизонтальне відображення. Валідаційні дані обробляються без аугментації, застосовується лише нормалізація значень пікселів до діапазону [0, 1].

Процес навчання контролювався системою callbacks: EarlyStopping для автоматичної зупинки при відсутності покращення валідаційної функції втрат протягом 5 епох з відновленням найкращих ваг, ReduceLROnPlateau для зменшення швидкості навчання в 2 рази при досягненні plateau на кривій валідаційних втрат з patience=3, та ModelCheckpoint для автоматичного збереження найкращої версії моделі на основі валідаційної точності. Компіляція моделі здійснювалась з оптимізатором Adam, функцією втрат categorical crossentropy та метриками accuracy і top-3 accuracy.

Динаміка навчання моделі представлена на рисунку 1, який відображає зміну точності класифікації протягом епох для тренувального та валідаційного наборів даних. Графік демонструє швидку збіжність на перших 10 епохах з подальшою стабілізацією результатів. Фактична кількість епох навчання склала 24 через спрацювання механізму EarlyStopping, що свідчить про ефективність обраної конфігурації та досягнення оптимального стану моделі без марної витрати обчислювальних ресурсів.

Аналіз кривих навчання показує помірний розрив між тренувальною (90,17%) та валідаційною (85,06%) точністю на фінальній епосі, що вказує на наявність обмеженого перенавчання на рівні 5,11%. Це є прийнятним для даної задачі, особливо враховуючи використання лише 10% датасету. Застосовані методи регуляризації (Dropout, аугментація даних) виявилися ефективними для обмеження перенавчання та забезпечення стабільної узагальнюючої здатності моделі.

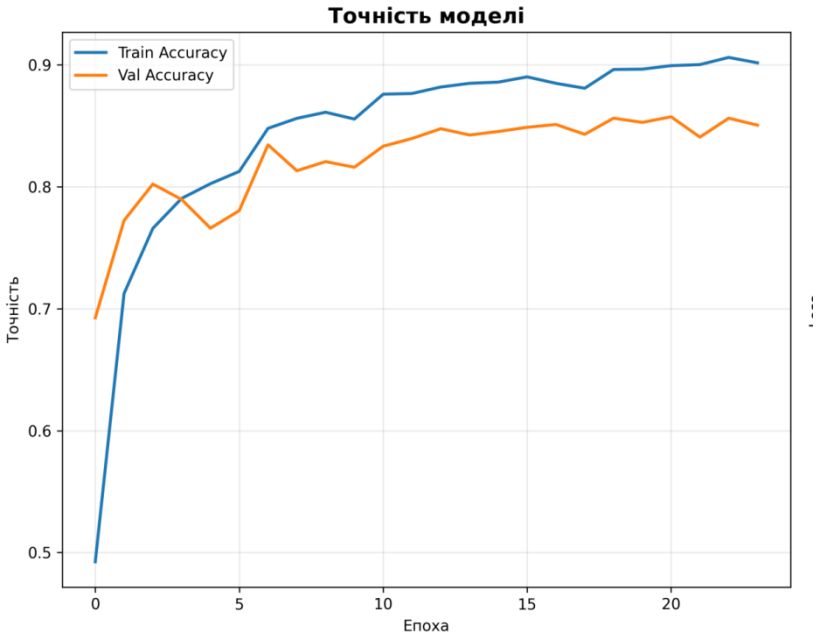


Рисунок 1 – Динаміка точності моделі під час навчання

Досягнута валідаційна точність 85,06% свідчить про ефективність обраного підходу для розпізнавання жестів за статичними зображеннями. Особливо вражаючим є показник top-3 accuracy на рівні 95,63%, що означає, що у переважній більшості випадків правильний жест входить до трійки найбільш вірогідних варіантів моделі. Це має практичне значення для побудови інтерактивних інтерфейсів, де система може надавати користувачеві декілька варіантів розпізнаного жесту для вибору.

Аналіз матриці плутанини виявив, що найкращу точність розпізнавання демонструють жести з чіткими візуальними характеристиками: F (F1-score 1,000), L (0,984), Q (0,983), nothing (0,974), space (0,921). Натомість найбільш проблемними виявилися візуально подібні жести: X (0,620), U (0,626), I (0,765), J (0,771), O (0,754), N (0,763), V (0,727), які потребують додаткового вдосконалення. Ці пари жестів часто плутаються між собою через тонкі відмінності в положенні пальців або кількості пальців, що є очікуваним результатом навіть для людей без спеціальної підготовки у жестовій мові.

Балансовані значення середньої precision (86,74%), recall (85,63%) та F1-score (85,65%) вказують на рівномірну якість розпізнавання для більшості класів без значного дисбалансу між хибнопозитивними та хибнонегативними помилками. Детальний звіт класифікації для кожного класу дозволяє ідентифікувати конкретні жести, що потребують покращення через збільшення кількості тренувальних прикладів або спеціалізовані техніки аугментації.

Створена система має декілька важливих переваг для практичного застосування. Використання transfer learning дозволило досягти високої точності навіть з 10% датасету, що демонструє ефективність підходу для задач з обмеженою кількістю даних. Модульна архітектура програмного забезпечення забезпечує легкість подальшого розширення функціоналу та інтеграції з іншими системами. Автоматизовані механізми збереження результатів, включаючи навчену модель у форматі Keras, детальні візуалізації, звіти класифікації та JSON файли з повною інформацією про експеримент, полегшують документування досліджень та порівняння різних конфігурацій [5].

Система може бути легко конвертована у формат TensorFlow Lite для розгортання на Android та iOS пристроях або у формат TensorFlow.js для виконання безпосередньо у веб-браузері без серверної обробки. Локальна обробка даних забезпечує повну конфіденційність користувача та можливість роботи без інтернет-з'єднання. Відсутність необхідності в спеціалізованому обладнанні (достатньо звичайної RGB камери) робить систему доступною для широкої аудиторії.

Перспективи подальших досліджень включають збільшення обсягу тренувальних даних до 50-100% датасету для підвищення точності до 90-95%, розширення функціональності для розпізнавання динамічних жестів з відеопотоку шляхом додавання темпоральної компоненти (LSTM або GRU шари), інтеграцію з системами трекінгу рук (MediaPipe Hands) для виділення області інтересу та підвищення робастності до різних умов зйомки, експериментування з більш сучасними архітектурами (EfficientNet, Vision Transformers) та розробку спеціалізованих технік аугментації для проблемних класів жестів.

На основі проведеного дослідження можна зробити наступні висновки. Створена система розпізнавання жестів на основі MobileNetV2 демонструє ефективний баланс між точністю класифікації (85.06%), компактністю моделі (2,93 млн параметрів) та швидкодією (3,75 мс на зображення), що робить її придатною для розгортання на пристроях з обмеженими ресурсами. Застосування transfer learning з попередньо навченими вагами ImageNet дозволило швидко адаптувати модель до специфіки розпізнавання жестів за 24 епохи навчання. Високе значення top-3 accuracy (95,63%) відкриває можливості для побудови інтерактивних інтерфейсів з верифікацією розпізнаних жестів користувачем. Детальний аналіз результатів класифікації виявив конкретні проблемні класи та напрямки вдосконалення системи. Модульна архітектура програмного забезпечення та автоматизовані механізми оцінювання забезпечують зручність проведення експериментів та документування результатів.

Література:

1. Pisharady P. K. Recent methods and databases in vision-based hand gesture recognition: A review / P. K. Pisharady, M. Saerbeck // Computer Vision and Image Understanding. – 2015. – Vol. 141. – P. 152-165.

2. Chollet F. Deep Learning with Python, Second Edition / F. Chollet. – Shelter Island: Manning Publications, 2021. – 504 p.

3. Sandler M. MobileNetV2: Inverted Residuals and Linear Bottlenecks / M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, L.-C. Chen // 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. – Salt Lake City, UT, USA, 2018. – P. 4510-4520.

4. Abadi M. TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems / M. Abadi, A. Agarwal, P. Barham [et al.] // arXiv preprint arXiv:1603.04467. – 2016. – 19 p.

5. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 3rd Edition / A. Géron. – Sebastopol: O'Reilly Media, 2022. – 861 p.

УДК 621.31
DOI: https://doi.org/10.32837/11300.31342

Нікольський Віталій Валентинович,
доктор технічних наук, професор, професор кафедри комп'ютерних наук
Міжнародний університет
vit_nik@ukr.net
Лорткіпанідзе Руслан,
здобувач 1 курсу другого (магістерського) рівня
спеціальності 123 – Комп'ютерна інженерія
Міжнародний університет
rockstargett@gmail.com

РОЗПОДІЛЕНА СИСТЕМА МОНІТОРИНГУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА НА БАЗІ LORAWAN

Анотація. *Розглянуто розподілену систему моніторингу навколишнього середовища на базі протоколів стеку LoRa та LoRaWAN, що дозволяє ефективно передавати невеликі пакети повідомлень (корисного навантаження) на великі відстані. Система поєднує контейнеризований стек (Docker) та механізм декодування повідомлень, а також компенсації їх втрат, на шарі додатку стеку протоколів LoRa та LoRaWAN.*

Актуальність роботи обумовлена зростаючим попитом на рішення інтернету речей (IoT, Internet of Things), що здатні забезпечити тривалу автономну роботу та зв'язку на великій відстані. Традиційні протоколи безпровідних персональних мереж (WPAN, Wireless Personal Area Network) не здатні задовольнити ці вимоги, тому створення системи на базі енергоефективних мереж далекого радіусу дії (LPWAN, Low-power Wide-area Network) [1] є оптимальним вибором для збору даних (повідомлень) від віддалених об'єктів.

У сегменті LPWAN-технологій основними конкурентними рішеннями для систем на базі LoRaWAN є NB-IoT та Sigfox-рішення. На відміну від LoRaWAN, NB-IoT працює у ліцензованому спектрі радіочастот та вимагає підтримки від операторів мобільного зв'язку. В свою чергу SigFox використовує дещо більш вузькосмуговий зв'язок і має суворіші обмеження на кількість та розмір повідомлень.

LoRaWAN [2] забезпечує двосторонній зв'язок і гнучкість у налаштуванні параметрів мережі (таких як коефіцієнт розтікання, або Spreading Factor). Основна відмінність такої системи полягає у високій чутливості приймача (до -148 дБм), що дає максимальну алгебраїчну суму підсилень та втрат потужності сигналу до передавача, відому як бюджет лінії.

Проект використовує багатошарову модульну програмну архітектуру, яку наведено на рис. 1, а саме:

1. Фізичний рівень (від кінцевих пристроїв до шлюзу).

2. Мережевий рівень, що представлений мережевим сервером ChirpStack.

3. Рівень застосунку, що представлений кількома рішеннями: MQTT-брокер повідомлень Mosquitto, середовище обробки даних Node-RED на базі фреймворку Node.js (виконує функцію декодера корисного навантаження повідомлень та компенсацію їхніх

втрат при передаванні), а також таблиця даних на базі програмного забезпечення (ПЗ) Ms Excel, куди раз на день звітуються дані з системи.

Модульність побудованої системи дозволяє легко інтегрувати нові сенсори, протоколи обробки та запису даних без переривання роботи основних компонентів. Основними функціональними модулями проекту є наступні:

1. Мережевий сервер ChirpStack, що управляє сесіями LoRaWAN та конвертації LoRa-пакетів даних у формат, зрозумілий для брокера повідомлень.

2. Декодер корисного навантаження на базі фреймворку Node-RED, що на рівні застосунку реалізує перетворення бінарного корисного навантаження.

3. Модуль компенсації втрат, реалізований за допомогою “сторожового” таймера (Watchdog). Він відслідковує надходження пакетів від кінцевих пристроїв та у разі відсутності пакета протягом встановленого інтервалу часу (у нашому випадку 3 сек., враховуючи слоти очікування девайсів класу А) автоматично вставляє нульовий маркер у кінцевий масив даних, що дає змогу користувачеві на рівні додатку зрозуміти поточний стан системи. Це гарантує, що наступні алгоритми обробки даних не інтерпретуватимуть затримку як нульове значення.

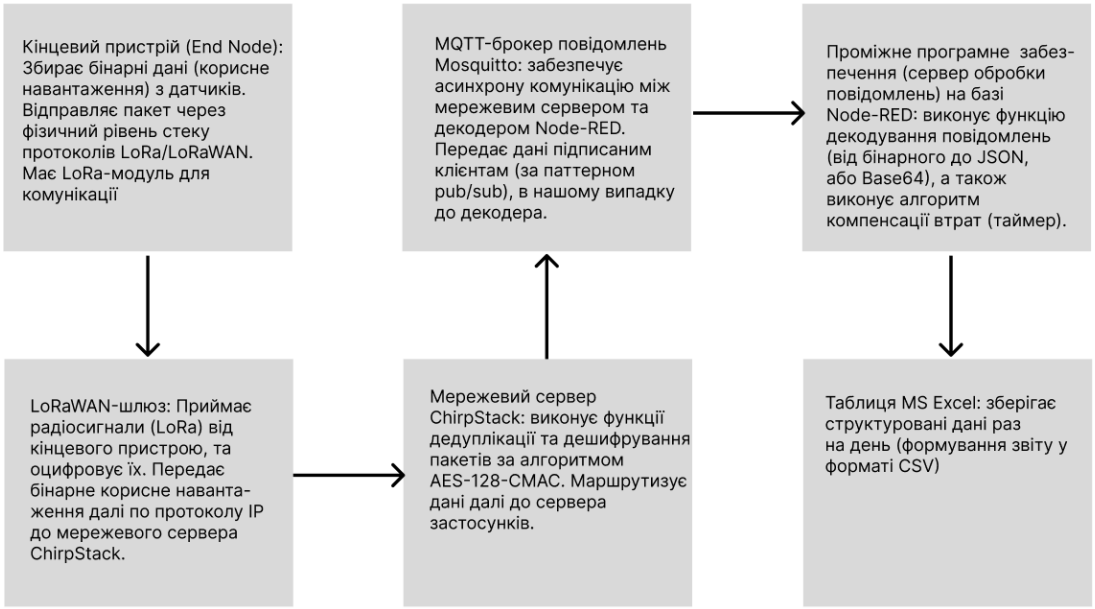


Рисунок 1 - Структурна схема програмної архітектури моніторингу на базі LoRaWAN

Надійність комунікації [3] критично залежить від параметрів радіоканалу. Натомість, моделювання каналу зв’язку грунтується на розрахунку бюджету лінії. Для оцінки надійності використовується запас зв’язку, який розраховується за наступною формулою:

Запас зв’язку = Потужність передавача (дБм) - Чутливість приймача (дБм).

При інженерному проектуванні також слід враховувати вплив зони Френеля [4] та необхідність кліренсу (блокування не більше 40 відсотків сигналу), щоб забезпечити необхідну розрахункову відстань зв’язку.

Існує багато прикладів застосування систем LoRaWAN у різних галузях та сценаріях [5], що є наступними:

1. У сільському господарстві є необхідність у моніторингу умов ґрунту, таких як вологість повітря та його температура, на великих територіях з низькою щільністю кінцевих

пристроїв.

2. Для моніторингу у рамках проектів накшталт “розумне місто” контроль рівня шуму, забруднення повітря, а також запити на моніторинг паркомісць залишаються актуальними.

3. У промисловій галузі системи LoRaWAN використовуються, наприклад, у контролі температури обладнання, або у моніторингу геолокації співробітників у їхній робочий час (будівельна сфера).

Таким чином, розроблена система є стійкою до інтервальних збоїв радіоканалу, та підтверджується критична необхідність у досягненні розрахункової дальності зв’язку при інженерному проектуванні. Система використовує модульну архітектуру, що забезпечує її гнучкість використання та підтримку багатоплатформності.

Література:

1. Shea S. TechTarget. Internet of things networking. URL: https://www.techtarget.com/iotagenda/definition/LPWAN-low-power-wide-area-network.

2. LoRaWAN Specification V1.0.4. LoRa Alliance. URL: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification

3. Alipio M., Bures M. Current testing and performance evaluation methodologies of LoRa and LoRaWAN in IoT applications: Classification, issues, and future directives. *ScienceDirect*. *Internet of Things*. URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660523003761

4. Lee S. Fresnel Zone: The Ultimate RF Engineering Guide. NumberAnalytics. URL: https://www.numberanalytics.com/blog/fresnel-zone-ultimate-rf-engineering-guide.

5. LoRaWAN - Most Common Applications and Use Cases. IoT for All. URL: https://www.iotforall.com/lorawan-most-common-applications-and-use-cases.

DOI: https://doi.org/10.32837/11300.31339

Колесник Олена Валеріївна
Студентка 2-го курсу магістратури
Заочної форми навчання
Спеціальність 172 Електронні комунікації та радіотехніка
Міжнародний університет
kolesnik.e.2025@gmail.com
Науковий керівник: д.т.н., проф. Мірошник М.А.
maryna.miroshnyk1@gmail.com

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЕТЕКЦІЇ ОБЛИЧЧЯ

Анотація. *У роботі представлено методику розробки інтелектуальної системи детекції обличчя, яка базується на використанні сучасних алгоритмів комп’ютерного зору та глибинного навчання. Система призначена для автоматичного розпізнавання об’єктів, класифікації обличчя та виявлення аномалій у візуальних даних. Запропоновано архітектуру, що поєднує ефективність нейронних мереж типу Convolutional Neural Networks (CNN) із можливостями хмарних сервісів для зберігання й обробки великого обсягу даних. Наведено результати експериментальних досліджень точності детекції та розглянуто шляхи оптимізації системи для мобільних і вебплатформ.*

Детекція обличчя є однією з ключових задач у сучасних системах комп’ютерного зору, що знаходить застосування у сферах безпеки, охорони здоров’я, промислової автоматизації, транспорту та цифрового контент-аналізу. З розвитком штучного інтелекту та глибинного навчання зросла ефективність систем розпізнавання об’єктів, що дозволило суттєво підвищити точність і швидкодію аналізу візуальної інформації.

Метою дослідження є розробка інтелектуальної системи детекції обличчя, здатної виконувати автоматичне виявлення та класифікацію об’єктів у реальному часі. Основні завдання включають аналіз існуючих підходів до детекції, розробку архітектури системи, навчання моделей та оптимізацію для практичного використання.

Система складається з трьох основних компонентів:

1. Модуль попередньої обробки, який виконує нормалізацію, масштабування та фільтрацію обличчя.
2. Модуль нейронної мережі, що реалізує алгоритм детекції на основі архітектур YOLOv8, Faster R-CNN або EfficientDet. Ці моделі поєднують високу точність з оптимальною швидкістю обробки.
3. Модуль аналітики та візуалізації, який формує результати детекції, відображає знайдені об’єкти, визначає їх координати та зберігає дані для подальшого аналізу.

Під час дослідження використано фреймворки TensorFlow, PyTorch та бібліотеку OpenCV. Для навчання моделі застосовувалися відкриті набори даних: COCO, ImageNet та Pascal VOC. Мережа проходила багатоетапне донавчання із застосуванням методів аугментації даних для підвищення стійкості до варіацій освітлення, поворотів та масштабів.

Особливу увагу приділено оптимізації продуктивності системи. Для забезпечення швидкої обробки зображень на пристроях з обмеженими ресурсами проведено квантилізацію ваг моделі, зменшення глибини нейронної мережі та використання бібліотек TensorFlow Lite і ONNX Runtime. Це дозволило досягти середньої швидкості 25–30 кадрів за секунду при точності виявлення (mAP) понад 90 %.

Для хмарної інтеграції обрано сервіси AWS Rekognition та Google Cloud Vision, що дозволяють обробляти великі обсяги зображень у паралельному режимі. Передача результатів між клієнтом і сервером здійснюється через REST API або WebSocket, що забезпечує низьку затримку й актуальність даних у реальному часі.

Крім традиційної класифікації, система підтримує виявлення аномалій, тобто таких зображень, які не відповідають типовим шаблонам. Для цього використано метод автоенкодера, який навчається відтворювати звичні структури об’єктів і сигналізує про відхилення. Ця функція може бути корисною у системах безпеки, промисловому контролі якості та медичній діагностиці.

Розроблена система має потенціал для інтеграції з мобільними застосунками та вебінтерфейсами. Завдяки використанню адаптивного дизайну та хмарної синхронізації користувач може отримувати результати детекції з будь-якого пристрою. У подальшому планується впровадити модуль розпізнавання контексту, який дозволить системі не лише визначати об’єкти, а й аналізувати їх взаємозв’язки на зображенні.

Висновки.

Розроблена інтелектуальна система детекції обличчя демонструє високу ефективність і точність у реальному часі. Вона може бути застосована у різних сферах – від безпеки до автоматизованого виробництва. Використання сучасних алгоритмів глибинного навчання, хмарних технологій та оптимізованих бібліотек забезпечує масштабованість і надійність рішення. Подальші дослідження передбачають удосконалення алгоритмів класифікації, розширення функціональності з використанням мультимодальних моделей (текст+зображення) та впровадження модулів прогнозування подій.

Література:

1. Miroshnyk, M., Shmatkov, S., Strilets, V., & Zats, O. (**2025**). Investigation of computer systems to detect intrusions and network anomalies. Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 65, 67-82. https://doi.org/10.26565/2304-6201-2025-65-06

2. Sharmila, B.S., Nagapadma, R. Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. Cybersecurity 6, 41 (2023). https://doi.org/10.1186/s42400-023-00178-5

3. Pakhomov Yu.V., Koroliova Ya.Yu., Demchenko K.V., Demenkova S.D. Using the method of anomaly search for detecting network attacks. V. N. Karazin Kharkiv National University Bulletin, series ‘Mathematical modelling. Information technologies. Automated control systems’. 2023. issue. 59. P.35-48. [in Ukrainian] https://doi.org/10.26565/2304-6201-2023-60-02

4. Gavrylenko S., Zozulia V. nvestigation of methods for detecting anomalies at the stage of data pre-processing. Control, Navigation and Communication Systems. 2022, Issue 1(67), P. 52-56. [in Ukrainian]. https://doi.org/10.26906/SUNZ.2022.1.052

5. Lykhach O., Ugryumov M., Shevchenko D., & Shmatkov S. Anomaly detection methods in sample datasets when managing processes in systems by the state. Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 2022, 53, 21-40. https://doi.org/10.26565/2304-6201-2022-53-03 [in Ukrainian].

6. Panchenko M.V., Bigdan A. M., Babenko T. V., Timofeev D. S. Identification of information security anomalies based on information system entropy analysis. Energy and automation, No. 1, 2022. DOI 10.31548/energiya [in Ukrainian].

7. Nicheporuk A.O., Nicheporuk A.A., Savenko O.S., Kazantsev A.D. An intelligent system for detecting anomalies and identifying devices of smart buildings using collective communication. Khmelnytskyi National University // ISSN 2221-3805. Electrical and computer systems. 2021. No. 34 (110) Information systems and technologies Users/Administrator/Downloads/3196-Article Text-2350-1-10-20210904.pdf [in Ukrainian].

8. Ruban I. V., Martovytskyi V. O., Partika S. O. Classification of anomaly detection methods in information systems. Armament systems and military equipment. 2016. no. 3. pp. 100-105. https://openarchive.nure.ua/server/api/core/bitstreams/7c434471-942c-40a7-b70c-0cc2655a42fe/content [in Ukrainian].

УДК 372.862
DOI: https://doi.org/10.32837/11300.31340

Русу Олександр Петрович, к.т.н.
Міжнародний університет
shurusu@ukr.net
Крупецький Кирило Андрійович
здобувач 2 курсу другого (магістерського) рівня
зі спеціальності 123 Комп’ютерна інженерія
Міжнародний університет

ЦИФРОВЕ КЕРУВАННЯ ІМПУЛЬСНИМИ ПЕРЕТВОРЮВАЧАМИ НАПРУГИ В КОМП’ЮТЕРНОМУ ОБЛАДНАННІ

Анотація. *У роботі розглянуто підхід до побудови цифрових контурів керування імпульсними перетворювачами напруги, що використовуються в сучасному комп’ютерному обладнанні, зокрема в системах Інтернету речей і мобільній електроніці. Показано, що використання мікроконтролерів загального призначення для реалізації цифрових алгоритмів стабілізації дозволяє відмовитися від спеціалізованих мікросхем-контролерів, зменшити габарити пристроїв та підвищити функціональну гнучкість. Наведено приклад реалізації підвищувального перетворювача напруги з цифровим контуром керування, виконаного без окремої мікросхеми контролера.*

Імпульсні перетворювачі напруги є невід’ємною складовою сучасного комп’ютерного обладнання. Вони забезпечують стабільне живлення компонентів системи, таких як процесори, контролери та периферійні модулі. Традиційно функції керування перетворювачами з імпульсним методом перетворення виконують спеціалізовані мікросхеми, що містять генератор, підсилювач помилки та широтно-імпульсний модулятор (ШІМ). Принцип дії полягає у порівнянні пилкоподібного сигналу з напругою помилки, яка є

різницею між вихідною та опорною напругою V_{REF}., після чого формується сигнал керування силовим ключем (рис. 1) [1].

Попри високу надійність, використання таких мікросхем збільшує апаратну складність, розміри друкованих плат і собівартість пристрою. У малогабаритних системах, таких як модулі Інтернету речей або робототехнічні платформи, надмірна кількість компонентів стає суттєвим обмеженням.

