МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Одеса
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Odesa
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

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

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Одеса
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Одеса : Міжнародний гуманітарний університет, 2025, 123 с.

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

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

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний 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 гуманітарний 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 гуманітарний університет, м.Одеса, Україна.

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

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.
СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний 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 гуманітарний університет, Одеса, Україна.
МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний 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 гуманітарний 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 гуманітарний університет, Одеса, Україна
ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ВІТАЛЬНЕ СЛОВО ПРЕЗИДЕНТА МІЖНАРОДНОГО ГУМАНІТАРНОГО 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 гуманітарному 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 гуманітарного університету, академік, доктор юридичних наук, професор, заслужений юрист України, Почесний громадянин міста Одеса

ВІТАЛЬНЕ СЛОВО РЕКТОРА МІЖНАРОДНОГО ГУМАНІТАРНОГО УНІВЕРСИТЕТУ КОСТЯНТИНА ВІКТОРОВИЧА ГРОМОВЕНКА

Шановні учасники Міжнародної науково-практичної конференції «Передові технології в інформаційно-комунікаційній інженерії»! Від імені усього колективу Міжнародного гуманітарного 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 гуманітарного університету, доктор юридичних наук, професор, заслужений юрист України

ЗМІСТ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Стрелковська І.В., Золотухін Р.В., Стрелковська Ю.О. ПРОГРАМНА РЕАЛІЗАЦІЯ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ТРАФІКУ СТАНДАРТІВ STANAG 4677 ТА ADATP-36 11

Суліма С.В., Савченко М.С. АДАПТАЦІЯ ВЕБ-ІНТЕРФЕЙСУ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ: АВТОМАТИЗОВАНИЙ ПІДХІД ДО ПОЛІПШЕННЯ ДОСТУПНОСТІ 16

Khniunin S.H., Shvedu M.I., Kolesnichenko I.O. APPLICATION OF IT-METHODS IN MARITIME INDUSTRY TASKS 20

Дорошук А.О. ВИМІРЮВАННЯ СПРИЙМАЄМОЇ ВІДСТАНІ МІЖ КОЛЬОРАМИ ІНТЕРФЕЙСУ 24

Ситніков А.С. УНІВЕРСАЛЬНІ ПІДХОДИ ДО ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ 28

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

Стрелковська І.В., Соловська І.М., Стрелковська Ю.О., Костенко М.О. ДЕТЕКТУВАННЯ ТРАФІКУ DDoS-АТАКИ НА ВЕБ-СЕРВЕРИ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ 31

Стрелковська І.В., Соловська І.М., Стрелковська Ю.О., Кольцов В.В. СПЛАЙН-АПРОКСИМАЦІЯ В ЗАДАЧАХ ВІЗУАЛІЗАЦІЇ ТА РЕНДЕРИНГУ 3D-ОБ'ЄКТІВ 35

Соловська І.М., Рудих А.П. АНАЛІЗ ВПЛИВУ FRONT-END-ФРЕЙМВОРКІВ НА ПРОДУКТИВНІСТЬ ТА ОПТИМІЗАЦІЮ ВЕБ-САЙТІВ 39

Русу О.П., Пшеничний О.С. СИСТЕМА КОМП'ЮТЕРНОГО ЗОРУ З ГОЛОСОВИМ КЕРУВАННЯМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ 43

Русу О.П., Лорткіпанідзе Р.Р., Черкас Н.С. ВЕБЗАСТОСУНОК MCLAB ДЛЯ НАВЧАННЯ ПРОГРАМУВАННЯ МІКРОКОНТРОЛЕРІВ 45

Проценко М.М. БЕЗПЕРЕРВНА ЕВОЛЮЦІЯ АРХІТЕКТУРИ ЧЕРЕЗ АВТОНОМНІ МУЛЬТИАГЕНТНІ RAG-СИСТЕМИ 49

Григор'єва Т.І., Крохмаль М.В. ЗАСТОСУВАННЯ ТЕНЗОРНОГО АНАЛІЗУ В ПРОГРАМНІЙ ІНЖЕНЕРІЇ 52

Русу О.П., Панков І.О., Черкас Н. С., Лазарєв К.О. ГОНОЧНИЙ РОБОТИЗОВАНИЙ БОЛІД «LINE TRACE CAR» 54

Григор'єва Т.І., Салагор В.І. ПРОГНОСТИЧНИЙ МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ ТА ЗБОЇВ У ПРОЦЕСІ ДІАГНОСТИЧНИХ ЕКСПЕРИМЕНТІВ ДЛЯ ВЕРИФІКАЦІЇ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ 57

Русу О.П., Крупецький К.А., Панков І.О. ВИКОРИСТАННЯ ЦИФРОВИХ КОНТУРІВ КЕРУВАННЯ В ІМПУЛЬСНИХ ПЕРЕТВОРЮВАЧАХ НАПРУГИ КОМП'ЮТЕРНОГО ОБЛАДНАННЯ 60

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Ковальчук Д.А. БЛОКЧЕЙН-ТЕХНОЛОГІЇ ТА ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА НЕЗМІННОСТІ ДАНИХ 64

Головатюк К.В. ФІШИНГ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ 67
Царенко Є.В. ВПЛИВ МІКРОСЕРВІСНОЇ ТА МОНОЛІТНОЇ АРХІТЕКТУРИ НА КІБЕРБЕЗПЕКУ СУЧАСНИХ ДОДАТКІВ.....69
Пахолюк О.І. ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ОПТИМІЗАЦІЇ ПРОЦЕДУР ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ 73
Димов М.В. РИЗИКИ ДЛЯ БЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ.....77
Khniunin S.H., Shvedu M.I. AN ANALYSIS OF ENTERPRISE OPERATIONAL STABILITY IN RELATION TO COMMUNICATION AND ENERGY SYSTEMS.....80
Єрьоменко А.Р. МЕТОДИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ 82
Петков Є.І. ТИПИ СПУФІНГ АТАК ТА ЗАСОБІВ ЗАХИСТУ В ЛОКАЛЬНИХ МЕРЕЖАХ 84

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

Пунченко Н.О. БШД ЯК НАДІЙНІСТЬ ПЕРЕДАЧІ ДАНИХ.....91
Уривський Л.О., Косогор А.В. ПОРІВНЯННЯ МОДЕЛЕЙ РОЗРАХУНКУ ЙМОВІРНОСТІ БІТОВОЇ ПОМИЛКИ ДЛЯ РІЗНИХ МОДУЛЯЦІЙ У КАНАЛІ ЗВ'ЯЗКУ ЗА УМОВ ЗМІННОЇ ЕНЕРГЕТИКИ 94
Уривський Л.О., Сколець А.В. МОДЕЛЮВАННЯ ПОКАЗНИКІВ QOS У СМО З УРАХУВАННЯМ САМОПОДІБНОГО ТРАФІКА: ПІДХІД НА ОСНОВІ РОЗПОДІЛУ ВЕЙБУЛЛА 99
Русу О.П., Гінжул В.М. ВИЗНАЧЕННЯ РОЗМІРІВ НАКОПИЧУВАЛЬНИХ ДРОСЕЛІВ ПЕРЕТВОРЮВАЧІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ 103

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

Горбачов В.Е., Хнюнін С.Г., Більдюгіна С.С., Горбачов П.В. АДАПТИВНЕ НАВЧАННЯ В КУРСІ ІНФОРМАТИКИ ТА ПРОГРАМУВАННЯ 106
Єрмакова С.С. ЦИФРОВІ ТРЕНДИ СУЧАСНОЇ ОСВІТИ.....109
Іванова О.С. ФІЛОСОФІЯ ОСВІТИ 4.0: ЦИФРОВІ ГОРИЗОНТИ СУЧАСНОЇ ОСВІТИ.....111
Єрмакова С.С., Биков А.В. ЦИФРОВА ОСВІТА: ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ 113
Іванова О.С., Кичка М.П. ІННОВАЦІЙНІ SMART-ТЕХНОЛОГІЇ В ПІДГОТОВЦІ ФАХІВЦІВ ЕКОНОМІЧНОГО ПРОФІЛЮ.....115
Єрмакова С.С., Шаповалов О.Ю. ФОРМУВАННЯ МОТИВАЦІЇ РОЗВИТКУ ЦИФРОВИХ НАВИЧОК У ЗДОБУВАЧІВ ОСВІТИ ЗА КРОС-КУЛЬТУРНОЮ МЕТОДИКОЮ.....118
Жигулін О.А. МЕТОДОЛОГІЯ ІНФОРМАЦІЙНОЇ ДУАЛЬНОСТІ, ТВОРЧОЇ РЕАБІЛІТАЦІЇ, ШТУЧНОГО ІНТЕЛЕКТУ, ДОПОВНЕНОЇ Й УЯВНОЇ РЕАЛЬНОСТІ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ НАВЧАННЯ ПІД ЧАС ВОЄННОГО СТАНУ 120

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАТИКА

УДК 621.391

Стрелковська І.В., *д.т.н., професор,*
декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний гуманітарний 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*
Вортінгський коледж, 1 Сандітон Вей, Вортінг, BN14 9FD, Велика Британія.

ПРОГРАМНА РЕАЛІЗАЦІЯ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ТРАФІКУ СТАНДАРТІВ STANAG 4677 ТА ADATP-36

Анотація. *В роботі пропонується програмна реалізація імітаційного моделювання трафіку стандартів STANAG 4677 та AdatP-36 щодо оцінки показників якості обслуговування трафіку цих стандартів. Представлено реалізацію генератора проміжків часу між вимогами та механізму буферизації пакетів трафіку ультракороткохвильових радіостанцій. Програмна реалізація імітаційного моделювання дозволяє розрахувати: середній інтервал між вимогами на обслуговування трафіку, 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.*

Автоматизовані системи управління (АСУ) з активним переміщенням користувачів низової ланки управління використовують протоколи стандартів STANAG 4677 та AdatP-36 як базовий механізм передачі інформації в низькошвидкісних мережах зв'язку [1-4]. На сьогоднішній день не існує математичних моделей або методів оцінки показників якості обслуговування трафіку цих стандартів, але створено узагальнену модель оцінки показників функціонування низькошвидкісних мереж зв`язку АСУ [2] та описано алгоритм роботи імітаційного моделювання радіомереж АСУ [1].

Метою роботи є програмна реалізація імітаційного моделювання трафіку стандартів STANAG 4677 та AdatP-36 щодо оцінки показників якості обслуговування трафіку цих стандартів.

Програмна модель трафіку стандартів STANAG 4677 та AdatP-36 в низькошвидкісних радіомережах АСУ відповідно до алгоритму роботи імітаційного моделювання трафіку протоколів JDSS та AdatP-36 в радіомережах АСУ [1, 2] передбачає реалізацію генератору інтервалів між вимогами та механізму буферизації пакетів трафіку. Реалізуємо генератор проміжків часу між вимогами на обслуговування для сервісу JDSS та AdatP-36 у вигляді структурного об'єкту програмування – класу, що дозволить створювати одразу декілька таких генераторів при імітаційному моделюванні. На рис. 1 показано лістинг програмного коду класу генератора.

Використання програмного коду, що показано на рис.1, дозволяє реалізувати генератор проміжків часу між вимогами за розподілом Вейбула з будь-якими параметрами k та λ. Такий підхід дозволяє використовувати цей генератор не тільки для імітації моделювання трафіку протоколів JDSS з AdatP 36, а й будь-який інший сервіс або протокол, в якому проміжки часу між вимогами на обслуговування підпорядковуються розподілу Вейбула [3]. В класі реалізовано три основні функції визначення:

- кількості пакетів за поточну секунду;
- кількості пакетів, що було створено цим генератором за весь час існування об’єкту;
- середнього часу надходження пакетів на обслуговування для цього генератора.

```
#include "weibullgenerator.h"

WeibullGenerator::WeibullGenerator(double k, double l) {
    kCoef = k;
    lCoef = l;
    weibullDist = new boost::random::weibull_distribution<>(kCoef, lCoef);
    timeCounter = 0.0;
    generatedPacketsCount = 0;
    timeSum = 0.0;
}

WeibullGenerator::~WeibullGenerator(){
    delete weibullDist;
}

int WeibullGenerator::getCountOfPacketsPerSecond(){
    int countOfPackets = 0;
    while(timeCounter < 1.0){
        double randomNumber = (*weibullDist)(rngDevice);
        timeSum+= randomNumber;
        generatedPacketsCount++;
        timeCounter+= randomNumber;
        countOfPackets++;
    }
    timeCounter-= 1.0;
    return countOfPackets;
}

int WeibullGenerator::getAllPacketsCount(){
    return generatedPacketsCount;
}

double WeibullGenerator::getAverageTimeBetweenPackets(){
    return timeSum/generatedPacketsCount;
}
```

Рисунок 1 – Лістинг програмного коду класу генератора проміжків часу між вимогами на обслуговування

Відповідно до робіт [1-4] та алгоритму роботи імітаційного моделювання трафіку протоколів JDSS та AdatP-36 в радіомереж АСУ [1] необхідно передбачити реалізацію механізму буферизації пакетів трафіку УКХ радіостанцій. Цей буфер повинен підтримувати можливість додавати та віддавати пакети трафіку з черги, перевіряти час знаходження пакетів в буфері та видаляти пакети, що приходять після переповнення максимального розміру цього буферу. На основі проведених досліджень в роботах [1, 4] бачимо, що буфер необхідно реалізовувати як чергу з алгоритмом заміщення FIFO (first in, first out). В якості елементу цієї черги пропонується розглянути структуру даних, елементами якої є розмір пакету даних та час знаходження в буфері. Час знаходженні в буфері буде дорівнювати нулю при додаванні цього пакету до буферу. На рис. 2 показано лістинг програмного коду класу буфера.

Використання програмного коду, що показано на рис.2, дозволяє реалізовувати механізм буферизації в УКХ радіостанціях з довільним розміром буферу та максимальним часом знаходження в черзі. Клас передбачає збереження будь-яких пакетів, що дозволяє використовувати цей буфер не тільки для трафіку протоколів JDSS з AdatP 36, а й будь-яких інших сервісів або протоколів. Щоб отримати показники функціонування буферу радіостанції в класі реалізовано п’ять основних функцій:

- додавання пакету в кінець черги буфера, якщо ж буфер переповнений, то функція повідомляє, що пакет втрачено;
- функція, яка визначає розмір наступного пакету для обслуговування;

- функція оновлення часу знаходження пакетів у буфері;
- функція визначення максимального часу знаходження пакетів в буфері;
- визначення кількості пакетів в буфері.

```
#include "buffer.h"

RadioBuffer::RadioBuffer(int timeoutBuffering, int maxBufferInBytes) {
    _timeoutBuffering = timeoutBuffering;
    _maxBufferSizeInBytes = maxBufferInBytes;
}

bool RadioBuffer::addPacketToBuffer(int packetSize){
    packetInBuffer tmp;
    tmp.bytesInBuffer = packetSize;
    tmp.timeInBuffer = 0;

    int currentBufferSize = 0;
    for(int i = 0; i <_buffer.size(); i++){
        currentBufferSize+=_buffer[i].bytesInBuffer;
    }
    if(currentBufferSize <= _maxBufferSizeInBytes){
        _buffer.push_back(tmp);
        return true;
    }else{
        return false;
    }
}

int RadioBuffer::getPacketFromBuffer(){
    if(_buffer.size() > 0){
        int packetSizeInFront = _buffer[0].bytesInBuffer;
        _buffer.pop_front();
        return packetSizeInFront;
    }else{
        return -1;
    }
}

void RadioBuffer::updateTimers(){
    for(int i = 0; i < _buffer.size(); i++){
        _buffer[i].timeInBuffer+=1;
    }
}

int RadioBuffer::checkTimeoutPackets(){
    int droppedPacket = 0;
    while(_buffer.size() > 0 && _buffer[0].timeInBuffer > _timeoutBuffering){
        droppedPacket++;
        _buffer.pop_front();
    }
    return droppedPacket;
}

int RadioBuffer::getBufferSize(){
    return _buffer.size();
}
```

Рисунок 2 – Лістинг програмного коду класу буферизаціїї пакетів для обслуговування

Для проведення імітаційного моделювання трафіку стандартів STANAG 4677 та AdatP-36 необхідно ввести наступні вхідні дані:

- максимальну полосу пропускання в радіоканалі (кбіт/с), яка залежить від режиму роботи та виробника УКХ радіостанції;
- ймовірність втрати даних в каналі у відсотках (%);
- максимальний розмір буферу (кБайт);
- максимальний час знаходження пакету в буфері (с);
- кількість сервісів JDSS та AdatP-36.

Після опрацювання вхідних даних та проведення моделювання програма розраховує наступні вихідні дані:

- середній інтервал між вимогами на обслуговування трафіку;
- загальну кількість згенерованих пакетів;
- середню полосу пропускання;
- кількість пакетів у буфері на теперішній час;
- кількість втрачених в радіоканалі пакетів;
- кількість втрачених пакетів через переповнення буферу;
- кількість втрачених пакетів через надмірне знаходження пакетів в буфері;
- відсоток втрачених пакетів.

Проведено моделювання використавши вхідні дані для режиму роботи Fixed Frequency УКХ радіостанції [1-3]:

- максимальна полоса пропускання в радіоканалі – 97 кбіт/с;
- ймовірність втрати даних в каналі – 2 %;
- максимальний розмір буферу – 50 кБайт;
- максимальний час знаходження пакету в буфері – 4с;
- кількість сервісів JDSS та AdatP-36 – 10.

Результати моделювання при генерації 100000 пакетів показано на рис. 3. Червона лінія на графіку – це максимальна полоса пропускання, яка задана користувачем, синій графік – це згенерований трафік для 10 сервісів STAMAG 4677 та AdatP-36, фіолетовий графік – це трафік, що передається по радіоканалу з урахування буферизації і максимальної полоси пропускання.

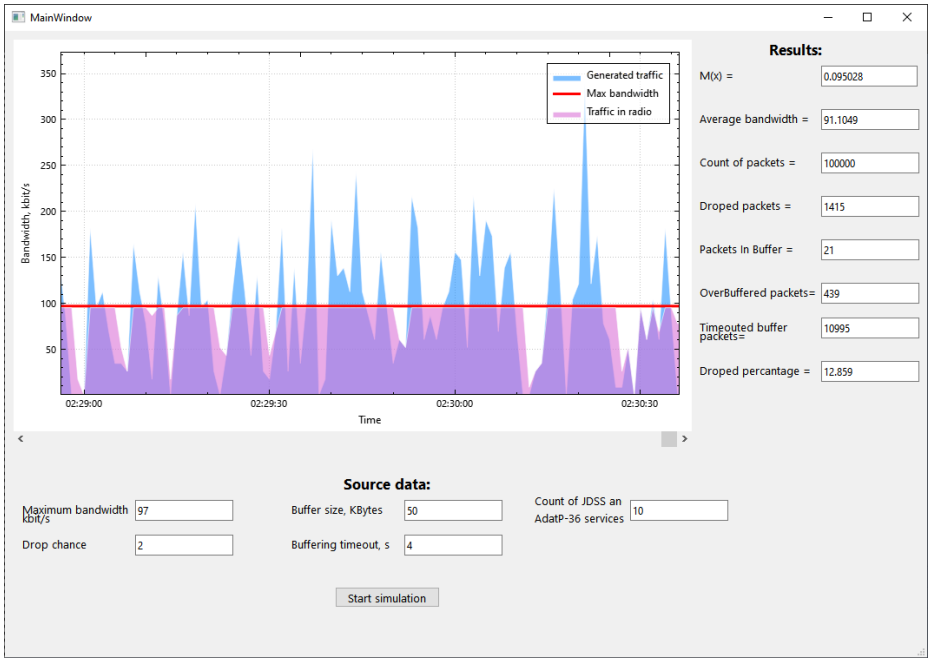


Рисунок 3 – Результати імітаційного моделювання

На основі проведеного імітаційного моделювання з використанням програмної моделі трафіку стандартів STANAG 4677 та AdatP-36 в низькошвидкісних радіомережах отримуємо наступні результати:

- середній інтервал між вимогами на обслуговування – 0,095 с;
- середня полоса пропускання згенерованого трафіку – 91,1 кбіт/с;
- кількість втрачених в радіоканалі пакетів – 1415;

- кількість втрачених пакетів через переповнення буферу – 439;
- кількість втрачених пакетів через надмірне знаходження пакетів в буфері – 10995;
- відсоток втрачених пакетів – 12,9 %.

Неважко бачити, що найбільшу частину втрачених пакетів (рис.3) припадає на надмірне знаходження пакетів в буфері. Це означає, що радіоканал був зайнятий, щоб передавати дані з буферу. Для мінімізації втрат для даного моделювання необхідно зменшити кількість сервісів JDSS та AdatP-36 або підвищити полосу пропускання. Для підвищення полоси пропускання можна використати широкополосний режим роботи радіостанції, що підвищить її полосу пропускання в декілька разів.

Висновки

1. Запропоновано реалізацію класу генератора проміжків часу між вимогами на обслуговування за розподілом Вейбула, який дозволяє імітувати довільну кількість сервісів JDSS та AdatP-36 та розраховувати кількість пакетів за поточну секунду, кількість пакетів, що було створено цим генератором за весь час існування об'єкту та середній час надходження пакетів на обслуговування для цього генератора.

2. Запропоновано реалізацію класу буферу як чергу з алгоритмом заміщення FIFO, який дозволяє додавати та виймати пакети з черги буфера, розраховувати поточну кількість пакетів в буфері, кількість втрачених пакетів, що знаходяться занадто довго в черзі або втрачені через заповнення буферу.

3. Проведено імітаційне моделювання 100000 пакетів трафіку з використанням програмної моделі трафіку стандартів STANAG 4677 та AdatP 36 при режимі роботи радіостанції FF з 10 сервісами JDSS та AdatP-36. Визначено, що загальний відсоток втрат складає 12,9% (12 859 пакетів). Найбільшу частину втрат складає втрачені пакети через надмірне знаходження пакетів в буфері – 10995. Для мінімізації втрат для даного моделювання необхідно зменшити кількість сервісів JDSS та AdatP-36 або підвищити полосу пропускання, змінивши режим роботи УКХ радіостанції.

Література

1. 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.

2. 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.

3. 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.

4. 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.

УДК 004.738.5:004.9-056.26

Суліма Світлана Валеріївна, к.т.н., доцент
Савченко Михайло Сергійович
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського» itssulima@gmail.com

АДАПТАЦІЯ ВЕБ-ІНТЕРФЕЙСУ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ: АВТОМАТИЗОВАНИЙ ПІДХІД ДО ПОЛІПШЕННЯ ДОСТУПНОСТІ

Анотація. *Запропоновано модульну бібліотеку JavaScript для автоматизованого покращення доступності веб-інтерфейсів у реальному часі. Система забезпечує адаптацію сайтів для користувачів з порушеннями зору, моторики та когнітивних функцій відповідно до стандартів WCAG 2.2. Проведено експериментальну перевірку, що підтвердила підвищення контрастності, ефективності навігації та видимості фокусу. Запропоновано рекомендації щодо інтеграції системи для створення інклюзивного цифрового середовища.*

Розробка та створення доступних веб-інтерфейсів мають вирішальне значення для забезпечення можливості ефективної навігації та використання онлайн-контенту особами з інвалідністю. Веб-доступність охоплює широкий спектр інвалідностей, включаючи порушення зору, слуху, моторики, когнітивних функцій та неврологічні порушення, і має на меті створення інклюзивного цифрового середовища для всіх користувачів[1]. Важливою основою для цих зусиль є Керівні принципи доступності веб-контенту (WCAG), які встановлюють стандарти для різних аспектів веб-дизайну, включаючи контрастність тексту, навігацію та синхронізацію медіа[2]. У міру розвитку технологій зростає необхідність дотримання цих стандартів доступності, що обумовлено як законодавчими вимогами, так і зростаючим визнанням важливості інклюзивності в цифрових просторах[3].

Проблема полягає не тільки в обізнаності, але й у складності впровадження функцій доступності в різних веб-інтерфейсах. Традиційні підходи часто вимагають значного ручного кодування, спеціалізованих знань та значного часу на розробку, що створює перешкоди для широкого впровадження. Крім того, існуючі рішення часто є фрагментарними і задовольняють лише конкретні потреби в доступності, а не забезпечують комплексну підтримку.

Серверні рішення, хоча і є комплексними, вимагають значних змін в інфраструктурі і можуть бути недоступними для всіх організацій. Клієнтські бібліотеки JavaScript пропонують більшу гнучкість, але часто не забезпечують повного покриття потреб доступності. Розширення браузера забезпечують керовані користувачем поліпшення доступності, але зазвичай працюють незалежно від особливостей дизайну веб-сайту.

Декілька бібліотек JavaScript вирішують конкретні проблеми доступності. Бібліотеки, такі як «ally.js», зосереджуються на управлінні фокусом, а «a11y-dialog» спеціалізується на доступних модальних діалогових вікнах. Однак ці рішення зазвичай вирішують окремі аспекти доступності, а не забезпечують всебічне покриття.

Дане дослідження вирішує ці проблеми шляхом розробки модульної бібліотеки JavaScript, яка забезпечує комплексні поліпшення доступності, зберігаючи при цьому простоту інтеграції та використання. Модульна конструкція бібліотеки дозволяє розробникам реалізовувати конкретні функції доступності за потреби, зменшуючи складність і забезпечуючи відповідність міжнародним стандартам.

Компоненти бібліотеки, які покращують зручність користування веб-сайтом для людей з різними видами інвалідності, є такими:

Компонент високої контрастності (highContrast.js) відповідає критеріям WCAG 2.2 1.4.3 (Мінімальний контраст), 1.4.6 (Покращений контраст) та 1.4.1 (Використання кольорів).

Він реалізує динамічне введення стилів для досягнення максимального контрасту між текстом та елементами фону. Реалізація передбачає динамічне введення CSS для стилів з високим контрастом, збереження оригінальних стилів для зворотної сумісності, підтримку складних макетів і вкладених елементів, застосування в режимі реального часу без оновлення сторінки. Компонент створює спеціальний елемент <style> з правилами CSS високого контрасту, які замінюють існуючі стилі, зберігаючи цілісність макета. Реалізація стратегічно використовує специфічність CSS і декларації !important, щоб забезпечити послідовне застосування в різних дизайнах веб-сайтів.

Компонент Focus Enhancement (focusMode.js) покращує візуальні індикатори фокусу, щоб відповідати критеріям WCAG 2.2 1.4.13 (Вміст при наведенні курсору або фокусі) та 2.4.7 (Видимий фокус). Він забезпечує чіткий візуальний зворотний зв'язок для навігації за допомогою клавіатури та покращує зручність використання для користувачів з порушеннями моторики. Особливості реалізації: покращені контури фокусу з настроюваними кольорами, ефекти тіні для покращення видимості, підтримка всіх елементів, на які можна навести фокус, динамічна обробка подій для станів наведення курсору та фокусу.

Компонент темного режиму (darkMode.js) відповідає критеріям WCAG 1.4.3, 1.4.11 (Контраст нетекстового вмісту) та забезпечує полегшення для користувачів із світлочутливістю або певними неврологічними захворюваннями. Особливості реалізації: інтелектуальні алгоритми інверсії кольорів, збереження зображень та медіа-вмісту, оптимізація для популярних платформ, вибіркове націлювання на елементи для збереження цілісності дизайну.

Компонент навігації за допомогою клавіатури (keyboardNav.js) покращує можливості навігації за допомогою клавіатури, виходячи за межі стандартних реалізацій браузерів, відповідаючи критеріям WCAG 2.1.1 (Клавіатура) та 2.1.2 (Відсутність клавіатурної пастки). Особливості реалізації: навігація за допомогою клавіш зі стрілками між елементами, на які можна навести фокус, просторова орієнтація для логічного потоку навігації, візуальний зворотний зв'язок для поточної позиції фокусу, пропуск навігації для складних макетів. Компонент реалізує новий алгоритм просторової навігації, який обчислює позиції елементів і визначає найбільш логічний шлях навігації на основі геометричних відносин, а не порядку DOM.

Компонент захисту від подвійного клацання (doubleClick.js) забезпечує захист від випадкових активацій, що особливо корисно для користувачів з порушеннями моторики або тремором. Він відповідає критеріям WCAG 3.3.2 (Мітки або інструкції) та 2.5.1 (Жести покажчиком). Особливості реалізації: налаштовувана затримка між клацаннями, обробка елементів для різних типів взаємодії, візуальний зворотний зв'язок під час періодів затримки, оголошення про доступність для екранних зчитувачів.

Компонент підтримки дислексії (dyslexiaMode.js) реалізує модифікації типографіки та інтервалів для поліпшення читабельності для користувачів з дислексією, відповідаючи критеріям WCAG 1.4.5 (Зображення тексту) та 3.1.5 (Рівень читання). Особливості реалізації: інтеграція шрифту OpenDyslexic, покращене інтервалювання між літерами та словами, покращена висота рядка та інтервалювання між абзацами, оголошення ARIA в режимі реального часу про зміни режиму.

Компонент масштабування тексту (increaseText.js) забезпечує динамічне регулювання розміру тексту з збереженням цілісності макета, відповідаючи критеріям WCAG 1.4.4 (Зміна розміру тексту) та 1.4.10 (Переформатування). Особливості реалізації: пропорційне масштабування всіх текстових елементів, збереження макета під час масштабування, можливість відновлення оригінального розміру, повідомлення про зміни для забезпечення доступності.

Система була протестована на репрезентативній вибірці веб-сайтів з різним рівнем складності. Критерії оцінки включали:

- Відповідність вимогам WCAG 2.2;
- Покращення зручності користування для користувачів із порушеннями зору,

моторики та когнітивних функцій;

- Продуктивність і стабільність системи.

Наприклад, для оцінки режиму фокусування та його відповідності заданій меті було розроблено невеликий скрипт (рис. 1), який перевіряє контрастність елементів. Скрипт дозволяє оцінити, наскільки помітним є фокус на інтерактивних елементах: коли ви наводите на нього курсор або фокусуєтеся на ньому (за допомогою клавіатури), він аналізує, як елемент виділяється — за допомогою контуру або тіні — і обчислює контраст між цими стилями та кольором фону. Результати відображаються в консолі і допомагають перевірити, чи відповідає фокус вимогам доступності.

Загальні результати такі.

Покращення контрасту:

- Базові коефіцієнти контрасту: 3.8:1 (нижче стандартів WCAG);
- Покращені коефіцієнти контрасту: 21:1 (перевищують стандарти AAA);
- Коефіцієнт покращення: збільшення в 5.5 разів.

Ефективність навігації:

- Стандартна навігація: 8 кроків для досягнення цільових елементів;
- Покращена навігація: 6 кроків для досягнення цільових елементів;
- Збільшення ефективності: зменшення необхідних дій на 25%.

Видимість фокусу:

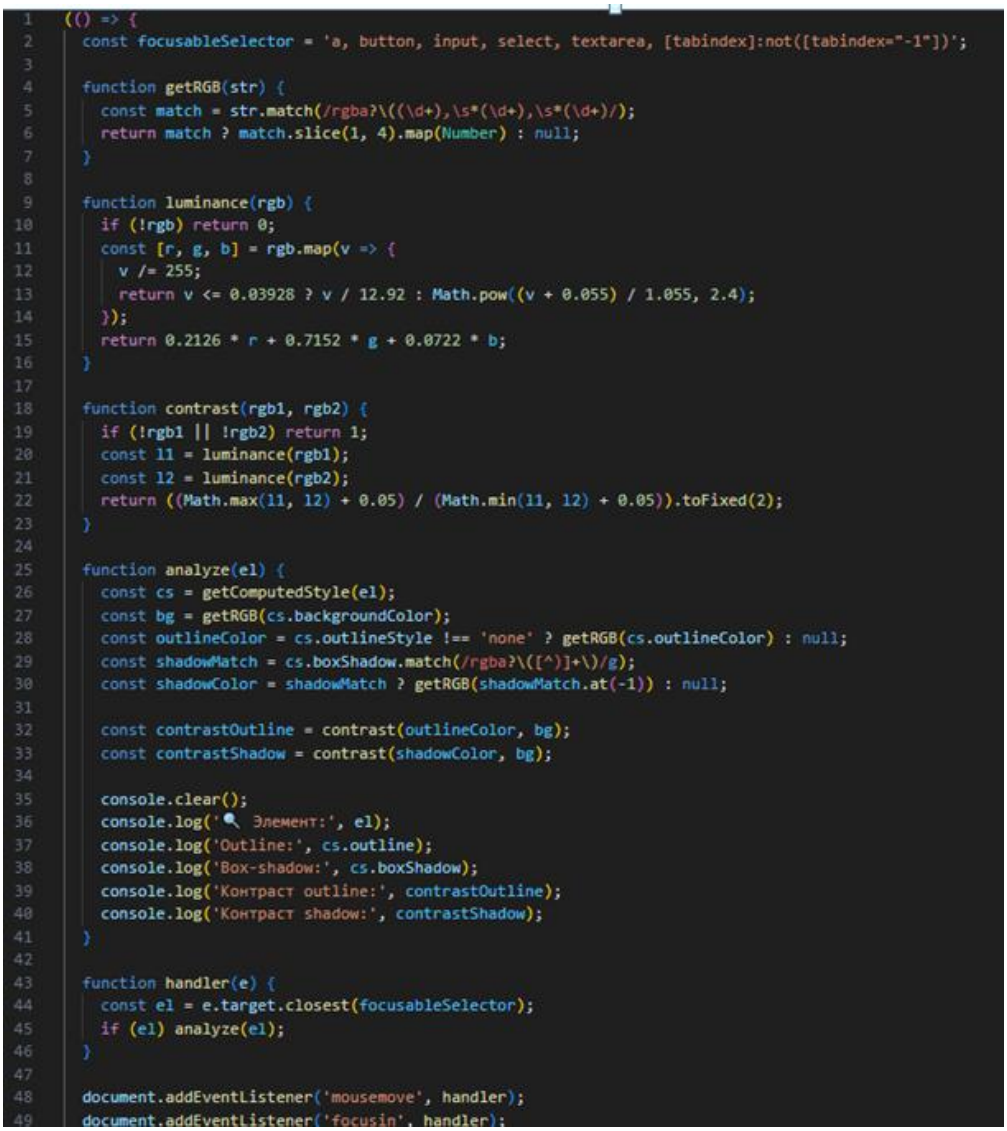
- Базова видимість фокусу: контраст 1:1 (невидимий);
- Покращена видимість фокусу: контраст 6.55:1;
- Відповідність: перевищує вимоги WCAG 2.2 (мінімум 3:1).

Оптимізація яскравості:

- Стандартна яскравість інтерфейсу: 84.0 люкс;
- Яскравість інтерфейсу в темному режимі: 30.0 люкс;
- Зменшення: зменшення яскравості екрана на 64%.

Покриття інтерактивних елементів:

- Елементи, покращені захистом від подвійного клацання: 93.1%;
- Підтримувані типи елементів: посилання, кнопки, прапорці, текстові блоки;
- Зменшення помилок: значне зменшення випадкових активацій.



```
(() => {
  const focusableSelector = 'a, button, input, select, textarea, [tabindex]:not([tabindex="-1"])';

  function getRGB(str) {
    const match = str.match(/rgba?\((\d+),\s*(\d+),\s*(\d+)/);
    return match ? match.slice(1, 4).map(Number) : null;
  }

  function luminance(rgb) {
    if (!rgb) return 0;
    const [r, g, b] = rgb.map(v => {
      v /= 255;
      return v <= 0.03928 ? v / 12.92 : Math.pow((v + 0.055) / 1.055, 2.4);
    });
    return 0.2126 * r + 0.7152 * g + 0.0722 * b;
  }

  function contrast(rgb1, rgb2) {
    if (!rgb1 || !rgb2) return 1;
    const l1 = luminance(rgb1);
    const l2 = luminance(rgb2);
    return ((Math.max(l1, l2) + 0.05) / (Math.min(l1, l2) + 0.05)).toFixed(2);
  }

  function analyze(el) {
    const cs = getComputedStyle(el);
    const bg = getRGB(cs.backgroundColor);
    const outlineColor = cs.outlineStyle !== 'none' ? getRGB(cs.outlineColor) : null;
    const shadowMatch = cs.boxShadow.match(/rgba?\([^)]+\)/g);
    const shadowColor = shadowMatch ? getRGB(shadowMatch.at(-1)) : null;

    const contrastOutline = contrast(outlineColor, bg);
    const contrastShadow = contrast(shadowColor, bg);

    console.clear();
    console.log('🔍 Элемент:', el);
    console.log('Outline:', cs.outline);
    console.log('Box-shadow:', cs.boxShadow);
    console.log('Контраст outline:', contrastOutline);
    console.log('Контраст shadow:', contrastShadow);
  }

  function handler(e) {
    const el = e.target.closest(focusableSelector);
    if (el) analyze(el);
  }

  document.addEventListener('mousemove', handler);
  document.addEventListener('focusin', handler);
```

Рис. 1. Код скрипта для оцінки режиму фокусування

Модульний підхід надає значні переваги як розробникам, так і кінцевим користувачам. Переваги для розробників включають: зменшення складності впровадження; вибіркове розгортання функцій; просте обслуговування та оновлення; чітка документація та приклади. Переваги для користувачів включають: негайне поліпшення доступності; персоналізований досвід доступності; відсутність погіршення продуктивності; безперебійна інтеграція з існуючими робочими процесами.

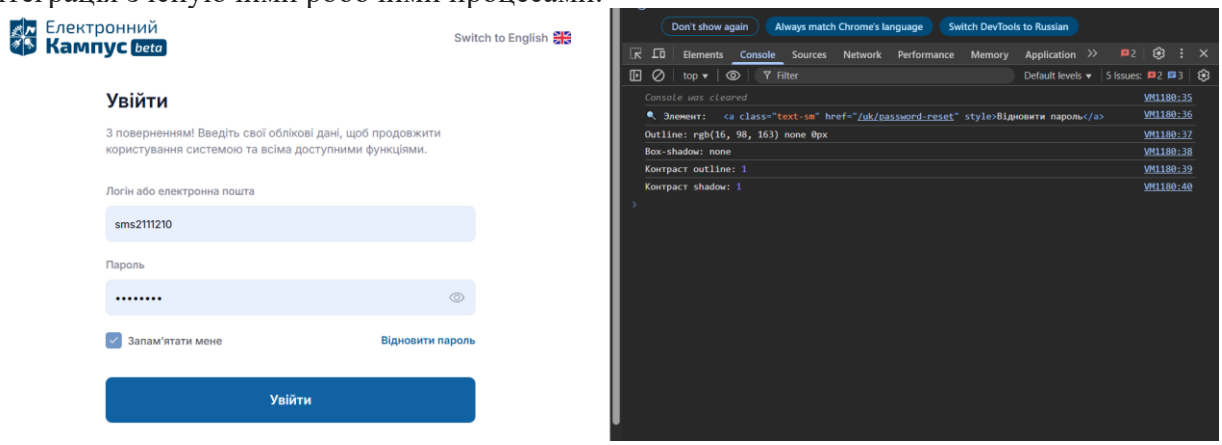


Рис. 2. Результат скрипту без увімкненого режиму фокусування

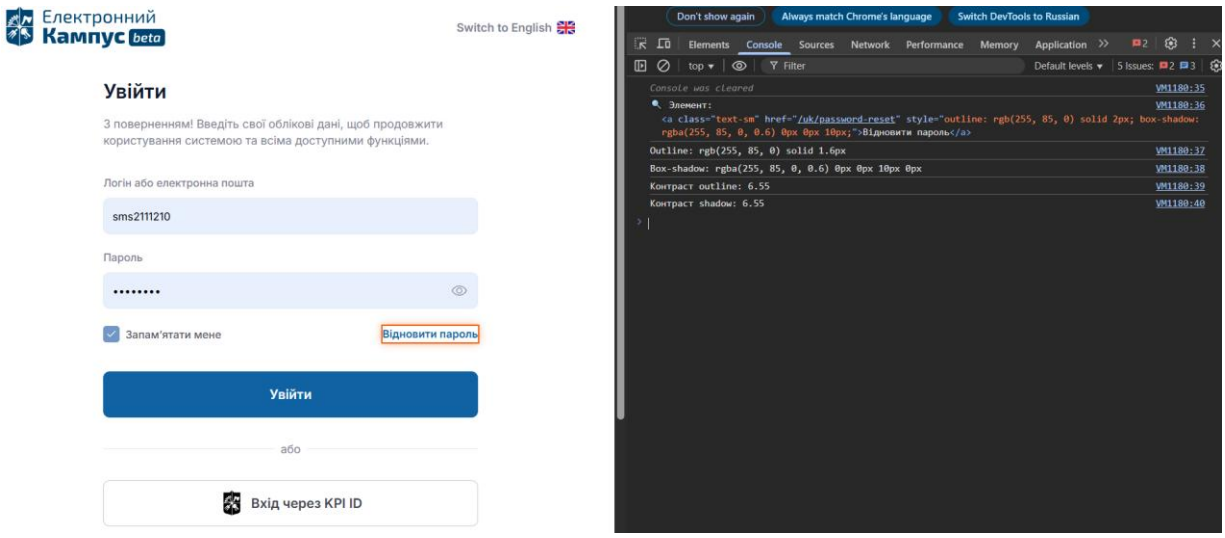


Рис. 3. Результат скрипту з увімкненим режимом фокусування

Висновки

У рамках цього дослідження було успішно розроблено та перевірено комплексну модульну бібліотеку JavaScript для покращення доступності веб-інтерфейсу. Бібліотека усуває критичні прогалини в існуючих рішеннях з доступності, надаючи уніфікований, простий в інтеграції підхід, який забезпечує відповідність стандартам WCAG 2.2, одночасно пропонуючи значну гнучкість та переваги в продуктивності.

Майбутня робота буде зосереджена на інтеграції аналізу поведінки на основі штучного інтелекту для більш глибокої персоналізації, розширенні підтримки мобільних платформ та покращенні можливостей адаптації для користувачів із складними, комбінованими інвалідностями.

Література

1. Emerging trends and technologies in web accessibility: navigating the future landscape [Електронний ресурс]. — Cheeky Monkey Media. — Режим доступу: https://www.cheekymonkeymedia.ca/blog/emerging-trends-and-technologies-in-web-accessibility-navigating-the-future-landscape/ — Дата звернення: 06.07.2025.

2. Adaptive Web Interfaces [Електронний ресурс]. — W3C. — Режим доступу: https://www.w3.org/WAI/RD/wiki/Adaptive_Web-Interfaces.html — Дата звернення: 06.07.2025.