Ефективною альтернативою є цифрове керування, коли функції контролера виконуються вбудованим мікроконтролером загального призначення [2, 3], який уже присутній у системі. Цей підхід дозволяє задіяти наявні апаратні ресурси – таймери, аналого-цифрові перетворювачі та компаратори – для реалізації алгоритмів стабілізації напруги програмним шляхом у реальному часі. Сигнал, пропорційний вихідній напрузі, подається на вхід АЦП мікроконтролера, де відбувається його аналіз і порівняння з опорною напругою. Результати обчислень визначають параметри ШІМ-сигналу, який формується апаратним таймером (рис. 2).

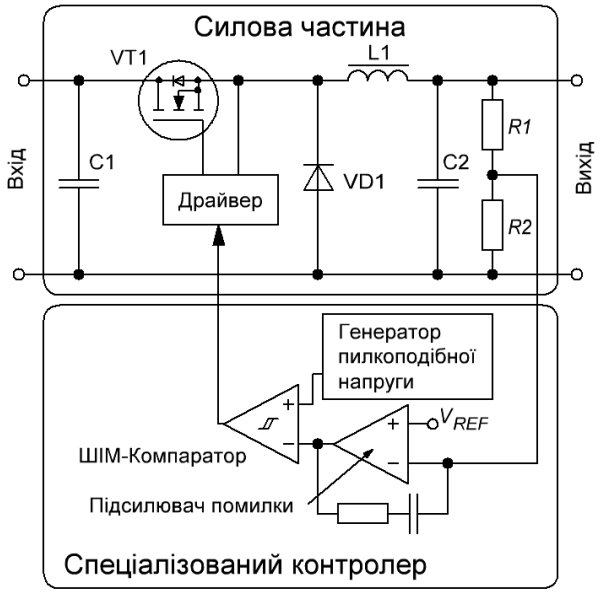


Рисунок 1 – Керування перетворювачем за допомогою спеціалізованих контролерів

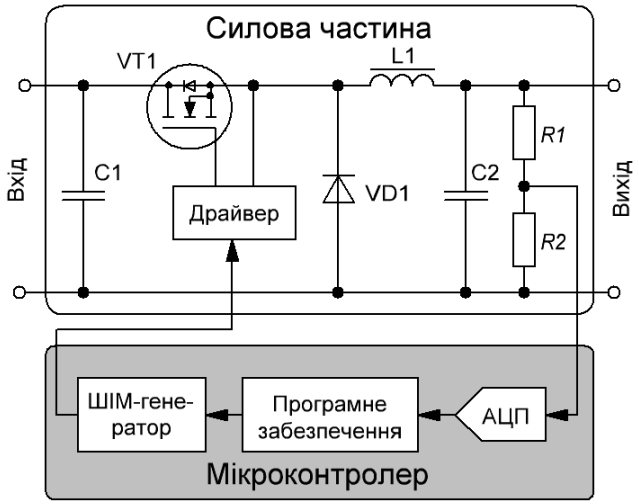


Рисунок 2 – Керування перетворювачем за допомогою цифрового контуру керування

Такий метод забезпечує повну керованість процесом енергоперетворення, гнучкість програмного налаштування та можливість впровадження адаптивних алгоритмів без змін у

схемотехніці. Крім того, цифровий контур дозволяє реалізувати додаткові функції – фільтрацію, компенсацію, діагностику та автоматичне коригування коефіцієнтів регулювання.

На рисунку 3 наведено приклад практичної реалізації цифрового керування в підвищувальному імпульсному перетворювачі, який використовується для живлення електродвигунів мобільної роботизованої платформи. Перетворювач, утворений компонентами *L1*, *VT1*, *VD1* та *C1–C4*, збільшує напругу літій-іонної акумуляторної комірки *GB1* (3,6 В) до напруги, необхідної для роботи тягових двигунів *M1* та *M2* (6 В). При цьому керування процесом перетворення (аналіз вихідної напруги та формування ШІМ-сигналів для керування транзисторним ключем *VT1*) здійснюється мікроконтролером *DD1*, у якості якого було обрано найбільш поширений мікроконтролер з сімейства 8-розрядних мікроконтролерів загального призначення STM8 (STM8S003F3P6). У якості опорної напруги була використана напруга живлення мікроконтролера стабілізована LDO-стабілізатором. Завдяки використанню цифрового контуру відпала потреба у зовнішній мікросхемі контролера, що дозволило мінімізувати кількість компонентів та спростити конструкцію.

Таким чином, цифрове керування імпульсними перетворювачами напруги є перспективним напрямом розвитку вузлів та систем комп'ютерної техніки, оскільки поєднує високу ефективність, компактність та простоту інтеграції в існуючі мікроконтролерні платформи.

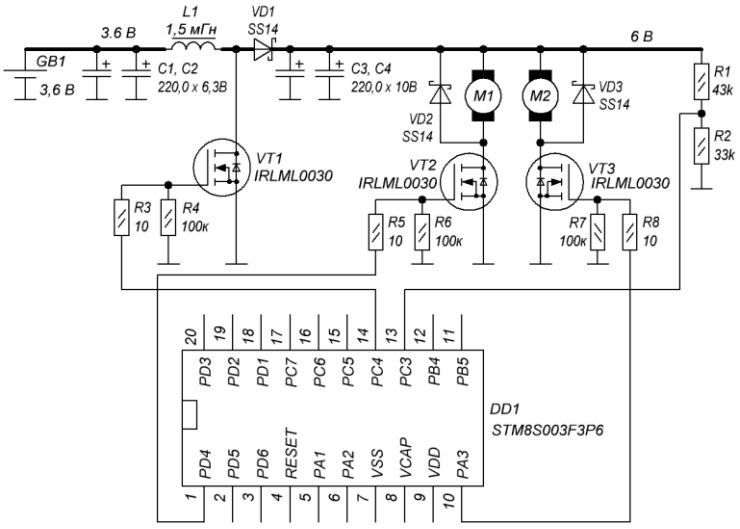


Рисунок 3 – Приклад використання цифрового контуру керування імпульсним підвищувальним перетворювачем

Висновки.

Цифрові контури керування імпульсними перетворювачами напруги забезпечують підвищену гнучкість, малі габарити та можливість адаптації до змін умов роботи без втручання в апаратну частину. Використання вже наявних ресурсів мікроконтролера дозволяє скоротити кількість компонентів, знизити вартість пристрою та забезпечити його функціональну модернізацію шляхом оновлення програмного забезпечення. Цей підхід відкриває перспективи створення компактних енергоефективних систем живлення для комп'ютерних і робототехнічних застосувань.

Література:

1. TL5002 – Pulse-Width-Modulation Control Circuit. Texas Instruments. 2000. 21 p.

2. Cem Unsalan, Duygun E. Barkana, H. Deniz Gurhan. Embedded Digital Control with Microcontrollers: Implementation with C and Python. John Wiley & Sons, 2021. 368 p.

3. Erickson R. W., Maksimovic D. Fundamentals of Power Electronics. Springer, 2020. 912 p.

УДК 621.382.2
DOI: https://doi.org/10.32837/11300.31334

Горбачов В. Е., к.т.н., доцент
Яровий Д. О., студент V курсу
Міжнародний університет
physmgu@gmail.com

ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ДАТЧИКІВ ТЕМПЕРАТУРИ У ЦИФРОВИХ СЕНСОРНИХ МЕРЕЖАХ

Анотація. *У роботі проведено експериментальні дослідження термочутливих властивостей польових транзисторів типів FEJT та MOSFET для створення високочутливих датчиків температури, придатних до використання у цифрових сенсорних мережах. Встановлено залежність струму насичення від температури та визначено чутливість детекторів. Запропоновано схеми мостового з'єднання транзисторів, які дозволяють суттєво підвищити чутливість і виправити лінійність вихідної характеристики датчиків при низькому енергоспоживанні. Крім того, мостові схеми характеризуються підвищеною стабільністю відносно змінень напруги живлення.*

Актуальність. Розвиток цифрових сенсорних мереж вимагає створення економічних високочутливих датчиків, здатних працювати у цифрових системах моніторингу фізичних величин, зокрема температури. Використання польових транзисторів в якості сенсорних елементів дозволяє поєднати високу точність вимірювань із низьким споживанням енергії, що є критично важливим для автономних бездротових сенсорних вузлів.

Формулювання проблеми. Більшість промислових температурних датчиків мають або обмежену чутливість, або підвищене енергоспоживання за рахунок необхідності додаткових пристроїв коригування чутливості, лінійності вихідної характеристики, стабілізації напруги живлення, то що [1]. Використання одиничного польового транзистора в якості сенсора забезпечує низьке споживання енергії, однак обмежується нелінійністю його вихідної характеристики [2]. Тому, питання вдосконалення параметрів таких пристроїв для підвищення точності вимірювань та узгодження їх із цифровими сенсорними мережами потребує додаткових досліджень [3].

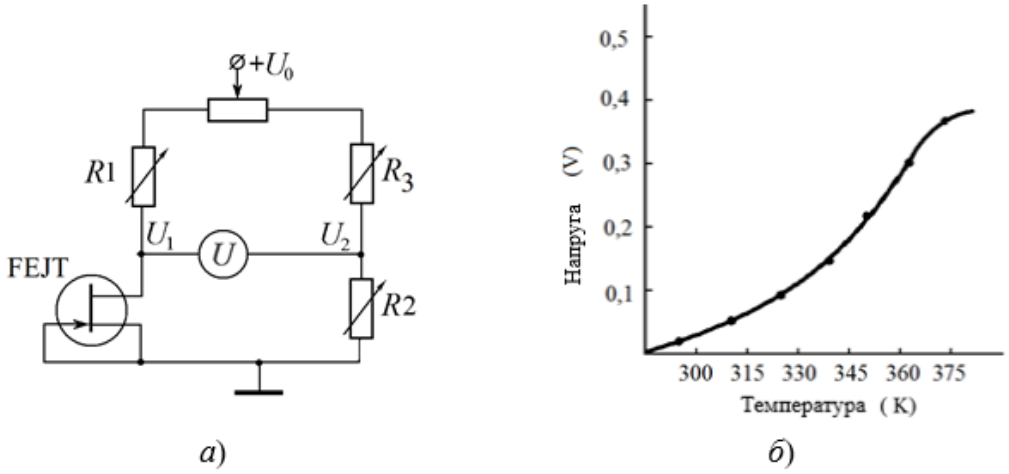
Мета роботи. Метою дослідження є визначення основних параметрів датчиків температури на основі польових транзисторів та розроблення таких схемних рішень, які забезпечують високу чутливість, лінійність і низьке енергоспоживання при можливості їх інтеграції в цифрові сенсорні мережі.

Методи дослідження. Дослідження залежності вихідного параметра датчика від температури проводилися на двох типах серійних промислових транзисторів: FEJT (польовий транзистор із керуючим p-n переходом, типу 2П202Г) та MOSFET (польовий метал-оксід-напівпровідниковий транзистор із вбудованим каналом, типу КП305). Були отримані теоретичні моделі залежності вихідної напруги датчика температури на польовому транзисторі із керуючим p-n переходом від температури та вихідної напруги датчика температури на польовому метал-оксід-напівпровідниковму транзисторі із керуючим p-n переходом від температури. Для перевірки теоретичної моделі було проведено комп'ютерний експеримент. Для цього було складено код розрахунку залежності вихідного параметру датчика в залежності від температури. Параметри транзисторів були обрані з заводських паспортів транзисторів.

Досліджено температурну залежність струму насичення FEJT і MOSFET. Для FEJT встановлено зменшення струму насичення зі зростанням температури, при цьому температурна чутливість датчика складала 7,5 μA/°C. У протилежність тому, для MOSFET зафіксовано збільшення струму насичення зі зростанням зовнішньої температури при цьому температурна чутливість датчика складала 6,8 μA/°C.

Отримані результати досліджень з використання транзисторів в якості чутливих до температури елементів підтверджують їх можливості, але також виявляють суттєві недоліки, такі як нелінійність вихідної характеристики та недостатня чутливість. Підвищення ефективності датчиків температури можливе завдяки мостовим конфігураціям, у яких реалізується взаємне підсилення сигналів від елементів з протилежною температурною поведінкою. Важливою перевагою мостових схем є той факт, що вихідним параметром датчиків є не абсолютне значення струму чи напруги, а різниця напруги у протилежних плечах мосту, завдяки чому такі датчики характеризуються підвищеною стабільністю відносно змінень напруги живлення.

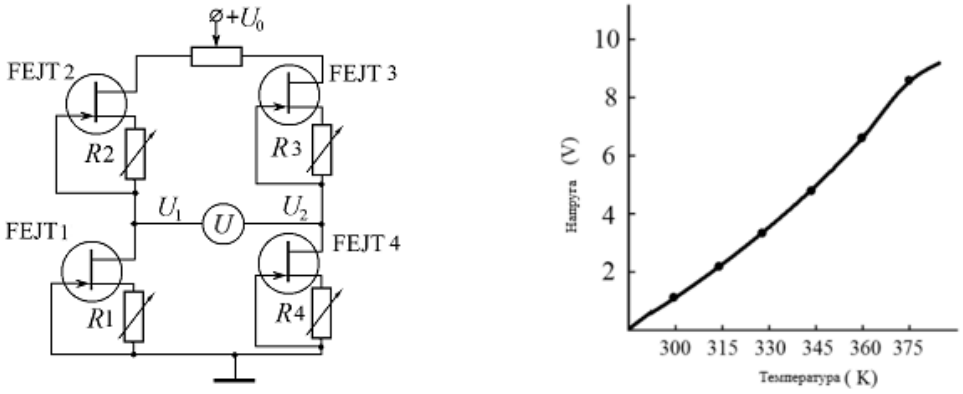
Запропоновано кілька схем покращення характеристик датчиків температури. Мостова схема на одному FEJT (рис. 1, *а*) забезпечила чутливість 5 мВ/°C. при споживанні 9,5 мВт. Але вихідна характеристика такого датчика температури є нелінійною (рис. 1, *б*).



а) *б*)

Рисунок 1 – Принципова схема мостового кола детектора температури на одному FEJT транзисторі (*а*) та його вихідної характеристики (*б*)

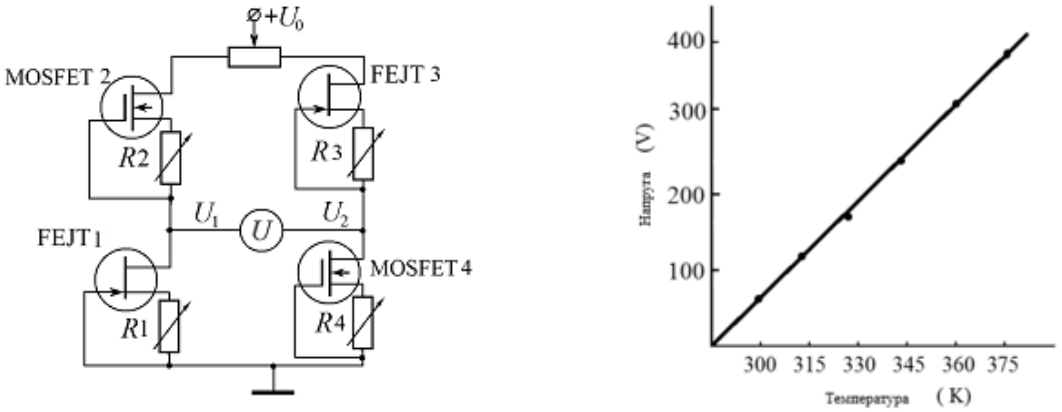
Мостова схема, зібраний на чотирьох транзисторах FEJT (рис. 2, *а*) підвищив чутливість до 110 мВ/°C при споживанні 41 мВт. Вихідна характеристика такого датчика температури є нелінійною (рис. 2, *б*).



а) *б*)

Рисунок 2 – Принципова схема мостового кола детектора температури на чотирьох FEJT транзисторах (*а*) та її вихіднай характеристика (*б*)

Комбінована схема датчика температури на двох транзисторах FEJT та на двох транзисторах MOSFET, які розташовані у протилежних діагоналях мосту (рис. 3, *а*), дала лінійну вихідну характеристику та найбільшу чутливість 320 мВ/°С при енергоспоживанні лише 38 мВт.



а) *б*)

Рисунок 3 – Принципова схема мостового кола детектора температури на двох транзисторах FEJT та на двох MOSFET (*а*) та її вихідної характеристики (*б*)

Отримані результати перевищують показники стандартних аналогових детекторів у кілька разів за чутливістю при суттєвому зниженні споживаної потужності.

Висновки. На основі серійних польових транзисторів можливо створювати високоефективні, малопотужні та лінійні температурні сенсори для цифрових сенсорних мереж. Комбіновані мостові схеми з FEJT і MOSFET забезпечують оптимальне співвідношення чутливості, енергоспоживання та стабільності, що робить їх перспективними для використання у системах моніторингу навколишнього середовища, промислових та наукових застосуваннях.

Література:

1. Diarah R. S. Types of Temperature Sensors / R. S. Diarah, C. Osueke, A. Adekunle // Wireless Sensor Networks - Design, Applications and Challenges. London: IntechOpen. – 2023. 110648. DOI: 10.5772/intechopen.110648.

2. Мартинюк В. Сенсори температури на базі CMOS / В. Мартинюк, О. Малюк // Вісник Хмельницького національного університету. – 2024. Т. 333, – № 2. – С. 380-388. DOI https://doi.org/10.31891/2307-5732-2024-333-2-59.

3. Осадчук Я. О. Дослідження автогенераторних параметричних сенсорів температури / Я. О. Осадчук, О. В. Осадчук, В. С. Осадчук // Вісник Хмельницького національного університету. – 2022. Т. 305, – № 1. – С. 175-183. DOI https://doi.org/ 10.31891/2307-5732-2022-305-1-175-183.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

DOI: https://doi.org/10.32837/11300.31328

Перчеклій Дмитро Володимирович
Здобувач, Міжнародний університет
dmytropercheklii@gmail.com
Науковий керівник Йона Лариса Григорівна

ДОСЛІДЖЕННЯ ІНТЕГРАЦІЇ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ПЛАТІЖНІ СИСТЕМИ

Анотація. *У даних тезах розглядаються ключові особливості впровадження технології блокчейн у сучасні платіжні системи. Проаналізовано основні переваги використання блокчейну — зокрема, підвищення рівня безпеки, прозорості операцій, швидкості виконання транзакцій і зменшення комісійних витрат. Також визначено основні проблеми, які виникають під час інтеграції цієї технології в існуючу банківську інфраструктуру: масштабованість, регуляторна невизначеність, технічна сумісність та потреба у кваліфікованих спеціалістах. Наведено приклади моделей, що поєднують традиційні платіжні системи з децентралізованими рішеннями, а також окреслено напрями подальших досліджень у цій сфері.*

Платіжні системи є невід'ємною складовою сучасної фінансової інфраструктури. Вони забезпечують швидке та безпечне переміщення коштів між користувачами, компаніями та державними установами. Однак більшість таких систем мають централізовану структуру, що робить їх залежними від посередників, регуляторів і технічних обмежень.

У традиційних міжбанківських розрахунках залучається велика кількість посередників: клірингові палати, банки-кореспонденти, процесингові центри. Через це операції можуть тривати кілька днів, а розмір комісій часто є суттєвим. Крім того, централізована архітектура створює певні ризики, адже збої чи атаки на центральний вузол можуть призвести до тимчасової зупинки всієї системи.

Поява технології блокчейн стала важливою подією у розвитку фінансових технологій. Вона дає змогу створювати розподілені бази даних, у яких усі учасники мають доступ до єдиного реєстру транзакцій. Завдяки цьому з'являється можливість здійснювати розрахунки напряму — без участі посередників. Такий підхід може суттєво змінити підхід до проведення платежів і підвищити ефективність фінансових операцій.

Метою цієї роботи є аналіз можливостей, переваг та проблем, пов'язаних із впровадженням технології блокчейн у платіжні системи.

Переваги інтеграції блокчейну в платіжні системи

1. Підвищена безпека.
   Блокчейн використовує криптографічні алгоритми, які забезпечують цілісність і захист даних. Кожна транзакція підтверджується мережею учасників і записується у вигляді блоку, що пов'язаний з попередніми. Підробити або змінити запис майже неможливо. Це знижує ризики шахрайства, подвійних платежів та несанкціонованого доступу.
2. Прозорість і довіра.
   Завдяки відкритій природі блокчейну всі учасники системи можуть бачити історію операцій (залежно від рівня доступу). Це полегшує аудит, звітність і підвищує довіру між сторонами. У корпоративних і банківських рішеннях використовуються приватні блокчейни, де доступ мають лише авторизовані учасники, що дозволяє поєднати прозорість і конфіденційність.

3. Менше посередників і нижчі витрати.
   Одна з головних переваг блокчейну — можливість здійснювати платежі безпосередньо між користувачами (P2P). Це усуває потребу у банках-кореспондентах і процесингових центрах, що значно скорочує час обробки транзакцій і зменшує витрати на комісії. Для міжнародних переказів це може бути особливо вигідно.
4. Висока швидкість транзакцій.
   Традиційні міжбанківські платежі можуть займати кілька днів, тоді як операції в блокчейні виконуються за секунди або хвилини. Сучасні рішення на базі приватних блокчейнів і систем другого рівня (Layer 2) дозволяють досягати тисяч транзакцій на секунду, що наближає їх за швидкодією до глобальних систем, таких як Visa або Mastercard.
5. Смарт-контракти.
   Це програмні алгоритми, які автоматично виконують умови угоди. У платіжних системах вони можуть застосовуватися для автоматичних розрахунків після виконання певних дій (наприклад, поставки товару чи виконання послуги). Це знижує кількість ручних операцій та помилок, а також підвищує ефективність бізнес-процесів.

   Основні виклики впровадження технології

1. Масштабованість.
   Одна з головних проблем блокчейну — обмежена кількість транзакцій, які система може обробити одночасно. Публічні блокчейни, як-от Bitcoin чи Ethereum, не здатні забезпечити швидкість, необхідну для масових платежів. Розробники шукають рішення — наприклад, використання алгоритму Proof-of-Stake або технології шардингу, що дозволяє розділяти навантаження між вузлами.
2. Сумісність систем.
   Існує безліч блокчейн-платформ (Ethereum, Ripple, Hyperledger, Corda тощо), які часто не взаємодіють між собою. Для створення єдиної глобальної платіжної екосистеми необхідна інтеграція між різними мережами та взаємодія з існуючими банківськими системами (SWIFT, SEPA).
3. Невизначеність у законодавстві.
   У різних країнах відсутні єдині правила щодо використання цифрових активів, оподаткування чи ідентифікації користувачів. Це створює ризики для компаній і банків, які хотіли б використовувати блокчейн у своїй діяльності.
4. Витрати енергії.
   Деякі блокчейн-мережі, особливо ті, що використовують алгоритм Proof-of-Work, споживають значні обсяги електроенергії. Це робить їх менш екологічними та дорогими в обслуговуванні.
5. Кадровий дефіцит і складність впровадження.
   Блокчейн-проєкти вимагають висококваліфікованих спеціалістів у галузі криптографії, безпеки та розробки децентралізованих систем. Поки що таких фахівців бракує, що ускладнює впровадження технології у великі платіжні мережі.

   Моделі інтеграції блокчейну

1. Транскордонні перекази.
   Блокчейн може використовуватися для обміну коштами між банками різних країн без

залучення посередників. Наприклад, мережа RippleNet уже пропонує рішення для швидких міжнародних платежів.

2. Використання стейблкоїнів.
   Стейблкоїни — це цифрові токени, вартість яких прив'язана до фіатної валюти (долара, євро чи гривні). Вони поєднують стабільність традиційних грошей із швидкістю криптовалют.
3. Цифрові валюти центральних банків (CBDC).
   Багато країн, зокрема Китай, ЄС та Україна, вивчають можливість випуску національних цифрових валют. Це дозволить державі контролювати грошовий обіг і водночас зробити платежі швидшими та доступнішими.
4. Децентралізовані фінанси (DeFi).
   DeFi-проєкти створюють нову фінансову екосистему, де користувачі можуть самостійно здійснювати платежі, кредити чи інвестиції без участі банків. Хоча цей напрям ще молодий, він показує потенціал для розвитку нових моделей платіжних систем.

Висновки.

Технологія блокчейн може суттєво покращити роботу платіжних систем — зробити їх безпечнішими, швидшими та дешевшими. Проте впровадження блокчейну — це складний процес, який вимагає часу, нових стандартів і законодавчої бази.

Найближчим часом, ймовірно, відбудеться не повна заміна старих систем, а поступовий перехід до гібридної моделі — коли традиційні платіжні мережі частково використовуватимуть блокчейн для розрахунків і взаємодії між банками.

Подальші дослідження мають бути спрямовані на вдосконалення сумісності між різними блокчейнами, зменшення енергоспоживання та розробку чітких правил для використання цієї технології у фінансовій сфері.

Література:

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource] / S. Nakamoto. – 2008. – Mode of access: https://bitcoin.org/bitcoin.pdf.

2. Tapscott D. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World / D. Tapscott, A. Tapscott. – Portfolio, 2016. – 368 p.

3. Buterin V. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform [Electronic resource] / V. Buterin. – 2014. – Mode of access: https://ethereum.org/en/whitepaper/

4. Global Blockchain Survey 2021 // Deloitte's 2021 Global Blockchain Survey. – 2021. – Mode of access: https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/global-blockchain-survey.html

5. Committee on Payments and Market Infrastructures (CPMI). Central bank digital currencies: foundational principles and core features / Bank for International Settlements (BIS). – October 2020. – 34 p.

6. A Guide to Blockchain Interoperability // ConsenSys. – 2023. – Mode of access: https://consensys.io/blockchain-explained/interoperability

7. Narayanan A. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction / A. Narayanan, J. Bonneau, E. Felten. – Princeton University Press, 2016. – 336 p.