3. Automated testing study identifies 57 percent of digital accessibility issues [Електронний ресурс]. — Deque. — Режим доступу: https://www.deque.com/blog/automated-testing-study-identifies-57-percent-of-digital-accessibility-issues/ — Дата звернення: 06.07.2025.

UDK 004.4:656.6

Khniunin S.H.
PhD in Technical Sciences, Associate Professor,
Department of Information Technologies,
International Humanitarian University,
Odessa, Ukraine
sergii.khniunin@gmail.com

Shvedu M.I.
2nd-year Master's student in F5 – “Cybersecurity and Information Protection”,
International Humanitarian University,
Odessa, Ukraine

blackangel2657@gmail.com

Kolesnichenko I.O.
2nd-year Master's student in F2 – “Software Engineering”,
International Humanitarian University,
Odessa, Ukraine
illy2003544@gmail.com

APPLICATION OF IT-METHODS IN MARITIME INDUSTRY TASKS

Abstract: *This paper analyses the steady growth of the maritime industry across sectors of the economy, transport, and logistics sectors, alongside the increasing use of software products tailored to this field. At present, graduates of maritime higher education institutions are predominantly trained to use existing IT-solutions. While they often possess strong operational skills, they frequently lack expertise in programming, algorithm design, and applied software engineering. It is proposed that the curriculum for the specialty F2 speciality in "Software Engineering" include dedicated modules addressing maritime-specific challenges. This integration would unlock new prospects for the advancement of both education and the maritime industry.*

Keywords: *software engineering, maritime industry, software development, maritime engineer training.*

The modern maritime industry is among the most rapidly developing sectors of the global economy, particularly in transport and logistics. The constant growth in maritime shipping volumes and increasing demands for safety and operational efficiency have driven the widespread adoption of advanced information technologies. Digitalisation has become a catalyst for transformations affecting both the technical infrastructure of maritime enterprises and approaches to specialist training [1].

Information technologies are now deeply embedded in all aspects of the maritime domain: shipping, port management, navigation systems, environmental monitoring, and marine construction. Particular importance is given to software solutions for computer-aided ship design (CAD systems), condition-based fleet maintenance systems, logistics chain monitoring platforms, satellite navigation services, and simulators used in crew training.

The software market is expanding rapidly, with dozens of new products emerging each year to meet the needs of the maritime sector. These tools not only automate routine operations but also provide innovative capabilities for analysis, forecasting, and decision-making.

Despite the rapid adoption of digital technologies, most maritime higher education institutions continue to focus on training students to use of existing IT-solutions. While graduates are typically proficient in using standard software tools, they often lack foundational knowledge of programming, algorithm design, and applied software development. This results in a gap between maritime engineering education and the demands of the modern digital landscape.

Meanwhile, maritime companies increasingly require specialists capable of adapting or even developing software solutions tailored to specific maritime challenges. Current educational offerings only partially meet this demand [2].

The F2 speciality in "Software Engineering" offers a promising bridge between IT and the maritime sector. Integrating maritime-specific content into the curriculum could help bridge this gap. The inclusion of dedicated modules focused on maritime industry tasks would foster interdisciplinary competence among students (see Figure 1).

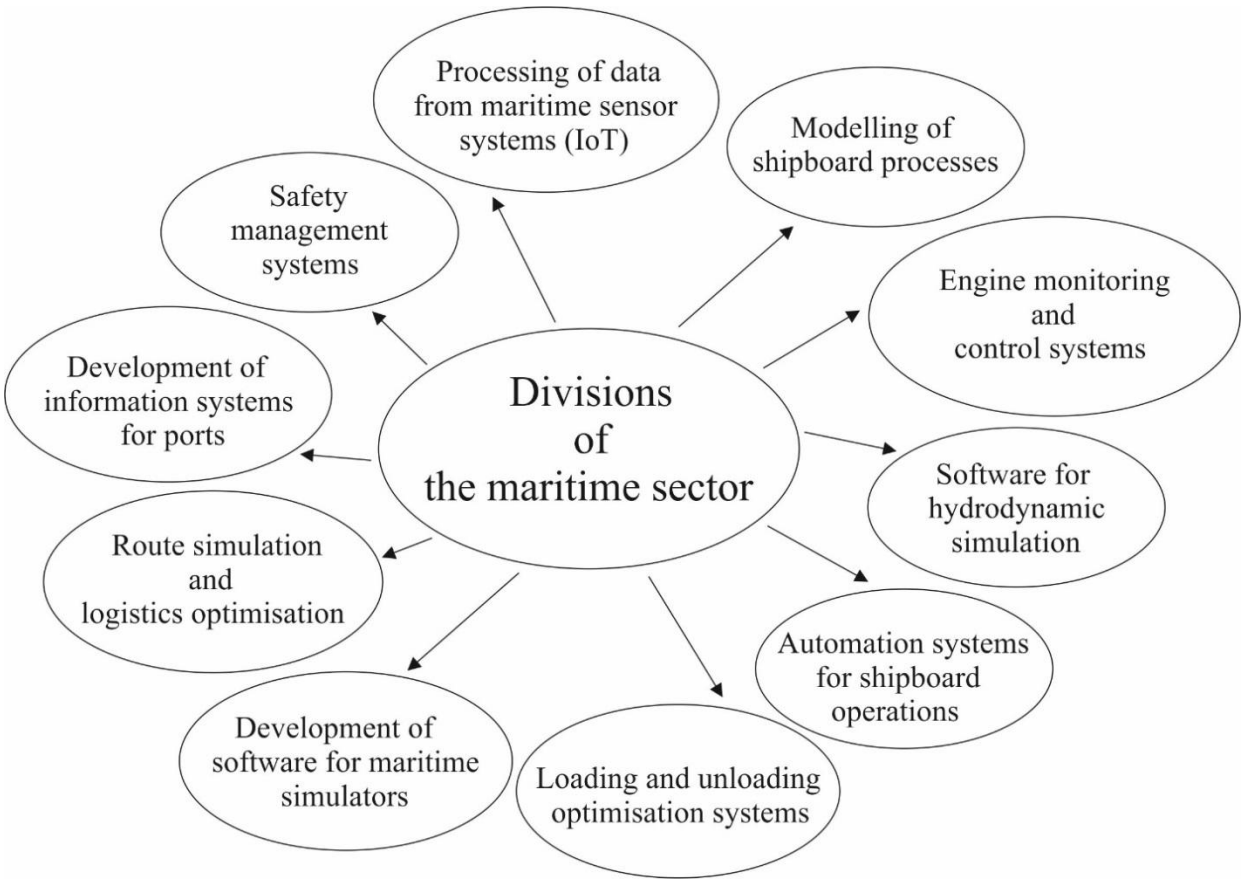


Figure 1 – Maritime Industry Modules for Integration into the F2 Software Engineering Curriculum

These modules may include:

- modelling of shipboard processes – creating digital simulations for analysing ship performance under various operational conditions, from navigation to energy consumption, enabling optimisation and increased operational efficiency;
- engine monitoring and control systems [3 – 5] – enabling real-time oversight of main and auxiliary engines, facilitating rapid response to anomalies, preventing failures, and reducing fuel consumption;
- hydrodynamic simulation software [6 – 12] – IT solutions used to compute water resistance, analyse flow around the hull, and optimise vessel shape to improve energy efficiency and seakeeping performance;
- shipboard process automation systems [13] – encompassing automatic control of engine rooms, ventilation, power supply, and pump systems, significantly reducing the need for manual intervention and enhancing reliability and safety;
- loading and unloading optimisation systems [14] – software for planning cargo operations, calculating vessel stability, even load distribution, and mooring duration, thereby improving port efficiency and reducing operational costs;
- development of maritime simulator software [15] – creating virtual environments to train crew in simulated emergency scenarios, improving preparedness without posing risks to real vessels or the environment;
- route simulation and logistics optimisation [16 – 18] – algorithms that model the most efficient routes considering weather, load, and economic factors, contributing to reduced delivery times and enhanced fleet competitiveness;
- port information systems development – platforms integrating data on vessel arrivals, cargo operations, maintenance, and resources, facilitating centralised management and operational transparency;

- safety management systems – including IT tools for threat detection, access control, personnel tracking, and emergency response coordination;

- processing of data from maritime sensor systems (IoT) involves gathering, analysing, and applying sensor data (e.g., temperature, pressure, motion, spills) to support informed decision-making and provide a comprehensive overview of vessel and environmental status.

Such an approach would position the F2 speciality in "Software Engineering" programme at the strategic intersection of IT and maritime engineering, shaping a new generation of versatile professionals well-versed in both digital and maritime technologies.

The maritime industry is undergoing a digital transformation that demands new strategies in professional training. Only synergy between traditional maritime education and contemporary IT disciplines can meet the challenges of today. Integrating IT-methods into the training of maritime engineers–particularly within the F2 speciality – opens promising pathways for the development of both the education system and the industry itself.

References:

1. ShipUniverse: Maritime Sector's Untapped Potential: Driving Global Economic Growth. URL: https://www.shipuniverse.com/news/maritime-sectors-untapped-potential-driving-global-economic-growth/ (date of access: 27.06.2025)

2. Батинський А.І., Хнюнін С.Г. Розробка моделі викладання загально технічних предметів з використанням сучасних інформаційних технологій // "Наука і освіта": Науково-практичний журнал Південного наукового Центру НАПН України. – 2010. – № 8/LXXXXV. Одеса. – С. 112 – 114.

3. Budashko V., Sandler A., Khniunin S. Improving the method of linear-quadratic control over a physical model of vessel with azimuthal thrusters // Eastern-European Journal of Enterprise Technologies. Energy-saving technologies and equipment. - 2023. - Vol. 1. - №. 2(121). - P. 49-71: DOI: 10.15587/1729-4061.2023.273934. [Scopus]

4. Sandler A., Budashko V., Khniunin S., Bogach V. Improving the mathematical model of a fiber-optic inclinometer for vibration diagnostics of elements in the propulsion system with sliding bearings// Eastern-European Journal of Enterprise Technologies. Applied physics. - 2023. - Vol. 5. - №. 5(125). - P. 24-31: DOI: 10.15587/1729-4061. 2023. 289773. [Scopus]

5. Budashko, V., Sandler, A., Khniunin, S., Bogach, V. Design of the pre-dictive management and control system for combined propulsion com-plex// Eastern-European Journal of Enterprise Technologies. Industry control systems. - 2024. - Vol. 5. - №. 2(131). - P. 90 - 102: DOI: 10.15587/1729-4061.2024.313627. [Scopus]

6. Хнюнін С.Г. Підвищення ефективності роботи азимутальної гвинторульової колонки на низьких швидкостях // "Морський та річковий флот: експлуатація і ремонт": міжнародна науково-технічна конференція 24.03.2022 – 25.03.2022. – Одеса: НУ «ОМА», 2022. – С. 56 – 60. http://www.onma.edu.ua/wp-content/uploads/2022/06/Tezysy-2022-1.pdf

7. Будашко В.В., Нікольський В.В., Хнюнін С.Г., Сандлер А.К. Використання примусової вентиляції подвійної дії в азимутальній гвинто-рульовій колонці на низьких швидкостях // «Суднова електроінженерія, електроніка і автоматика»: XII міжнародна науково-технічна конференція 22.11.2022 – 23.11.2022. – Одеса: НУ «ОМА», 2022. – С. 150 – 154. http://femire.onma.edu.ua/docs/conf/SEEEA-2022.22.11.22.pdf

8. Будашко В.В., Хнюнін С.Г. Підвищення експлуатаційних характеристик азимутальної гвинто-рульової колонки // XI Наукова конференція «Наукові підсумки 2022 року»: Збірка наукових праць 20.12.2022. – Харків, Х: Технологічний центр, 2022. – С. 42. https://entc.com.ua/download/Збірник тез_11_Наукової конференції_НАУКОВІ ПІДСУМКИ 2022 РОКУ_.pdf

9. Будашко В.В., Нікольський В.В., Онищенко О.А., Хнюнін С.Г. Компенсація деградаційних ефектів під час взаємодії азимутального потоку з корпусом судна // Матеріали науково-технічної конференції "Морський та річковий флот: експлуатація і ремонт". 24.03.2015 – 25.03.2015. Частина 2. – Одеса: ОНМА. – 2015. С. 207 – 209.

10. Nikolskyi V., Budashko V., Khniunin S. The monitoring system of the Coanda effect for the tension-leg platform's // The 12th International Conference on Engine Room Simulators: Proceeding. – Istanbul Technical University, Istanbul, 19 – 20 November, 2015. – P. 45 – 48.

11. Budashko V.V., Nikolskyi V.V., Onishchenko O.A., Khniunin S.H. Physical modelling effects degradation by interaction azimuthal flow with hull // The 12th International Conference on Engine Room Simulators: Proceeding. – Istanbul Technical University, Istanbul, 19 – 20 November, 2015. – P. 49 – 52.

12. Vitaliy Budashko, Vitaliy Nikolskyi, Oleg Onishchenko, Sergii Khniunin Decision support system's concept for design of combined propulsion complexes // Eastern-European Journal of Enterprise Technologies. – 2016. – 3/8 (81). – P. 10 – 21. [Scopus]

13. Журавльов Ю. І., Сандлер А. К., Карпілов О. Ю., Хнюнін С.Г. Вдосконалення засобу контролю повітряного середовища у машинному приміщені при роботі з вуглеводневими речовинами // Автоматизація суднових технічних засобів: наук.-техн. зб. – 2024. – Вип. 29. – Одеса: НУОМА. – С. 43 – 53. DOI: 10.31653/1819-3293-2024-1-29-43-53

14. Нікольський В.В., Хнюнін С.Г., Накул Ю.О. Рекомендації щодо використання системи завантаження контейнеровозу // «Суднові комп'ютерно-інтегровані технології»: міжнародна науково-технічна конференція 08.11.2018 – 09.11.2018. – Одеса: НУ «ОМА», 2018.

15. Gorb S.I., Nirolskyi V.V., Shapo V.F., Khniunin S.H. Programming controllers the integrated development environment: traning manual. Practice. – Odessa: National University "Odessa Maritime Academy", 2017. – 164 p.

16. Пакети прикладних програм в інформаційних технологіях: навчальний посібник / А.В. Камєнєва, С.Г. Хнюнін, К.І. Камєнєв. – Одеса: НУ «ОМА», 2021. – 284 с.

17. Камєнєва А.В., Хнюнін С.Г. Інформаційні технології в менеджменті: навчальний посібник. / А.В. Камєнєва, С.Г. Хнюнін – Одеса: НУ «ОМА», 2018. – 253 с.

18. Комп`ютеризоване управління проєктами [Текст]: методичні вказівки для виконання лабораторних робіт з дисципліни «Комп`ютеризоване управління проєктами» / С.Г. Хнюнін – Одеса: НУОМА, 2024. – 73 с.

УДК 004.92

Дорошук А. О.
Національний університет «Одеська політехніка»
9482084@stud.op.edu.ua

ВИМІРЮВАННЯ СПРИЙМАЄМОЇ ВІДСТАНІ МІЖ КОЛЬОРАМИ ІНТЕРФЕЙСУ

Анотація. *Запропоновано програмне забезпечення для вимірювання кольорів довільної області на екрані, що дозволяє визначати координати кольору в просторі CIELAB, в якому колір представлений світлосилою та двома хроматичними складовими, а також різницю між двома кольорами за допомогою формули CIEDE2000. Отримані результати дозволяють визначати сприймаєму різницю між кольорами та можливість розрізнити їх візуально.*

При створенні контенту, такого як дизайн веб-сторінок, анімація, інтерфейс програми важливим є вибір кольорів відповідно до вимог ергономіки [1-2]. Для цього необхідно точно визначати властивості кольорів, що застосовані. При поєднанні інтерфейсу з готовими зображеннями або іншими програмами актуальним є вирішення задачі вибору комфортного

для людини поєднання кольорів. Для вимірювання кольору певної області екрана застосовується відповідне програмне забезпечення, приклад якого продемонстровано в [3].

Основними функціями є власне вимірювання кольору і перегляд його координат, зміна розміру апертури, перегляд збільшеної області в межах апертури. Недоліком даних програм є неможливість виміряти одночасно два кольори та різницю між ними за допомогою стандартизованої метрики. Відповідно, було обрано відстань CIEDE2000 у якості метрики відстані між двома виміряними кольорами [4], яка визначена в стандарті з колориметрії створеним Міжнародною комісією з освітлення (CIE). Вона дозволяє виміряти відстань кольоророзрізнення, що корелює з відносною сприйманою різницею між кольорами, визначеною емпірично. В ході дослідів, проведених МакАдамом, знайдено 25 еліпсів [5], в межах яких людина не розрізняє кольори. Найбільш проблематичною зоною кольорової діаграми в задачі побудови еліпсів для довільного кольору є синя. Відповідно, для більш точної відповідності експериментальним даним еліпси в цій області необхідно обернути проти годинникової стрілки. Для коригування візуальної неоднорідності кольорового простору CIELAB призначені відповідні вагові функції. Коригуючі коефіцієнти дозволяють налаштувати умови середовища. Для визначення відстані CIEDE2000 [4] використовується формула (1):

$$\Delta E_{00}^{*} = \sqrt{\left(\frac{\Delta L'}{k_L S_L}\right)^2 + \left(\frac{\Delta C'}{k_C S_C}\right)^2 + \left(\frac{\Delta H'}{k_H S_H}\right)^2 + R_T \cdot \left(\frac{\Delta C'}{k_C S_C}\right) \cdot \left(\frac{\Delta H'}{k_H S_H}\right)} \quad (1)$$

де

$\Delta L'$ - різниця світлоти;

$\Delta C'$ - різниця цвітності;

$\Delta H'$ - різниця кольорового тону;

k_L, k_C, k_H - коригуючі коефіцієнти світлоти, цвітності та тону відповідно;

S_L, S_C, S_H - вагові функції світлоти, цвітності та кольорового тону відповідно;

R_T - функція повороту;

ΔE_{00}^{*} - відстань між кольорами.

Розглянемо більш детально еліпси, що визначені експериментальним шляхом та за допомогою розглянутої формули. На рис. 1 еліпси МакАдама позначено білим кольором, а еліпси, визначені за формулою CIEDE2000 (1) для тих самих кольорів позначені чорним.

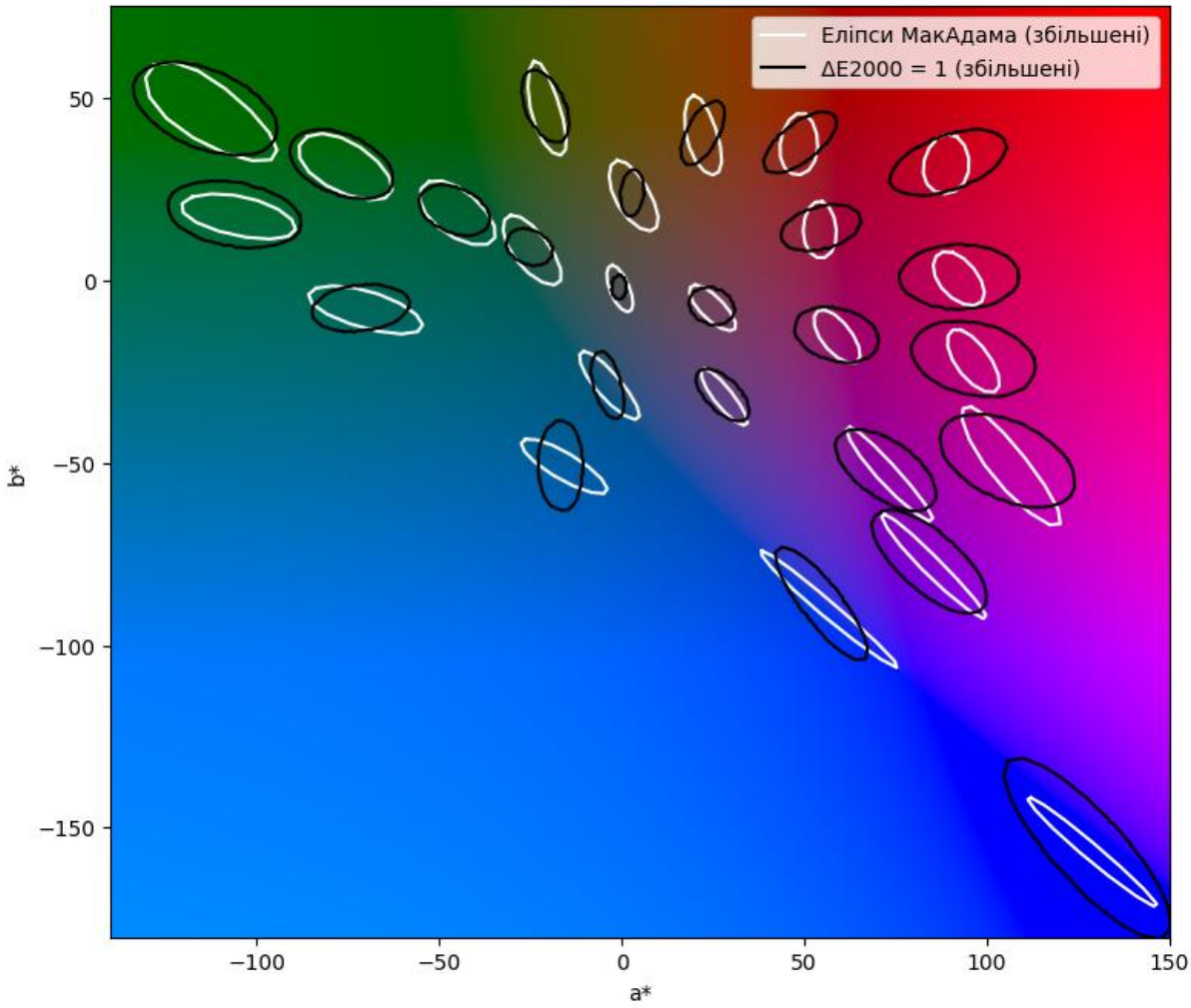


Рисунок 1 — Еліпси кольорозрізнення

Бачимо, що еліпси, що побудовані за формулою є наближеними до експериментальних даних.