DOI: https://doi.org/10.32837/11300.31330

Петков Євген Ігорович.
Аспірант, спеціальність 125 Кібербезпека та захист інформації,
Міжнародний університет
yepetkov@gmail.com
Науковий керівник
Йона Лариса Григорівна, к.т.н.,
Завідувач, доцент кафедри комп'ютерної інженерії та інноваційних технологій
Факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародного університету
yonalarisa66@gmail.com

ПРИНЦИПИ РОБОТИ DOS, DDOS АТАК ТА ЗАСОБИ ЗАХИСТУ ПРОТИ НИХ

Анотація. *Дослідження розглядає загальні принципи роботи DoS, DDoS атак, методи виявлення та засоби захисту проти них.*

У сучасному цифровому середовищі захист інформаційних систем є ключовим елементом роботи будь-якої організації. Серед найпоширеніших і найсерйозніших загроз для стабільності серверів та мереж виділяються DoS (Denial of Service) та DDoS (Distributed Denial of Service) атаки. Їхня основна мета — вивести ресурс із строю, зробити його недоступним для користувачів, завдати фінансових втрат або пошкодити репутацію компанії.

DoS-атаки (Denial of Service) базуються на принципі перевантаження ресурсів цільової системи, що призводить до її недоступності для легітимних користувачів. Атакуючий генерує величезну кількість запитів або трафіку, спрямованого на сервер, мережевий пристрій чи додаток, перевищуючи їхню пропускну здатність або обчислювальні можливості. Це може бути досягнуто шляхом надсилання пакетів SYN без завершення TCP-з'єднання (SYN-флуд), надмірного використання протоколів ICMP (наприклад, ping-флуд), або експлуатації вразливостей у програмному забезпеченні. Внаслідок цього сервер витрачає всі доступні ресурси на обробку шкідливого трафіку, не залишаючи можливостей для обслуговування реальних запитів, що й забезпечує відмову в обслуговуванні. Приклад DoS-атаки зображено на рис.1.

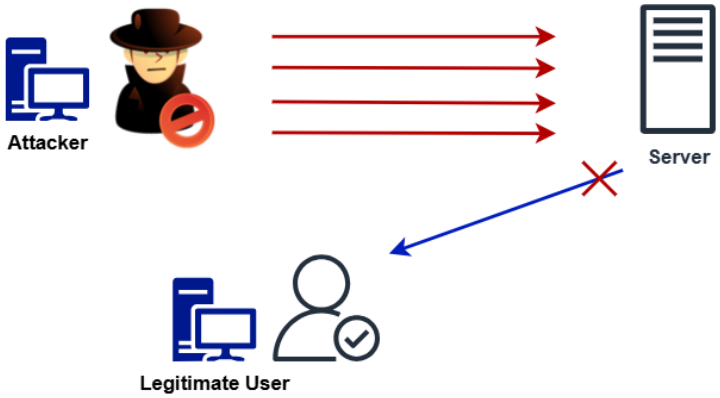


Рисунок 1 – Принцип роботи DoS-атаки

DDoS-атаки (Distributed Denial of Service) базуються на принципі розподіленого перевантаження ресурсів цільової системи за рахунок великої кількості заражених пристроїв,

об’єднаних у ботнет. Зловмисник, або так званий ботмайстер, інфікує тисячі чи навіть мільйони комп’ютерів, смартфонів та IoT-пристроїв шкідливим програмним забезпеченням, після чого Сервер Керування (Command and Control Server) одночасно активує їх для створення потужного потоку трафіку на адресу жертви. Такий трафік може бути об’ємним (наприклад, UDP-flood або DNS-ампліфікація), спрямованим на рівень додатків (HTTP-flood із GET чи POST-запитами) або поєднувати кілька методів одночасно. Завдяки розподіленій природі атаки обсяг шкідливих запитів значно перевищує можливості звичайної DoS-атаки, що ускладнює їхнє фільтрування й блокування, часто призводячи до повної недоступності сервера або мережі для справжніх користувачів.

Для виявлення DoS та DDoS-атак, можуть використовуватись методи:

- Моніторинг трафіку. Постійне відстеження в реальному часі обсягу запитів і трафіку в мережі, або на серверне обладнання. Атака виявляється при аномальному сплеску (наприклад, зростання трафіку на 300% від базового рівня). Використовуються такі протоколи як NetFlow/ sFlow (аналіз потоків пакетів) та SNMP (моніторинг стану пристроїв), разом із системами моніторингу.
- Аналіз логів подій. Перегляд серверних і мережевих логів на наявність підозрілих IP-адрес, геолокацій або повторюваних шаблонів (наприклад, масові запити з однієї підмережі). Використовуються SIEM-системи (Splunk, ELK), які збирають, корелюють і аналізують логи з різних джерел.
- Сигнатурний аналіз. Порівняння вхідного трафіку з базою відомих сигнатур атак (наприклад, SYN-флуд, HTTP-флуд). Ефективний проти типових, раніше зафіксованих векторів атак. Тут можуть використовуватись IDS/IPS (Intrusion Detection System, Intrusion Prevention System - системи виявлення та запобігання вторгнень), які аналізують трафік у реальному часі, виявляють аномалії (наприклад, надмірну кількість півз’єднань) і можуть автоматично блокувати шкідливі джерела або обмежувати трафік.

Засоби захисту від DoS/DDoS-атак вимагають багатошарового підходу, що охоплює різні рівні та ділянки IT-інфраструктури. На мережевому рівні розгортаються апаратні та програмні фаєрволи (як NGFW – Next Generation Filrewalls), разом із системами виявлення та запобігання вторгнень (IDS/IPS), які аналізують сигнатури атак і блокують аномальний трафік; балансувальники навантаження (наприклад, F5 Big-IP, NGINX, HAProxy) розподіляють запити між серверами та автоматично відсікають підозрілі джерела. На рівні транспортної мережі провайдера ефективні техніки BGP FlowSpec, а також blackhole routing для перенаправлення шкідливого трафіку в «чорну діру». Хмарні рішення (Cloudflare, Akamai, AWS Shield Advanced, Azure DDoS Protection) забезпечують глобальну мережу розподілення трафіка (CDN - Content Delivery Network), а також хмарні Анти-DDoS сервіси, де трафік очищається від атак до надходження на кінцевий сервер замовника; вони здатні витримувати атаки об’ємом у сотні Gbps/Tbps. На рівні додатків може застосовуватись WAF (Web Application Firewall), який фільтрує HTTP/HTTPS-запити, блокуючи шкідливі та надмірні запити; функції rate limiting та throttling обмежують кількість запитів з однієї IP (наприклад, не більше 100 запитів/хв), а CAPTCHA та JavaScript-челенджі відсіюють ботів. Додатково можуть впроваджуватись чорні та білі списки IP, геоблокування (дозвіл трафіку лише з певних країн), резервні канали зв’язку через кількох провайдерів, а також регулярне оновлення ПЗ, патчинг вразливостей (CVE) і навчання персоналу — все це разом створює стійку систему захисту, здатну виявляти, зменшувати вплив та відновлюватися після DoS/DDoS-атак будь-якої складності.

Висновок. DoS і DDoS-атаки становлять одну з найсерйозніших загроз для стабільності та безпеки будь-якої IT-інфраструктури. Їх небезпека полягає в тому, що вони відносно прості у реалізації, але водночас надзвичайно складні для повного запобігання та нейтралізації. Навіть короткочасна атака може призвести до зупинки бізнес-процесів,

фінансових та репутаціних втрат компанії. Однак завдяки розвитку сучасних технологій — таких як хмарні платформи з вбудованими механізмами безпеки, системи інтелектуального аналізу мережевого трафіку, а також алгоритми машинного навчання для виявлення аномалій — сьогодні можливо суттєво підвищити ефективність захисту. Важливо використовувати гібридний підхід до кіберзахисту, який поєднує різні методи моніторингу, фільтрації та реагування на атаки. Такий багаторівневий захист дозволяє своєчасно виявляти DoS і DDoS-атаки та мінімізувати їхній вплив.

Література:

1. Тези всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених «Екзистенційні виклики освіти, науки, безпеки та здоров'я в сучасних умовах: пошуки молодих вчених». Петков Є.І. «Аналіз поточного стану криптографічних протоколів». URL: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/book/372.

2. Петков Є. І. Типи спуфінг атак та засобів захисту в локальних мережах / Є. І. Петков // Передові технології в інформаційно-комунікаційній інженерії (ATICE'2025) : матеріали Міжнародної конференції / за заг ред. С. В. Ківалова ; Міжнародний університет. Одеса : Видавничий дім «Гельветика», 2025. С. 85-90. URL: https://hdl.handle.net/11300/30133; DOI: 10.32837/11300.30133

3. Cloudflare's 2025 Q2 DDoS threat report. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/.

4. Cloudflare's 2025 Q1 DDoS Threat Report. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/.

5. Cloudflare. What is a DDoS attack? URL: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/.

6. Fortinet. What Is The Difference Between DoS Attacks And DDoS Attacks? URL: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

7. AWS. DDoS Attack Protection. URL: https://aws.amazon.com/shield/ddos-attack-protection/.

8. F5. F5 DDoS Protection: Recommended Practices. URL: https://www.f5.com/pdf/products/ddos-protection-recommended-practices.pdf.

DOI: https://doi.org/10.32837/11300.31332

Бєліков Дмитро Вячеславович
Міжнародний університет
iriska3434dima@gmail.com
Науковий керівник: Йона Лариса Григорівна зав.каф. КІmaIT, доцент, к.т.н.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ ЗАГРОЗ

Анотація. *Соціальна інженерія (СІ) є домінуючим вектором кібератак, посиленим генеративним ШІ (GenAI). Дослідження аналізує ландшафт загроз 2024-2025 років та обґрунтовує необхідність переходу від фокусування на 'Click Rate' до 'Reporting Rate' як ключової метрики стійкості. На основі аналізу запропоновано комплексну, багаторівневу стратегію 'Defense-in-Depth', що поєднує технічні (DMARC), адміністративні (PoLP, IR Plan) та інноваційні людські методи.*

1. Психологічна парадигма сучасної кіберзагрози

Сучасний ландшафт кібербезпеки демонструє тривожний парадокс. Організації інвестують мільярдні кошти в технологічні засоби захисту, проте переважна більшість успішних кібератак — до 98% — покладаються не на технічні експлойти, а на маніпуляцію.

Соціальна інженерія (СІ) оминає технологічні бар'єри, націлюючись безпосередньо на "людський фактор".

Ефективність СІ ґрунтується на експлуатації фундаментальних психологічних механізмів та когнітивних попереджень, які є невід'ємною частиною людської поведінки. Зловмисники цілеспрямовано використовують принципи переконання, ідентифіковані Робертом Чалдіні, такі як Авторитет (імперсонація керівництва), Терміновість (вимога негайної дії) та Соціальний доказ. Це перетворює загрозу із суто технічної на психологічну, роблячи традиційні методи захисту недостатньо ефективними.

2. Новий каталізатор: Вплив Генеративного ШІ (GenAI)

Якщо СІ завжди було ефективним, то поява генеративного ШІ (GenAI) у 2024-2025 роках стала потужним «підсилювачем загрози». GenAI докорінно змінює економіку та ефективність атак, руйнуючи традиційний компроміс зловмисників між масштабом та якістю. Це призвело до появи нового класу загроз: «масово-персоналізованих атак».

Ключові вектори посилення атак за допомогою GenAI:

Бездоганні фішингові приманки: GenAI дозволяє масово створювати ідеально написані, контекстуально обізнані листи на будь-якому мові, що імітують стиль спілкування конкретної особи.

Клонування голосу та Deepfakes: Технології GenAI використовують для створення переконливих атак Vishing (голосовий фішинг), де зловмисник говоритиме голосом керівника або колеги.

Інтерактивні атаки в реальному часі: ШІ-агенти можуть підтримувати "живу" взаємодію з жертвою, миттєво генеруючи переконливі відповіді на її запитання та розвіюючи сумніви.

3. Вимірювання стійкості: Перехід від Click Rate до Reporting Rate

Для протидії новим загрозам потрібна адекватна система вимірювання. Традиційні симуляції фішингу (наприклад, за допомогою Gophish) є дієвим методом кількісної оцінки вразливості персоналу, що вимірює «Phish-prone Percentage» (Click Rate). Цей показник фіксує відсоток співробітників, які натиснули на шкідливе посилання.

Однак, фокусування лише на цій метриці є помилкою, оскільки вона вимірює виключно невдачу. Зріла програма безпеки повинна вимірювати стійкість (Resilience). Набагато ціннішою метрикою є Reporting Rate (коефіцієнт звітування) — відсоток співробітників, які розпізнали загрозу та повідомили про неї у службу безпеки. Ефективна програма захисту має демонструвати чітку динаміку: одночасно зниження Click Rate при зростанні Reporting Rate.

4. Комплексна багаторівнева стратегія захисту (Defense-in-Depth)

Результати аналізу доводять, що покладатися лише на один рівень захисту (технології чи тренінги) — недостатньо. Ефективний захист вимагає інтегрованої, багаторівневої стратегії "Defense-in-Depth", що діє на трьох ключових рівнях.

4.1. Рівень 1: Технічний захист (DMARC)

Перший рівень має на меті автоматично блокувати якомога більше загроз. У контексті СІ, що покладається на спуфінг (підробку) email-адреси, ключовим є впровадження протоколів автентифікації пошти. Тільки DMARC з коректно налаштованим "вирівнюванням" (Alignment) та політикою p=reject є найефективнішим технічним контрзаходом. Він вимагає, щоб домен, який бачить користувач у полі `From:`, збігався з доменом, що пройшов автентифікацію SPF/DKIM, блокуючи найпоширеніші тактики обману.

4.2. Рівень 2: Адміністративний захист (PoLP та IR Plan)

Цей рівень діє як "обмежувач шкоди".

Принцип найменших привілеїв (PoLP): Ця концепція вимагає, щоб користувачам надавався лише мінімально необхідний рівень доступу. PoLP не запобігає успішному фішингу, але драматично обмежує шкоду, блокуючи швидке латеральне переміщення та ескалацію привілеїв.

План реагування на інциденти (IR Plan): Наявність задокументованого та відрепетованого IR Plan є критичною. Найважливішими є те, що найшвидшим тригером для цього плану є не лише технічні засоби (SIEM/EDR), а й сам співробітник, який негайно повідомляє про інцидент.

4.3. Рівень 3: Людський захист ("Людський брандмауер")

Це фінальний рівень захисту. "Людський брандмауер" - це не пасивна стіна, а активна система виявлення. Проте традиційні щорічні тренінги є неефективними. Для побудови дієвого "людського брандмауера" потрібний перехід до безперервного, гейміфікованого мікронавчання. Цей підхід, заснований на поведінковій науці (напр., модель B=MAP Фогга) та гейміфікації (балі, значки, лідерборди), використовує позитивні психологічні стимули для боротьби з негативними маніпуляціями зловмисників.

Висновки.

Соціальна інженерія залишається домінуючою та найбільш небезпечною загрозою, оскільки вона націлена на незмінну людську психологію. Поява GenAI лише посилює цю загрозу, демократизуючи складні, персоналізовані атаки.

Дослідження стверджує, що ефективна захист не може бути досягнута жодним окремим рішенням. Він вимагає побудови глибоко інтегрованої системи Defense-in-Depth, де кожен рівень підтримує інший:

1. Технічні засоби (DMARC) відсіюють 99% автоматизованих атак.
2. Адміністративні політики (PoLP, IR Plan) стримують та обмежують шкоду від тих атак, що пройшли.
3. Людський брандмауер, навчений через безперервну гейміфікацію, слугує найдосконалішим сенсором, що виявляє цільові, згенеровані ШІ атаки, та негайно активує План реагування на інциденти.

Лише така синергетична стратегія здатна забезпечити реальну стійкість організації в умовах сучасного ландшафту кіберзагроз.

Література:

1. Cost of a Data Breach Report 2024/IBM Security; Ponemon Institute. 2024. URL: https://www.ibm.com/reports/data-breach.

2. 2024 Data Breach Investigations Report (DBIR) / Verizon. 2024. URL: https://www.verizon.com/business/resources/reports/dbir/.

3. 2024 Phishing by Industry Benchmarking Report / KnowBe4. 2024. URL: https://www.knowbe4.com/hubfs/final_2024_phishing_benchmark_report.pdf.

4. Чалдіні Р. Психологія впливу. Упевнюйте та досягайте успіху!. Харків: КОД, 2024. 608 с.

5. Computer Security Incident Handling Guide : NIST Special Publication 800-61 Rev. 3/National Institute of Standards and Technology. 2025. URL: https://csrc.nist.gov/pubs/sp/800-61/r3/final.

DOI: https://doi.org/10.32837/11300.31335

Чебанюк Олексій Дмитрович
бакалавр, спеціальність
014«Середня освіта (Інформатика та програмування)»
Міжнародний університет
chebanuk@gmail.com
Динін Борис Іванович
бакалавр, спеціальність
121 «Інженерія програмного забезпечення»
Міжнародний університет
borisdynin757@gmail.com
Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент
Міжнародний університет
yonalarisa66@gmail.com

РОЗРОБКА ТА РЕАЛІЗАЦІЯ ВИСОКОПРОДУКТИВНОЇ СИСТЕМИ ДЛЯ АГРЕГАЦІЇ ТА АНАЛІЗУ МЕТРИК КРИПТОВАЛЮТНИХ РИНКІВ У РЕАЛЬНОМУ ЧАСІ

***Анотація**. У роботі представлено архітектуру та реалізацію програмного комплексу для збору, обробки та аналізу високочастотних даних із криптовалютних бірж. Система, розроблена мовою програмування Rust, використовує асинхронну модель, багатопотокову обробку та обмін повідомленнями через ZMQ для досягнення високої продуктивності. Описано ключові модулі: обробник потоку угод, калькулятор метрик, система розрахунку рейтингу ліквідності та механізми інтеграції із зовнішніми аналітичними сервісами. Отримані результати демонструють ефективність системи для моніторингу ринку в реальному часі.*

Криптовалютні ринки характеризуються високою волатильністю та величезним обсягом торгових даних, що генеруються щомиті. Для ефективного аналізу, моніторингу та ухвалення торгових рішень необхідні інструменти, здатні обробляти ці потоки інформації в режимі реального часу з мінімальними затримками. Метою даної роботи є розробка високопродуктивної системи, здатної агрегувати необролені дані про угоди з різних бірж і на їх основі розраховувати комплексні аналітичні метрики. В якості основного інструменту розробки було обрано мову Rust завдяки її фокусу на безпеці, конкурентності та продуктивності**.**

Розроблена система побудована на модульній архітектурі, що передбачає чітке розмежування функціональності між окремими компонентами. Кожен модуль виконує специфічне завдання відповідно до своєї ролі в загальній структурі, що сприяє підвищенню керованості та спрощенню процесу розробки, тестування й супроводу. Взаємодія між модулями реалізована за допомогою асинхронних каналів зв'язку, що забезпечують незалежність виконання та зменшення затримок у передачі даних. Як транспортний механізм використовується брокер повідомлень ZMQ (ZeroMQ), який підтримує високопродуктивну обробку повідомлень, масштабованість та гнучкість у конфігурації комунікаційних шаблонів (наприклад, publish-subscribe, request-reply, push-pull). Такий підхід дозволяє ефективно адаптувати систему до змін вимог, розширювати її функціональність без суттєвого втручання в існуючу структуру та забезпечує стійкість до збоїв окремих компонентів.

Основними компонентами системи є:

1. Менеджер циклів (Loop Manager): Центральний компонент, який ініціалізує та керує всіма робочими процесами: отримання даних, обчислення метрик, збереження стану,

очищення буферів та публікація результатів. Він створює пул робочих потоків для паралельної обробки вхідних повідомлень.

2. Обробник повідомлень (Message Processor): Відповідає за парсинг та валідацію JSON-повідомлень про угоди, що надходять за підпискою ZMQ. Після обробки дані направляються до сховища метрик.

3. Сховище метрик (Metrics Storage): Потокобезпечне сховище в оперативній пам'яті, реалізоване з використанням техніки шардування для мінімізації блокувань. Дані зберігаються в циклічних буферах для різних часових інтервалів (секунди, хвилини, 10-хвилинні відрізки), що дозволяє оптимізувати процес розрахунків, забезпечуючи їх негайне виконання у реальному часі.

4. Калькулятор метрик (Metrics Calculator): Ядро аналітичної підсистеми. Використовуючи бібліотеку Polars, він на основі даних з Metrics Storage розраховує широкий спектр показників:

- обсяги торгів (загальний, на купівлю, на продаж);
- зміна ціни у відсотках за різні інтервали;
- швидкість торгів (транзакцій на секунду);
- кількість та обсяг великих угод;
- відсоткове співвідношення купівель та продажів;
- зміна відкритого інтересу (Open Interest).

5. Обробники зовнішніх даних: Система включає модулі для отримання додаткових даних, таких як OBPI (Order Book Price Imbalance), Open Interest та сигнали від зовнішніх систем (NATRs), що збагачує внутрішній набір метрик.

6. Розрахунок рейтингу ліквідності (Liquidity Rating): Спеціалізований модуль, який на основі набору зважених параметрів (обсяги за різні періоди, швидкість торгів та ін.) обчислює інтегральний рейтинг ліквідності для кожної торгової пари.

7. Публікатор ZMQ (ZMQ Publisher): Після кожного циклу обчислень система публікує розраховані метрики в топік ZMQ, роблячи їх доступними для інших сервісів (наприклад, торгових ботів або дашбордів).

Ключові технічні рішення

Для забезпечення високої продуктивності та відмовостійкості були застосовані такі підходи:

- Асинхронність та багатопотоковість: Використання tokio та rayon дозволяє ефективно розпаралелювати завдання: отримання даних, їх обробка та розрахунок метрик відбуваються одночасно, не блокуючи один одного.

- Ефективне зберігання даних: Застосування циклічних буферів для зберігання часових рядів дозволяє уникнути постійного перерозподілу пам'яті та забезпечує швидкий доступ до даних для розрахунків ковзних вікон.

- Динамічна обробка списку монет: Система автоматично відстежує делістинг монет (DelistedCoinHandler), видаляючи їх зі сховищ, що запобігає накопиченню неактуальних даних.

- Персистентність: Реалізовано механізм періодичного збереження стану Metrics Storage на диск (SaverHandler), що дозволяє відновлювати роботу системи після перезапуску без втрати накопичених даних.

Розроблений програмний комплекс охоплює повний цикл збору, обробки та візуалізації ринкових даних, включаючи інтеграцію з API провідних бірж, механізми кешування, а також

систему сповіщень про аномальні події. Особливу увагу приділено аналітичному модулю, який надає користувачеві розширений набір метрик для оцінки ринкової динаміки, серед яких — унікальний рейтинг ліквідності, що враховує як обсяг торгів, так і глибину ордербуку.

Висновки.

У ході виконання роботи було спроєктовано та реалізовано багатокомпонентну програмну систему, призначену для глибокого аналізу криптовалютних ринків у режимі реального часу. Архітектура рішення передбачає чітке розділення функціональних модулів, що забезпечує високу масштабованість, гнучкість та зручність супроводу. Ключовим технологічним вибором стала мова програмування Rust, яка завдяки своїй безпечній моделі пам'яті, високій продуктивності та підтримці паралельних обчислень, дозволила реалізувати ефективну обробку великих обсягів даних із мінімальними затримками.

Система спроєктована з урахуванням перспективи подальшого розвитку: її модульна структура дозволяє легко інтегрувати нові алгоритми, підключати додаткові джерела даних, а також адаптувати функціонал під потреби конкретних сценаріїв - від побудови складних аналітичних панелей до реалізації алгоритмічних торгових стратегій та систем автоматизованого моніторингу. Таким чином, створене рішення не лише задовольняє поточні вимоги до аналізу криптовалютних ринків, а й формує надійну основу для подальших досліджень і розробок у сфері фінансових технологій.

Література:

1. Hintjens P. ZeroMQ: Messaging for Many Applications. O'Reilly Media, 2013. – 502 p.
2. Polars User Guide [Electronic resource] // Polars Documentation. – Mode of access: access:https://pola-rs.github.io/polars-book/user-guide/.
3. Rust Documentation [Electronic resource] // The Rust Programming Language. – Mode of access: https://rust-lang.org/learn.
4. Binance API Documentation access:https://www.binance.com/en/binance-api

DOI: https://doi.org/10.32837/11300.31336

Тімофєєв Олександр Олександрович
бакалавр, спеціальність 125
«Кібербезпека та захист інформації»
Міжнародний університет
timofeev.kraken@gmail.com
Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент
Міжнародний університет
yonalarisa66@gmail.com

ФОРМАЛЬНІ МЕТОДИ АНАЛІЗУ ВРАЗЛИВОСТЕЙ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

***Анотація**. У роботі досліджено вразливості систем електронного документообігу (СЕД) з використанням формальних методів моделювання. Запропоновано методику аналізу на основі моделі загроз STRIDE та інструментів формальної верифікації NuSMV і TLA+. Виявлено та усунуто логічні помилки в протоколах документообігу. Показано, що формальна верифікація досягає 100% ефективності у виявленні критичних вразливостей, що підтверджує доцільність її застосування в критичних системах.*

Системи електронного документообігу є критично важливими компонентами сучасної цифрової інфраструктури, які забезпечують управління документами, автоматизацію бізнес-процесів та захист інформації. Однак із розширенням функціональності СЕД зростають і вимоги до їх інформаційної безпеки. Документи часто містять конфіденційні дані, що робить ці системи привабливою ціллю для кіберзлочинців [1, 2].

Традиційні методи тестування не завжди здатні виявити приховані логічні вади в протоколах документообігу, що може призвести до порушення конфіденційності, цілісності або доступності інформації. У зв'язку з цим актуальним є застосування формальних методів моделювання та верифікації для математично обґрунтованої перевірки властивостей безпеки СЕД [3, 4]. Метою дослідження було розробити методику аналізу вразливостей систем електронного документообігу з використанням формальних методів, провести моделювання типових загроз і оцінити ефективність захисних механізмів.

На основі аналізу сучасних СЕД було розроблено матричну модель загроз, що класифікує загрози за рівнями (глобальні, організаційні, технічні, операційні, користувацькі) та типами активів (документи, користувачі, канали зв'язку, сервери, програмне забезпечення). Такий підхід забезпечує багатовимірне представлення ризиків і дозволяє точніше ідентифікувати вразливі компоненти СЕД.

Результати дослідження засвідчили, що найбільшу небезпеку для функціонування СЕД становлять саме технічні загрози, які мають потенціал спричинити критичні порушення конфіденційності, цілісності та доступності інформації. До найпоширеніших і найнебезпечніших технічних загроз віднесено несанкціонований доступ до документів, що може призвести до витоку або модифікації чутливої інформації; крадіжку облікових даних, яка відкриває шлях до компрометації облікових записів користувачів; атаки типу «людина посередині» (MITM) та фішингові кампанії, що спрямовані на перехоплення або підробку автентифікаційних даних; розподілені атаки на відмову в обслуговуванні (DDoS), які здатні паралізувати роботу системи; а також використання шкідливого програмного забезпечення, включно з експлуатацією вразливостей і наявністю бекдорів у програмному коді. Усі ці загрози потребують особливої уваги при проєктуванні, впровадженні та аудиті СЕД, оскільки вони можуть мати як безпосередні, так і відкладені наслідки для інформаційної безпеки організації.

Для систематизації загроз застосовано модель **STRIDE**, яка охоплює шість категорій [5]:

— **S**poofing (підміна особи);

— **T**ampering (порушення цілісності);

— **R**epudiation (відмова від дій);

— **I**nformation Disclosure (розголошення інформації);

— **D**enial of Service (порушення доступності);

— **E**levation of Privilege (ескалація привілеїв).

У межах дослідження було здійснено формальне моделювання протоколу обробки платіжного документа в електронній банківській системі. Як приклад було обрано типовий протокол, що охоплює послідовність етапів: створення документа, підпис бухгалтера, підпис керівника, передача до банку та архівування.

[Створення] → [Підпис бухгалтера] → [Підпис керівника] → [Передача до банку] → [Архів]

Для формалізації цього процесу застосовано підхід скінченного автомата, в якому кожен етап обробки представлено як окремий стан, а дії користувачів — як переходи між

станами. Така модель дозволяє чітко описати логіку документообігу, виявити потенційні вразливості та забезпечити основу для подальшої формальної верифікації властивостей безпеки протоколу.

Для перевірки коректності протоколу сформульовано властивості у логіці LTL (Linear Temporal Logic):

Цілісність маршруту: документ не може бути переданий до банку без підпису керівника:

$$G\ (\neg(status = \text{"sent\_to\_bank"}) \vee signed\_by(\text{"manager"}))$$

Повна автентифікація: архівування можливе лише після підписання обома особами:

$$G\ (status = \text{"archived"} \rightarrow signed\_by(\text{"accountant"}) \wedge signed\_by(\text{"manager"}))$$

Контроль доступу**:** лише уповноважені користувачі можуть виконувати відповідні дії:

$$G\ (\neg(user.role \neq \text{"accountant"} \wedge action = \text{"sign"}))$$

Для верифікації використано інструменти NuSMV та TLA+. NuSMV дозволяє виконати символьну перевірку моделей, а TLA+ — описати дії та перевірити інваріанти системи [6, 7].

Виявлена вразливість: у результаті формальної перевірки було виявлено логічну неоднозначність у переході між станами «підпис керівника» та «передача до банку», яка дозволяла обійти перевірку підпису бухгалтера.

До виправлення:

```
next(docStatus) := case
  docStatus = "signed_by_manager" : "sent_to_bank";
  ...
esac;
```

Після виправлення:

```
next(docStatus) := case
  docStatus = "signed_by_manager" & signed_by_accountant = TRUE :
    "sent_to_bank";
  ...
esac;
```

Після усунення вади модель успішно пройшла верифікацію для всіх сформульованих властивостей безпеки.

Для оцінки ефективності захисних механізмів застосовано кількісні критерії у відсотках:

— Висока ефективність: 85–100%

— Середня ефективність: 60–84%

— Низька ефективність: <60%

Результати оцінки представлено у Табл.1.

Таблиця 1 — Ефективність захисних механізмів

Критерій оцінювання	Результат перевірки	Ефективність, (%)	Рівень
Цілісність маршруту документа	Виявлено та усунуто логічну ваду	95	Висока
Контроль доступу	Дії обмежені відповідно до ролей	90	Висока
Незаперечність дій	Підтверджено формально	100	Висока
Стійкість до загроз (STRIDE)	Виявлено потенційні сценарії	80	Середня→ Висока
Відповідність ISO/IEC 27001	Властивості узгоджено з вимогами	90	Висока
Формальна перевірка властивостей	Виконуються в усіх сценаріях	100	Висока

Найвищу ефективність - на рівні 100% - продемонстрували механізми незаперечності дій та формальної верифікації, що було підтверджено інструментальним аналізом із використанням засобів моделювання та перевірки властивостей системи. Застосування формальних методів дозволило не лише виявити приховані логічні вади, недоступні для традиційного тестування, але й забезпечити гарантії виконання критичних вимог безпеки, зокрема цілісності, автентичності та незаперечності дій користувачів у межах протоколу документообігу. Такий результат свідчить про високу надійність обраного підходу в контексті критичних інформаційних систем, де помилки можуть мати значні правові та фінансові наслідки. Водночас, механізм стійкості до загроз, хоча й продемонстрував базову ефективність у загальних сценаріях, потребує подальшого уточнення логіки реагування для специфічних випадків, зокрема при нестандартних послідовностях дій, змінених ролях користувачів або умовах часткової компрометації каналів зв’язку. Це вимагає розширення моделі загроз, деталізації сценаріїв атаки та адаптації механізмів захисту до динамічного середовища функціонування СЕД. Подальші дослідження мають бути спрямовані на інтеграцію адаптивних механізмів реагування та контекстно-орієнтованої логіки перевірки, що дозволить підвищити загальну стійкість системи до складних і комбінованих типів загроз.

Висновки.

У межах проведеного дослідження було розроблено методику аналізу вразливостей систем електронного документообігу (СЕД), що поєднує модель загроз STRIDE із формальними методами верифікації, зокрема NuSMV та TLA+. Застосування формальної верифікації дозволило виявити критичну логічну ваду в протоколі документообігу, яка залишалася непоміченою під час традиційного тестування та могла спричинити порушення регламенту обробки документів. Експериментальні результати підтвердили ефективність формальних методів і механізмів незаперечності, які забезпечили 100% виявлення порушень, що свідчить про їхню доцільність у критичних СЕД. Комбіноване використання STRIDE та формальної верифікації забезпечує багаторівневий захист і гарантує виконання властивостей безпеки в усіх можливих сценаріях функціонування системи. Отримані результати мають практичну цінність і можуть бути використані при розробці, аудиті та вдосконаленні СЕД у банківському секторі, державних установах і корпоративних середовищах.

Література:

1. Гриценко О. В. Інформаційна безпека в електронному документообігі: теорія і практика. Харків: Фоліо, 2021. 256 с.
2. Ковальов С. В. Класифікація загроз інформаційній безпеці в системах електронного документообігу // Інформаційна безпека. 2023. № 2. С. 45–52.
3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO, 2013. 30 p.
4. Коваленко А. А., Куценко Т. Г., Шаповал А. С., Ситник О. В., Ні Я. С. Огляд методів аналізу безпечного програмного забезпечення // Системи управління, навігації та зв'язку. 2025. №1. С. 156–161.
5. STRIDE Threat Modeling / Microsoft. URL: https://learn.microsoft.com/en-us/security/compass/stride-threat-modeling (дата звернення: 10.11.2025).
6. Cimatti A., Clarke E., Giunchiglia F., Roveri M. NuSMV: A New Symbolic Model Verifier // International Journal on Software Tools for Technology Transfer. 2002. Vol. 2, No. 4. URL: https://nusmv.fbk.eu
7. Lamport L. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers. Boston: Addison-Wesley, 2002. 384 с.
8. Йона Е. О., Йона Л. Г., Терешко В. С. Криптографічний захист електронного документообігу // Цифрові технології. 2013. № 13. С. 142–146.

УДК 004.056.53 : 004.89
DOI: https://doi.org/10.32837/11300.31338

Головатюк К.В.
студент факультету Кібербезпека, спеціальність 125
Міжнародний університет
kostya93.06@gmail.com
Науковий керівник Григор'єва Т.І.

ОПТИМІЗАЦІЯ ПРОЦЕСІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ АТАКАХ ФІШИНГУ ІЗ ЗАСТОСУВАННЯМ НЕЧІТКОЇ ЛОГІКИ

Анотація. *В роботі проведено аналіз основних каналів поширення фішингових атак та визначені ключові фактори, що впливають на рівень ризику. Запропоновано використання нечіткої логіки для оптимізації процесів виявлення, аналізу та протидії фішинговим атакам (email-phishing, smishing, vishing). Проведено дослідження статистичних даних про успішність різних каналів атак. Запропонована модель із застосуванням нечіткої логіки, яка дозволяє оцінити ризик загрози та адаптувати реакцію систем кібербезпеки відповідно до ступеня ризику.*

У сучасному цифровому світі фішинг займає одне з провідних місць серед кіберзагроз за масштабами та наслідками. Тому тема дослідження є актуальною. Фішинг - це форма атаки соціальної інженерії, коли зловмисники вводять жертву в оману з метою викрадення даних або інфікування пристроїв шкідливим програмним забезпеченням [1]. Найпоширенішими каналами для фішингу є електронна пошта, фальшиві сайти, повідомлення у месенджерах, SMS та телефонні дзвінки - інструменти, які дозволяють атакуючим імітувати комунікацію від банку, державної установи або знайомого контакту, щоб викликати довіру й змусити користувача виконати небезпечну дію: перейти за посиланням, ввести паролі чи завантажити файл.

Фішинг спирається не лише на технічні вразливості, а й на психологічний вплив: страх, терміновість, цікавість або соціальний тиск підвищують імовірність помилки користувача. Особливо небезпечним фішинг стає в умовах гібридної війни проти України, коли атаки цілеспрямовано спрямовуються на громадян, державні інститути, критичну інфраструктуру, медіа та благодійні організації [1]. У таких випадках фішинг може слугувати елементом інформаційно-психологічної операції з метою дестабілізації, компрометації осіб або зриву роботи важливих державних механізмів. Державні структури в Україні щодня фіксують сотні подібних атак, спрямованих на поширення дезінформації, крадіжку даних та ін.

Існують різні форми фішингу, кожна зі своїми механіками та ризиками.

У межах адресних атак, зокрема spear-phishing, злочинці попередньо збирають інформацію про жертву, щоб повідомлення виглядало максимально переконливо. Часто використовуються прикріплені документи з шкідливими макросами у форматі Excel, як-от у випадках розгортання інструментарію Cobalt Strike проти українських користувачів, зафіксованих у 2023–2024 роках [2].

Spear-phishing, як цільова атака, значно ефективніший за масовий фішинг. Використання персоналізованих звернень, знань про коло контактів або посадову діяльність робить такі листи правдоподібними, іноді - навіть незаперечно достовірними на перший погляд. Це підвищує шанси користувача натиснути небезпечне посилання або завантажити інфікований файл, що відкриває доступ до внутрішніх систем організації.

Серед особливо небезпечних форм фішингу вирізняється також фармінг - автоматичне перенаправлення користувача на підроблений сайт через зміну файлу hosts або DNS-записів. Такий тип атаки особливо складно виявити та заблокувати, і на сьогодні не існує гарантованих способів повної протидії [2].

Фармінг небезпечний тим, що жертва навіть не підозрює, що її перенаправили на фальшиву копію знайомого ресурсу. Візуально все виглядає коректно: дизайн, логотип, структура сайту і навіть сертифікат безпеки можуть бути підроблені або вкрадені. Зловмисник отримує всі дані, які користувач вводить - логіни, паролі, банківську інформацію тощо. Через це такі атаки мають високий коефіцієнт успішності, особливо проти користувачів, які не звикли перевіряти URL-адресу чи цифрові сертифікати.

Відомі випадки вішингу - телефонних дзвінків з комп’ютерним голосом, що імітує службу безпеки банку. Жертву просять ввести 16-значний номер карти та інші персональні дані через клавіатуру телефону [2]. Атака може бути доповнена психологічним тиском, коли злочинець повідомляє про "негайне блокування рахунку".

Така схема працює завдяки автоматизованим дзвінкам (робо-дзвінкам), які можуть охопити десятки тисяч номерів за добу. Навіть невеликий відсоток довірливих користувачів може принести шахраям значні прибутки. Особливо небезпечно це для літніх людей, які менш обізнані з цифровими загрозами.

За підрахунками, 70% фішингових атак у соціальних мережах досягають своєї мети. Найпоширенішими платформами для атак є Facebook, LinkedIn та Telegram, де зловмисники поширюють фішингові посилання або використовують скрипти для перехоплення браузера (browser hooking) [1], [2].

Соціальні мережі надають зловмисникам зручний інструмент для вивчення потенційних жертв, побудови фальшивих акаунтів, проведення атак під виглядом «друга» чи знайомого, а також широкого розповсюдження шкідливого контенту. Особливу загрозу становлять вкладення, які відкриваються в браузері без попереджень, або «опитування», що збирають персональні дані.

Важливу роль відіграє економічна мотивація атак. Згідно з аналітичними оцінками, масований фішинг може приносити прибуток до 14 тисяч доларів з мільйона листів, тоді як цільовий фішинг - до 150 тисяч доларів лише з тисячі надісланих повідомлень. У другому випадку успішність досягає 50% через високий рівень персоналізації атаки [2].

Це свідчить про комерціалізацію кіберзлочинності, де фішинг використовується не лише хакерами-одинаками, а й організованими групами з чіткою структурою, фінансуванням і навіть розподілом ролей. У деяких випадках зловмисники пропонують послуги «фішинг як сервіс» (Phishing-as-a-Service), коли будь-хто може купити доступ до готових інструментів атаки.

Окрім фінансових втрат, наслідками фішингу є витік критично важливої інформації, зокрема даних облікових записів, конфіденційної кореспонденції, внутрішніх документів. Такі атаки часто є початковою ланкою для масових заражень шкідливим ПЗ, включно з бекдорами, кейлогерами та інструментами для повного контролю над інфраструктурою [2].

Таким чином, одна фішингова атака може відкрити ворота до повномасштабної компрометації системи. У разі втрати корпоративного доступу - це загрожує зривом операцій, фінансовими штрафами, репутаційними втратами та навіть кримінальною відповідальністю за порушення законодавства у сфері захисту персональних даних.

Урядова команда CERT-UA постійно фіксує нові фішингові сайти, які імітують державні портали. Наприклад, підроблений сайт portal.nazk.org.ua маскувався під офіційний реєстр декларацій portal.nazk.gov.ua. Громадянам рекомендується звертати увагу на домен .gov.ua, уникати відкриття підозрілих листів і не вводити дані без перевірки сайту [3].

Цей приклад ще раз доводить, наскільки легко зловмисники можуть імітувати навіть офіційні ресурси, якщо користувачі не звикли уважно перевіряти адреси сторінок. Саме тому особливої ваги набуває просвіта та цифрова гігієна населення, а також застосування технологічних заходів - фільтрів, антивірусів, моніторингу, оновлення DNS/сертифікатів.

Разом з тим традиційні підходи виявлення («атака/не атака») не завжди ефективні через невизначену та адаптивну природу фішингових кампаній. Тут корисніші гнучкі моделі оцінки ризику, зокрема підхід на основі нечіткої логіки, який дозволяє вводити ступені ризику і оперувати нечіткими змінними: рівень довіри до відправника, схожість домену, персоналізація повідомлення, історія реакції користувача, канал доставки (e-mail, SMS, телефон) на їх підставі приймати гнучкі рішення - блокувати, попереджати чи передавати на ручну перевірку.

Наприклад, статистичні показники свідчать, що успішність різних каналів варіює: у 2024 році приблизно 8-9 кліків на 1000 email-листів, smishing демонструє значно вищу середню «успішність» (приблизно 8% у деяких дослідженнях), а vishing - близько 6-7% у симульованих тестах. На підставі таких даних нечітка модель може присвоювати каналу більшу вагу (наприклад, SMS як «високий ризик») і комбінувати її з показниками персоналізації й схожості домену, формуючи кінцевий рівень ризику.

В роботі запропоновано побудова математичної моделі оцінки ризику з використанням нечіткої логіки. Для оцінки ризику фішингової атаки пропонуються такі змінні для застосування моделі на основі нечіткої логіки:

A - схожість домену (низька/середня/висока);

B - персоналізація повідомлення (низька/середня/висока);

C - історія реакції користувача (обережний/сумнівний/необережний);

D - канал (email/SMS/телефонний дзвінок).

Рівень загрози (E) будемо визначати за допомогою функції:

$$E = f(A, B, C, D).$$

Наприклад, якщо (D = SMS) і (B = висока) і (A = середня/висока) → ризик загрози (E) = високий, або якщо (D = телефон) і (C = необережний) → ризик загрози (E) = середній-високий.

Роботизований контакт (бот-дзвінок або SMS-авторозсилка) має провести тестування реакції адресату. За результатами цього тестування нечітка модель має визначити «ступінь зацікавленості». Якщо ступінь перевищує встановлений поріг, то має підключитися живий оператор. Якщо ступінь менша за поріг, процес завершується або ставиться на паузу. Процес оптимізації пропонується реалізувати через мінімізацію цільової функції ризику.

Таким чином, на практиці побудована модель дозволить автоматично блокувати або попереджати про повідомлення з високим ризиком, передавати сумнівні випадки на ручну перевірку, оптимізувати розподіл ресурсів (що дозволяє операторам концентруються на високоризикових контактах, а не на масових низькоризикових потоках).Запропонована модель дозволяє системі безпеки адаптуватися до змін у загрозах, наприклад, якщо зростає персоналізація в SMS-кампаніях, то система безпека підвищує вагу показника B).

Застосування нечіткої логіки може покращує точність виявлення фішингових атак у ситуаціях невизначеності та робить захист пропорційним рівню ризику. Однак технічні системи самі по собі не вирішать проблему повністю: необхідна тісна взаємодія між державними органами, приватним сектором і громадянським суспільством, постійний обмін інформацією про індикатори компрометації, а також регулярне навчання користувачів.

Фішинг - це комплексна загроза на стику технологій, психології та економіки злочинності. Ефективна протидія потребує одночасно інвестицій у технології, впровадження адаптивних моделей оцінки ризику і системну роботу з підвищення цифрової обізнаності населення - тільки так можна знизити ймовірність успішних атак і мінімізувати їхні наслідки в умовах сучасної кібернетичної війни.

Особливої важливості набуває тісна взаємодія між державними органами, приватними компаніями та громадянським суспільством, адже тільки спільними зусиллями можна забезпечити реальний захист у цифровій війні, що точиться сьогодні на кіберфронті України.

Висновки:

1. Проведений аналіз показав, що фішинг залишається однією з найпоширеніших і найнебезпечніших кіберзагроз сучасності. Основними каналами поширення є електронна пошта, SMS, соціальні мережі та телефонні дзвінки, які поєднують технічні прийоми зі способами психологічного впливу на користувача.

2. Запропоновано підхід до оцінювання ризику фішингових атак із використанням нечіткої логіки, який дозволяє гнучко враховувати такі параметри, як схожість домену, рівень персоналізації повідомлення, історія реакцій користувача та канал доставки. Це дає можливість системам кібербезпеки адаптувати реакцію до рівня загрози, зменшуючи навантаження на аналітиків і підвищуючи точність виявлення атак.

3. В роботі побудовано математичну модель із застосуванням нечіткої логіки, яка дозволяє оцінити ризик загрози та адаптувати реакцію системи кібербезпеки відповідно до ступеня ризику.

4. Реалізація нечіткої моделі в процесах моніторингу та реагування сприятиме оптимізації використання ресурсів, скороченню часу реагування на інциденти й зниженню кількості успішних атак. Поєднання технологічних засобів, обміну даними між установами та підвищення цифрової грамотності користувачів є ключовими умовами ефективної протидії фішингу в умовах сучасної кібервійни.

Література:

1. Бурячок А. І. Інформаційна безпека в умовах гібридної війни: фішинг як інструмент соціальної інженерії. // Науково-аналітичний вісник. – 2023. – №4. – С. 110–140.

2. Інформаційна безпека: проблеми правового забезпечення та технологічного супроводу. – К.: Інститут інформації, безпеки і права, 2022. – 358 с.

3. CERT-UA. Як убезпечитися від фішингового сайта? [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/article/2808

УДК 004.421.2:004.036.5
DOI: https://doi.org/10.32837/11300.31360

Проценко М.М.
здобувач вищої освіти третього (аспірантського рівня)
спеціальності 123 – Комп'ютерна інженерія
Науковий керівник: Мірошник М. А.
доктор технічних наук, професор
Міжнародний університет
місто Одеса, Україна

ПОРІВНЯЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДІВ ТЕСТУВАННЯ БЕЗПЕКИ LLM-КОДУ: SAST, DAST, GRAPH-BASED ТА СИНТЕЗ ГІБРИДНОГО ПІДХОДУ

Анотація. *У сучасному програмуванні великі мовні моделі (LLM) широко застосовуються для автоматичної генерації коду, однак дослідження 2025 року показують, що такий код нерідко містить вразливості безпеки [1]. Традиційні методи тестування – статичний аналіз безпеки (SAST) та динамічне тестування (DAST) – не завжди справляються з цими викликами. SAST-інструменти сканують вихідний код до його виконання, але генерують багато хибних спрацювань і не розуміють повної семантики застосунку. DAST-підходи перевіряють програму під час роботи, виявляючи лише явні проблеми та пропускаючи приховані дефекти, особливо у складних системах.*

LLM відкривають нові можливості для аналізу коду. Моделі здатні розуміти семантику і помічати небезпечні патерни, які складно формалізувати правилами. GPT-4 успішно розпізнав близько 94% тестових уразливостей, тоді як провідний SAST-сканер виявив лише ~34% [2]. Водночас LLM можуть генерувати некоректні висновки (галюцинації), тому напряму довіряти їм ризиковано. Це зумовило появу гібридних систем, що поєднують строгість статичного аналізу з семантичним міркуванням LLM. Інструмент SAST-Genius, який інтегрує LLM у конвеєр статичного сканування, досягає точності понад 90% при повноті ~95%, тоді як типовий аналізатор демонструє лише ~60% через хибні спрацювання [3]. Експеримент показав зменшення хибних попереджень на ~91% (з 225 до 20) при використанні LLM як постфільтра [3]. Таким чином, симбіоз SAST та LLM дає суттєвий виграш у точності виявлення вразливостей.

LLM також підвищують ефективність динамічного тестування. LLM-асистовані системи генерують цілеспрямовані тестові вектори замість випадкового фаззингу. Система HGFuzzer, керована мовною моделлю, спровокувала 85% відомих уразливостей менш ніж за хвилину, що у 24+ рази швидше за традиційні фаззери, і виявила 9 нових уразливостей з CVE-ідентифікаторами [4]. У пентестингу LLM-агенти самостійно планують і здійснюють атаки, знаходячи в декілька разів більше шляхів експлуатації завдяки розумінню коду й документації.

Для великих кодових баз перспективним є графовий аналіз. Подання програми як графа властивостей коду (CPG), що поєднує синтаксичне дерево, граф потоку управління та граф потоків даних, дозволяє відстежувати складні взаємозв'язки. Модель Hound з підходом "relation-first" підвищила повноту виявлення з 8.3% до 31.2% (чотирикратне зростання) порівняно з базовим LLM-сканером [6]. Граф знань дає ширший контекст: агент простежує шлях від зовнішнього вводу через функції до критичної точки, знаходячи логічні уразливості. Підхід GRASP інтегрує граф правил безпечного кодування в процес генерації, підвищуючи частку безпечних рішень на ~16–20% для різних LLM [3].

На основі аналізу літератури пропонується синтезований гібридний фреймворк, що об'єднує SAST, DAST і графовий аналіз під керуванням LLM-агента. Архітектура включає шість ключових компонентів: Одноагентний модуль – єдиний LLM-агент для статичного й поверхневого динамічного аналізу невеликих проєктів. Багатоагентний модуль – група

спеціалізованих агентів (сканер, фаззер, аналізатор залежностей), що паралельно перевіряють різні аспекти безпеки у великих базах. Ієрархічний модуль – багаторівнева структура: верхній агент-планувальник визначає стратегію, підлеглі детально аналізують компоненти. Корективний модуль – механізм самоперевірки: після кожного етапу LLM переглядає висновки, виявляє помилки й повторює аналіз. Адаптивний модуль – автоматично підлаштовує глибину аналізу під складність проєкту, оптимізуючи швидкість і повноту. Графовий модуль – представляє кодову базу як граф (CPG), забезпечуючи контекст про структуру та потоки даних.