Для визначення координат кольору в просторі CIELAB необхідно спочатку знайти координати в просторі CIEXYZ [5], помноживши вектор координат в просторі RGB на відповідну матрицю (2):

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.4124564 & 0.3575761 & 0.1804375 \\ 0.2126729 & 0.7151522 & 0.0721750 \\ 0.0193339 & 0.1191920 & 0.9503041 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (2)$$

Далі визначаємо власне координати в просторі CIELAB за наступною формулою (3):

$$\begin{aligned} L^* &= 116 f(Y/Y_n) - 16 \\ a^* &= 500 f\big((X/X_n) - f(Y/Y_n)\big) \\ b^* &= 200 f\big((Y/Y_n) - f(Z/Z_n)\big) \end{aligned} \quad (3)$$

, де L^*, a^*, b^* - координати кольору в просторі CIELAB, X_n, Y_n, Z_n - координати білої точки в просторі CIEXYZ.

Функція f описана наступним рівнянням (4):

$$f(x) = \begin{cases} x^{1/3} & \text{if } x > \left(\frac{6}{29}\right)^3 \\ \frac{841}{108}x + \frac{4}{29} & \text{otherwise} \end{cases} \quad (4)$$

Отримані координати кольору можуть бути застосовані для визначення відстані між двома кольорами. Формула (1) розроблена таким чином, що значення відстані 1 відповідає мінімальній помітній різниці між кольорами.

Для визначення координат кольорів та відстані між ними було створено програмний засіб, інтерфейс якого зображено на рис. 2.

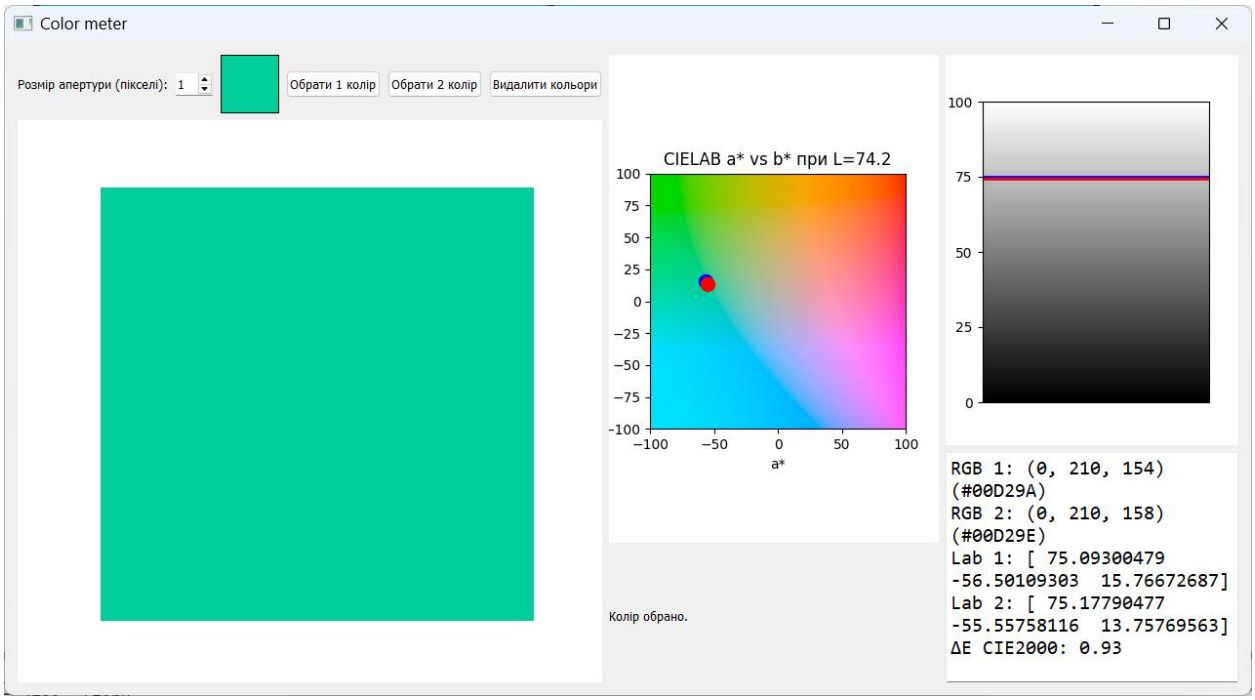


Рисунок 2 — Інтерфейс програми

Для розробки було використано мову програмування Python, бібліотеки tkinter та matplotlib. Було передбачено можливість зміну розміру апертури, в межах якої визначається усереднений колір області на екрані, візуалізацію координат кольору в просторі CIELAB. Координати кольору також надані в просторі RGB в десятковій та шістнадцятковій системах числення, які є найпоширенішими представленнями кольору при його визначенні для інтерфейсу веб-сторінок, пікселів зображення тощо. У якості прикладу визначили різницю між двома кольорами, результати наведено в табл. 1.

Таблиця 1 — Порівняння кольорів

№ кольору	R	G	B	L*	a*	b*	CIEDE2000
Колір 1	0	210	154	75.09	-56.5	15.77	0.93
Колір 2	0	210	158	75.18	-55.56	13.76	

Було визначено, що створене програмне забезпечення дозволяє визначати, чи є різниця між кольорами двох областей на екрані помітною для людини. В розглянутому прикладі відстань між кольорами є меншою, ніж поріг кольорозрізнення, тому вони сприймаються однаково.

Література

1. Kuo, L., Chang, T., & Lai, C. C. (2021). Visual effect and color matching of dynamic image webpage design. Color Research & Application, 46(6), 1321-1331.

2. Fernandez, S. V., Majid, M. A., Bakar, N. A. A., & Fakhreldin, M. (2021, August). Enhanced colour scheme assessment tool (COSAT 2.0) for improving webpage Colour selection. In 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM) (pp. 459-464). IEEE.

3. Microsoft PowerToys Color Picker [Electronic resource] // Microsoft Corporation. – [2024]. – Mode of access: https://learn.microsoft.com/en-us/windows/powertoys/color-picker

4. ISO/CIE 11664-6: 2022. Colorimetry-part 6: CIEDE2000 colour-difference formula. 2022.

5. Shamey, Renzo, ed. Encyclopedia of color science and technology. Cham: Springer International Publishing, 2023.

Ситніков А.С.
Магістр спеціальності 121 Інженерія програмного забезпечення
Міжнародний Гуманітарний Університет
м. Одеса, Україна

УНІВЕРСАЛЬНІ ПІДХОДИ ДО ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Анотація.*У тезах розглядаються сучасні універсальні підходи до інженерії програмного забезпечення, з акцентом на архітектурні рішення, автоматизацію розробки, інструменти CI/CD, інтеграцію безпеки (DevSecOps), а також практичне застосування в реальних проєктах: вебсайтах, телеграм-ботах, іграх та мобільних застосунках. Розкривається важливість побудови масштабованих, адаптивних та безпечних систем у рамках цифрової трансформації. Подано актуальні приклади, цитати та джерела.*

У сучасних умовах цифрова трансформація охоплює практично всі сфери діяльності — від державного управління та бізнесу до освіти, медицини та розваг. Це створює високий попит на ефективне, масштабоване та безпечне програмне забезпечення. Сьогодні інженерія ПЗ — це не просто процес написання коду, а комплексна дисципліна, що охоплює архітектурне планування, управління життєвим циклом програм, автоматизоване тестування, забезпечення якості, інтеграцію безпеки та взаємодію з користувачем. Як зазначено у [1], «інженерія ПЗ у XXI столітті вимагає синергії архітектурної дисципліни, гнучкості розробки та інтеграції кібербезпеки на всіх етапах життєвого циклу».

Вибір архітектури програмного забезпечення має фундаментальне значення. Залежно від складності проєкту, можуть застосовуватись монолітні підходи (актуальні для простих ботів чи MVP-рішень), компонентно-орієнтовані архітектури (для мобільних застосунків), або мікросервісні рішення, які найчастіше використовуються у великих вебплатформах із розподіленою логікою. Успішні проєкти — такі як інформаційні сайти, застосунки з API, телеграм-боти чи ігрові сервери — реалізують чітке розділення відповідальності між компонентами, що полегшує підтримку та масштабування.

Автоматизація розробки — ще один ключовий елемент. Інструменти CI/CD, такі як GitHub Actions, GitLab CI чи Jenkins, дозволяють реалізувати безперервну інтеграцію та доставку змін у коді. Це дає змогу зменшити час між написанням функціоналу та його запуском, а також запобігає помилкам у процесі розгортання. Docker забезпечує ізоляцію середовища, що особливо важливо під час тестування та роботи з кількома проєктами одночасно. Як зазначає Котляр С.Ю., «автоматизація розробки ПЗ є основою надійності та швидкості поставок цифрових продуктів» [2].

Безпека все частіше розглядається не як окрема фаза розробки, а як невід'ємна частина всього процесу. Модель DevSecOps передбачає інтеграцію безпекових практик у всі стадії CI/CD. Статичний аналіз коду, перевірка залежностей, використання токенів з обмеженим терміном дії, шифрування даних, обмеження прав доступу — усе це реалізується не тільки у великих компаніях, а й у проєктах середнього рівня. За словами Плахтія В.М., «DevSecOps дозволяє не просто реагувати на загрози, а попереджати їх завдяки структурованому безпековому підходу до кожного етапу життєвого циклу ПЗ» [3, с. 215].

Навіть у звичайному телеграм-боті або мобільному застосунку важливо впроваджувати захист API, авторизацію через OAuth2, хешування паролів, валідацію введених даних та шифрування конфіденційної інформації. Застосування шифрування особливо актуальне для систем, які зберігають або передають персональні дані. Наприклад, в ігрових сервісах необхідно захищати збереження прогресу, автентифікацію та з'єднання з сервером через TLS.

Практичне значення таких підходів очевидне. У типових проєктах студентів та молодих розробників — сайт з авторизацією, чат-бот з функціоналом розсилки, мобільний додаток для обліку завдань або навіть проста гра з онлайн-компонентом — всі ці приклади передбачають вирішення схожих інженерних задач: архітектурне проектування, робота з базами даних, безпечна передача даних, масштабованість, UX-дизайн, збір аналітики тощо. У таких проєктах активно використовуються фреймворки Django, Flask, Node.js, FastAPI, бібліотеки Pyrogram, Telebot, засоби візуалізації даних, хмарні сервіси на зразок Firebase та ін.

Інженерія ПЗ також включає командну взаємодію. Робота з Git, проведення code-review, написання технічної документації, участь у спринтах за методологією Scrum — усе це формує професійний підхід до створення якісного ПЗ. За словами українських викладачів технічних університетів, «розуміння інструментів командної роботи підвищує не лише продуктивність, але й якість кінцевого ПЗ» [1, с. 137].

Культура відповідального програмування передбачає не лише знання мов програмування чи фреймворків, а й розуміння важливості безпеки, підтримуваності коду, дотримання етичних принципів та захисту персональних даних. Особливої уваги заслуговують знання в області шифрування, зокрема застосування алгоритмів AES, RSA, а також підходів до безпечного зберігання інформації у клієнт-серверних додатках та іграх.

Таким чином, універсальні підходи до інженерії ПЗ дозволяють будувати рішення, які підходять для найрізноманітніших задач: від простих інформаційних сайтів до складних систем з інтеграцією API, від ботів для автоматизації до повноцінних мобільних додатків або клієнт-серверних ігор. Усе це підтверджує актуальність універсальної бази знань в рамках спеціальності 121 — інженерія програмного забезпечення.

Висновки.

Сучасна інженерія програмного забезпечення передбачає комплексний підхід до створення гнучких, безпечних та масштабованих рішень. Використання архітектурних шаблонів, впровадження CI/CD, інтеграція безпеки, автоматизація тестування та підтримка командної розробки є ключовими складовими якісного програмного продукту.

Універсальність підходів дозволяє адаптувати їх до проєктів будь-якого рівня складності, що робить такі знання особливо цінними у сучасних умовах цифрової трансформації.

Література

1. Коваленко В.В. Сучасні принципи інженерії програмного забезпечення: навч. посіб. — Київ: ІТГІП НАН України, 2020. — 228 с.

2. Котляр С.Ю. DevOps та автоматизація розробки ПЗ // Науковий вісник ХНУРЕ. — 2021. — №32. — С. 112–119.

3. Плахтій В.М., Іванченко О.О. Основи безпеки програмного забезпечення. — Одеса: ОНУ, 2019. — 312 с.

4. OWASP Foundation — https://owasp.org

5. GitLab CI/CD — https://docs.gitlab.com/ee/ci

6. Telegram Bot API — https://core.telegram.org/bots/api

7. Firebase Docs — https://firebase.google.com/docs

8. Unity Docs — https://docs.unity3d.com

9. JWT Introduction — https://jwt.io/introduction

10. Trello Docs — https://developer.atlassian.com/cloud/trello

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

УДК 004.738.5:004.8

Стрелковська І.В., д.т.н., професор,
Міжнародний гуманітарний університет,
i.strelkovskaya@mgu.edu.ua
Соловська І.М., к.т.н., доцент,
Міжнародний гуманітарний університет,
i.solovskaya@mgu.edu.ua,
Стрелковська Ю.О., к.ю.н., доцент
Worthing college
4800632s@gmail.com
Костенко М.О., магістр 2 року навчання,
Міжнародний гуманітарний університет,
kostenko.web.dev@gmail.com

ДЕТЕКТУВАННЯ ТРАФІКУ DDoS-АТАКИ НА ВЕБ-СЕРВЕРИ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Анотація: *Розглянуто задачу детектування трафіку DDoS-атак (HTTP GET-flood, HTTP POST-flood), які спрямовані на суттєве перевантаження Веб-серверів. Встановлено, що для детектування трафіку DDoS-атак прикладного рівня L7 доцільним є використанням машинного навчання. Запропоновано використання сплайн-апроксимації на базі кубічних сплайнів для детектування сегментів з аномальними сплесками та коливаннями трафіку, з подальшою класифікацією легітимного та шкідливого DDoS-трафіку за допомогою методу k-найближчих сусідів KNN. Розроблений підхід дозволяє детектувати DDoS-трафік та прийняти рішення щодо зміни стратегії керування мережним трафіком в реальному часі.*

Ключові слова: детектування, DDoS-атака, DDoS-трафік, HTTP GET-flood, HTTP POST-flood, сплайн-апроксимація, машинне навчання, легітимний трафік, шкідливий трафік, метод k-найближчих сусідів KNN

Важливим завданням забезпечення безпеки функціональності Веб-серверів від атак відмови в обслуговуванні DDoS (Distributed Denial of Service Attack) є детектування початку DDoS-атаки, пов'язане зі зростанням інтенсивності запитів, наприклад, HTTP GET-flood та HTTP POST-flood, значним перевантаженням та неможливостями доступу до Веб-серверів. Відомо [1-2], що процес детектування трафіку DDoS-атаки може бути виконаний за допомогою аналізу «сигнатур» або аномалій шкідливого трафіку, використовуючи «сигнатури» шкідливого трафіку або визначаючи аномалії трафіку, які виникають за рахунок різкого збільшення інтенсивності надходження запитів відмінне від визначених порогових значень характеристик легітимного трафіку. Удосконалення механізмів та збільшення масштабів DDoS-атак часто ускладнює вищезазначені завдання та потребує пошуку нових підходів до детектування DDoS-трафіку. Таким рішенням може бути використання підходу на базі сплайн-апроксимації з використанням кубічних сплайнів для детектування сегментів з аномальними сплесками та коливаннями трафіку, з подальшою класифікацією легітимного та шкідливого DDoS-трафіку за допомогою методу k-найближчих сусідів KNN.

Використання сплайн-апроксимації для вирішення завдань оцінки характеристик трафіку запропоновано авторами в роботах [1-2], а підхід щодо класифікації трафіку на основі алгоритмів машинного навчання розглянуто в роботах [3-5], де автори пропонують

виявлення аномалій DDoS-трафіку на основі різних методів, таких як, логістична регресія, метод опорних векторів та дерева рішень, метод k-найближчих сусідів KNN. Такий підхід до класифікації дозволяє з різним ступенем точності класифікувати легітимний та шкідливий трафік, адаптуватися до змін у мережному трафіку і виявляти DDoS-атаки у реальному часі. Робота [6] присвячена порівнянню результатів використання машинного навчання для визначення аномалій DDoS-трафіку, встановлено, що доцільним є використання машинного навчання у поєднанні з іншими підходами, такими як нечітка логіка, статистичний аналіз, генетичні алгоритми та інші.

В даній роботі запропоновано альтернативне до вищерозглянутих рішень, яке базується на використанні сплайн-апроксимації для детектування DDoS-трафіку та дозволяє на першому етапі визначити сегменти з аномальними сплесками та коливаннями трафіку, а на другому, за допомогою методу класифікації k-найближчих сусідів KNN виконати класифікацію легітимного та шкідливого DDoS-трафіку.

Метою даної роботи є детектування DDoS-трафіку на Веб-сервери з використанням сплайн-апроксимації на базі кубічних сплайнів та подальшої класифікації легітимного та шкідливого трафіку за допомогою методу k-найближчих сусідів KNN.

Розглянемо перший етап детектування DDoS-атаки на прикладі HTTP GET-flood та HTTP POST-flood запитів до Веб-сервера. DDoS-атака HTTP-Flood прикладного рівня L7 моделі OSI спрямована безпосередньо на Веб-сервери та сервери Веб-додатків, яка виконує переповнення Веб-серверу значною кількістю HTTP-запитів, що робить його нездатним обробляти легітимні запити користувачів. Виконаємо детектування шкідливого HTTP GET-flood трафіку за допомогою сплайн-апроксимації на базі кубічних сплайн-функцій, використовуючи [7], передбачаючи, що завданням детектування є виявлення аномалій та коливань трафіку. В якості вихідного легітимного та шкідливого Flood-трафіку використаємо DataSet трафіку HTTP GET-flood [8], що показано на рис. 1. Використаємо кубічний сплайн для HTTP GET-flood трафіку, показаного на рис. 1 на проміжку [1000;1500].

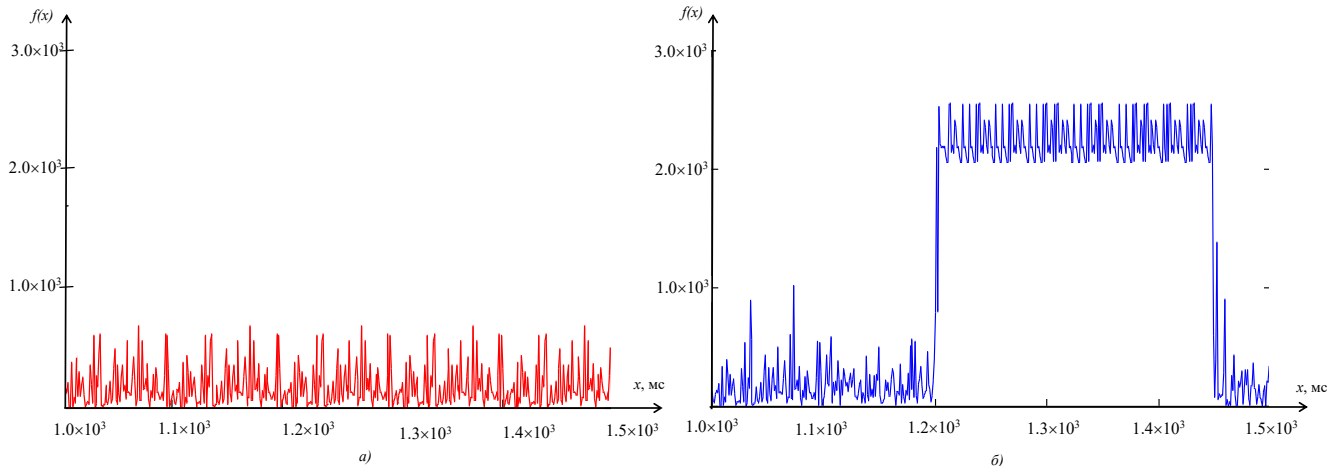


Рисунок 1 – Легітимний трафік (*а*) та шкідливий HTTP GET-flood трафік DDoS-атаки (*б*)

Нехай на відрізку [0;T] задані значення Flood-трафіку DDoS-атаки $f(x)$. 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 [9]

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

Згідно [9], інтерполяційний кубічний сплайн $S_3(f; x)$ відповідає умовам:

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

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:

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

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

Розглянемо трафік на проміжку [1000;1500] мс (рис. 1), задавши рівномірну сітку розбиття та крок детектування Δ = 10 мс. Легітимний трафік має вигляд рис. 1,*а*, трафік DDoS-атаки HTTP GET-flood показаний трасою рис. 1,*б*, на проміжку [1200;1210] мс відбувся різкий сплеск інтенсивності HTTP GET запитів, кількість яких є понад 2.5×10^3, при цьому така аномальність зберігається на проміжку часу [1200;1450] мс.

Для детектування використовуємо сплайн-апроксимацію на базі кубічних сплайн-функцій, яка дозволяє на першому етапі визначити аномалії інтенсивності надходження шкідливих HTTP GET-запитів у заданих вузлах інтерполяції. Легітимний трафік HTTP GET-запитів, показано на рис. 1,*а*, має рівномірну структуру та помірні сплески інтенсивності запитів, які становлять від 0.3×10^3 до 0.9×10^3. На першому етапі детектування, використовуючи кубічний сплайн вигляду (3) та умови (1-2), отримаємо сплайн-апроксимацію на базі кубічної сплайн-функції детектування трафіку HTTP GET-flood, фрагмент якої показано на рис. 2.

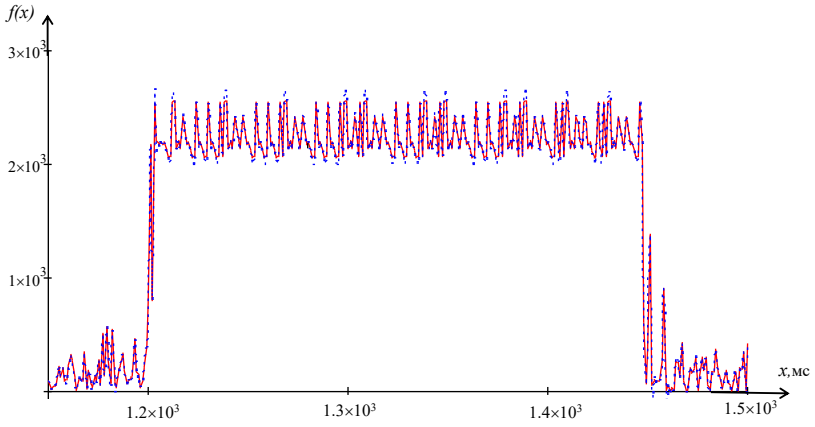


Рисунок 2 – Сплайн-апроксимація HTTP GET DDoS-трафіку на відрізку [1200;1500] мс

Другий етап детектування відбувається шляхом класифікації трафіку, як легітимного та шкідливого трафіку, за допомогою методу k-найближчих сусідів [10], який використовується для пошуку подібності між наявними значеннями легітимного та шкідливого DDoS-трафіку на базі метрики Евкліда, відстані $d_{\text{Euclidean}}$ між заданими значеннями легітимного та шкідливого трафіку:

$$d_{\text{Euclidean}} = \sqrt{\sum_{i=1}^{n}(x_{i,j} - y_{i,j})^2}, \tag{4}$$

де $x_{i,j}$ – поточне значення інтенсивності легітимного трафіку, $y_{i,j}$ – значення інтенсивності шкідливого трафіку HTTP GET-запитів, n – кількість вимірів.

Для класифікації використано програмне забезпечення машинного навчання Weka 3.8.6 [11] в якому проведено навчання, валідація та тестування методу k-найближчих сусідів для класифікації DDoS-трафіку. Отримані результати зведено в табл. 1.

Таблиця 1– Результати класифікації легітимного та шкідливого трафіку на основі методу k-найближчих сусідів

Метод	Коефіцієнт кореляції	Середня абсолютна похибка	Середньоквад-ратична помилка	Відносно-абсолютна похибка	Відносно-квадратична помилка кореня
k-найближчих сусідів	0,968	186,75	227,27	23,94 %	32,75 %

Для визначення точності результатів класифікації трафіку використаємо значення середньої абсолютної похибки MSE (Mean Squared Error) [10]:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\sqrt{(x_{est} - x_{real})^2 + (y_{est} - y_{real})^2}, \quad (5)$$

де x_{est}, y_{est} – значення інтенсивності шкідливого трафіку HTTP GET-запитів, визначені в ході експерименту; x_{real}, y_{real} – значення інтенсивностей легітимного трафіку, L – кількість значень.

Отримані результати розрахунку середньої абсолютної похибки MSE класифікації трафіку зведені в табл. 2.

Таблиця 2 – Визначення середньої абсолютної похибки MAPE класифікації трафіку

Значення середньої абсолютної похибки MSE	Legal traffic	HTTP GET
Класифікатор k-найближчих сусідів	43,2%	52,3%

Висновки

1. Розглянуто трафік DDoS-атаки на базі Flood-трафіку (HTTP GET-flood, HTTP POST-flood), який спрямовано на суттєве перевантаження Веб-ресурсів. Встановлено, що для детектування трафіку DDoS-атак доцільним є використання методів машинного навчання.

2. Запропоновано використання сплайн-апроксимації на базі кубічних сплайнів для детектування сегментів з аномальними сплесками та коливаннями трафіку з подальшою класифікацією легітимного та шкідливого DDoS-трафіку за допомогою методу k-найближчих сусідів KNN.

3. Розроблений підхід дозволяє детектувати DDoS-трафік та прийняти рішення щодо зміни стратегії керування мережним трафіком в реальному часі.

Література

1. Strelkovskaya I., Solovskaya I., Strelkovska J. Detection of cyberattack flood traffic using spline approximation. Scientific achievements of contemporary society. Proceedings of the 4th International scientific and practical conference. Cognum Publishing House. London, United Kingdom. 2024. pp. 21-27.

2. Strelkovskaya I., Kivalov S. «Detection and prediction of DDoS cyber attacks using spline functions», IEEE TCSET 2022: 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, February 22-26, 2022. – P. 710-713.

3. Ветлицька, О. С., Треньова, К. О. (2024). Виявлення атак у мережах Інтернету речей методами машинного навчання. Сучасний захист інформації, 1(57), 39–49.

4. P.D. Bojovi, I. Basicevi, S. Ocovaj, M. Popovic (2019) A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. Computers & Electrical Engineering 73 (2019): 84-96.

5. Imran, Jamil F., Kim D. An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments. Sustainability. – 2021. – Vol. 13, no. 10057.

6. Петляк Н. Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». – 2025. – Вип. 1, С. 180-186.

7. Strelkovskaya I., Solovskaya I., Strelkovska J. Spline-Approximпation and Spline-Extrapolation Methods in Telecommunication Problems, Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems. Vol. 212, Springer, Cham, 2021, P. 3-22.

8. https://www.kaggle.com

9. Ahlberg J.H., Nilson E.N., Walsh J.L. The Theory of Splines and Their Applications, Academic Press, New York, 1967.

10. Strelkovskaya I., Solovskaya I., Strelkovskaya J., Paskalenko V. Complex spline approximation in positioning problems. Radioelectronics and Communications Systems. 2022. Vol. 65 (7). P. 376–385.

11. https://ml.cms.waikato.ac.nz/weka/

УДК 004.942

Стрелковська І.В., д.т.н., професор,
Міжнародний гуманітарний університет,
i.strelkovskaya@mgu.edu.ua
Соловська І.М., к.т.н., доцент,
Міжнародний гуманітарний університет,
i.solovskaya@mgu.edu.ua,
Стрелковська Ю.О., к.ю.н., доцент
Worthing college
4800632s@gmail.com
Кольцов В.В., магістр 2 року навчання,
Міжнародний гуманітарний університет,
vladkoltsov@ukr.net

СПЛАЙН-АПРОКСИМАЦІЯ В ЗАДАЧАХ ВІЗУАЛІЗАЦІЇ ТА РЕНДЕРИНГУ 3D-ОБ'ЄКТІВ

Анотація: *Розглянуто задачу підвищення точності візуалізації та рендерингу 3D-об'єктів за допомогою сплайн-апроксимації. Запропоновано використання інтерполяційного параметричного сплайну в процесі моделювання кривих та поверхонь 3D-об'єкту у процедурі візуалізації та рендерингу. Встановлено, що застосування інтерполяційного параметричного кубічного сплайну забезпечує зниження обчислювальної складності, масштабованість рішень і суттєво спрощує процес моделювання.*

Ключові слова: сплайн-апроксимація, 3D-моделювання, 3D-модель, візуалізація, рендеринг, інтерполяційний параметричний сплайн, точність, похибка

Стрімкий розвиток технологій та методів 3D-моделювання зумовлено зростанням попиту на створення інтерактивних, гнучких у редагуванні 3D-об'єктів, структур та середовищ. 3D-моделі забезпечують високий рівень точності та деталізації, що дає змогу візуалізувати об’єкти у різних конфігураціях, з урахуванням їхніх функціональних і конструктивних особливостей. Особливу актуальність 3D-моделювання набуває у поєднанні з технологіями доповненої AR (Augmented Reality) та віртуальної VR (Virtual Reality) реальностей, які забезпечують ефект повного занурення. Завдяки цьому створюються умови для взаємодії користувача з віртуальним контентом, що особливо важливо у сфері Веб-дизайну, освіти, інженерії та анімації. Анімовані сцени на основі 3D-об’єктів, сприяють наочній демонстрації зовнішнього вигляду 3D-об’єкта та принципам його функціонування [1-3].

Прогрес у сфері технологій, подальший розвиток 3D-моделювання, вимоги до візуалізації та рендерінгу, супроводжуються зростанням складності геометричних і аналітичних задач. Це, зокрема, зумовлено необхідністю створення більш реалістичних, динамічних та інтерактивних віртуальних 3D-середовищ, що потребують обробки великих обсягів вихідних даних, високого рівня деталізації та точності при побудові гнучких форм [4-7]. Одним із ключових викликів у цьому контексті є математичне описання кривих та поверхонь, яке має забезпечувати не лише зовнішню точність, а й функціональну адаптивність під час анімації, симуляції деформацій або взаємодії об'єктів. Особливо критичним таке завдання є у розробці відеоігор, VR/AR-додатків, де потрібно формувати плавні траєкторії руху, природні згиби та реалістичну поведінку тіл під впливом зовнішніх факторів. Відтворення таких процесів є складним з обчислювальної точки зору і вимагає ефективних рішень з високим рівнем адаптивності [4-7].

На основних етапах 3D-моделювання до кривих і поверхонь висувається низка вимог, серед яких: компактність параметричного опису, висока гладкість на з'єднаннях, керованість осциляцією, а також здатність до локального редагування без потреби в перерахунку всієї моделі. З огляду на це, особливої актуальності набуває використання сплайн-апроксимації на базі сплайн-функцій, зокрема інтерполяційних параметричних сплайнів. Відомо [5], що використання сплайнів є досить простим, а сплайн-функції мають високу збіжність та можуть масштабуватися на окремих ділянках, забезпечуючи необхідну точність.

Використання параметричних сплайнів авторами в роботах [1-3] забезпечує рішення низки задач, серед яких 3D-моделювання на етапі формування кривих та поверхонь з метою наближення форми кривих до форми моделюємого 3D-об’єкту, 3D-моделювання для побудови кривих та поверхонь у тривимірному форматах для опису форми моделюємого 3D-об’єкту з метою мінімізації похибок наближення. В даній роботі запропоновано використання параметричних сплайнів для візуалізації та рендерінгу 3D-об’єктів за допомогою апроксимації кривих та поверхонь з наперед заданими умовами плавності переходів.

Метою даної роботи є підвищення точності 3D-моделювання об’єктів за допомогою сплайн-апроксимації на базі інтерполяційних параметричних сплайнів.

Розглянемо інтерполяцію кривих параметричними лінійними сплайн-функціями. Нехай на деякій кривій L задано послідовність точок $P_i = (x_i; y_i)$, $i = 0, 1, \dots, N$. Виконаємо параметризацію кривої L:

$$\begin{cases} x = x(s); \\ y = y(s), \end{cases} \quad (1)$$

де s – параметр довжини дуги кривої L.

Точці $P_i = P(x_i, y_i)$ відповідає значення

$$\begin{cases} x_i = x(s_i); \\ y_i = y(s_i), \end{cases} \quad i = \overline{0, N}. \tag{2}$$

Інтерполяційний лінійний параметричний сплайн, який заданий на проміжку між точками P_i та P_{i+1}, має вигляд [8-10]:

$$\begin{cases} S_1(x;s) = (1-t)x_i + tx_{i+1}; \\ S_1(y;s) = (1-t)y_i + ty_{i+1}. \end{cases}, \tag{3}$$

де $t = (s - s_i)/l_i$, $l_i = s_{i+1} - s_i$, $i = 0,1,...,N-1$.

Розіб'ємо проміжок зміни параметру s таким чином $s_0 < s_1 < ... < s_N$ та знайдемо значення функції у точках розбиття s_i, $i = \overline{0, N}$, причому виконуються умови (2), де [9-10]:

$$S_1(x;s_i) = x_i, \; S_1(y;s_i) = y_i, \; i = 0,1,...,N. \tag{4}$$

Розглянемо побудову параметричного лінійного сплайну для заданої кривої *L*, утвореної лініями каркасу модельованого 3D-об'єкту, точками $P_0 = (x_0; y_0)$, $P_i = (x_i; y_i)$, $P_{i+1} = (x_{i+1}; y_{i+1})$ та $P_N = (x_N; y_N)$, які зображені на рис. 1,*а*. Інтерполяційну криву параметричного лінійного сплайну вигляду (1), яку отримано в ході розрахунків, показано пунктирною лінією (рис. 1,*б*).

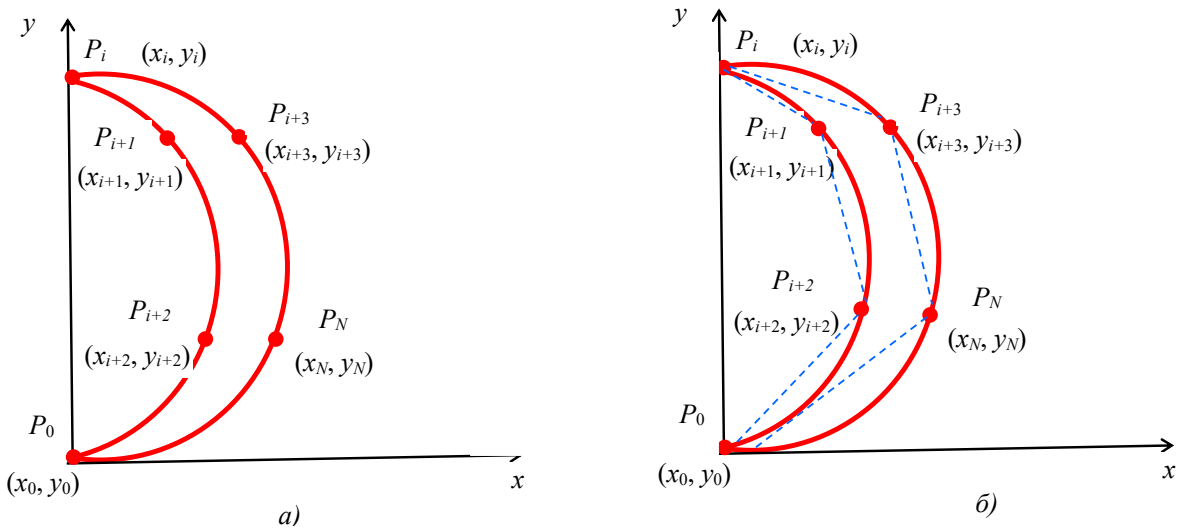


Рисунок 1 – Крива *L* каркасу модельованого 3D-об'єкту (*а*) та крива параметричного лінійного сплайну (*б*)

Отримано криву параметричного лінійного сплайну, яка апроксимує криву каркасу модельованого 3D-об'єкту, причому чим ближче буде наближення до кривої каркасу, тим менше буде похибка апроксимації. Для розрахунку похибки апроксимації $R_1(s)$ параметричним лінійним сплайном використаємо формулу (5) [9]:

$$R_1(S) = \sqrt{\left|S_1(x;s) - x(s)\right|^2 + \left|S_1(y;s) - y(s)\right|^2}. \tag{5}$$

Таблиця 1 – Похибка сплайн-апроксимації на базі параметричного лінійного сплайну

Проміжок	Значення похибки
$[x_0;x_1]$	5,71

$[x_1;x_2]$	7,50
$[x_2;x_3]$	8,25
…	…
$[x_{N-1};x_N]$	31,71
…	…

Висновки

1. Для візуалізації та рендерингу кривих та поверхонь 3D-об’єктів в процесі моделювання запропоновано використання інтерполяційного параметричного лінійного сплайну.

2. Для заданої кривої, утвореної лініями каркасу модельованого 3D-об’єкту, побудовано криву параметричного лінійного сплайну, визначено похибки апроксимації.

3. Встановлено, що застосування інтерполяційних параметричних сплайнів сприяє зниженню обчислювальної складності, забезпечує масштабованість рішень і суттєво спрощує процес 3D-моделювання.

Література

1. Стрелковська І.В., Соловська І.М., Стрелковська Ю.О. Застосування параметричних сплайн-функцій в моделюванні Вісник Хмельницького національного університету. – Т.1, № 3, С. 228-233.
2. Стрелковська І.В. Сплайн-апроксимація в 3D-моделюванні / І.В. Стрелковська, І.М. Соловська // Матеріали VIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених «Гуманітарний і інноваційний ракурс професійної майстерності: Пошуки молодих вчених», м. Одеса, 18 листопада 2022 р. – С. 390-394.
3. Стрелковська І.В. Сплайн-апроксимація в 3D-моделюванні / І.В. Стрелковська, І.М. Соловська, Н. Снігур, В. Малюга // Матеріали міжнародної конференції «Передові технології в інформаційно-комунікаційній інженерії», м. Одеса, 17-20 липня 2023 р. – С. 22-26.
4. Ільїна І.В., Біжко О.В. Аналіз особливостей візуалізації тривимірних об’єктів. Системи управління, навігації та зв’язку, 2016, 2: 88-92.
5. Сітко Д.О., Гніденко М.П., Крилов О.С. Сплайн-функції в задачах інтерполяції. Наукові записки ДУІКТ – 2024. – №2 (6). – С. 171-178.
6. Bühler Peter. 3D Mit Blender: Modeling-Animation-Rendering. Springer Fachmedien Wiesbaden GmbH, 2022.
7. Sari Aswita, Usman Ari, Handoko Divi. Comparison Analysis of 3D Animation Rendering With Cycles Methods and Workbench in Blender. Journal of Data science and Visualization, 2022.
8. 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.
9. Ahlberg J.H. The Theory of Splines and Their Applications / J.H. Ahlberg, E.N. Nilson, J.L. Walsh // Academic Press, New York, 1967.
10. Larry L. Spline Functions: Basic Theory / L. Larry, S. Schumaker // Cambridge University Press, New York, 2007.

УДК 004.738.5:004.8

Соловська І.М., к.т.н., доцент,
Міжнародний гуманітарний університет,
i.solovskaya@mgu.edu.ua,
Рудих А.П., магістр 2 року навчання,
Міжнародний гуманітарний університет,
rudyhanton9@gmail.com

АНАЛІЗ ВПЛИВУ FRONT-END-ФРЕЙМВОРКІВ НА ПРОДУКТИВНІСТЬ ТА ОПТИМІЗАЦІЮ ВЕБ-САЙТІВ

Сучасний підхід до розробки та просування Веб-сайтів зумовлює приділення уваги до показників ефективності роботи Веб-сайтів, які є критично важливим фактором для забезпечення позитивного користувацького досвіду UX (User Experience), високої конкурентоспроможності бізнесу та успішного SEO-просування [1]. Однією з ключових складових, що впливають на ці аспекти, є вибір технологічного стеку, зокрема Front-end-фреймворку, який визначає логіку побудови інтерфейсу користувача, швидкість завантаження Веб-сайту, масштабованість і підтримку адаптивного дизайну сайту. У процесі Веб-розробки вибір Front-end-фреймворку (React, Vue.js, Angular, jQuery) напряму впливає не лише на структуру проєкту, а й на технічні показники продуктивності [1-4]. Google постійно вдосконалює підходи до оцінювання Веб-сайтів, впроваджуючи стандарти оптимізації, такі як Lighthouse та CWV (Core Web Vitals), які стають критеріями ранжування сторінок у пошукових системах [2]. Тому питання аналізу технічних характеристик популярних сучасних Front-end-фреймворків, порівняння їх впливу на час завантаження сторінок, взаємодію з браузером, можливості lazy loading, SSR (Server-Side Rendering), CSR (Client-Side Rendering), а також інструментів для оптимізації ресурсу є актуальним.

Метою даної роботи є порівняння Front-end-фреймворків (React, Vue.js, Angular, jQuery) показників продуктивності Веб-сайтів для подальшої оптимізації на базі DataSet відкритого публічного набору HTTP Archive.