Фреймворк працює як адаптивний конвеєр. Спочатку статичний аналізатор сканує код, LLM відсіює хибні спрацювання та додає пояснення. Динамічний модуль генерує цільові тести або експлойти для підтвердження уразливостей. Паралельно графовий модуль будує карту компонентів і потоків, виявляючи комплексні логічні вразливості. LLM-агент формує консолідований звіт з доказами та рекомендаціями. Корективний цикл генерує патчі, після чого аналіз повторюється до досягнення критеріїв безпеки.

Дослідження підтверджують ефективність компонентів підходу. LLM-підсилений статичний аналіз досягає F1-міри 0.93 проти 0.55 у класичних сканерів [3]. GPT-4 знаходить утричі більше уразливостей, ніж звичайний SAST [2]. Агент SecureFixAgent підвищив точність виправлень на 13.5% і знизив хибні спрацювання на 11% [5]. Графовий аналіз (Hound) виявляє у чотири рази більше уразливостей на рівні програми [6]. Таким чином, поєднання методів з логікою LLM забезпечує більш повне тестування безпеки.

Адаптивний гібридний фреймворк тестування безпеки LLM-коду поєднує сильні сторони SAST, DAST і графового аналізу, долаючи їхні обмеження. Завдяки LLM агенти глибоко аналізують код, відсівають помилкові попередження, генерують сценарії атак та пропонують виправлення автоматично. Оглянуті дослідження показують, що такі системи виявляють більше реальних уразливостей, швидше підтверджують експлуатацію і генерують якісніші патчі, ніж традиційні підходи. Це робить гібридні LLM-методи перспективним напрямком для DevSecOps. Подальші розробки зосередяться на покращенні узгодженості LLM, зниженні витрат і тіснішій інтеграції з інструментами розробки для промислового масштабування. Поєднання штучного інтелекту з класичними методами безпеки здатне суттєво підвищити стійкість програмного забезпечення до кіберзагроз.

Література:

1. Sabra A., Schmitt O., Tyler J. Assessing the Quality and Security of AI-Generated Code: A Quantitative Analysis. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2508.14727 (дата звернення: 04.11.2025).

2. Tehrani M.G., Sultanow E., Buchanan W.J., Houmani M., Fodja C.H.D. LLM vs. SAST: A Technical Analysis on Detecting Coding Bugs of GPT-4 Advanced Data Analysis. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2506.15212 (дата звернення: 04.11.2025).

3. Agrawal V., Ahi K. LLM-Driven SAST-Genius: A Hybrid Static Analysis Framework for Comprehensive and Actionable Security. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2509.15433 (дата звернення: 04.11.2025).

4. Xu H., Zhao Y., Wang H. Directed Greybox Fuzzing via Large Language Model. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2505.03425 (дата звернення: 04.11.2025).

5. Gajjar J., Subramaniakuppusamy K., Puthal R., Ranaware K. SecureFixAgent: A Hybrid LLM Agent for Automated Python Static Vulnerability Repair. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2509.16275 (дата звернення: 04.11.2025).

6. Mueller B. Hound: Relation-First Knowledge Graphs for Complex-System Reasoning in Security Audits. arXiv Computer Science, 2025. URL: https://arxiv.org/abs/2510.09633 (дата звернення: 04.11.2025).

DOI: https://doi.org/10.32837/11300.31361

Лавров Андрій Вікторович

Здобувач факультету кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність 122 Комп'ютерні науки
Міжнародний університет
lavrs6nh@gmail.com
Керівник: д.т.н., професор кафедри Радівілова Т.А.

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЕЛЕКТРОННИХ ПЛАТЕЖІВ В УКРАЇНІ

Анотація. *У роботі проаналізовано сучасний стан розвитку електронних платежів в Україні, а також визначено основні тенденції, виклики та перспективи подальшого зростання галузі. Розглянуто вплив цифровізації фінансового сектору, появу нових платіжних технологій та впровадження державних ініціатив, спрямованих на підвищення безпеки електронних транзакцій. Особливу увагу приділено розвитку мобільного банкінгу, платіжних сервісів на базі NFC та цифрових гаманців.*

Ключові слова: електронні платежі, фінтех, цифровізація, банківські технології, кібербезпека, платіжні системи, мобільний банкінг.

Стрімкий розвиток інформаційних технологій і фінансових сервісів в Україні за останнє десятиліття суттєво змінив підхід до здійснення фінансових операцій. Якщо раніше більшість платежів відбувалася через банківські каси або термінали, то сьогодні понад 75% транзакцій здійснюється в електронному форматі. Такі зміни стали можливими завдяки розвитку фінансових технологій (FinTech), появі інноваційних рішень для мобільних і безконтактних платежів, а також загальному зростанню рівня цифрової грамотності населення.

Актуальність теми зумовлена переходом України до економіки без готівки, який підтримується Національним банком України (НБУ). Зокрема, стратегія Cashless Ukraine передбачає зниження частки готівкових розрахунків до 10% у найближчі роки. У цьому контексті ключовими драйверами розвитку є системи Apple Pay, Google Pay, monobank, Revolut, а також українські платіжні інновації, такі як «Дія.Платежі» та інтеграція QR-платежів.

Станом на 2025 рік ринок електронних платежів в Україні демонструє стабільне зростання. Обсяг безготівкових операцій щорічно збільшується на 20–25%, а кількість користувачів мобільного банкінгу перевищує 25 мільйонів. Водночас, актуальною залишається проблема кіберзагроз — фішинг, підміна платіжних сторінок, витік персональних даних. Для її вирішення банки активно впроваджують багатофакторну автентифікацію, токенізацію карткових даних та моніторинг транзакцій у реальному часі за допомогою алгоритмів машинного навчання.

Перспективи подальшого розвитку галузі пов'язані з інтеграцією технологій блокчейну, впровадженням цифрової гривні (e-hryvnia), розширенням сфери open banking та зростанням частки мікроплатежів через IoT-пристрої. Крім того, очікується подальше вдосконалення нормативної бази відповідно до директиви PSD2 ЄС, що сприятиме залученню міжнародних платіжних систем і підвищенню рівня прозорості транзакцій.

Висновки.

1. Україна впевнено рухається до повноцінної цифрової економіки, у якій електронні платежі є базовим елементом фінансової екосистеми.
2. Основними напрямами подальшого розвитку є підвищення рівня кібербезпеки, розширення доступу до фінансових сервісів та впровадження цифрової валюти НБУ.
3. Перспективними технологіями залишаються блокчейн, open banking і машинне навчання для захисту електронних транзакцій.

4. Державна політика та активна участь FinTech-компаній створюють сприятливі умови для переходу України до моделі cashless-суспільства.

Література:

1. Національний банк України. Безготівкові розрахунки у 2024 році суттєво переважали серед операцій з платіжними картками. – Режим доступу: https://bank.gov.ua/ua/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami (дата звернення: 06.11.2025).

2. Національний банк України. У 2024 році СЕП продовжувала безперебійно працювати та інноваційно розвиватися. – Режим доступу: https://bank.gov.ua/ua/news/all/u-2024-rotsi-sep-prodovjuvala-bezperebiyno-pratsyuvati-ta-innovatsiyno-rozvivatisya (дата звернення: 06.11.2025).

3. Національний банк України. Картковий ринок за дев'ять місяців 2024 року: частка безготівкових операцій продовжує зростати. – Режим доступу: https://bank.gov.ua/ua/news/all/kartkoviy-rinok-za-devyat-misyatsiv-2024-roku-chastka-bezgotivkovih-operatsiy-prodovjuye-zrostati (дата звернення: 06.11.2025).

4. UKR.NET. Система електронних платежів НБУ обробила 483 млн операцій за рік: які платежі найпопулярніші. – Режим доступу: https://www.ukr.net/news/details/economics/109008745.html (дата звернення: 06.11.2025).

5. Академічні візії. Стан і тенденції розвитку ринку електронних платежів в Україні. – Режим доступу: https://academy-vision.org/index.php/av/article/download/1799/1666/1706 (дата звернення: 06.11.2025).

UDC 004.056.55
DOI: https://doi.org/10.32837/11300.31365

Onatskyi Oleksii,
Candidate of technical sciences, associate professor,
International Humanitarian University, Odessa, Ukraine
onatsky@meta.ua
Zharova Oksana,
Candidate of physical and mathematical sciences, associate professor,
Odessa polytechnic state university, Odessa, Ukraine
Ksenia.gds@gmail.com

COMPARATIVE ANALYSIS OF HOMOMORPHIC PROPERTIES OF ASYMMETRIC CRYPTOSYSTEMS RSA AND PAILLIER

Abstract. *This study conducts a comparative analysis of homomorphic properties in RSA and Paillier cryptosystems. With growing demands for secure cloud computing and IoT applications, homomorphic encryption enables operations on encrypted data without decryption. The research implements both systems in Python, analyzing their mathematical foundations and performance. Results show RSA multiplicative homomorphism poses security risks, while Paillier additive homomorphism, though computationally heavier, provides secure privacy-preserving operations. Paillier excels in electronic voting and secure data analytics, whereas RSA remains optimal for traditional encryption. The findings guide cryptosystem selection based on specific security and functionality requirements in modern applications.*

Modern requirements for data processing, particularly in cloud computing schemes, Internet of Things, and secure voting systems, highlight the problem of information confidentiality. Classical cryptosystems require data decryption to perform any operations on them, which creates risks of data leakage. The solution to this problem is homomorphic encryption – a class of cryptographic schemes that allows performing mathematical operations on ciphertexts, obtaining a

result that, after decryption, corresponds to the result of the same operations performed on plaintexts. The RSA cryptosystem, although not designed as fully homomorphic, demonstrates homomorphic properties regarding the multiplication operation. In contrast, the Paillier cryptosystem was specifically designed with powerful homomorphic properties regarding addition, making it a key tool for many practical applications. Thus, the relevance of the research lies in comparing the classical RSA cryptosystem and the homomorphic Paillier cryptosystem to determine their advantages, disadvantages, and possible directions of practical application. To conduct a comparative analysis of the functioning algorithms and implementation features of RSA and Paillier cryptosystems, mathematical foundations, areas of effective application and computational complexity, as well as comparing their characteristics from the perspective of security, efficiency, and homomorphic encryption capabilities.

The RSA cryptosystem was developed in 1977 by R. Rivest, A. Shamir, and L. Adleman [1, 2]. It is based on a one-way function – the product of two large prime numbers, whose factorization is a computationally complex task. For the RSA algorithm $\left[E(m_1)E(m_2)\right] \bmod n = E(m_1 m_2) \bmod n$, which demonstrates multiplicative homomorphism, where $E(m_1)$ and $E(m_2)$ – ciphertexts of two messages.

The Paillier cryptosystem, proposed by Pascal Paillier in 1999 [3, 4], is based on the complexity of computing the *n*-residue function modulo n^2. It is distinguished by a unique property – additive homomorphism, which means the ability to perform addition operations on encrypted data without their decryption. For the Paillier algorithm

$$\left[E(m_1)E(m_2)\right] \bmod n^2 = E(m_1 + m_2) \bmod n^2,\ E(m_1)^k \bmod n^2 = E(k\,m_1) \bmod n^2,$$

which demonstrates additive homomorphism.

The research used methods of theoretical analysis and mathematical modeling. To practically confirm the properties of RSA and Paillier algorithms, tools of the Python programming environment were applied, particularly the SymPy library (a library for symbolic mathematical computations in Python). Models of key generation, message encryption and decryption processes were implemented, and the homomorphism of RSA and Paillier cryptosystems was verified. The comparison was carried out according to the following criteria: length of cryptographic keys; execution time of encryption/decryption operations; support of homomorphic properties. RSA and Paillier algorithms include three main stages: key generation, encryption, and decryption [1, 2].

The result of executing the program code is shown in Fig. 1 – 5.

```
================================================================================================
         COMPARATIVE ANALYSIS OF RSA AND PAILLIER CRYPTOSYSTEMS
================================================================================================
1. DATA INPUT:
------------------------------------------------------------------------------------------------
Choose input data type (1 - numbers, 2 - text): 1
Enter first number: 23
Enter second number: 61
Enter key length (bits) [512]: 100

2. KEY GENERATION:
------------------------------------------------------------------------------------------------
RSA Keys:
  Public key  (e, n): (65537, 27014142956232615339005549221171725665041592692410806475022 9)
  Private key (d, n): (834203923200994353160496063499770843386971402295122451438 73,
                       27014142956232615339005549221171725665041592692410806475022 9)
  Private key  (hex): d=D4A2588B1F92347E1306DA5A1967A6899987014E1C2E9E941

Paillier Keys:
  Public key  (n, g): (396715656050536708961692760932240264459811676959572130477 3,
                       396715656050536708961692760932240264459811676959572130477 4)

  Private key (lambda, mu, n): (396715656050536708961692760820239570730132880202535507408 0,
                                322314338574677341862113083927991935756671663459037375237 6,
                                396715656050536708961692760932240264459811676959572130477 3)
  Private key (hex): lambda=A1CB0C0DE8896998F378C1BE620350B6386843A9522BDA20
                     mu=83732FE5A134A47B0702C92166412F7A3CDF718A0C342E38
```

Figure 1 – Data input. Key generation for RSA and Paillier cryptosystems

```
3. ENCRYPTION:
------------------------------------------------------------------------------------------------
RSA Encryption (numbers):
  23 -> 23528604538132694558777972856237631012776062230234317743046 3
  23 (hex) -> 257BB4EEDF531559E60EA5D99C6DB483DC4CEDEA47B43BE5BF
  61 -> 60118280450905581787621741506285336529404368764732344974376
  61 (hex) -> 993D0226BACD536BF61EE93319EB9E82CDC3AE0ED478D3C28
  Encryption time: 0.98 ms, 0.86 ms

Paillier Encryption (numbers):
  23 -> 68953827188599490864001896474232537573007905109385337895124526784829708408798429512073505298053115790187415913482 9
  Random r for 23: 36663955037636330825578849063592328143957614597817884248 0
  Random r (hex): EF3E54066E4753B8265ABC5B7F100A254CD4DE9CD3AAF70

  61 -> 14366884597946863884553412288404164048237776602422903238666244388382242653257796932282030553936891457107183687513690
  Random r for 61: 13819614842304427948487875976888703415114503451130530868 1
  Random r (hex): 5A2D5C9E01A20451474195F7E04D96B5CFC0BFE82C27A09

  Encryption time: 34.65 ms, 34.38 ms
```

Figure 2 – Encryption for RSA and Paillier cryptosystems

```
4. DECRYPTION:
------------------------------------------------------------------------------------------------
RSA Decryption (numbers):
  23528604538132694558777972856237631012776062230234317743046 3 -> 23
  257BB4EEDF531559E60EA5D99C6DB483DC4CEDEA47B43BE5BF -> 23
  60118280450905581787621741506285336529404368764732344974376 -> 61
  993D0226BACD536BF61EE93319EB9E82CDC3AE0ED478D3C28 -> 61
  Decryption time: 18.96 ms, 18.77 ms

Paillier Decryption (numbers):
  68953827188599490864001896474232537573007905109385337895124526784829708408798429512073505298053115790187415913482 9 -> 23
  14366884597946863884553412288404164048237776602422903238666244388382242653257796932282030553936891457107183687513690 -> 61
  Decryption time: 33.88 ms, 33.49 ms
```

Figure 3 – Decryption for RSA and Paillier cryptosystems

```
5. HOMOMORPHIC OPERATIONS:
--------------------------------------------------------------------------------------------------------------------------------------------
RSA Homomorphic Multiplication:
  Enc(23) * Enc(61) = Enc(1403)
  Result ciphertext: 11957331675345133245529837276036806453223004797413637149957O
  Result ciphertext (hex): 130C93AD498C88BF80D11C52B5FE1B94610ABA57DFD52C5232
  Decrypted result: 1403
  Expected result: 1403
  Validation: ✅

Paillier Homomorphic Addition:
  Enc(23) + Enc(61) = Enc(84)
  Result ciphertext: 654576960331059033737808714752134674381841175918416665633467911425353165329474741625108675308475476657787779227460O
  Decrypted result: 84
  Expected result: 84
  Validation: ✅

Paillier Homomorphic Multiplication by Constant (3):
  3 * Enc(23) = Enc(69)
  Result ciphertext: 17961821872494793541805248670643971922344699476899913870776638341085624747320997105066462062237617161142920764708340
  Decrypted result: 69
  Expected result: 69
  Validation: ✅

6. BENCHMARKING (100 iterations):
--------------------------------------------------------------------------------------------------------------------------------------------
  RSA Encryption: 0.80 ms
  RSA Decryption: 19.93 ms
  Paillier Encryption: 49.77 ms
  Paillier Decryption: 33.74 ms

  Fastest operation: RSA Encryption (0.80 ms)

  Speed ratio: Paillier ≈ 62.0 times slower than RSA
```

Figure 4 – Homomorphic operations for RSA and Paillier cryptosystems

```
7. VERIFICATION AND CONCLUSIONS:
----------------------------------------
RSA encryption/decryption correctness: ✅
Paillier encryption/decryption correctness: ✅
RSA homomorphic multiplication: ✅
Paillier homomorphic addition: ✅
Paillier homomorphic multiplication by constant: ✅

   CONCLUSIONS:
• RSA: ✅ CORRECT
• Paillier: ✅ CORRECT
• RSA homomorphic multiplication: ✅ WORKS
• Paillier homomorphic addition: ✅ WORKS
• Paillier multiplication by constant: ✅ WORKS
• Paillier is approximately 62.0 times slower than RSA
```

Figure 5 – Verification and conclusions for RSA and Paillier cryptosystems

Homomorphic properties. The RSA cryptosystem demonstrates multiplicative homomorphism. However, this property makes it vulnerable to chosen-ciphertext attacks, which requires special padding schemes (for example, OAEP – Optimal Asymmetric Encryption Padding) for practical use, which, in turn, destroy homomorphism. Thus, it is not suitable for performing operations on encrypted data. The Paillier cryptosystem possesses additive homomorphism, which is secure and intentionally built into the system design, but requires more memory and time to perform operations.

Mathematical foundations. RSA security is based on the complexity of solving the factorization problem of large numbers. Paillier security is based on the complexity of solving the decisional composite residuosity problem modulo n^2, which is considered more complex.

Computational complexity. Encryption and decryption operations in Paillier are more computationally complex due to working with modulus n^2, while RSA uses modulus n.

Areas of application. Due to its additive homomorphism, the Paillier system has found wide application in:

– electronic voting (vote counting without decryption);

– secure cloud computing (finding data sums);

– machine learning with privacy preservation (calculating averages, sums of squares, etc.);

– secure medical research;

– electronic payment order systems.

The multiplicative homomorphism of RSA has more limited applications, for example, for building blind signature protocols.

Conclusions. The conducted comparative analysis leads to the conclusion that although both RSA and Paillier, have homomorphic properties, they are fundamentally different in their nature and practical value. The RSA cryptosystem, being the first widely known asymmetric system, has limited and potentially dangerous multiplicative homomorphism. The RSA cryptosystem remains one of the most reliable and widespread asymmetric encryption algorithms, which is effectively used for data protection and implementation of digital signatures. In contrast, the Paillier cryptosystem is a specialized and secure tool that implements additive homomorphism, making it indispensable for modern applications where operations need to be performed on encrypted data without their disclosure. Consequently, the selection of an appropriate cryptosystem is contingent upon the specific requirements of the intended application: RSA remains the standard for ensuring confidentiality and authentication, while Paillier is the optimal choice for implementing homomorphic computations, particularly for addition, which is important in tasks of analyzing confidential data in cloud environments, electronic voting, financial services, and user privacy protection. Further research should be directed towards optimizing homomorphic algorithms, reducing their computational complexity and integration with post-quantum protection methods, opening new opportunities for creating secure, efficient, and confidential information technologies of the future.

References:

1. Онацький О. В., Йона Л. Г. Белова Ю. В. Криптографічний захист інформації: навчальний посібник з дисципліни «Криптографічний захист інформації». Держ. ун-т інтелект. технологій і зв'язку. – Одеса: Астропринт, 2023. 252 с.

2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія. – Харків: Видавництво «Форт», 2012. 880 с.

3. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT), Prague. Czech Republic, May 1999, Pp. 223-238.

4. The Paillier's Cryptosystem and Some Variants. [Electronic resource] – Mode of access: https://scispace.com/pdf/the-paillier-s-cryptosystem-and-some-variants-revisited-186lebbhcg.pdf

DOI: https://doi.org/10.32837/11300.31377

Ковальчук Д. А.
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
denys.kovalchuk1@gmail.com
Науковий керівник: Йона Л. Г.
Кандидат технічних наук,
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій
Міжнародного університету м. Одеса, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СКЛАДОВА ГІБРИДНИХ КІБЕРОПЕРАЦІЙ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ВИКЛИКИ БЕЗПЕКИ

***Анотація**. У тезах розглянуто соціальну інженерію як один із ключових інструментів гібридних кібероперацій, що поєднує технічні та психологічні засоби впливу. Проаналізовано сучасні тенденції розвитку соціально-інженерних методів, їх роль у дестабілізації інформаційного простору та підриві довіри до цифрових систем. Визначено основні канали поширення таких атак, а також виклики, що постають перед системами кібербезпеки держави, бізнесу та суспільства. Запропоновано напрями підвищення рівня кіберстійкості та соціальної відповідальності користувачів.*

Сучасні гібридні конфлікти характеризуються поєднанням традиційних та кіберінструментів впливу, серед яких соціальна інженерія посідає особливе місце. На відміну від класичних технічних атак, соціально-інженерні операції спрямовані на маніпулювання людською поведінкою, емоціями та когнітивними особливостями. Це робить їх надзвичайно ефективними, адже навіть найзахищеніші інформаційні системи залишаються вразливими через «людський фактор».

В умовах війни, яку веде Російська Федерація проти України, соціальна інженерія використовується не лише для викрадення даних чи фінансових ресурсів, але й як засіб інформаційно-психологічного тиску на населення, деморалізації та дезінформації. З огляду на це, дослідження соціальної інженерії як складової гібридних кібероперацій набуває стратегічного значення для національної безпеки.

Метою роботи є аналіз сучасних тенденцій розвитку соціально-інженерних методів у контексті гібридних кібероперацій та визначення ефективних стратегій протидії таким загрозам.

Сутність соціальної інженерії у контексті гібридних атак

Соціальна інженерія — це сукупність методів психологічного впливу, спрямованих на отримання конфіденційної інформації або спонукання користувача до певних дій, які порушують політику безпеки системи. У гібридних кіберопераціях вона виступає мостом між технічними засобами злому та інформаційно-психологічними кампаніями.

Типовими прикладами є фішинг, спір-фішинг, вішинг, смішинг, використання deepfake-технологій, а також поширення дезінформації у соціальних мережах. Такі атаки часто мають на меті не лише отримання доступу до систем, а й формування певних наративів або створення недовіри до офіційних джерел.

Інструменти та канали реалізації соціально-інженерних впливів

Соціальні платформи, електронна пошта та месенджери є основними каналами поширення соціально-інженерних атак. В умовах глобальної цифровізації користувачі щодня отримують сотні інформаційних повідомлень, що створює ідеальні умови для маніпуляцій.

Атакувальники активно застосовують методи OSINT (розвідка відкритих джерел) для збору персональних даних, які потім використовують для індивідуалізації атак. Широке використання генеративного штучного інтелекту, зокрема для створення фейкових зображень, аудіо та текстів, суттєво підвищує рівень достовірності таких впливів.

Виклики для системи кібербезпеки

Основною проблемою протидії соціальній інженерії є складність виявлення атак, що не містять безпосередніх технічних ознак злому. Більшість інцидентів відбувається через помилки користувачів, які піддаються психологічному тиску або довіряють неправдивій інформації.

Для держави та організацій це означає потребу у зміні підходів до кіберзахисту: від технічної до комплексної соціотехнічної моделі безпеки, що враховує людський чинник. Значну роль відіграють навчальні програми з кіберграмотності, тестування персоналу на стійкість до фішингу та розвиток культури кібербезпеки.

Шляхи протидії соціально-інженерним загрозам

Протидія соціальній інженерії потребує синергії технологічних і поведінкових стратегій. До ефективних напрямів належать:

- впровадження програм постійного навчання працівників із моделюванням реальних сценаріїв атак;
- моніторинг і аналіз поведінкових аномалій користувачів у корпоративних мережах;
- використання систем штучного інтелекту для виявлення фішингових повідомлень і deepfake-контенту;
- розвиток державних інформаційних кампаній з підвищення обізнаності населення щодо кіберзагроз.

Важливо, щоб кіберзахист розглядався не лише як технічне завдання, а як соціальний процес, що охоплює освіту, етику, психологію та комунікацію.

Висновки.

Соціальна інженерія є однією з ключових складових сучасних гібридних кібероперацій, оскільки дозволяє зловмисникам впливати на свідомість і поведінку людей, обходячи технічні засоби захисту. Її особливість полягає у використанні психологічних прийомів, емоційного тиску, дезінформації та маніпуляцій довірою, що робить людину найслабшою ланкою у системі кібербезпеки.

У контексті повномасштабної війни, розв’язаної Російською Федерацією проти України, соціальна інженерія стала одним із головних інструментів інформаційного та кібернетичного впливу. Російські кіберактивності часто поєднують класичні технічні атаки (злами, DDoS, крадіжки даних) із кампаніями психологічного тиску, спрямованими на деморалізацію населення, поширення панічних настроїв та підрив довіри до державних інституцій.

Приклади таких дій включають фішингові розсилки, що імітують офіційні повідомлення державних органів, створення фейкових сторінок благодійних фондів, а також масштабні кампанії з дезінформації в соціальних мережах, спрямовані на спотворення сприйняття подій на фронті.

Досвід України демонструє, що протидія соціально-інженерним загрозам має не лише технічний, а й національно-безпековий характер. Формування культури кіберграмотності серед громадян, підвищення обізнаності про механізми інформаційного впливу та розвиток державних комунікаційних стратегій є необхідними умовами кіберстійкості країни.

Комплексна система протидії соціальній інженерії повинна поєднувати технологічні, психологічні, освітні та правові інструменти. Зокрема, ефективною є інтеграція штучного інтелекту для виявлення маніпуляцій, проведення тренінгів для державних службовців і критичної інфраструктури, а також співпраця між державними органами, науковими установами та громадським сектором у сфері інформаційної безпеки.

Отже, соціальна інженерія у гібридних кіберопераціях є не лише технічною проблемою, а складним соціально-психологічним викликом, що загрожує національній безпеці. Подальші дослідження мають бути спрямовані на розробку моделей оцінювання ризиків соціально-інженерних атак у контексті воєнного протистояння, формування

ефективних стратегій кіберосвіти та створення адаптивних систем захисту, здатних враховувати людський чинник у цифровому середовищі.

Література:

1. Sarker H. I. AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. 2024.

2. Gray J. Practical Social Engineering: A Primer for the Ethical Hacker. 2022.

3. Hamid Jahankhani, Babak Akhgar, Peter Cochrane, Mohammad Dastbaz “Policing in the Era of AI and Smart Societies”.

4. Cyble. (2024). Ukraine's Cyberthreat Landscape 2024. URL: https://cyble.com/blog/ukraine-cyberthreat-landscape-2024/.

5. European Parliament. (2025). Cybersecurity: main and emerging threats. URL: https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats.

УДК 004.056.53 : 004.021 : 519.85
DOI https://doi.org/10.32837/11300.31378

Григор’єва Т.І., кандидат технічних наук, доцент,
Мельник В.В., здобувач вищої освіти ступеня доктора філософії
спеціальності F5 - Кібербезпека та захист інформації
Міжнародний університет, місто Одеса
tig15090808@gmail.com
valikysimys.melnyk@gmail.com

АНАЛІЗ МЕТОДІВ ОПТИМІЗАЦІЇ БЕЗПЕКИ БАЗ ДАНИХ

Анотація. *В роботі представлено аналіз різноманітних математичних підходів до оптимізації безпеки баз даних. Розглянуто сильні та слабкі сторони графових, статистичних, ймовірнісних, матричних та тензорних методів. Визначено, що вибір конкретного підходу залежить від специфіки завдання, наприклад, моделювання зв'язків, виявлення аномалій, управління ризиками, компресія даних, та вимог до обчислювальної ефективності. Зроблено висновок про необхідність гібридизації цих методів для побудови високонадійних та адаптивних систем захисту даних.*

У сучасних інформаційних системах безпека баз даних є критичним чинником забезпечення цілісності, конфіденційності та доступності корпоративних даних. Зростання складності загроз, зокрема цілеспрямованих атак, внутрішніх інцидентів і багатовимірних аномалій у поведінці користувачів, потребує впровадження більш формалізованих методів аналізу. Тому дуже актуальними стають оптимізаційні підходи, що використовують графові, статистичні, матричні та тензорні моделі для оброблення великих обсягів даних і виявлення прихованих закономірностей, які неможливо розпізнати за допомогою традиційних засобів контролю доступу чи простого моніторингу активності.

Традиційні методи забезпечення безпеки баз даних зосереджуються на таких аспектах, як, по-перше, управління дозволами користувачів, по-друге, відстеження активності користувачів та системних подій. А також, використання систем виявлення вторгнень та забезпечення конфіденційності даних, як під час зберігання, так і під час передачі. Ці методи є необхідними, але їхня ефективність знижується, коли потрібно проаналізувати неочевидні, складні взаємозв'язки між різними елементами системи безпеки, що характерно для сучасних розподілених середовищ.

Графові моделі можуть бути ефективними для візуалізації складних взаємозв’язків, виявлення прихованих каналів витоку даних та аналізу поведінки користувачів у контексті

доступу до критичних ресурсів. Представимо бази даних у вигляді орієнтованого або неорієнтованого графу, де вузли відповідають користувачам, таблицям, запитам або транзакціям, а ребра – зв’язкам між ними. Такий підхід дозволяє моделювати структуру доступу, виявляти циклічні залежності, а також застосовувати алгоритми пошуку аномалій.

Використання графових алгоритмів, наприклад, пошуку шляху, таких як BFS або DFS [1] дозволяє швидко перевірити наявність несанкціонованого або опосередкованого доступу користувача до критичних даних. Графові алгоритми можуть бути застосовані для ідентифікації неочікуваних шаблонів поведінки або аномальних зв'язків. Наприклад, алгоритм PageRank [1] може допомогти виявити аномальні вузли, що сприяє швидшому виявленню інцидентів. Графові моделі дозволяють проводити системний аналіз інформаційної безпеки, моделювати граф атак та оцінювати потенційні ризики, що допомагає приймати обґрунтовані управлінські рішення щодо пріоритезації заходів захисту.

Порівняно з традиційними реляційними підходами, графові методи забезпечують вищу швидкість та гнучкість при аналізі зв'язків, що критично важливо в умовах реального часу для систем кібербезпеки. Інтеграція графових методів у системи захисту баз даних є перспективним напрямом оптимізації кібербезпеки. Вони не замінюють традиційні заходи, а доповнюють їх, надаючи потужний інструмент для моделювання, аналізу та візуалізації складних взаємозв'язків у великих обсягах даних. Графові методи ідеально підходять для завдань, де ключовим є аналіз топології мережі доступу, прав користувачів та потенційних шляхів атак.

Статистичні методи орієнтовані на аналіз агрегованих характеристик даних, таких як середнє значення, дисперсія, кореляція та гістограми частот. Вони дозволяють швидко оцінити нормальність поведінки користувачів, виявити пікові навантаження, а також побудувати профілі активності. У поєднанні з ймовірнісними моделями, такими як байєсівські мережі, марковські процеси або моделі прихованих марковських ланцюгів, статистичні методи забезпечують прогнозування ризиків, оцінку ймовірності порушення політик безпеки та адаптивне реагування на зміну поведінки користувачів.

Описова статистика застосовується для узагальнення даних, розрахунку середніх значень, дисперсії, частоти подій. Це допомагає адміністраторам безпеки швидко оцінити загальний стан системи та виявити відхилення від типових параметрів, наприклад, незвичайно велика кількість невдалих спроб входу за короткий проміжок часу. Статистичні та ймовірнісні методи є основою для систем виявлення аномалій та прогнозування загроз. Вони використовуються для аналізу поведінки користувачів, де на основі історичних даних формується "нормальна" базова лінія активності [2]. Ці методи ефективні там, де потрібна кількісна оцінка відхилень та мінімізація хибних спрацьовувань. Ймовірнісні моделі, зокрема Байєсівські мережі, застосовуються для управління ризиками та діагностики першопричин інцидентів, забезпечуючи роботу з невизначеністю та неповними даними.

Інференційна статистика дозволяє робити висновки про генеральну сукупність на основі вибіркових даних. Методи перевірки гіпотез використовуються для підтвердження або спростування припущень про загрози.

Регресійний аналіз використовується для прогнозування майбутньої поведінки системи або виявлення залежностей між різними змінними, наприклад, залежність між часом доби та типом виконуваних запитів, що може вказувати на аномалії. Перевага статистичних методів полягає в математичній строгості та можливості кількісної оцінки відхилень, що забезпечує об'єктивну основу для прийняття рішень.

Ймовірнісні методи розширюють можливості статистики, інтегруючи елементи невизначеності та ризику безпосередньо в моделі безпеки. Байєсівські моделі є потужним інструментом для представлення ймовірнісних залежностей між різними подіями безпеки.

Вони дозволяють оновлювати ймовірності загроз в режимі реального часу на основі нових даних (свідчень), що надходять від систем моніторингу. Байєсівські мережі використовуються для діагностики першопричин інцидентів та прогнозування розвитку атак. Ймовірнісні моделі лежать в основі кількісної оцінки ризиків інформаційної безпеки. Використання ймовірнісних моделей дозволяє обчислити очікувані збитки від потенційних загроз. Марковські моделі застосовуються для моделювання послідовностей подій, наприклад, етапів багатоланкової атаки. Аналіз переходів між станами дозволяє ідентифікувати найбільш ймовірні шляхи проникнення та розробити контрзаходи.

Ймовірнісні методи забезпечують гнучкість у роботі з неповними або зашумленими даними та дозволяють інтегрувати експертні знання в кількісні моделі. Таким чином, статистичні та ймовірнісні методи є потужними інструментами оптимізації безпеки баз даних. Використання статистичних та ймовірнісних методів дозволяє виявляти загрози та управляти ризиками. Інтеграція цих методів у сучасні архітектури безпеки забезпечує більш високий рівень стійкості інформаційних систем до сучасних кіберзагроз, що робить їх ключовим компонентом комплексного захисту даних.

Матричні методи, зокрема сингулярне розкладання матриці (SVD), аналіз головних компонент (PCA) та негативне матричне факторизування (NMF), дозволяють виявляти латентні структури у даних доступу [3]. Наприклад, SVD може бути використане для побудови матриці доступу, де кожен елемент відображає силу зв’язку між користувачем і ресурсом, а низькорівневі сингулярні значення – потенційні аномалії. PCA дозволяє зменшити розмірність логів доступу, зберігаючи найбільш значущі компоненти, що сприяє швидкому виявленню відхилень. NMF, завдяки своїй інтерпретованості, дозволяє класифікувати запити за темами доступу та побудувати поведінкові шаблони користувачів.

Матриці суміжності використовуються для моделювання мережевих з'єднань між серверами баз даних та клієнтами. Аналіз власних значень цих матриць може допомогти виявити аномальну мережеву активність або несанкціоновані з'єднання.

Тензорні методи є узагальненням матричних моделей на багатовимірні дані, що включають часові, контекстні та структурні виміри. Вони дозволяють моделювати складні залежності між запитами, користувачами, типами доступу та часовими інтервалами. Тензорна факторизація, зокрема CP або Tucker розкладання [4], забезпечує виявлення багатовимірних патернів, що не доступні при двовимірному аналізі. Це особливо корисно для побудови адаптивних систем моніторингу, які враховують контекст доступу, історію взаємодій та динаміку змін у поведінці користувачів.

Матричні та тензорні підходи є перспективними напрямами оптимізації безпеки баз даних. Використання матричних та тензорних методів дозволяє ефективно моделювати, аналізувати та стискати великі обсяги даних безпеки, виявляючи приховані патерни та аномалії. Впровадження цих методів, особливо тензорного аналізу для багатовимірних даних, забезпечує значне підвищення рівня захисту інформаційних систем.

Висновки:

1. Жоден із розглянутих підходів не є універсальним рішенням для всіх завдань безпеки баз даних. Графові методи чудово підходять для аналізу зв'язків, статистичні та ймовірнісні – для виявлення аномалій та оцінки ризиків, а матричні та тензорні – для ефективної обробки та компресії великих масивів даних.
2. Оптимізація безпеки баз даних майбутнього полягає в інтеграції цих методів у гібридні системи, які можуть використовувати сильні сторони кожного підходу для побудови багаторівневого, проактивного та інтелектуального захисту інформації.
3. Математичне моделювання в контексті безпеки баз даних є фундаментом для побудови інтелектуальних систем захисту, які здатні адаптуватися до нових загроз,

масштабуватися відповідно до обсягів даних та забезпечувати стійкість цифрових екосистем.

Література:

1. Pushap Goyal. (2025). The Role of Databases in Cybersecurity and Threat Detection: Advancements through Spanner Graph Technology. Journal of Computer Science and Technology Studies, 7(5), 544-557. https://doi.org/10.32996/jcsts.2025.7.5.61.

2. Habeeb Omotunde, & Maryam Ahmed. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of CyberSecurity, 2023, 115-133. https://doi.org/10.58496/MJCSC/2023/016.

3. Martin Stoll (2020) A literature survey of matrix methods for data science: GAMM - Mitteilungen published by Wiley-VCH GmbH on behalf of Gesellschaft f\xFCr Angewandte Mathematik und Mechanik. https://doi.org/10.1002/gamm.202000013.

4. Kolda, T.G. and Bader, B.W. (2009) Tensor Decompositions and Applications. SIAM Review, 51, 455-500. https://doi.org/10.1137/07070111X.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УДК 621.391
DOI https://doi.org/10.32837/11300.31379

Стрелковська І.В., д.т.н., професор,
декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний університет, Одеса, Україна
i.strelkovskaya@mgu.edu.ua
Золотухін Р.В., начальник департаменту програмування
ТОВ «Телекарт-Прилад», Одеса, Україна
zolotukhinrv@gmail.com
Стрелковська Ю.О., кандидат юридичних наук, доцент
Ворзінг коледжу, Сандітон Вей, Ворзінг, BN14 9FD, Велика Британія.

МЕТОДИКА ПРОГНОЗУВАННЯ КІЛЬКОСТІ АБОНЕНТІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ В НИЗЬКОШВИДКІСНИХ РАДІОМЕРЕЖАХ ЗВ'ЯЗКУ

Анотація. *У роботі представлено підхід до прогнозування кількості абонентів автоматизованої системи управління, що функціонує в умовах низькошвидкісних радіомереж зв'язку. Запропоновано методику визначення граничної кількості користувачів системи на основі аналізу ймовірності обслуговування, отриманої шляхом імітаційного моделювання. Розроблене програмне забезпечення дозволяє змінювати кількість абонентів, оцінювати пропускну здатність, втрати в радіоканалі та поведінку буфера радіостанції. Результати моделювання дозволяють визначати межу стабільної роботи системи та зменшити ймовірність відмови в обслуговуванні.*

Ключові слова: прогнозування, імітаційне моделювання, АСУ, JDSS, ADatP-36, ймовірність обслуговування, низькошвидкісні радіомережі.

Автоматизовані системи управління (АСУ), що функціонують у низькошвидкісних радіомережах зв'язку, є важливим компонентом сучасних інформаційно-комунікаційних інфраструктур. У таких мережах застосовуються протоколи JDSS стандарту STANAG 4677 та ADatP-36, розроблені для роботи в умовах обмеженої пропускної здатності, великої затримки та нестабільності сигналу [1, 2]. Планування кількості абонентів в таких системах є критичним завданням, оскільки перевищення пропускної здатності призводить до зростання втрат пакетів, переповнення буфера і, як наслідок, зниження ймовірності обслуговування. У сучасних АСУ, що функціонують на базі низькошвидкісних радіомереж зв'язку, важливим чинником підвищення ефективності є здатність точно прогнозувати кількість активних абонентів. Це дозволяє оптимізувати розподіл пропускної здатності, визначати допустимі режими навантаження та забезпечувати необхідну якість обслуговування (QoS).

Метою роботи є розробка методики прогнозування кількості абонентів автоматизованої системи управління в низькошвидкісних радіомережах зв'язку шляхом імітаційного моделювання процесів обміну даними та визначення граничної ймовірності обслуговування.

АСУ побудовані на базі низькошвидкісних радіомережах зв'язку є важливою складовою сучасних військових, промислових та транспортних комплексів. Ці системи забезпечують оперативну взаємодію між підсистемами управління, передачу телеметричної інформації, команд і звітів у реальному часі. Особливістю таких систем є робота в умовах

обмежених радіоресурсів, змінних характеристик каналу передачі даних, наявності перешкод та високих вимог до надійності зв'язку.

У радіомережах АСУ часто застосовуються протоколи JDSS (STANAG 4677) та ADatP-36, які призначені для забезпечення сумісності систем зв'язку в умовах низьких швидкостей передачі. Такі мережі зазвичай мають пропускну здатність до 100 кбіт/с, високий рівень джитеру, втрати даних до 1–5 %, а також значні затримки, що ускладнює планування трафіку [1, 2]. При цьому навіть незначне перевищення навантаження може призвести до деградації системи, втрати даних і зниження ймовірності обслуговування.

Проблема прогнозування кількості абонентів, які можуть одночасно обслуговуватися системою без втрати якості зв'язку, є надзвичайно актуальною. Вона поєднує аспекти телекомунікаційного моделювання, теорії масового обслуговування, теорії ймовірностей та системного аналізу. Використання імітаційного моделювання в цьому контексті дозволяє не лише теоретично оцінити параметри роботи мережі, але й перевірити їх на практиці з використанням реалістичних даних трафіку, які відповідають розподілу Вейбула [3].

Методика дослідження базується на застосуванні імітаційного моделювання процесів обміну даними між абонентами АСУ, що функціонують у радіомережах з обмеженою пропускною здатністю. Основу моделі становить програмне забезпечення, що було розроблено на основі [3, 4, 5], яке дозволяє відтворювати характер трафіку протоколів JDSS і ADatP-36, а також оцінювати ключові параметри якості обслуговування (QoS) — середню затримку, пропускну здатність, ймовірність втрат та коефіцієнт обслуговування.

Модель складається з трьох основних компонентів:

1. Генератор трафіку, який створює випадкові інтервали між вимогами на обслуговування згідно з розподілом Вейбула з параметрами k≈0.43, λ≈0.34, що були експериментально підтверджені у роботах [1].
2. Механізм буферизації, реалізований за алгоритмом FIFO (first in – first out), який враховує максимальний розмір черги та час перебування пакету у буфері.
3. Модуль статистичного аналізу, який підраховує кількість обслужених і втрачених пакетів, обчислює середню пропускну здатність і ймовірність обслуговування за формулою [3]:

$$P_{\text{обс}} = \frac{N_{\text{обс}}}{N_{\text{обс}} + N_{\text{втр}}},$$

де $P_{\text{обс}}$ – ймовірність обслуговування;

$N_{\text{обс}}$ – кількість обслужених пакетів;

$N_{\text{втр}}$ – кількість втрачених пакетів.

У межах експерименту кількість абонентів системи поступово збільшується до досягнення граничного стану — коли $P_{\text{обс}}$ зменшується нижче допустимого порогу. Це дозволяє визначити максимальну кількість абонентів, які можуть стабільно функціонувати в мережі без зменшення якості обслуговування.

Для проведення дослідження використаємо наступні вихіжні дані:

- пропускна здатність 97 кбіт/с у режимі *Fixed Frequency*,
- ймовірність втрат у каналі — 2 %;
- максимальний розмір буфера — 50 кБайт
- час очікування пакету в буфері— 4 с;
- допустимий поріг ймовірності обслуговування - 0,8;

- кількість згенерованих пакетів в одній імітації - 100000.

Змінюючи кількість користувачів у межах від 5 до 15, проводиться серія моделювань для визначення залежності між кількістю абонентів, середньою пропускною здатністю та ймовірністю обслуговування, результати зведено в табл. 1.

Приклад роботи моделювання при генерації 100000 пакетів показано на рис. 1. Червона лінія на графіку – це максимальна полоса пропускання, яка задана користувачем, синій графік – це згенерований трафік для 10 сервісів STANAG 4677 та AdatP-36, фіолетовий графік – це трафік, що передається по радіоканалу з урахування буферизації і максимальної полоси пропускання.

Таблиця 1 – Результати проведення моделювання трафіку JDSS та ADatP-36

Кількість сервісів JDSS та AdatP-36	Середня полоса пропускання, кбіт/с	Кількість втрачених в радіоканалі пакетів	Кількість втрачених пакетів через переповнення буферу	Кількість втрачених пакетів через надмірне знаходження пакетів в буфері	Ймовірність обслуговування, %
5	45,8	1824	0	226	97,95
6	54,7	1683	1	782	97,54
7	66,6	1634	0	2547	95,82
8	74,2	1609	25	4156	94,22
9	83,3	1515	131	7259	91,1
10	90,82	1379	286	10334	88,01
11	101,7	1434	175	20020	78,37
12	110,6	1357	1456	18893	78,3
13	119,4	1239	2719	21737	74,3
14	127,8	1195	3942	24219	70,64
15	140,9	1119	6427	27513	64,95

На основі проведеного імітаційного моделювання з використанням програмної моделі трафіку стандартів STANAG 4677 та AdatP-36 в низькошвидкісних радіомережах отримуємо, що максимально допустима кількість сервісів JDSS та AdatP-36 не повинна перевищувати 10 для режиму роботи радіостанції Fixed Frequency і допустимого порогу ймовірності обслуговування 80%.

Рисунок 1 – Результати імітаційного моделювання

Висновки:

1. Розроблено методику прогнозування кількості абонентів АСУ, що побудовані на базі низькошвидкісних радіомереж зв'язку, на основі імітаційного моделювання трафіку протоколів JDSS і ADatP-36.

2. Створено програмне забезпечення, що дозволяє визначати ймовірність обслуговування системи при зміні кількості користувачів і параметрів радіоканалу: режим роботи, полоса пропускання, ймовірність втрат, розмір буферу.

3. Отримані результати дозволяють визначати граничну кількість абонентів, середню полосу пропускання, кількість втрачених в радіоканалі пакетів, кількість втрачених пакетів через переповнення буферу, кількість втрачених пакетів через надмірне знаходження пакетів в буфері, відсоток втрачених пакетів. для кожного режиму роботи радіостанції.

Література:

1. Strelkovskaya I.V. Modeling of telecommunication components of automated control systems in low-bandwidth radio networks / I.V. Strelkovskaya, R.V. Zolotukhin, A.O. Makoganiuk // In: P. Vorobiyenko, M. Ilchenko, I. Strelkovska. Current Trends in Communication and Information Technologies. Lecture Notes in Networks and Systems, 2021,. Springer, Cham, DOI: https://doi.org/10.1007/978-3-030-76343-5_9, P 150-170.

2. Strelkovskaya I., Zolotukhin R., "Research of low-bandwidth radionetworks QoS parameters" in Information and Telecommunication Sciences, International Research Journal, Volume 11, Number 1(20), January-June 2020, DOI: https://doi.org/10.20535/2411-2976.12020.77-81.6.

3. Strelkovskaya, I., Zolotukhin, R. (2025). Simulation Modeling Algorithm of Low-Bandwidth Radio Network of Automated Control Systems. In: Dovgyi, S., Siemens, E., Globa, L.,

Kopiika, O., Stryzhak, O. (eds) Applied Innovations in Information and Communication Technology. ICAIIT 2024. Lecture Notes in Networks and Systems, vol 1338. Springer, Cham. https://doi.org/10.1007/978-3-031-89296-7_2, PP 17-33.

4. Стрелковська, І., Золотухін, Р., Григор'єва, Т. (2022). Узагальнена модель оцінки показників функціонування низькошвидкісних мереж зв`язку автоматизованих систем управління. Інфокомунікаційні та комп'ютерні технології, 1(03), 153-168. https://doi.org/10.36994/2788-5518-2022-01-03-09.

5. Стрелковська І.В., Золотухін Р.В., Стрелковська Ю.О. Програмна реалізація імітаційного моделювання трафіку стандартів STANAG 4677 та ADATP-36. Третя міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025), Одеса, 18 липня 2025 р.

УДК 621.314
DOI https://doi.org/10.32837/11300.31381

Русу Олександр Петрович, к.т.н., доц.
Міжнародний університет
shurusu@ukr.net
Гінжул Владислав Михайлович
здобувач 2 курсу другого (магістерського) рівня
зі спеціальності 172 Електронні комунікації та радіотехніка
Міжнародний університет

ШЛЯХИ ОПТИМІЗАЦІЇ МАСОГАБАРИТНИХ ПОКАЗНИКІВ ПЕРЕТВОРЮВАЧІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Анотація. *У роботі проведено дослідження закономірностей, які визначають масогабаритні показники індуктивних елементів, що застосовуються в імпульсних перетворювачах напруги телекомунікаційного обладнання. Отримано математичні співвідношення, які відображають взаємозв'язок між магнітними параметрами магнітопровода, струмовими навантаженнями та енергетичними характеристиками у межах одного циклу перетворення. Показано, що мінімізація розмірів індуктивних елементів можлива завдяки підвищенню частоти комутації, використанню матеріалів із покращеними магнітними властивостями та удосконаленню теплових умов роботи. Результати дослідження дають змогу визначати допустимі межі габаритів індуктивних компонентів у високочастотних системах живлення телекомунікаційних пристроїв.*

У сучасних телекомунікаційних системах перетворення електричної енергії реалізується переважно за допомогою імпульсних перетворювачів, які забезпечують високу ефективність та стабільність роботи. Постійне вдосконалення схемотехніки силової частини спрямоване на зменшення енергетичних втрат і покращення масогабаритних характеристик [1]. Одним із найважливіших завдань у цьому напрямі є оптимізація розмірів індуктивних компонентів, які істотно впливають на загальні параметри вузлів живлення.

Накопичувальний дросель імпульсного перетворювача складається з обмоток провідника, намотаних на магнітопровід, що концентрує магнітне поле та забезпечує зв'язок із зовнішнім електричним колом (рис. 1) [2].