DataSet було отримано з [5] Google BigQuery для якого відібрано Веб-сайти, у коді яких автоматично виявлено один із зазначених Front-end-фреймворків (React, Vue.js, Angular, jQuery) [6-9] та здійснено аналіз для десктопної версії (client = 'desktop').

```
query="""
SELECT
  LOWER(app) AS framework,
  date,
  client,
  ROUND(median_lighthouse_score_performance, 2) AS performance,
  ROUND(median_bytes_total / 1024, 1) AS total_kb,
  ROUND(median_bytes_js / 1024, 1) AS js_kb,
  ROUND(pct_eligible_origins_with_good_cwv * 100, 1) AS good_cwv_pct
FROM
  httparchive.core_web_vitals.technologies
WHERE
  LOWER(app) IN ('react', 'vue.js', 'angular', 'jquery')
  AND client = 'desktop'
  AND date = '2025-06-01'
ORDER BY performance DESC
"""
df_metrics = client.query(query).to_dataframe()
df_metrics
```

За допомогою коду створено SQL-запит до BigQuery-таблиці httparchive.core_web_vitals.technologies, для отримання даних про продуктивність та розмір ресурсів Front-end-фреймворків, а саме, React, Vue.js, Angular, jQuery. У запиті обираються наступні дані: назва фреймворку (нижнім регістром), дата, клієнт, продуктивність (performance), загальний розмір сторінки (total_kb), розмір JS (js_kb) та відсоток сайтів із CWV (good_cwv_pct); дані сортуються за продуктивністю за спаданням; результат перетворюється у DataFrame (df_metrics) для подальшої аналітики у Python.

Для проведення дослідження обрано наступні метрики: Lighthouse performance score, Core Web Vitals, обсяг JavaScript, загальний розмір сторінки [2].

Lighthouse performance score, інтегральна оцінка від 0 до 1 (або 0–100), яка узагальнює продуктивність сторінки на основі шести базових показників: FCP (First Contentful Paint) – час, коли браузер виводить перший елемент DOM; LCP (Largest Contentful Paint) – час появи найбільшого видимого елемента; Speed Index – наскільки швидко з'являється вміст, TTI (Time to Interactive) – час, коли сторінка стає повністю інтерактивною, TBT (Total Blocking Time) – сумарний час блокування головного потоку, CLS (Cumulative Layout Shift) – стабільність верстки під час завантаження.

Метрика Lighthouse моделює реальне користувацьке сприйняття швидкості і зручності завантаження. Результати порівняння Front-end-фреймворків (React, Vue.js, Angular, jQuery) за критеріями Lighthouse показано на рис. 1. Проведений аналіз дозволяє стверджувати, що найбільшу продуктивність здатний забезпечити фреймворк jQuery - 0,65, а найнижчу фреймворк Angular – 0,52.

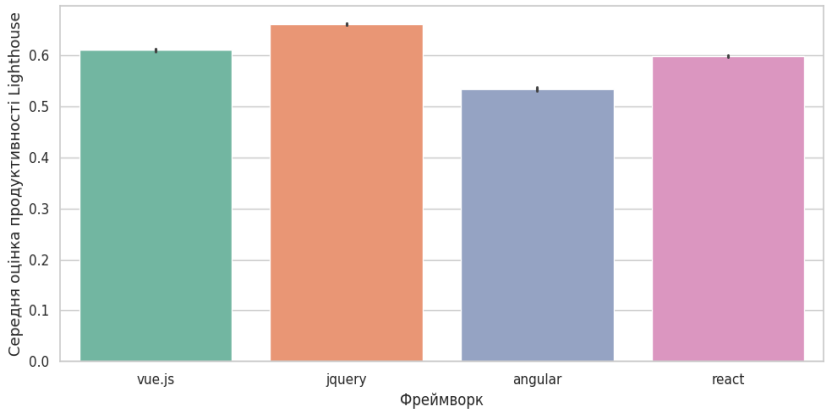


Рисунок 1 – Порівняння продуктивності Веб-сайту з використанням Front-end-фреймворків (React, Vue.js, Angular, jQuery) за середньою продуктивністю Lighthouse

Наступна метрика Core Web Vitals (CWV) – це показник, що відображає частку сайтів (у відсотках), які відповідають трьом основним критеріям Google: LCP (Largest Contentful Paint) менше 2.5 сек – швидкість завантаження основного контенту; FID (First Input Delay) менше 100 мс – швидкість першої взаємодії; CLS (Cumulative Layout Shift) менше 0.1 – стабільність макету при завантаженні.

Збільшення показника CWV дозволяє стверджувати про те, що більшість сайтів на базі певного фреймворку відповідають вимогам Google щодо користувацького досвіду UX. Результати порівняння Front-end-фреймворків за критерієм Core Web Vitals показано на рис. 2. Найвищий відсоток Веб-сайтів, що відповідають критерію CWV, має jQuery – 44,3%, а найнижчий – фреймворк Angular – 16,5%.

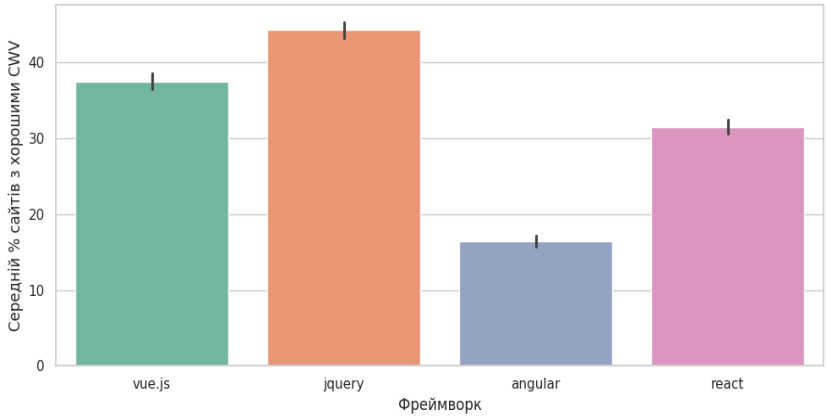


Рисунок 2 – Порівняння Веб-сайтів з використанням Front-end-фреймворків (React, Vue.js, Angular, jQuery) за відсотком сайтів, що відповідають показникам CWV

Загальний розмір сторінки (Total_kb) – сумарний обсяг усіх завантажених ресурсів Веб-сторінки (HTML, CSS, JavaScript, зображення, шрифти тощо). Значення Total_kb є важливим, адже означає швидкість завантаження сайту та кращий користувацький досвід. Результати порівняння показано на рис. 3. Найменший середній розмір мають Веб-сайти на jQuery – 1050,1 kb, найбільший – на Angular – 1414,2 kb. Такі результати пояснюються особливостями фреймворку jQuery, який не є повноцінним SPA-фреймворком, а використовується переважно як невелика JS-бібліотека для маніпуляцій з DOM та інтеграції динамічних елементів. Це не вимагає додаткових об'ємних ресурсів, типових для сучасних фреймворків.

Натомість Angular є комплексним фреймворком із великою кількістю вбудованих модулів, CLI-структурою та потужними механізмами двостороннього зв'язку даних, що збільшує загальний розмір сторінки навіть за мінімальної конфігурації проекту. Саме тому вебсайти на Angular мають найбільший середній обсяг завантажених ресурсів серед аналізованих технологій.

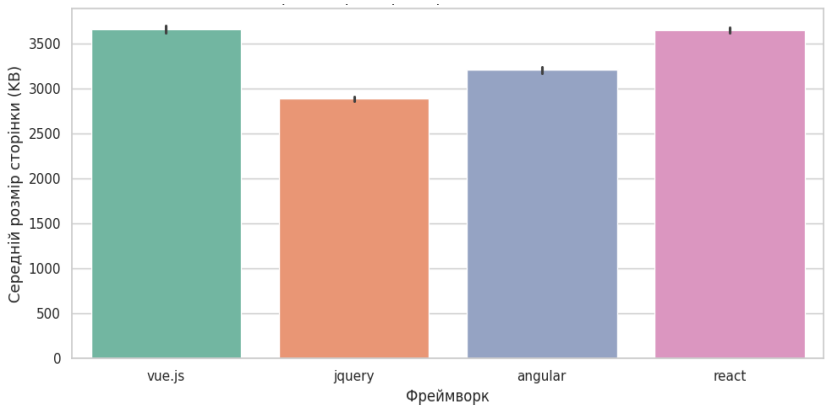


Рисунок 3 – Порівняння Веб-сайтів з використанням Front-end-фреймворків (React, Vue.js, Angular, jQuery) за середнім розміром усіх завантажених ресурсів сторінки

Обсяг JavaScript (JS_kb) – показник, що відображає сумарну вагу JS-коду, завантаженого Веб-сторінкою. Велике значення JS _kb є індикатором перевантаженості Front-end, що негативно впливає на показники часу інтерактиву Time to Interactive (TTI), часу блокування Total Blocking Time (TBT) та загальну продуктивність. Результати порівняння Front-end-фреймворків за обсягом JavaScript показано на рис. 4. Найменший обсяг має jQuery – 319,4 kb, найбільший – Angular – 641,8 kb.

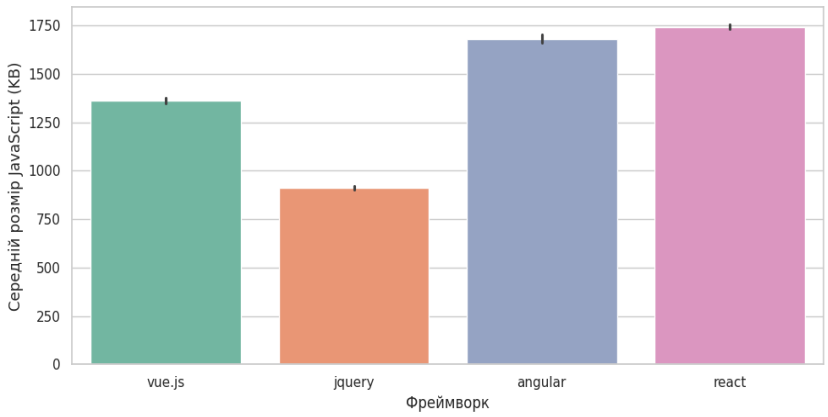


Рисунок 4 – Порівняння Веб-сайтів з використанням Front-end-фреймворків (React, Vue.js, Angular, jQuery) за середнім розміром файлу JavaScript Веб-сторінки

Проведений порівняний аналіз показників продуктивності Веб-сайтів на базі Front-end-фреймворків (React, Vue.js, Angular, jQuery) дозволив сформувати усереднені значення показників продуктивності, обсягу за загальним обсягом Веб-сайту, JavaScript та швидкісних показників CWV для чотирьох найпоширеніших Front-end-фреймворків React, Vue.js, Angular, jQuery. Результати наведено в табл. 1.

Таблиця 1 – Усереднені значення показників продуктивності для Front-end-фреймворків React, Vue.js, Angular, jQuery

Фреймворк	Продуктивність	Загальний обсяг Веб-сайту, kb	Обсяг JavaScript	Швидкісні показники CWV, %
React	0.61	1323.4	596.2	34.7
Vue.js	0.63	1251.0	488.1	37.5
Angular	0.52	1414.2	641.8	16.5
jQuery	0.67	1050.1	319.4	44.3

Висновки

1. Проведено порівняний аналіз показників продуктивності Веб-сайтів на базі Front-end-фреймворків (React, Vue.js, Angular, jQuery) за значеннями показників продуктивності, обсягу за загальним обсягом Веб-сайту, JavaScript та швидкісних показників CWV.

2. Встановлено, що фреймворк jQuery показує найкращі показники продуктивності Lighthouse та відповідності Core Web Vitals завдяки мінімальному обсягу JavaScript-коду. Фреймворк Angular поступається іншим фреймворкам – має найбільший середній розмір сторінки та JS, найнижчі показники продуктивності Lighthouse і найменший відсоток сайтів, що відповідають метриці CWV. Vue.js та React мають схожі значення метрик, проте Vue.js показує дещо кращу оптимізацію порівняно з React.

3. Проведене дослідження підтверджує, що вибір Front-end-фреймворку безпосередньо впливає на продуктивність, користувацький досвід UX та SEO Веб-сайтів, що є критично важливим для комерційних та високонавантажених веб-проєктів.

Література

1. Web Academy. Актуальні фреймворки для Front-end розробника: https://web-academy.ua/

2. Optimizing Web Vitals using Lighthouse: https://web.dev/articles/optimize-vitals-lighthouse

3. Miguel Grinberg. Flask Web Development: Developing Web Applications with Python, O'Reilly Media; 2nd edition, 2018, 474 p.

4. Kolawole Mangabo. Full Stack Django and React: Get hands-on experience in full-stack web development with Python, React, and AWS, 2023, 432 p.

5. DataSet відкритого публічного набору HTTP Archive core_web_vitals.technologies

6. Front-end-фреймворк React https://react.dev

7. Front-end-фреймворк Vue.js https://vuejs.org

8. Front-end-фреймворк Angular https://angular.io

9. Front-end-фреймворк jQuery https://jquery.com

УДК 372.862, 519.876.5

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Пшеничний Олександр Сергійович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 122 Комп'ютерні науки
Міжнародний гуманітарний університет
alexdichemix@gmail.com

СИСТЕМА КОМП'ЮТЕРНОГО ЗОРУ З ГОЛОСОВИМ КЕРУВАННЯМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ДИСТАНЦІЙНІЙ ФОРМІ НАВЧАННЯ

Анотація. *Розглянуто розробку системи комп'ютерного зору з голосовим керуванням на основі штучного інтелекту для інтерактивного робота. Наведено стислий опис апаратної та програмної архітектури, що поєднує Raspberry Pi, Arduino, камеру, мікрофон і 3D-друковану голову робота. Система здатна розпізнавати обличчя та положення людини, обробляти голосові команди й питання, а також генерувати відповіді за допомогою AI-моделі. Результати впровадження демонструють, що інтеграція комп'ютерного зору та голосового інтерфейсу дозволяє створити ефективну автономну платформу для освіти, автоматизації та асистивних технологій..*

Сучасний розвиток робототехніки, систем штучного інтелекту й автоматизації суттєво змінює підходи до створення пристроїв, що взаємодіють із людиною. Актуальність розробки таких систем зумовлена не лише високим попитом на асистивні та навчальні рішення, а й загальною тенденцією до впровадження природних інтерфейсів "людина–машина", які базуються на розпізнаванні зображень і мови.

Запропонована система об'єднує комп'ютерний зір, голосове керування й алгоритми штучного інтелекту в одному пристрої. У її апаратну архітектуру входять:

- **Raspberry Pi** — центральний модуль, що здійснює обробку відеопотоку, реалізацію алгоритмів комп'ютерного зору та інтеграцію з AI-моделлю;
- **Arduino** — плата для керування сервоприводами, які забезпечують рух голови робота;
- **Камера** — використовується для відеоспостереження, визначення положення й ідентифікації людини в кадрі;
- **Мікрофон** — забезпечує прийом голосових команд та питань від користувача;

- **3D-друкована голова** — як механічна та естетична частина системи, що може фізично повертатись у бік співрозмовника.

Програмна частина створена на мові Python із використанням бібліотек **OpenCV** (для аналізу відео й розпізнавання облич), **SpeechRecognition** (для обробки голосу) та нейромережевої AI-моделі (наприклад, GPT) для генерації відповідей на питання користувача. Передбачено інтеграцію текст-у-мову (Text-to-Speech) для озвучування відповідей робота.

Взаємодія компонентів відбувається наступним чином.

Камера захоплює відеопотік, Raspberry Pi визначає координати обличчя користувача та обраховує потрібний кут повороту голови, цю інформацію надсилає Arduino, яка відповідно обертає сервопривід. Мікрофон приймає голосову команду, що обробляється Python-модулем для розпізнавання мови, далі питання передається в AI-модель, яка генерує змістовну відповідь. Робот відповідає користувачу голосом через синтезатор мови.

Особливістю системи є комплексність підходу — поєднання комп'ютерного зору, голосового керування, фізичного руху та генерації розумних відповідей у реальному часі. Це дозволяє реалізувати максимально "живу" взаємодію між людиною і машиною. На відміну від окремих рішень, які лише розпізнають команди або виконують прості рухи, розроблений пристрій здатний підтримувати діалог і стежити за людиною під час спілкування.

Дана система може бути застосована:

- у навчальному процесі як інтерактивний демонстратор технологій комп'ютерного зору й AI;
- як асистивний пристрій для людей з порушенням рухливості або мовлення;
- для автоматизації презентацій, виставок, роботів-гідів чи приймальних систем;
- у наукових експериментах, пов'язаних із тестуванням природної взаємодії людини та робота.

Подальший розвиток може включати розширення мовної підтримки, інтеграцію додаткових сенсорів (жести, емоції), підключення до інтернету речей (IoT) і застосування у сфері "розумного будинку".

Таким чином, розроблена система демонструє практичні можливості поєднання сучасних апаратних та програмних рішень для створення автономного, "розумного" та інтерактивного пристрою, що здатний стати частиною повсякденного життя, навчального процесу або сфери обслуговування.

Висновки. У роботі представлено інтерактивну систему комп'ютерного зору з голосовим керуванням на основі штучного інтелекту, яка забезпечує природну та зручну взаємодію між людиною і роботом. Система поєднує сучасні апаратні (Raspberry Pi, Arduino, камера, мікрофон, 3D-друкована голова) та програмні засоби (OpenCV, SpeechRecognition, AI-модель) для реалізації функцій розпізнавання образу, голосового інтерфейсу, генерації відповідей та фізичного стеження за співрозмовником.

Практичне впровадження продемонструвало, що така комплексна інтеграція дозволяє створити гнучку й універсальну платформу для освітніх, асистивних, демонстраційних та дослідницьких цілей.

Подальший розвиток полягає у розширенні функціональності системи — додаванні аналізу жестів, емоцій, багатомовності, інтеграції з іншими AI-сервісами й IoT-рішеннями.

Література

1. Vosk Speech Recognition Toolkit. URL: https://alphacephei.com/vosk/
2. OpenCV Documentation. URL: https://docs.opencv.org/
3. Raspberry Pi Documentation. URL: https://www.raspberrypi.org/documentation/
4. Arduino Documentation. URL: https://www.arduino.cc/reference/en/
5. Ben Lutkevich. What is a Microcontroller and How Does it Work? URL: https://www.techtarget.com/iotagenda/definition/microcontroller

6. Рижова А.Р. Оникієнко Ю.О. Аналіз особливостей використання ресурсів мікроконтролера для розпізнавання мовлення. Мікросистеми, Електроніка та Акустика. Київ, КПІ ім. І.Сікорського. 2022. Т. 27, вип. 2. С.265406–1 – 265406–7.
7. Русу О.П. Універсальна віртуальна лабораторія для традиційної та дистанційної форм навчання. Матеріали VIII всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених «Гуманітарний і інноваційний ракурс професійної майстерності: пошуки молодих вчених». Одеса, Україна, 18 листопада 2022 р. С. 385 – 388.
8. Русу О.П., Маркітан А.С., Султанзаде Н.Р. Віртуальна лабораторія для програмування мікроконтролерів. Матеріали IX всеукраїнської мультидисциплінарної конференції «Чорноморські наукові студії». Одеса, Україна, 12 травня 2023 р. С. 214 – 216.
9. Integrated Development Environment (IDE) MPLAB X. URL: https://www.microchip.com/en-us/tools-resources/develop/mplab-x-ide
10. Proteus: PCB Design and Circuit Simulator Software. URL: https://www.labcenter.com/

УДК 378.14, 004.9

Русу Олександр Петрович,
к.т.н., доцент кафедри комп'ютерних наук
Міжнародний гуманітарний університет
shurusu@ukr.net

Лорткіпанідзе Руслан,
здобувач 1 курсу другого (магістерського) рівня
спеціальності 123 – Комп'ютерна інженерія
Міжнародний гуманітарний університет
rockstargett@gmail.com

Черкас Нікіта Сергійович
здобувач 2 курсу першого (бакалаврського) рівня
спеціальності 172 – Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет
nikitacerkas131@gmail.com

ВЕБЗАСТОСУНОК MCLAB ДЛЯ НАВЧАННЯ ПРОГРАМУВАННЯ МІКРОКОНТРОЛЕРІВ

Анотація. *Розглянуто навчальний вебзастосунок McLab, що дозволяє симулювати у браузері роботу схем на основі мікроконтролерів без потреби фізичного створення електричної схеми. Вебзастосунок McLab поєднує функції віртуальної лабораторії, системи управління навчальним контентом, а також забезпечує моделювання роботи мікроконтролерів у реальному часі. Описано відмінності від існуючих рішень, наведено опис та структурну схему вебзастосунку, основних функціональних модулів, інтерфейс та варіанти освітніх сценаріїв.*

Сервіси, що дозволяють перевіряти працездатність програмного забезпечення для мікроконтролерів без фізичного моделювання електричної частини схеми, мають великий попит у початківців в електроніці, радіоаматорів, студентів, а також працівників, що підвищують кваліфікацію. Зокрема подібні застосунки можуть активно використовуватися в університетах як частина навчального процесу. Однак наразі в Україні та світі кількість програмного забезпечення, яке б поєднувало переваги EdTech-застосунків та вебсимуляторів, істотно обмежена, що обумовлює актуальність проведеної роботи

Найбільш відомим програмним забезпеченням, що дозволяє вирішити цю проблему, є Proteus Design Suite [1] та Tinkercad Circuits [2]. Proteus Design Suite, створений компанією Labcenter Electronics, є відомим емулятором електричних схем, зокрема і мікроконтролерів. Однак це програмне забезпечення має функціонально перевантажений користувацький інтерфейс, для роботи з яким потрібна певна попередня підготовка. Tinkercad Circuits є онлайн-сервісом від компанії Autodesk, який підтримує лише симуляцію мікроконтролерів, що використовуються на платах платформи Arduino, що суттєво обмежує варіативність застосування цього програмного забезпечення.

На відміну від наведених вище прикладів, веб-застосунок McLab є не лише платформою для моделювання мікроконтролерів, а й повноцінною системою управління навчанням, що поєднує теоретичну та практичну частини. Таким чином, платформа McLab займає проміжне положення між браузерними симуляторами та стаціонарним програмним забезпеченням.