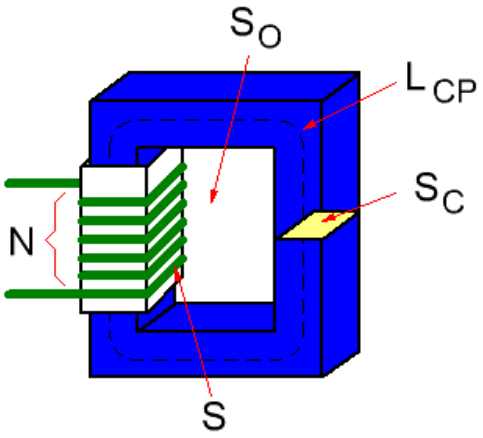


Рисунок 1 – Конструкція накопичувального дроселя імпульсного перетворювача

До основних геометричних параметрів магнітопроводу належать довжина середньої магнітної лінії L_{CP}, площа поперечного перерізу сердечника S_C та площа вікна S_O для розміщення обмоток. Робочий об'єм магнітопровода V, який бере участь у процесі енергоперетворення, визначається добутком L_{CP} на S_C, тобто:

$$V = S_C L_{CP} \tag{1}$$

У процесі роботи струм I, що протікає через обмотку, спричиняє її нагрівання відповідно до закону Джоуля-Ленца. Площа S, яку займає провідник у вікні магнітопроводу, залежить від кількості обвитків N та густини струму J:

$$S = N\frac{I}{J} \tag{2}$$

Кількість обвитків N, відповідно до закону Фарадея, визначає взаємозв'язок між зміною магнітного потоку ΔФ у магнітопроводі та напругою U, прикладеною до обмотки впродовж часу Δt:

$$\Delta\Phi = \frac{U\Delta t}{N} \tag{3}$$

Магнітний потік у сердечнику дорівнює добутку магнітної індукції B на площу S_C. Тоді зміна потоку ΔФ прямо пропорційна зміні індукції ΔВ при незмінній площі поперечного перерізу:

$$\Delta\Phi = S_C \Delta B \tag{4}$$

Після підстановки виразів (3) та (4) у формулу (2) одержуємо узагальнену залежність, що пов'язує напругу на обмотці з геометричними параметрами магнітного кола:

$$S = \frac{IU\Delta t}{JS_C\Delta B} \tag{5}$$

Аналіз цього співвідношення показує, що площа S, яку займає обмотка, залежить від густини струму J у провіднику та магнітної індукції B в осерді. Для забезпечення необхідного енергетичного рівня індуктивного елемента параметри магнітопроводу повинні задовольняти умову:

$$S_O S_C \geq \frac{IU\Delta t}{J\Delta B} \tag{6}$$

Отримані залежності свідчать, що розміри дроселів пропорційні кількості енергії, яку необхідно передати за один цикл. Тому оптимізація масогабаритних показників індуктивних елементів імпульсних перетворювачів телекомунікаційного обладнання можлива за умов використання матеріалів з вищою магнітною індукцією B, підвищення допустимої густини струму J або збільшення частоти комутації.

Висновки. На основі проведеного аналізу встановлено, що масогабаритні характеристики індуктивних елементів імпульсних перетворювачів визначаються кількістю енергії, яка передається через магнітне коло за цикл роботи. Отримані аналітичні співвідношення (1) – (6) дозволяють оцінити вплив густини струму в обмотках і магнітної індукції в осерді на необхідну площу для розміщення провідників. Мінімізація розмірів можлива при використанні сучасних магнітних матеріалів, оптимізації теплових умов і підвищенні робочої частоти перетворювачів. Зазначені результати можуть бути використані під час проєктування високоефективних джерел живлення телекомунікаційних пристроїв.

Література:

1. Zehendner M., Ulmann M. Power Topologies Handbook. Texas Instruments, 2016. 216 p.
2. Erickson R. W., Maksimovic D. Fundamentals of Power Electronics. Springer, 2020. 912 p.

УДК 004.738.5
DOI https://doi.org/10.32837/11300.31384

Грищенко А.О.,студент,
Педяш В.В., к.т.н., доцент,
Міжнародний університет,
a-gr@ukr.net

АВТОМАТИЗОВАНЕ КОНФІГУРУВАННЯ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ ВІДКРИТИХ ПРОГРАМНИХ ЗАСОБІВ

Анотація. *Робота присвячена дослідженню та практичній реалізації системи автоматизованого конфігурування мережевого обладнання на основі відкритих програмних засобів. Розглянуто концепцію Infrastructure as Code та її застосування для адміністрування мережевої інфраструктури. Розроблено модульну систему автоматизації на мові Python з використанням бібліотеки Netmiko для налаштування лабораторного SIP-стенду на базі обладнання Cisco. Проведено порівняльний аналіз ефективності ручного та автоматизованого підходів до конфігурування, який продемонстрував скорочення часу налаштування у 60 разів при підвищенні надійності та відтворюваності конфігурацій.*

Сучасні корпоративні мережі характеризуються зростаючою складністю інфраструктури, великою кількістю пристроїв різних виробників та необхідністю оперативного реагування на зміни бізнес-вимог. Традиційний підхід до адміністрування мережевого обладнання через ручне введення команд стає неефективним та схильним до помилок людського фактора. Це обумовлює потребу у впровадженні автоматизованих систем управління конфігураціями, які забезпечують швидкість, точність та відтворюваність налаштувань [1].

Метою даної роботи є розробка та дослідження системи автоматизованого конфігурування мережевої інфраструктури на основі відкритих програмних засобів із застосуванням концепції Infrastructure as Code.

Концепція Infrastructure as Code передбачає опис інфраструктури у вигляді програмного коду, який може бути версіонований, повторно використаний та автоматично застосований до цільових систем [2]. Цей підхід забезпечує декларативність конфігурацій, їх відтворюваність та можливість аудиту всіх змін. У сфері мережевого адміністрування IaC дозволяє зберігати конфігурації пристроїв у текстових файлах, які легко піддаються

версіонуванню в системах контролю версій типу Git, та автоматично розгортати їх на обладнанні різних виробників.

Для практичної реалізації системи автоматизації було обрано мову програмування Python завдяки її простоті, широкій екосистемі бібліотек для роботи з мережевим обладнанням та кросплатформеності [3]. Основним інструментом взаємодії з пристроями виступає бібліотека Netmiko, яка надає високорівневий інтерфейс для роботи з SSH-з'єднаннями та підтримує специфіку командних інтерфейсів різних виробників мережевого обладнання. Архітектура розробленої системи побудована на принципах модульності та відокремлення конфігураційних даних від програмної логіки [4].

Програмна частина системи автоматизації реалізована у вигляді модульного Python-проєкту, архітектура якого побудована з дотриманням принципів Infrastructure as Code та відокремлення конфігураційних даних від програмної логіки. Структура проєкту представлена у таблиці 1, де показано організацію файлів та каталогів з описом призначення кожного елемента системи.

Центральним елементом архітектури є файл devices.yaml, який виконує роль декларативного опису інфраструктури та містить параметри підключення до кожного мережевого пристрою, включаючи IP-адресу, облікові дані, тип пристрою для коректної ініціалізації драйвера Netmiko та шлях до файлу конфігурації. Формат YAML обраний через його високу читабельність та зручність ручного редагування без спеціалізованих інструментів. Власне конфігураційні команди для кожного пристрою винесені в окремі текстові файли у каталозі configs/, що дозволяє версіонувати їх у системах контролю версій та змінювати конфігурації без втручання в програмний код [5]. Головний скрипт main.py реалізує логіку управління процесом автоматизації: зчитування параметрів пристроїв з YAML-файлу, встановлення SSH-з'єднань через контекстний менеджер Netmiko, виконання попередніх exec-команд при необхідності, застосування основної конфігурації з текстових файлів та збереження змін у енергонезалежну пам'ять пристроїв командою write memory.

Таблиця 1 – Структура файлів проєкту автоматизації

Шлях до елементу	Опис призначення
sip_automation/	Кореневий каталог проєкту
main.py	Головний виконавчий скрипт Python з логікою підключення та конфігурування
devices.yaml	Конфігураційний файл з параметрами підключення до пристроїв
configs/	Каталог для текстових файлів конфігурацій окремих пристроїв
configs/cisco_2960.txt	Файл конфігурації комутатора з налаштуваннями VLAN та портів
configs/cisco_2811.txt	Файл конфігурації маршрутизатора з налаштуваннями CME, DHCP та SIP
logs/	Каталог для автоматично створюваних журналів виконання

Лабораторний стенд для апробації розробленої системи включає маршрутизатор Cisco 2811, комутатор Cisco 2960 та два IP-телефони Cisco 7942G. Мережева топологія спроектована з використанням технології віртуальних локальних мереж: VLAN 10 виділено виключно для голосового трафіку IP-телефонів, VLAN 100 — для трафіку управління. Маршрутизатор виконує роль комплексного сервера, що включає функції CME (Cisco Unified Communications Manager Express), DHCP-сервера для автоматичної роздачі IP-адрес, TFTP-сервера для доставки прошивок і конфігураційних файлів телефонам, а також SIP-реєстратора [4]. На маршрутизаторі налаштовано два фізичні інтерфейси: Fa0/0 отримує IP-адресу через DHCP для можливого підключення до Інтернету, а Fa0/1 використовується для внутрішньої комунікації з комутатором через технологію "router-on-a-stick" з підінтерфейсами Fa0/1.10 (192.168.10.1) для VLAN 10 та Fa0/1.100 (192.168.100.1) для VLAN 100. Логічна схема мережевої топології представлена на рисунку 1.

Центральним елементом архітектури є файл devices.yaml, який виконує роль декларативного опису інфраструктури та містить параметри підключення до кожного мережевого пристрою, включаючи IP-адресу, облікові дані, тип пристрою для коректної ініціалізації драйвера Netmiko та шлях до файлу конфігурації. Формат YAML обраний через його високу читабельність та зручність ручного редагування без спеціалізованих інструментів. Власне конфігураційні команди для кожного пристрою винесені в окремі текстові файли у каталозі configs/, що дозволяє версіонувати їх у системах контролю версій та змінювати конфігурації без втручання в програмний код [5]. Головний скрипт main.py реалізує логіку управління процесом автоматизації: зчитування параметрів пристроїв з YAML-файлу, встановлення SSH-з'єднань через контекстний менеджер Netmiko, виконання попередніх exec-команд при необхідності, застосування основної конфігурації з текстових файлів та збереження змін у енергонезалежну пам'ять пристроїв командою write memory.

Програма використовує високорівневий метод send_config_from_file бібліотеки Netmiko, який автоматично входить у режим глобальної конфігурації, виконує команди з файлу послідовно та коректно обробляє коментарі і порожні рядки. Модульна архітектура проєкту забезпечує чіткий поділ обов'язків: базова ініціалізація пристроїв з налаштуванням SSH-доступу виконується вручну один раз, а вся подальша функціональна конфігурація застосовується автоматично, що робить процес розгортання стенду швидким, відтворюваним і надійним.

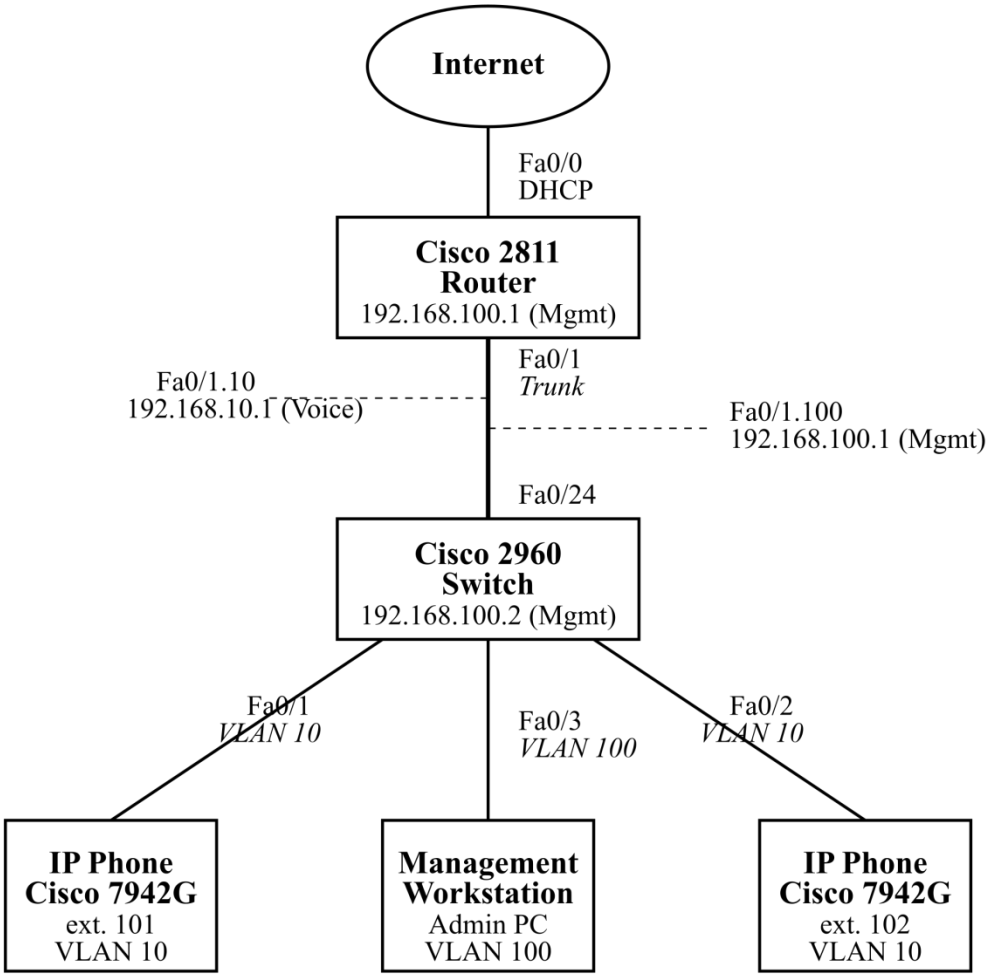


Рисунок 1 – Логічна схема топології лабораторного SIP-стенду

Дослідження ефективності розробленої системи проводилося шляхом порівняльного аналізу часових витрат між ручним та автоматизованим підходами до конфігурування обладнання. Для забезпечення чистоти експерименту обидва пристрої були повністю скинуті

до заводських налаштувань, після чого виконувалася базова ініціалізація для забезпечення SSH-доступу. Результати вимірювань представлено у таблиці 2, де показано детальне розбиття загального часу на окремі етапи процесу конфігурування.

Таблиця 2 – Порівняння часових витрат на конфігурування обладнання

Етап процесу	Ручне конфігурування	Автоматизоване конфігурування
Базова ініціалізація пристроїв	15 хв	15 хв
Налаштування комутатора Cisco 2960	8 хв	12 с
Налаштування маршрутизатора Cisco 2811	22 хв	18 с
Перевірка конфігурації та виправлення помилок	12 хв	0 хв
Документування виконаних дій	10 хв	0 хв (автоматичне логування)
Загальний час після базової ініціалізації	52 хв	30 с
Загальний час з урахуванням ініціалізації	67 хв	15 хв 30 с

Аналіз результатів виявляє значне скорочення часу на етапі безпосереднього конфігурування пристроїв з тридцяти хвилин ручної роботи до тридцяти секунд автоматизованого виконання, що становить прискорення у шістдесят разів. Особливо помітною є економія часу на етапі налаштування маршрутизатора, конфігурація якого містить значно більше команд порівняно з комутатором через наявність налаштувань CME, DHCP, TFTP та SIP-сервісів. При ручному конфігуруванні адміністратор витрачає додатковий час на перевірку правильності введення кожної команди та виправлення синтаксичних помилок, тоді як автоматизована система виконує всі команди послідовно з гарантованою коректністю. Документування виконаних дій при ручному підході вимагає окремих зусиль для створення звітів, тоді як розроблена система автоматично веде детальний лог з мітками часу для кожної операції, що створює повний аудит-слід для подальшого аналізу та дотримання вимог комплаєнсу.

Дослідження стійкості системи до помилок включало серію тестів з навмисним внесенням різноманітних проблемних ситуацій: відсутність файлу конфігурації, недоступність пристрою через мережу, невірні облікові дані та синтаксичні помилки у командах. У всіх випадках система коректно перехоплювала виключення, записувала детальну інформацію про помилку в лог-файл з вказівкою IP-адреси проблемного пристрою та продовжувала обробку наступних пристроїв у списку без аварійного завершення. Це критично важливо для масштабних інфраструктур, де тимчасова недоступність одного пристрою не повинна блокувати конфігурування решти обладнання. Важливим результатом дослідження стало підтвердження повної відтворюваності конфігурації: після кожного повного скидання обладнання запуск автоматизаційного скрипта гарантовано відновлював ідентичну робочу конфігурацію з усіма функціональними можливостями, що особливо цінно для навчальних лабораторій та забезпечення швидкого відновлення після інцидентів у корпоративному середовищі.

На основі проведеного дослідження можна зробити наступні висновки. Розроблена система автоматизації конфігурування мережевого обладнання на основі Python та Netmiko забезпечує значне скорочення часових витрат на адміністрування при одночасному підвищенні надійності та відтворюваності конфігурацій. Застосування концепції Infrastructure as Code дозволяє версіонувати конфігурації в системах контролю версій, швидко розгортати ідентичні налаштування та вести повний аудит-слід всіх змін. Модульна архітектура рішення з чітким розділенням виконавчого коду, конфігураційних даних та журналів забезпечує масштабованість та можливість адаптації для різних типів мережевого

обладнання. Економія часу адміністратора досягає 60-кратного прискорення порівняно з ручним підходом, що при щотижневому використанні дає економію понад 25 годин робочого часу за академічний рік.

Література:

1. Edelman J., Oswalt M., Lowe S. Network Programmability and Automation: Skills for the Next-Generation Network Engineer. 2-ге вид. – Sebastopol (CA) : O'Reilly Media, 2021. – 464 с.

2. Morris K. Infrastructure as Code: Managing Servers in the Cloud. 2-ге вид. – Sebastopol (CA) : O'Reilly Media, 2020. – 368 с.

3. Jorepalli S., Bairy V. Leveraging Network Automation with Python, Terraform, and Ansible to Enhance Security and Operational Efficiency in Large-Scale Networks. – International Journal of Intelligent Systems and Applications in Engineering, Vol. 12, No. 23s, 2024. – С. 2009-2016.

4. Cisco Systems. Cisco Unified Communications Manager Express System Administrator Guide. Release 12.0. – San Jose (CA) : Cisco Systems Inc., 2019. – 892 с.

5. Humble J., Farley D. Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation. – Boston (MA) : Addison-Wesley Professional, 2010. – 512 с.

DOI: https://doi.org/10.32837/11300.31385

Вакарчук Анна Олександрівна
Міжнародний університет
sunny120606@gmail.com
Прядка Станіслав Андрійович
Міжнародний університет
stanislav.priadka65@gmail.com

ВПЛИВ ІНТЕРФЕРЕНЦІЇ НА РОБОТУ БЕЗДРОТОВИХ МЕРЕЖ У ЩІЛЬНИХ МІСЬКИХ СЕРЕДОВИЩАХ

Анотація. *Управління завадами стало критичною проблемою в щільних бездротових мережах через збільшення кількості підключених пристроїв та обмежену доступність радіочастотного спектру. У даній доповіді розглядаються передові методи управління інтерференцією в щільних бездротових мережах з акцентом на поліпшення пропускної здатності мережі, якості сигналу та загальної продуктивності.*

Повсюдна наявність і поширення бездротових пристроїв, особливо в густонаселених міських районах, створили складне і перевантажене радіочастотне середовище, в якому інтерференція стала серйозною проблемою для надійного, стабільного і високоякісного бездротового зв'язку. Впровадження передових технологій зв'язку, таких як 5G, посилило проблему інтерференції у густонаселених міських районах. Інтерференція може значно погіршити продуктивність мережі, що призведе до зниження швидкості передачі даних, збільшення затримки і погіршення якості обслуговування користувачів. Ефективне тестування інтерференції має вирішальне значення для виявлення та вирішення цих проблем з метою забезпечення надійної та ефективної роботи мережі.

Проблеми бездротових комунікаційних мереж у районах із щільною міською забудовою

Густонаселені міські середовища ставлять перед бездротовими комунікаційними мережами низку особливих проблем. Ось деякі з основних проблем:

1. Висока щільність пристроїв. Велика кількість бездротових пристроїв у міських районах може призвести до значних завад і перевантажень. Кожен пристрій конкурує за

обмежені ресурси спектру, що призводить до інтерференції в одному каналі та сусідніх каналах. Ці завади можуть погіршити продуктивність мережі, зменшити пропускну здатність і збільшити затримку [2].

2. Фізичні завади. Міські середовища заповнені будівлями, транспортними засобами та іншими спорудами, які можуть заважати проходженню бездротових сигналів або відбивати їх, що призводить до ослаблення сигналу, багатопроменевого згасання та проблем із покриттям [3].

3. Повторне використання частот. Необхідність повторного використання частотних діапазонів у густонаселених районах може призвести до завад у межах одного каналу, коли сусідні пристрої, що працюють на одному каналі, створюють завади один одному. Повторне використання частот є необхідністю в густонаселених міських районах для найбільш ефективного використання обмеженого спектру.

4. Зовнішня інтерференція. Немережеві пристрої, такі як мікрохвильові печі, бездротові камери та інші електронні пристрої, можуть випромінювати сигнали, які створюють завади для бездротових комунікаційних мереж у міських умовах.

5. Мобільність та динамічні середовища. Динамічний характер міського середовища, з транспортними засобами та людьми, що постійно рухаються, ускладнює управління мережею та зменшення завад. Зміни у фізичному середовищі можуть змінити схеми поширення та створити нові джерела завад.

6. Потреба у високій пропускній здатності. У міських районах часто спостерігається високий попит на пропускну здатність мережі через поширення додатків, що вимагають великого обсягу даних, таких як потокове відео, онлайн-ігри та пристрої Інтернету речей. Задоволення цього попиту при одночасному зменшенні завад є значним викликом.

7. Питання безпеки та конфіденційності. Висока щільність пристроїв та відкритий характер бездротового зв’язку роблять міські мережі вразливими до загроз безпеки, таких як прослуховування, несанкціонований доступ та атаки типу «відмова в обслуговуванні».

Вплив інтерференції на мережі 802.11

Бездротовий зв’язок – це спільне середовище, невидиме для ока. Зазвичай ми дізнаємося про проблеми з продуктивністю WLAN від кінцевих користувачів та під час тестування. Дві причини поганої продуктивності Wi-Fi – це інтерференція в одному каналі (CCI) та інтерференція в сусідньому каналі (ACI). Добре продумана конструкція WLAN може допомогти зменшити кількість CCI/ACI, що застосовуються під час впровадження. Інструменти візуалізації, такі як програмне забезпечення для обстеження місця, допомагають інженеру відобразити обидва ефекти. Після впровадження обстеження для перевірки гарантують, що бездротова мережа працює відповідно до проекту. Це включає перевірку кількості CCI/ACI.

Інтерференція в одному каналі виникає, коли кілька передавачів працюють на одній частоті в одній і тій же області. У таких умовах станції дотримуються протоколу CSMA/CA, передаючи дані тільки тоді, коли носій не зайнятий. Зі збільшенням конкуренції, що часто трапляється в районах з високою щільністю населення, станції зазнають затримок, чекаючи, поки інші закінчать передачу, і оновлюють свої таймери за допомогою вектора розподілу мережі (NAV).

Інтерференція сусідніх каналів виникає, коли передачі на каналах, що перекриваються або на сусідніх каналах, спричиняють витік сигналу, додаючи шум і спотворення. ACI зазвичай є більш шкідливою, ніж CCI, оскільки канали, що перекриваються, можуть спотворювати сигнали або спричиняти помилкові оцінки чистоти каналу (CCA). Коли це відбувається, станції без необхідності відкладають зв’язок, що призводить до погіршення продуктивності мережі [2].

Техніки та стратегії управління інтерференцією в щільних бездротових мережах

Для вирішення проблем, пов'язаних з завадами в умовах щільного бездротового середовища, було розроблено та впроваджено низку технічних рішень і стратегій. Ці підходи спрямовані на зменшення впливу завад, оптимізацію продуктивності мережі та забезпечення надійного бездротового з'єднання. До основних технічних рішень з управління завадами належать:

1. Розподіл і планування каналів:

– динамічний або статичний розподіл каналів мінімізує завади в одному каналі;

– повторне використання частот у різних областях і використання неперекриваючих (ортогональних) каналів допомагає запобігти завадам у сусідніх каналах;

2. Регулювання потужності:

– адаптивне регулювання потужності: регулює потужність передачі на основі відстані та рівня завад;

– оптимізація потужності: збалансовує силу сигналу та завади для підвищення ефективності [4].

3. Формування променю та MIMO:

– формування променю (Beamforming) – це технологія, що направляє сигнали у певний напрямок, зменшуючи завади в інших місцях та підвищуючи ефективність систем MIMO;

– MIMO: використовує кілька антен для одночасних потоків даних, покращуючи пропускну здатність та стійкість до завад [6].

4. Сучасні технології усунення інтерференції дозволяють відфільтрувати небажані сигнали та поліпшити якість зв'язку:

– алгоритми SIC дозволяють відокремити та усунути інтерференційні сигнали, покращуючи якість бажаного сигналу;

– Технології адаптивного фільтрування динамічно пристосовуються до мінливих моделей інтерференції, забезпечуючи усунення інтерференції у режимі реального часу.

5. Когнітивне радіо та динамічний доступ до спектру дозволяє пристроям виявляти перевантаження та динамічно перемикатися на менш завантажені частоти для кращого використання спектру.