Веб-застосунок McLab побудований за класичною архітектурою клієнт-сервер, де є окрема клієнтська частина (frontend) і серверна частина (backend), які взаємодіють між собою. Структурну схему застосунку зображено на рис. 1. Клієнтська частина побудована на основі фреймворку Nuxt 3 [3] із використанням бібліотеки стилів Tailwind CSS [4] та бібліотеки SVG.js [5], що використовуються для роботи графічного інтерфейсу. Ця частина системи оброблює команди користувача та забезпечує інтерактивність елементів керування. До переліку основних функції клієнтської частини входять завантаження бінарних файлів у форматі .HEX (прошивок мікроконтролерів), а також керування симуляцією роботи. Крім того, frontend-частина застосунку забезпечує аутентифікацію та авторизацію користувача, що реалізовані за допомогою бібліотек vee-validate [6] та Zod Forms [7].

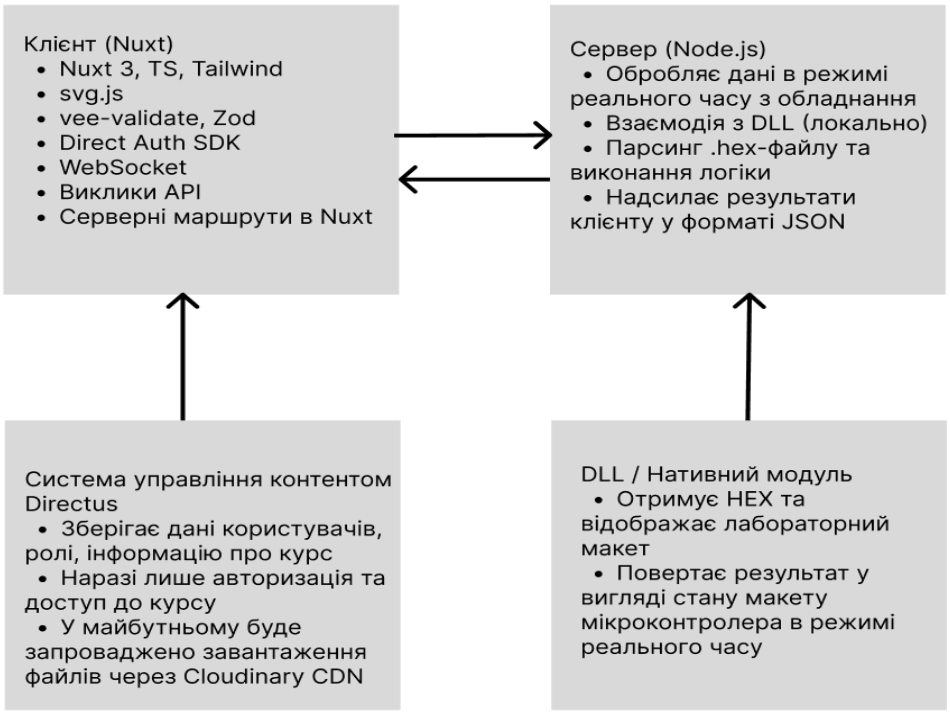


Рисунок 1 – Структурна схема веб-застосунку McLab

Серверна частина застосунку, що написана на основі фреймворку Node.js [8], забезпечує двосторонню комунікацію між frontend та backend частинами у реальному часі через веб-сокети. Відповідно до обраної моделі, серверна частина отримує прошивку мікроконтролера, розпаковує її та передає на виконання у нативний DLL-модуль, який забезпечує симуляцію поведінки мікроконтролера в режимі, наближеному до реального часу. Результатом моделювання є стан портів мікроконтролера, який повертається у клієнтську частину системи у форматі JSON.

Система менеджменту контенту реалізована на основі Directus CMS [9]. Вона зберігає інформацію про користувачів: курси, які вони проходять, дані про авторизацію та автентифікацію тощо. Наразі Directus CMS використовується лише для авторизації та доступу до системи, однак у майбутньому функціонал цього модуля буде розширено.

Архітектурно вебзастосунок McLab має модульну структуру: модуль користувацького інтерфейсу, серверну частину, модуль DLL-емуляції мікроконтролерів, модулі рендерингу макетів мікроконтролерів на схемі, а також сховище медіа (Cloudinary CDN [10]). Модульність дозволяє планувати масштабування вебзастосунку в майбутньому, додавати підтримку нових мікроконтролерів та забезпечує високий рівень гнучкості для різних навчальних сценаріїв.

Зовнішній вигляд інтерфейсу вебзастосунку McLab наведено на рис. 2. З його допомогою можна завантажувати прошивки та запускати їх симуляцію, спостерігати за поведінкою схеми (анімація), панорамувати схеми тощо.

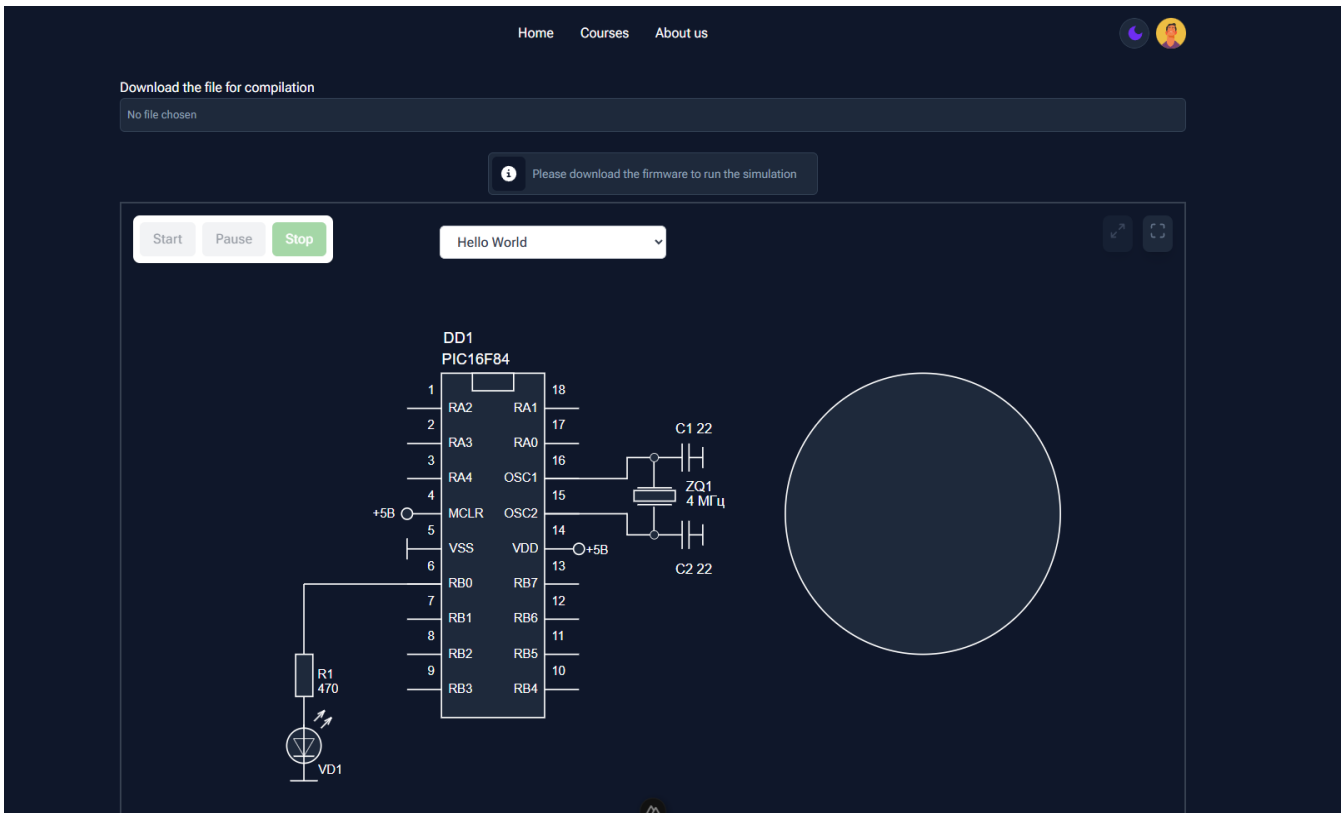


Рисунок 2 – Зовнішній вигляд веб-застосунку McLab

Існують три варіанти використання вебзастосунку McLab: базовий, розширений і преміум. До базового пакету входить доступ до віртуальної лабораторії та відеоуроки курсу, де користувач може самостійно вивчати матеріал і виконувати практичні завдання. Розширений варіант включає усі можливості базового пакету, а також можливість надсилати завдання на перевірку викладачам, що дає змогу отримувати зворотній зв'язок. До преміум пакету входить весь функціонал розширеного пакету, та доступ до списку завдань для самоперевірки та можливість спілкування в чаті з викладачами, що сприяє більш ефективному навчанню.

Таким чином, вебзастосунок McLab ефективно вирішує проблему обов'язкової необхідності фізичного середовища для моделювання та перевірки програмного забезпечення для мікроконтролерів. На створеній платформі користувач може запустити моделювання мікроконтролера та одразу побачити результат виконання коду, протестувати логіку та, за необхідності, його скорегувати. Графічний інтерфейс вебзастосунку відображає реальні стани виводів мікроконтролера – саме так, як це може виглядати на фізичній платі під керуванням реального мікроконтролера, тобто, анімація на екрані повністю відповідає реальній роботі пристрою. Усе дозволяє позиціонувати вебзастосунок McLab у якості одного з базових інструментів для навчання програмування мікроконтролерів, що підтримує усі існуючі форми навчання, зокрема дистанційну освіту, як в синхронному, так і в асинхронному режимах.

Література

1. Introduction to Proteus. The Engineering Knowledge. URL: https://www.theengineeringknowledge.com/introduction-to-proteus/.

2. Official Guide to TInkercad Circuits. Tinkercad. URL: https://www.tinkercad.com/blog/official-guide-to-tinkercad-circuits

3. Introduction. Get started with Nuxt v3. URL: https://nuxt.com/docs/getting-started/introduction

4. Installing Tailwind CSS with Vite. Tailwind CSS. URL: https://tailwindcss.com/docs/installation/using-vite

5. Getting started with SVG.js v3.1. SVG.js. URL: https://svgjs.dev/docs/3.1/getting-started

6. vee-validate. Node Package Manager. URL: https://www.npmjs.com/package/vee-validate

7. Intro to Zod. Zod. URL: https://zod.dev/v4

8. Node.js Documentation. Node.js. URL: https://nodejs.org/api/all.html#all_synopsis_usage

9. Directus Docs. Directus CMS. URL: https://directus.io/docs

10. Docs Home Page. Cloudinary Image & Video API Platform. URL: https://cloudinary.com/documentation

Проценко М.М.

здобувач вищої освіти третього (аспірантського рівня)

спеціальності 123 – Комп'ютерна інженерія

Науковий керівник: ***Мірошник М. А.***

доктор технічних наук, професор

Міжнародний гуманітарний університет

місто Одеса, Україна

БЕЗПЕРЕРВНА ЕВОЛЮЦІЯ АРХІТЕКТУРИ ЧЕРЕЗ АВТОНОМНІ МУЛЬТИАГЕНТНІ RAG-СИСТЕМИ

Анотація. *Запропоновано теоретичну модель безперервної еволюції програмної архітектури через інтеграцію автономних мультиагентних систем з технологіями доповненої генерації на основі пошуку (RAG) для автоматизації архітектурного проектування та адаптації. Проведено аналіз фреймворку MAAD з чотирма спеціалізованими агентами (аналітик, моделювальник, дизайнер, оцінювач), механізмів їх координації та використання RAG для доступу до архітектурних знань. Обґрунтовано теоретичні переваги мультиагентного підходу для вирішення проблем традиційного*

архітектурного управління та запропоновано напрямки подальших досліджень щодо експериментальної валідації та розробки практичних інструментів.

У сучасному світі програмні системи характеризуються зростаючою складністю та динамічністю вимог, що створює значні виклики для традиційних методів архітектурного управління. Проведене дослідження зосереджується на теоретичному аналізі можливостей інтеграції автономних мультиагентних систем з технологіями доповненої генерації на основі пошуку (RAG) для забезпечення безперервної еволюції програмної архітектури. Актуальність цієї проблематики зумовлена розривом між швидкістю змін бізнес-вимог та здатністю архітектурних команд адаптувати системи до цих змін [1].

Традиційні підходи до архітектурного проектування базуються на періодичних оглядах та експертних рішеннях, що вимагає значних часових ресурсів. Концепція еволюційної архітектури передбачає постійні інкрементальні зміни з автоматизованою валідацією через фітнес-функції. Аналіз літератури виявив, що спроби використання окремих LLM стикаються з проблемою генерації неточного контенту. Дослідження показують, що мультиагентна взаємодія суттєво підвищує якість результатів через взаємну валідацію та дебати між агентами [2].

Особливу увагу приділено аналізу фреймворку Knowledge-based Multi-Agent Architecture Design (MAAD), який демонструє ефективність використання чотирьох спеціалізованих агентів для автоматизації архітектурного проектування. Фреймворк використовує знання з трьох джерел: існуючих системних проектів, авторитетної літератури та експертних знань. На основі цього аналізу пропонується розширена теоретична модель для забезпечення безперервної архітектурної еволюції [1].

У запропонованій моделі агент-аналітик обробляє та інтерпретує вимоги до системи, виявляючи приховані залежності та архітектурно-значущі аспекти. Агент-моделювальник формує високорівневі архітектурні рішення, включаючи вибір архітектурних стилів, технологічного стеку та створення концептуальних представлень. Використання RAG-технологій дозволяє звертатися до бази знань з успішними архітектурними рішеннями [3].

Агент-дизайнер деталізує архітектурні рішення до рівня імплементації через створення UML-діаграм та специфікацій інтерфейсів. Теоретична модель передбачає вбудовані механізми перевірки відповідності принципам SOLID. Агент-оцінювач забезпечує безперервну валідацію через систему фітнес-функцій, які охоплюють продуктивність, безпеку, підтримуваність та масштабованість [1].

Ключовим елементом системи є механізми координації між агентами через структуровані протоколи комунікації. Обмін інформацією відбувається з використанням механізмів фільтрації та пріоритизації. При конфліктах застосовуються протоколи

переговорів або арбітражні механізми. Колективне прийняття рішень враховує індивідуальні переваги агентів [2].

Інтеграція RAG-технологій створює додатковий рівень інтелектуальності через доступ до обширних баз архітектурних патернів та документації. Дослідження показують, що RAG покращує прийняття рішень через заземлення агентів на зовнішніх знаннях. Поєднання семантичного пошуку з контекстуальним аналізом дозволяє знаходити релевантні рішення [4].

Дослідження автоматизації оркестрації мікросервісів демонструє ефективність фітнес-функцій для тестування через множинні виміри: продуктивність, безпеку, коректність та якість коду. Безперервна еволюція дозволяє системам адаптуватися без масштабних переробок. Автоматизована валідація забезпечує раннє виявлення проблем [5].

Теоретичний аналіз виявив потенційні виклики: складність початкового налаштування, питання довіри до автоматизованих рішень, масштабованість для великих проектів. Водночас переваги включають скорочення часу на архітектурні зміни, підвищення якості рішень та зниження технічного боргу.

Результати дослідження свідчать про значний потенціал безперервної еволюції архітектури через автономні мультиагентні RAG-системи. Запропонована модель демонструє можливість вирішення ключових проблем сучасного архітектурного управління. Подальші дослідження мають зосередитися на експериментальній валідації та розробці механізмів реалізації для різних типів систем.

Література

1. Zhang Y., Li R., Liang P., Sun W., Liu Y. Knowledge-Based Multi-Agent Framework for Automated Software Architecture Design. arXiv preprint arXiv:2503.20536, 2025. URL: https://arxiv.org/abs/2503.20536 (дата звернення: 13.07.2025).

2. Talebirad Y., Nadiri A. Multi-agent collaboration: Harnessing the power of intelligent LLM agents. arXiv preprint arXiv:2306.03314, 2023. URL: https://arxiv.org/abs/2306.03314 (дата звернення: 13.07.2025).

3. Du Y., Li S., Torralba A., Tenenbaum J.B., Mordatch I. Improving factuality and reasoning in language models through multiagent debate. arXiv preprint arXiv:2305.14325, 2023. URL: https://arxiv.org/abs/2305.14325 (дата звернення: 13.07.2025).

4. Wang L., Ma C., Feng X., Zhang Z., et al. A Survey on Large Language Model based Autonomous Agents. Frontiers of Computer Science, 2024. Vol. 18(6). URL: https://arxiv.org/abs/2308.11432 (дата звернення: 13.07.2025).

5. Bucchiarone A., Dragoni N., Dustdar S., et al. Towards automating microservices orchestration through data-driven evolutionary architectures. Software and Systems Modeling, 2024. Vol. 23, P. 387–409. URL: https://link.springer.com/article/10.1007/s11761-024-00387-x (дата звернення: 13.07.2025).

УДК 004.4:517.96

Григор'єва Т.І., к.т.н., доцент
Крохмаль М.В., аспірант
n.krokhmal@gmail.com
Міжнародний гуманітарний університет, місто Одеса

ЗАСТОСУВАННЯ ТЕНЗОРНОГО АНАЛІЗУ В ПРОГРАМНІЙ ІНЖЕНЕРІЇ

Анотація. *Робота присвячена вирішенню проблеми аналізу багатовимірних даних у програмній інженерії, де традиційні векторно-матричні методи є недостатньо ефективними. Запропоновано використання тензорного аналізу для представлення даних у вигляді багатовимірних масивів, що зберігає структурні та контекстуальні взаємозв'язки. Такий підхід дозволяє підвищити точність прогнозування дефектів, аналізувати технічні недоліки та оптимізувати тестування. Обґрунтовано доцільність інтеграції тензорних моделей та їх синтезу з глибоким навчанням.*

Розвиток сучасних програмних систем характеризується експоненціальним зростанням обсягів даних та ускладненням їх архітектурних залежностей. Традиційні методи аналізу, що базуються на векторно-матричних представленнях, демонструють обмежену ефективність при моделюванні багатовимірних взаємозв'язків між параметрами програмного продукту (модулі, користувачі, конфігурації, часові ряди) [1]. Ця обмеженість призводить до втрати контекстуальної інформації та, як наслідок, до зниження точності предиктивних моделей та аналітичних висновків. Відповідно виникає задача розробки методів, що здатні адекватно репрезентувати та аналізувати багатовимірні структури даних у програмній інженерії [2].

Тензорний підхід забезпечує представлення даних у вигляді багатовимірних масивів, де кожна вісь (мода) відповідає за окремий атрибут системи, такий як функціональний модуль, метрика коду, автор зміни чи версія. Це дозволяє зберігати структурну цілісність та глибокі контекстуальні взаємозв'язки, що існують між цими атрибутами. На відміну від векторних моделей, які вимагають "випрямлення" даних у двовимірну таблицю і неминуче призводять до втрати інформації про взаємодію, тензор зберігає цілісну картину. Це дає можливість виявляти складні, нелінійні патерни.

Ефективність тензорних моделей проявляється у вирішенні прикладних задач. Замість аналізу окремих, ізольованих факторів, тензорний підхід дозволяє моделювати систему як єдиний багатовимірний простір, що відкриває нові аналітичні можливості. У галузі прогнозування дефектів, тензорний аналіз дозволяє вийти за межі кореляцій низького порядку та ідентифікувати нетривіальні, багатофакторні комбінації, що є предикторами програмних помилок. Стає можливим виявлення латентних патернів, що передують виникненню дефектів. Аналогічним чином, підхід забезпечує методологічну основу для кількісної оцінки та аналізу ризиків, пов'язаних із технічним боргом.

Тензорні моделі також надають потужний інструментарій для оптимізації процесів регресійного тестування. Шляхом моделювання складних взаємозв'язків між змінами у

кодовій базі, тестовими випадками та історичними даними про збої, система може розраховувати пріоритети для тестів, що максимізує ймовірність раннього виявлення регресій та раціоналізує використання тестових ресурсів. Крім того, ці методи виявляються ефективними для аналізу архітектури програмних компонентів, зокрема, для виявлення прихованих, неявних залежностей між ними. Застосування технік тензорної декомпозиції дозволяє "просвітити" структуру системи, візуалізуючи латентні зв'язки, які не є очевидними при аналізі вихідного коду чи традиційних діаграм залежностей [3].

Ключова стратегічна ефективність тензорних методів реалізується не стільки в ізольованому застосуванні, скільки в синергетичному синтезі з іншими передовими аналітичними підходами та глибокій інтеграції в існуючі інструменти й процеси розробки програмного забезпечення. Цей двовекторний підхід, що поєднує практичну імплементацію та теоретичну комбінаторику, дозволяє трансформувати тензорний аналіз із вузькоспеціалізованого інструменту в фундаментальний елемент сучасної, керованої даними інженерії програмного забезпечення [4,5].

Перший вектор ефективності, практична інтеграція, передбачає впровадження тензорних моделей безпосередньо в конвеєри безперервної інтеграції та доставки (CI/CD), що кардинально змінює парадигму контролю якості. Такий крок перетворює статичний аналіз коду на динамічний, безперервний процес, що забезпечує аналітику в реальному часі. З кожною новою зміною в кодовій базі система отримує можливість автоматично перераховувати ризики, прогнозувати ймовірність внесення дефектів та оцінювати вплив змін на загальну стабільність архітектури, переводячи контроль якості з реактивного режиму в проактивний та надаючи командам розробки миттєвий зворотний зв'язок.