6. Ущільнення мережі та малі комірки:

– розгортання малих комірок може допомогти поліпшити просторове повторне використання спектру, зменшивши інтерференцію між комірками;

– техніки управління інтерференцією між малими комірками та макрокомірками мають вирішальне значення для ефективного розгортання щільних мереж малих комірок.

7. Просторове повторне використання:

– інноваційні методи підвищення ефективності використання спектру за допомогою просторового повторного використання, такі як вдосконалені методи планування та розподілу ресурсів, можуть допомогти зменшити завади в щільних бездротових мережах [4].

Висновок.

В даному дослідженні ми розглянули критичну проблему впливу інтерференції на роботу щільних бездротових мереж. Вивчивши різні типи завад, основні методи та стратегії їх усунення, а також нові технології, які можуть революціонізувати управління інтерференцією, ми отримали цінну інформацію для вирішення цього складного питання.

Література:

1. Interference Testing in Dense Urban Environments: A Research Paper: https://www.ijirmps.org/papers/2024/2/232222.pdf

2. Reducing Wi-Fi Channel Interference: https://www.networkcomputing.com/wi-fi/reducing-wifi-channel-interference
3. Measurement of Attenuation by Building Structures in Cellular Network Bands: https://vbn.aau.dk/ws/portalfiles/portal/287592036/mat_attenuation_VBN.pdf
4. High Reuse Efficiency of Radio Resources in Urban Microcellular Systems: https://www.researchgate.net/publication/3154548_High_Reuse_Efficiency_of_Radio_Resources_in_Urban_Microcellular_Systems
5. Interference Management in Dense Wireless Networks: https://www.researchgate.net/publication/384635499_Interference_Management_in_Dense_Wireless_Networks
6. Дослідження методів обробки сигналів у MIMO системах: https://tit.dut.edu.ua/index.php/telecommunication/article/view/2592/2468

DOI: https://doi.org/10.32837/11300.31386

Вакарчук Анна Олександрівна
Міжнародний університет
sunny120606@gmail.com
Димов Максим Віталійович
Міжнародний університет
mak.dymov@gmail.com

ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ АНТЕННИХ РЕШІТОК ДЛЯ АДАПТИВНОГО УПРАВЛІННЯ ПРОМЕНЕМ У МОБІЛЬНИХ МЕРЕЖАХ 5G/6G

Анотація. *Досліджено ключові аспекти застосування інтелектуальних антенних решіток для реалізації адаптивного управління променем у мобільних мережах п'ятого та шостого поколінь (5G/6G). Проаналізовано переваги АУП, такі як підвищення спектральної ефективності, мінімізація інтерференції та покращення якості обслуговування. Розглянуто основні виклики та сучасні алгоритмічні підходи до формування променя, зокрема з використанням методів машинного навчання. Робота демонструє критичну важливість IAP для забезпечення високої пропускної здатності та надійності, яких вимагають стандарти 5G та 6G.*

Ключові слова: інтелектуальні антенні решітки (IAP), адаптивне управління променем (АУП), 5G, 6G, MIMO, спектральна ефективність, машинне навчання (ML).

Стрімкий розвиток мобільних мереж п'ятого (5G) та перехід до стандартів шостого (6G) поколінь зумовлюють експоненціальне зростання вимог до пропускної здатності, надійності з'єднання та мінімізації затримок. Для задоволення цих вимог необхідне впровадження нових технологічних рішень, ключовим з яких є адаптивне управління променем (АУП) на базі інтелектуальних антенних решіток (IAP) [1].

Актуальність дослідження полягає в тому, що традиційні антенні системи з широкою діаграмою спрямованості не здатні забезпечити необхідну спектральну ефективність та енергоефективність у щільних міських забудовах. IAP, завдяки здатності формувати вузькі, керовані промені сигналу безпосередньо в напрямку абонента, дозволяють вирішити дві критичні проблеми: компенсацію високих втрат при поширенні сигналу у міліметровому діапазоні (mmWave) та суттєве зниження рівня міжканальної інтерференції.

Проте, реалізація ефективного АУП у динамічних сценаріях 5G/6G є складним науково-технічним завданням. Воно вимагає розробки високопродуктивних алгоритмів, здатних в реальному часі відстежувати мобільність абонентів та адаптуватися до змін у радіоканалі, що робить дослідження в цій галузі пріоритетним [2].

Метою даного дослідження є аналіз сучасних підходів до реалізації інтелектуальних антенних решіток та алгоритмів адаптивного управління променем, а також оцінка їх ефективності для підвищення ключових показників продуктивності (KPI) мобільних мереж 5G та 6G.

Інтелектуальні антенні решітки (IAP) є фундаментальною технологією для реалізації стандартів 5G та майбутніх мереж 6G. Їхня ключова особливість полягає у здатності до просторової селекції, що досягається шляхом когерентної обробки сигналів від множини антенних елементів [3]. На відміну від традиційних секторних антен, IAP формують вузькоспрямовані промені, динамічно адаптуючи їхню форму та напрямок. Цей процес, відомий як адаптивне управління променем (АУП) або "бімформінг", полягає у концентрації енергії радіосигналу в напрямку конкретного абонентського пристрою, одночасно формуючи "нулі" діаграми спрямованості в напрямку джерел завад [4].

Незважаючи на переваги, ефективна реалізація АУП у щільних та динамічних міських сценаріях (Urban Macro/Micro) стикається з низкою викликів. Зокрема, висока мобільність абонентів вимагає наднизьких затримок при перерахунку та оновленні конфігурації променя (beam tracking), а складність радіоканалу (багатопроменеве поширення, швидкі зміни) ускладнює отримання точної та своєчасної інформації про стан каналу (Channel State Information, CSI) [5].

Практична цінність технологій АУП найповніше розкривається у складних сценаріях експлуатації мереж 5G/6G, де традиційні підходи є неефективними.

Мережі у місцях високої щільності (High-Density Venues), таких як на стадіонах, у концерт-холах або на транспортних вузлах АУП дозволяє одночасно обслуговувати тисячі абонентів. Завдяки просторовому ущільненню (SDMA), технологія формує індивідуальні промені для груп користувачів, мінімізуючи взаємну інтерференцію та підтримуючи високу пропускну здатність [4].

Високомобільні додатки (High-Mobility Scenarios) для систем зв'язку "автомобіль-до-всього" (V2X), АУП є критичним для підтримки стабільного з'єднання з транспортними засобами, що рухаються на високій швидкості. Це вимагає предиктивних алгоритмів відстеження променя (beam tracking), часто реалізованих на базі ML, для миттєвої адаптації до зміни положення абонента [6].

Розгортання у діапазоні mmWave для компенсації високих втрат при поширенні сигналу та чутливості до блокування (наприклад, будівлями або тілом людини), АУП використовується для формування "гострих" променів з високим коефіцієнтом підсилення. Це є основою для надання послуг фіксованого бездротового доступу (FWA) у щільній міській забудові [1, 5].

Висновок.

Проведене дослідження підтверджує, що інтелектуальні антенні решітки та технологія адаптивного управління променем є критично важливими компонентами для повноцінної реалізації потенціалу мобільних мереж 5G та майбутніх систем 6G. Вони забезпечують необхідне підвищення спектральної та енергетичної ефективності, дозволяючи компенсувати високі втрати сигналу в міліметровому діапазоні [1] та мінімізувати інтерференцію в щільних мережах.

Аналіз показав, що основним викликом залишається висока обчислювальна складність алгоритмів АУП, особливо в умовах високої мобільності абонентів та швидких змін стану радіоканалу (CSI) [5]. Сучасні підходи, що інтегрують методи машинного навчання (ML), демонструють значний потенціал для вирішення цих проблем [2, 6]. ML-моделі здатні предиктивно аналізувати радіооточення та оптимізувати конфігурацію променя з меншою затримкою, ніж традиційні алгоритми, що відкриває шлях до створення по-справжньому адаптивних та високоефективних мобільних мереж.

Література:

1. A Survey of Millimeter Wave (mmWave) Communications for 5G: Opportunities and Challenges / Ali H. et al. // IEEE Access. – 2023. – Vol. 11. – P. 34502-34520. [Електронний

ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/10091395 (дата звернення: 02.11.2025).

2. Machine Learning-Based Beamforming Algorithm for Massive MIMO Systems in 5G Networks / Y. Zhang, Q. Wu, J. Wang // IEEE Wireless Communications Letters. – 2024. – Vol. 13, No. 4. – P. 1045-1049. [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/10410408 (дата звернення: 02.11.2025).

3. An Overview of Massive MIMO for 5G and 6G / F. A. P. de Figueiredo, T. L. Marzetta // IEEE Latin America Transactions. – 2022. – Vol. 20, No. 2. – P. 216-224. [Електронний ресурс]. – Режим доступу: https://latamt.ieeer9.org/index.php/transactions/article/view/5886 (дата звернення: 02.11.2025).

4. Survey of Beamforming Techniques in Advanced 5G and 6G Wireless Technologies / S. K. Singh, R. Kumar // International Journal of Innovative Engineering and Emerging Technologies. – 2024. – Vol. 9, No. 3. – P. 1-10. [Електронний ресурс]. – Режим доступу: http://www.journal-iiie-india.com/1_may_24/123_online_may.pdf (дата звернення: 02.11.2025).

5. AI for CSI Prediction in 5G-Advanced and Beyond / W. Shi, J. Liu, Z. Wei // arXiv preprint arXiv:2504.12571. – 2025. [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2504.12571 (дата звернення: 02.11.2025).

6. Machine Learning Based Beam Tracking in mmWave Systems / J. Kim, H. Lee // KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science (EECS). – 2022. [Електронний ресурс]. – Режим доступу: https://www.diva-portal.org/smash/get/diva2:1544084/FULLTEXT01.pdf (дата звернення: 02.11.2025).

DOI: https://doi.org/10.32837/11300.31387

Вакарчук Анна Олександрівна
Міжнародний університет
sunny120606@gmail.com
Рущін Владислав Сергійович
Міжнародний університет
ryshin2504@gmail.com

СТВОРЕННЯ СИСТЕМИ “РОЗУМНИЙ ПАРКІНГ” З ВИКОРИСТАННЯМ ДАТЧИКІВ РУХУ ТА WI- FI/LORAWAN

Анотація. *У роботі розглянуті питання розробки системи «розумний паркінг», що визначає зайнятість паркомісць за допомогою датчиків руху та передає дані через Wi-Fi або LoRaWAN. Актуальність теми пов’язана з необхідністю оптимізації паркувального простору та підвищення ефективності міської інфраструктури. Проаналізовано технології IoT, сенсори та можливості бездротових мереж. Запропоновано архітектуру, що включає датчик, мікроконтролер, сервер та веб-інтерфейс для відображення статусу місць у реальному часі.*

Сучасні міста дедалі більше стикаються з проблемою нестачі доступних паркомісць, перевантаженням транспортних вузлів та нераціональним використанням існуючої інфраструктури. У великих міських агломераціях значна частина заторів формується саме через те, що водії змушені витрачати час на пошук вільного паркомісця. За даними міжнародних досліджень, у середньому водій витрачає до 20–30% загального часу руху на маневрування, очікування та пошук місця для паркування[1]. Це створює додаткове навантаження на дороги, підвищує рівень забруднення повітря, а також погіршує якість життя мешканців.

Технології Інтернету речей (IoT) відкривають можливості для комплексної автоматизації міської інфраструктури, включаючи паркувальні системи[2]. Використання

датчиків руху, ультразвукових сенсорів, бездротових каналів передачі даних Wi-Fi та LoRaWAN дозволяє в режимі реального часу відстежувати зайнятість паркомісць, передавати інформацію на сервер та забезпечувати доступ користувачам через веб-інтерфейс або мобільний застосунок.

Таким чином, створення системи «розумний паркінг» є актуальним завданням для розвитку Smart City-технологій. Така система допомагає зменшити навантаження на дорожній рух, оптимізувати використання паркувальних площ, зменшити викиди CO_2 та підвищити комфорт користувачів. А головне , подібний проєкт може бути впроваджений у реальних умовах з мінімальними витратами, що робить його практично значущим і соціально корисним.

Метою роботи є створення прототипу системи «розумний паркінг», яка здатна автоматично визначати наявність або відсутність автомобіля на певному паркомісці та передавати відповідні дані до центрального сервера через Wi-Fi або LoRaWAN залежно від архітектури паркувальної зони.

Принцип роботи системи полягає у послідовній взаємодії сенсорної, обчислювальної та серверної частин. Спершу сенсор визначає, чи перебуває автомобіль на паркомісці. Отримані дані зчитуються мікроконтролером, який передає інформацію до мережі через Wi-Fi або LoRaWAN[3-5]. Сервер приймає ці дані, опрацьовує їх та оновлює відповідну базу. Після цього у веб-інтерфейсі автоматично змінюється статус вибраного місця, і користувач отримує доступ до актуальної карти паркінгу в режимі реального часу.

Наукова новизна роботи полягає в поєднанні доступних апаратних компонентів, таких як ESP32 та LoRa-модулі, з енергоефективними каналами зв’язку та можливістю масштабування системи для покриття великих територій[6]. Розроблений підхід є універсальним і може адаптуватися до різноманітних сценаріїв використання.

Практична цінність системи визначається широкими можливостями її впровадження: від житлових масивів і комерційних центрів до бізнес-кампусів та муніципальних паркувальних зон. Розробка легко модернізується, допускає встановлення додаткових сенсорів і може бути інтегрована з існуючими міськими сервісами, що робить її корисною для оптимізації транспортної інфраструктури.

Висновок.

Розробка прототипу системи «розумний паркінг», що визначає зайнятість паркомісць за допомогою датчиків руху та передає дані через Wi-Fi або LoRaWAN має вагоме значення. Актуальність теми пов’язана з необхідністю оптимізації паркувального простору та підвищення ефективності міської інфраструктури.

Проаналізовано технології IoT, сенсори та можливості бездротових мереж. Запропоновано архітектуру, що включає датчик, мікроконтролер, сервер та веб-інтерфейс для відображення статусу місць у реальному часі.

Література:

1. Розумні системи паркування: тенденції та можливості для українських міст [Електронний ресурс]. – Режим доступу: https://hub.kyivstar.ua/articles/rozumni-systemy-parkuvannya-tendencziyi-ta-mozhlyvosti-dlya-ukrayinskyh-mist.

2. Розумне місто [Електронний ресурс]. – Режим доступу: https://deps.ua/ua/knowegable-base/reference-information/67697.html

3. Adelantado, Ferran, et al. “Understanding the Limits of LoRaWAN.” IEEE Communications Magazine, vol. 55, no. 9, 2017, pp. 34–40, [Електронний ресурс]. – Режим доступу:https://arxiv.org/pdf/1607.08011.pdf, https://doi.org/10.1109/mcom.2017.1600613.

4. Park, Youngchoon, et al. Building an Effective IoT Ecosystem for Your Business. 1 Jan. 2017, [Електронний ресурс]. – Режим доступу: https://link.springer.com/book/10.1007/978-3-319-57391-5.

5. “Semi-Industrial LoRaWAN® Gateway.” Milesight, [Електронний ресурс].– Режим доступу: https://www.milesight.com/iot/product/lorawangateway/ug65 .

6. “Hikvision ANPR System | Twin Way.” The Electric Gate Shop, [Електронний ресурс].– Режим доступу: https://www.theelectricgateshop.co.uk/5268- Hikvision-ANPR-System-Twin-Way.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

УДК 372.862:004
DOI: https://doi.org/10.32837/11300.31395

Горбачов В. Е., к.т.н., доцент
Бєльдюгіна С. С., здобувач 2 курсу магістратури
Міжнародний університет
physmgu@gmail.com

АДАПТИВНЕ НАВЧАННЯ В ОНЛАЙН КУРСІ ІНФОРМАТИКИ ТА ПРОГРАМУВАННЯ

Анотація. *У статті досліджено особливості впровадження методики адаптивного навчання в шкільний онлайн-курс інформатики. Розкрито теоретичні засади адаптивного підходу та його значення для формування індивідуальної освітньої траєкторії учня. Запропоновано структуру курсу з вивчення інформатики та програмування, що передбачає можливість вибору учнем рівня складності навчального матеріалу та індивідуальних завдань відповідно до його навчальних цілей, інтересів і пізнавальних можливостей. Така організація навчального процесу сприяє розвитку самостійності, формуванню відповідального ставлення до навчання та підвищенню мотивації учнів до вивчення інформатики. Зазначено, що використання адаптивних механізмів у цифровому освітньому середовищі забезпечує ефективнішу диференціацію навчання, створює умови для персоналізованого підходу та підвищує результативність освітнього процесу.*

На сьогодні шкільний курс інформатики для 10-11 класів профільного навчання [1] містить дев’ять розділів, перевантажених навчальною інформацією, що негативно впливає на ефективність засвоєння матеріалу. У кожному класі існує значна різниця в рівні підготовки учнів: частина школярів уже має базові навички програмування, тоді як інші володіють лише елементарними користувацькими знаннями, обмеженими переглядом контенту в соціальних мережах.

Спрощення навчального матеріалу призводить до зниження інтересу серед більш підготовлених учнів, тоді як його ускладнення створює труднощі для менш підготовлених. Тому сучасна методика навчання інформатики потребує інноваційних підходів, які б, з одного боку, полегшували сприйняття складних понять, а з іншого – зберігали мотивацію та зацікавленість учнів із вищим рівнем підготовки.

Метою даної роботи є обґрунтування доцільності використання методики адаптивного навчання при викладанні інформатики та програмування в старших класах. Такий підхід забезпечує кращу диференціацію навчального процесу й сприяє глибшому розумінню матеріалу учнями з різними рівнями базових знань.

У педагогічній практиці вже існує низка методів, спрямованих на підвищення доступності складного навчального матеріалу: алгоритмізація, візуалізація, скрайбінг, гейміфікація, метод проектів, використання технологій віртуалізації та елементів штучного інтелекту тощо. Проте серед них адаптивний метод навчання є одним із найефективніших, хоча й найбільш ресурсозатратних.

Основний принцип адаптивного навчання полягає у створенні такої структури освітнього курсу, за якої учень має можливість самостійно обирати траєкторію навчання відповідно до власних цілей, здібностей і темпу засвоєння знань.

Результати сучасних досліджень свідчать [2, 3], що використання адаптивного підходу є найбільш результативним за умови його поєднання з іншими педагогічними методами, такими, як:

- метод алгоритмізації навчального матеріалу;

- метод чіткої мети;
- метод диференціації;
- метод планування подій;
- метод попереднього читання (підготовки).

Методи алгоритмізації та постановки чіткої мети забезпечують краще розуміння навчального матеріалу, сприяючи систематизації знань і концентрації уваги учнів на конкретних результатах.

Відповідно до типової навчальної програми з інформатики [3], курс було структуровано на дев'ять логічно завершених блоків:

1 Мова програмування та структури даних.
2 Сучасні інформаційні технології.
3 Аналіз і візуалізація даних.
4 Електронні публікації.
5 Комп'ютерна графіка та мультимедіа.
6 Бази даних.
7 Алгоритми.
8 Веб-технології.
9 Парадигми та технології програмування.

Метод чіткої мети полягає у донесенні до учнів конкретних навчальних завдань у межах кожного блоку. Чітке визначення цілей навіть складного рівня ефективніше, ніж загальні формулювання на кшталт «докласти всіх зусиль для вивчення теми».

Диференціація забезпечує можливість вибору рівня складності навчального матеріалу, що особливо важливо в умовах різнорівневої підготовки школярів. Однак розроблення системи рівнів потребує значних зусиль викладача, адже вимагає детальної структуризації змісту курсу.

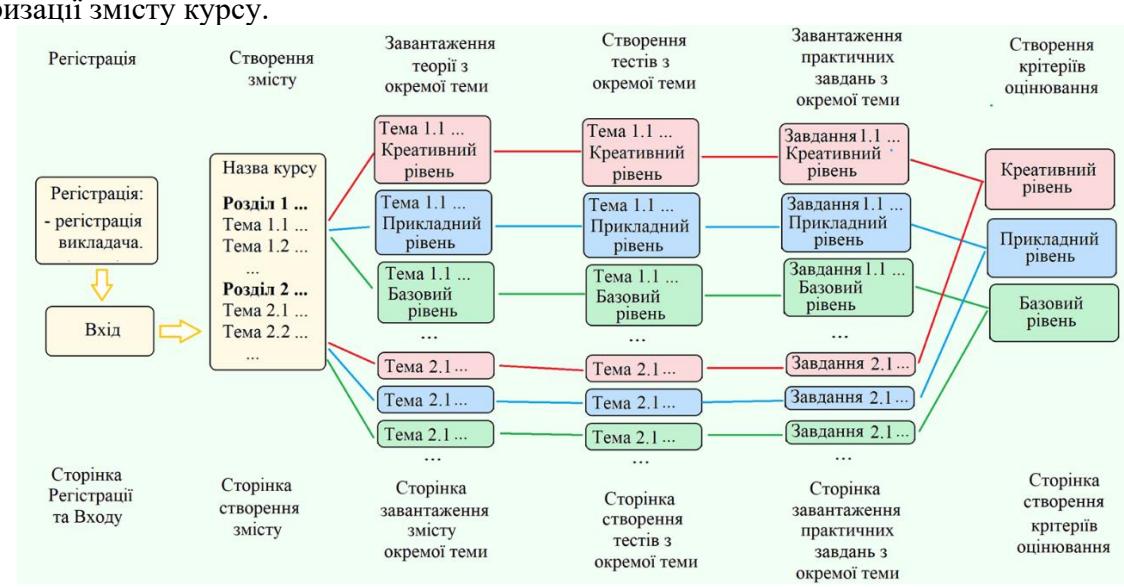


Рисунок 1 – Диференціальна структура «Адаптивний курс інформатики»

Метод планування подій сприяє розвитку самостійності, оскільки дозволяє учням орієнтуватися в освітньому процесі та планувати власну діяльність.

Метод попереднього читання (підготовки) передбачає ознайомлення учнів зі структурою курсу, його цілями, рівнями складності й особливостями виконання завдань до початку вивчення кожного блоку.

Наприклад, під час вивчення теми «Візуалізація даних. Вибір типу діаграми. Інфографіка» учням пропонується практичне завдання — візуалізація параметрів об'єктів за роками. Відповідно до рівня складності завдання може виконуватися як:

- базовий рівень – побудова простого графіка;
- прикладний рівень – створення гістограми;

- креативний рівень – розроблення власної інфографіки з використанням декількох типів діаграм.

Зовнішній вигляд прикладів виконаних практичних завдань для різних рівнів складності показано на рис. 2.

Рисунок 2 – Зовнішній вигляд прикладів виконаних практичних завдань для різних рівнів складності за темою «Візуалізація даних. Вибір типу діаграми. Інфографіка»

Освітня платформа «Адаптивний курс інформатики» створена як інструмент для реалізації принципів адаптивного навчання. Вона надає можливість учням обирати рівень складності (базовий, прикладний або креативний) відповідно до їхніх здібностей та навчальних потреб. При цьому базовий рівень дозволяє опанувати матеріал на мінімальний позитивний бал, а креативний — забезпечує найвищий результат та стимулює пізнавальну активність.

Платформа є корисною як для вчителів, що впроваджують інноваційні педагогічні технології, так і для учнів, які потребують індивідуальної траєкторії навчання або мають прогалини в знаннях.

Висновок. На базі шкільного курсу інформатики сформовано таку структуру онлайн освітньої платформи «Адаптивний курс інформатики» при якій учень у процесі навчання повинен обрати один з трьох рівнів складності послідовності блоків знань та навчальних завдань, що відповідає його можливостям та здібностям

Література:

1. Інформатика. Навчальна програма для 10-11 класів (профільне навчання). Офіційний сайт Міністерства освіти і науки України. Режим доступу: https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/osvitni-programi/navchalni-programi-dlya-10-11-klasiv.

2. Сікора Я. Б. Віртуальна реальність як інструмент адаптивного навчання в цифровому освітньому середовищі / О. І. Яценко, М. Г. Погребняк // Академічні візії. – 2024. – № 28. – С. 1-12. DOI: https://doi.org/10.5281/zenodo.10725643.

3. Дем'яненко В. М. Модель адаптивної навчальної системи інформаційного простору відкритої освіти / В. М. Дем'яненко // Інформаційні технології та засоби навчання. – 2020. - Т. 77. – N. 3. – С. 27-38. DOI: 10.33407/itlt.v77i3.3603.

4. Інформатика. Навчальна програма для 10-11 класів загальноосвітніх навчальних закладів. Офіційний сайт Міністерства освіти і науки України. Режим доступу: https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/osvitni-programi/navchalni-programi-dlya-10-11-klasiv.

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING (ATICE'2025)

Odesa, Ukraine, November 14, 2025

Conference Proceedings (winter forum)

ODESA 2025

ГЕЛЬВЕТИКА
ВИДАВНИЧИЙ ДІМ
WWW.HELVETICA.UA

Підписано до друку 03.10.2025 р. Формат 60x84/16.
Папір офсетний. Гарнітура Gabriola. Цифровий друк.
Ум. друк. арк. 6,28. Наклад 100. Замовлення № 1025-207
Віддруковано з готового оригінал-макета.

Видавництво: Видавничий дім «Гельветика» 65101,
Україна, м. Одеса, вул. Інглезі, 6/1
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 6424 від 04.10.2018 р.

Надруковано: Друкарня «Айс Принт»
Тел: +38 (063) 231-92-82, +38 (099) 192-00-33
Site: ice-print.com.ua
E-mail:info@ice-print.com.ua