Другий вектор, теоретичний синтез, полягає у комбінації тензорного аналізу з теорією графів та методами глибокого навчання, що формує концептуальну основу для створення гібридних інтелектуальних систем. У таких системах теорія графів відповідає за моделювання структурної топології програмного продукту, зокрема його архітектурних зв'язків та залежностей, тоді як тензорний аналіз доповнює цю структурну картину, детально описуючи багатовимірні атрибутивні дані кожного елемента системи. Глибоке навчання, в свою чергу, виступає як аналітичне ядро, здатне обробляти ці складні, гетерогенні дані та виявляти в них нелінійні, приховані закономірності. В результаті такі гібридні системи набувають здатності до комплексного, цілісного аналізу програмного коду, одночасно враховуючи як його структурні, так і багатовимірні атрибутивні характеристики.

Пріоритетні напрями досліджень включають розробку методології для оптимального представлення даних та автоматичного вибору декомпозиції, а також вирішення проблеми обчислювальної складності через адаптивні алгоритми для потокової обробки. Актуальним є створення предметно-орієнтованих форматів, формалізація критеріїв якості та інтерпретованості моделей. Практичним результатом має стати розробка формалізованої методології застосування тензорного аналізу, що включає алгоритми вибору декомпозиції та метрики для інтерпретації результатів.

Застосування тензорних методів є потужним інструментом та являє собою значний методологічний прогрес в аналізі складних багатовимірних залежностей, що іманентно притаманні сучасним процесам розробки програмного забезпечення. Ці методи виступають ефективним засобом подолання фундаментальних обмежень, властивих класичним векторно-матричним підходам, які демонструють низьку ефективність при моделюванні систем із великою кількістю взаємопов'язаних параметрів.

Література

1. Dr. Tirumala Haripriya, Dr. Dattatreya P. Mankame, Dr. Basavaraj Patil, Abhijeet Das, Nidhi Jindal, Gauri Jindal. Statistical Learning Methods for Predictive Analytics in Engineering Management.Nanotechnology Perceptions 20 No. S14 (2024) P. 834-847. https://doi.org/10.62441/nano-ntp.vi.2855

2. Di Wang, Yao Zheng, and Guodong Li. High-dimensional low-rank tensor autoregressive time series modeling. Journal of Econometrics, 238(1):105544, 2024. https://doi.org/10.1016/j.jeconom.2023.105544

3. Vineet Bhatt, Sunil Kumar, Seema Saini. Tucker decomposition and applications. International Conference on Technological Advancements in Materials Science and Manufacturing. Volume 46, Part 20, 2021, P. 10787-10792. https://doi.org/10.1016/j.matpr.2021.01.676

4. Pooya Rostami Mazrae, Tom Mens, Mehdi Golzadeh, and Alexandre Decan. 2023.On the usage, co-usage and migration of CI/CD tools: A qualitative analysis. Empirical Software Engineering 28, 2 (2023), 52. https://doi.org/10.1007/s10664-022-10285-5

5. João Faustino , "DevOps Benefits: A Systematic Literature Review," Journal of Software: Practice and Experience, vol. 52, no. 9, 2022, pp. 1905-1926.

УДК 608.4

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Панков Іван Олексійович
здобувач 2 курсу першого (бакалаврського) рівня
спеціальності 123 – Комп'ютерна інженерія
Міжнародний гуманітарний університет
pankovi6287@gmail.com

Черкас Нікіта Сергійович
здобувач 2 курсу першого (бакалаврського) рівня
спеціальності 172 – Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет
nikitacerkas131@gmail.com

Лазарєв Кіріл Олегович
здобувач 3 курсу першого (бакалаврського) рівня
спеціальності 122 – Комп'ютерні науки
Міжнародний гуманітарний університет
lazarevkirill10@gmail.com

ГОНОЧНИЙ РОБОТИЗОВАНИЙ БОЛІД «LINE TRACE CAR»

Анотація. *Розглянуто конструкція та електрична схема гоночного роботизованого боліда «Line Trace Car», розробленого командою «Odesa Racers» на основі мікроконтролера STM8S103F3P6. Особливу увагу приділено апаратній і програмній частині машинки, яка рухається по лінії. Використання оригінальних технічних рішень дозволило зменшити кількість електронних компонентів та зменшити вагу машинки до 70 г, що позитивно позначилось на її швидкісних характеристиках.*

Роботизовані машинки, що їздять по лінії, вже тривалий час користуються популярністю серед молоді, що цікавиться технологіями та інноваціями. Попри свою відносну простоту, ці електромеханічні пристрої з програмним керуванням не лише демонструють сучасні технічні можливості, а й виступають ефективним засобом навчання. Роботи цього типу використовуються для тестування і вдосконалення технологій автономного керування, що може бути застосовано в майбутньому для безпілотних

автомобілів. Вони зацікавлюють молодь науково-технічною сферою та стають невід'ємною частиною STEM-освіти. В цілому, роботизовані машинки, що їздять по лінії, є не лише засобом розваги, а й відіграють значну роль у розвитку сучасних технологій та формуванні майбутніх інженерів і програмістів.

Окремим напрямом у розвитку роботизованих машинок, що їздять по лінії, є реалізація їх у формі гоночних болідів. Це відкриває додаткові можливості для проведення змагань між командами, під час яких учасники створюють апаратну частину та програмне забезпечення для проходження трас різної складності. Це сприяє розвитку навичок програмування, інженерного мислення та розумінню принципів автоматизації. Подібні заходи особливо приваблюють школярів і студентів, які активно беруть участь у конкурсах і змаганнях з робототехніки. Саме такими змаганнями і стала «E-Formula 3.0», фінал якої відбувся у Національному технічному університеті «Дніпровська політехніка» 7 червня 2025 року [1].

Зовнішній вигляд гоночного роботизованого боліду «Line Trace Car» наведено на рис. 1. Корпус боліду створено у формі «Летючого Голландця» (що є другою назвою боліду), який було роздруковано на 3D-принтері.

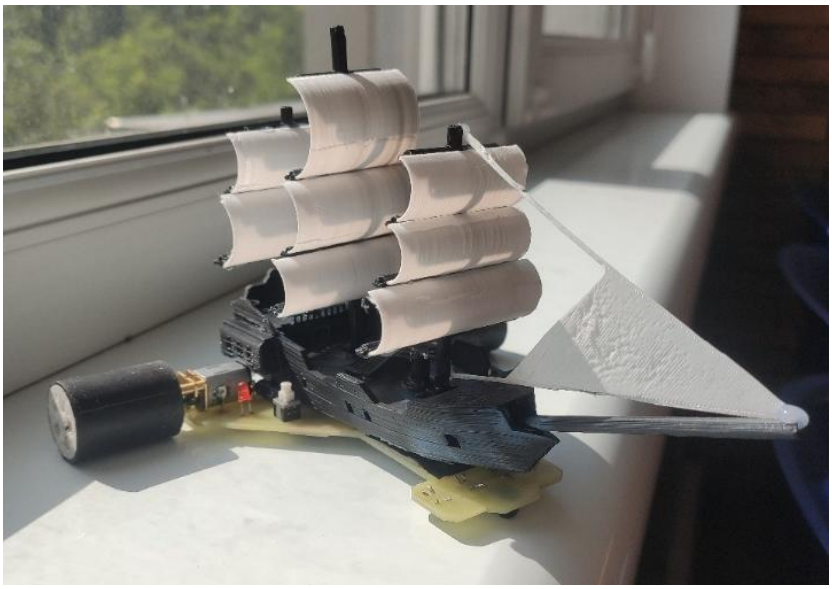


Рисунок 1 – Зовнішній вигляд гоночної роботизованої машинки, що їздять по лінії

Шасі машинки, що одночасно є друкованою платою, виготовлено із одностороннього фольгованого склотекстоліту і зображено на рис. 2. На ньому розташовані двигуни та інші електронні компоненти.

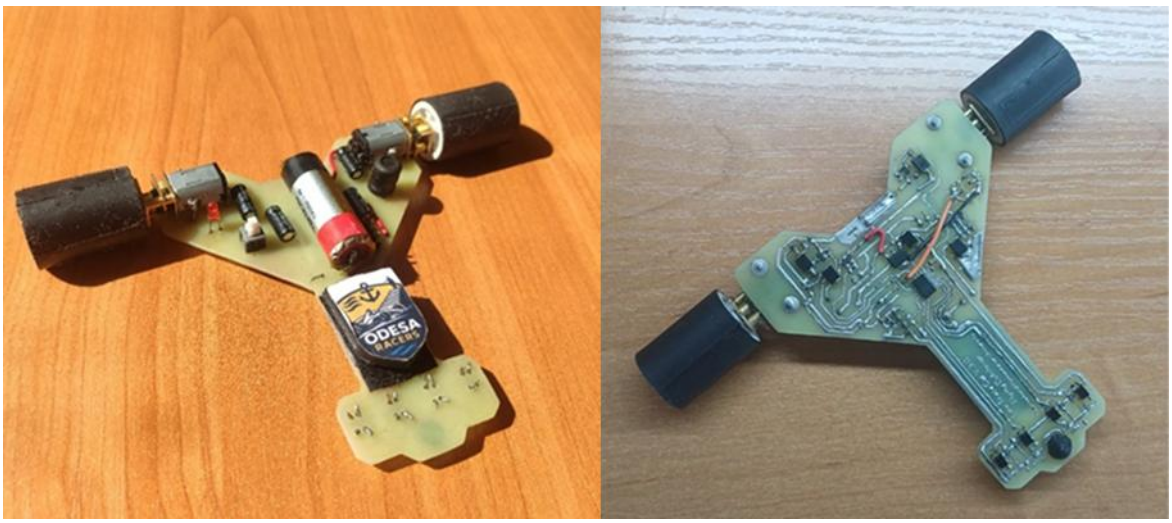


Рисунок 2 – Друкована плата-шасі

У якості двигунів були використані колекторні мікродвигуни із вбудованим редуктором, що при напрузі живлення 6 В забезпечують швидкість обертання 2000 об/хв із номінальним крутним моментом 0,02 кг/см [2]. У якості рушіїв боліда застосовувалися пластикові колеса, виготовлені за допомогою 3D-друку, шини були виготовлені з листової гуми. Передньою точкою опори машинки стала пластикова півсфера, надрукована на 3D-принтері.

Електрична схема плати зображена на рис. 3. У якості датчиків лінії були використані оптопари KTIR0821DS виробництва компанії Kingbright [3]. Вихідна напруга кожної оптопари пропорційна рівню освітленості і тому вона може приймати будь-яке значення в діапазоні від нуля до напруги живлення.

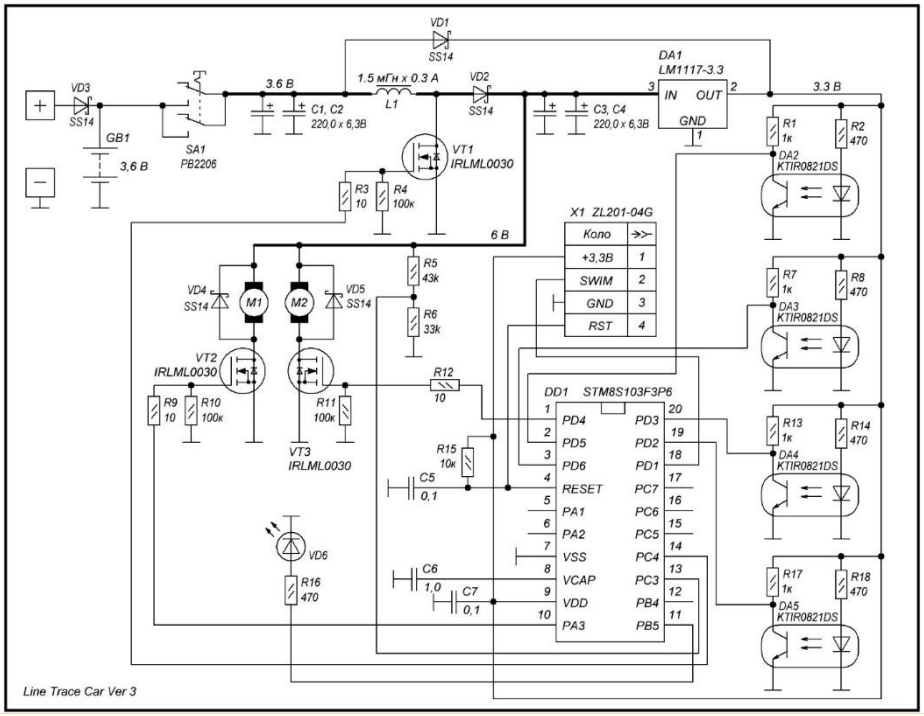


Рисунок 3 – Електрична схема друкованої плати-шасі

Сигнали з виходів оптопар оброблюються мікроконтролером, який здійснює керування всіма вузлами боліда. У гоночному боліді, що розглядається в цій статті, використовується мікроконтролер STM8S103F3P6 [4], розташований безпосередньо на платі.

Керування двигунами здійснюється за допомогою широтно-імпульсної модуляції через два ключі, реалізовані на польових транзисторах із ізольованим затвором IRLML0030 [5].

Живлення машинки відбувається від акумулятора із номінальною напругою 3,6 В. Напруга 6 В, яка необхідна для забезпечення потрібної потужності двигунів, формується за допомогою підвищувального імпульсного перетворювача, утвореного дроселем L1 (1,5 мГн, 0,3 А), транзистором VT1 (IRLML0030) та діодом VD2 (SS14). Особливістю цього рішення є стабілізація вихідної напруги за допомогою програмного забезпечення (цифровий контур керування).Заряд акумулятора відбувається за допомогою зовнішнього зарядного пристрою, який підключається до спеціальних контактних площадок на платі за допомогою роз'ємів типу «Крокодил».

Використання спеціалізованих рішень, зокрема використання спеціалізованої друкованої плати, цифрових контурів керування підвищувальним стабілізатором напруги та відмова від спеціалізованих драйверів керування колекторними двигунами дозволило зменшити кількість електронних компонентів та зменшити вагу боліду до 70 г, що добре позначилось на його швидкісних характеристиках.

Література

1. Фінал змагань «E-Formula 3.0». URL: https://www.facebook.com/share/p/1cnFQPfLds/

2. Мікродвигун з редуктором 6В 2000 RPM. URL: https://www.rcscomponents.kiev.ua /product/minimotor-iz-reduktorom-6vdc-2000-ob-khv-12gan20-10-2000rpm-3-9vdc_185872.html

3. Фототранзистор KTIR0821DS Kingbright. URL: https://www.rcscomponents.kiev.ua/ product/ktir0821ds_78210.html

4. Мікроконтролер STM8S103F3P6 STMicroelectronics. URL: https://www.rcscomponent s.kiev.ua/product/stm8s103f3p6.html

5. Польові транзистори із ізольованим затвором IRLML0030. URL: https://www. rcscomponents.kiev.ua/product/irlml0030trpbf_37076.html

УДК 004.421.2

Григор'єва Т.І., к.т.н., доцент
tig15090808@gmail.com
Салагор В.І., аспірант
Міжнародний гуманітарний університет, місто Одеса

ПРОГНОСТИЧНИЙ МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ ТА ЗБОЇВ У ПРОЦЕСІ ДІАГНОСТИЧНИХ ЕКСПЕРИМЕНТІВ ДЛЯ ВЕРИФІКАЦІЇ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

Анотація. *Розглянуто прогностичний метод виявлення аномалій та збоїв у процесі діагностичних експериментів, що використовуються для верифікації систем критичного призначення. Запропоновано підхід на основі машинного навчання, тензорного аналізу та обробки часових рядів, що дозволяє здійснювати раннє виявлення відхилень у поведінці компонентів системи. Основною метою є забезпечення превентивної діагностики, зменшення ризиків відмови, а також підвищення точності та надійності процесу верифікації. Запропоновано застосування моделей автокодерів, рекурентних нейронних мереж і методів розкладу тензорів для побудови адаптивної системи моніторингу. Отримані результати демонструють високу ефективність запропонованого методу в умовах складної багатокомпонентної діагностики систем критичного призначення.*

Верифікація комп'ютерних систем критичного призначення є необхідною умовою забезпечення їхньої функціональної надійності, особливо в умовах зростання складності архітектур та варіативності середовищ виконання. Одним із найбільш перспективних підходів до виявлення дефектів ще до їх активного прояву є прогностичний метод виявлення аномалій [1], що базується на обробці результатів діагностичних експериментів у реальному або квазіреальному часі.

Сутність прогностичного методу полягає у створенні динамічної моделі поведінки системи, яка формується на основі накопичених спостережень та індикаторів її стану в ході імітаційних або активних діагностичних впливів. На відміну від реактивних методів [2], які фіксують вже наявні збої, прогностичний підхід орієнтований на ідентифікацію трендів, закономірностей та відхилень, що свідчать про потенційне наближення до відмови або нестабільного стану.

У сучасних умовах функціонування технічних та програмно-апаратних систем критичного призначення особливої актуальності набуває проблема своєчасного виявлення аномалій та потенційних збоїв. Зокрема, значну роль відіграє прогностичний аналіз, що дозволяє не лише фіксувати збої постфактум, а й прогнозувати їх на етапі формування. В межах діагностичних експериментів така прогностична модель забезпечує превентивну верифікацію поведінки систем, мінімізуючи ризики зниження надійності та функціональної деградації.

Основу побудови прогностичної моделі становить обробка масивів даних, отриманих під час експериментального моніторингу, включаючи телеметричні параметри, структурні логі файли, записи про помилки, сигнали від сенсорів тощо. Одним із ключових підходів є застосування машинного навчання, зокрема моделей глибокого навчання, що дозволяють виявляти приховані закономірності в часових рядів, багатовимірних масивах та контекстуальних зв'язках між компонентами системи. Автокодери, згорткові нейронні мережі, рекурентні моделі LSTM забезпечують формування репрезентативних ознак нормального функціонування, відхилення від яких можуть інтерпретуватись як сигнали потенційної несправності.

Поряд із нейронними підходами активно застосовуються статистичні методи, такі як аналіз дисперсії, кореляційний аналіз, виявлення викидів за допомогою методу меж (threshold-based detection) та байєсівські моделі. Особливу увагу приділяється побудові моделей часової динаміки, які з використанням архітектур ARIMA або нейронних послідовних моделей дозволяють прогнозувати зміну параметрів системи та встановлювати критичні точки переходу до потенційної аномалії.

Додатково високоефективним є використання тензорного аналізу, що дозволяє моделювати системи у вигляді багатовимірних структур. Методи CP-розкладу та розкладу Такера [3] забезпечують зменшення розмірності даних та виділення факторів, пов'язаних із поведінкою елементів системи у часі та просторі. Такий підхід є надзвичайно продуктивним для систем з багатьма вхідними каналами діагностики, де тензорна репрезентація дозволяє виявити крос-канальні взаємозв'язки та синхронні відхилення параметрів, що не виявляються при класичному аналізі.

Критичним етапом є верифікація прогностичних моделей у режимі реальних або змодельованих діагностичних експериментів. Це дозволяє оцінити рівень точності, чутливості та специфічності побудованої моделі, а також адаптувати її до нових умов роботи. Гібридні моделі, що поєднують правила логічного виведення з машинним навчанням, забезпечують додаткову інтерпретованість результатів, що є важливим для систем безпеки, де необхідно не тільки фіксувати збій, а й аргументовано пояснювати його причину.

Таким чином, прогностичний метод виявлення аномалій і збоїв у процесі діагностичних експериментів є ключовим інструментом підвищення надійності та стабільності систем критичного призначення. Застосування нейромережевих, статистичних та тензорних методів у поєднанні з сучасними алгоритмами обробки даних створює

можливості для адаптивного й превентивного моніторингу, що відповідає вимогам індустріального стандарту цифрової трансформації критичних систем.

У рамках реалізації методу система спостереження формує багатовимірний часовий ряд параметрів: $\mathrm{X(t)} = \{x_1(\mathrm{t}), x_2(\mathrm{t}), \ldots, x_n(\mathrm{t})\}$, де x_i (t) – значення *i*-ої контрольної змінної у момент часу *t*. Змінні можуть включати навантаження на процесор, затримку обробки запитів, частоту відмов, кількість повторних спроб виконання, стан буферів, параметри мережі тощо. Побудову прогностичної моделі можна здійснити за допомогою методів регресійного аналізу або рекурентних нейронних мереж (наприклад, LSTM), які дозволяють враховувати як довгострокову залежність між подіями, так і короткотермінові відхилення. Прогностичну функцію ризику для визначення порогу ризику представимо у вигляді: $R(t) = \| X(t) - \hat{X}(t) \|$, де $\hat{X}(t)$ – реконструкція моделі. Порівняння прогнозованого значення з пороговим значенням дозволяє активувати попереджувальні дії, наприклад, запуск додаткового тестування; перезапуск підозрілих модулів; ізоляцію вузлів, що поводяться атипово; формування діагностичного звіту для оператора.

Забезпечення превентивної діагностики, зменшення ризиків відмови та підвищення точності й надійності процесу верифікації є ключовими пріоритетами в розробці та експлуатації систем критичного призначення. Превентивна діагностика дозволяє виявляти відхилення від нормальної поведінки системи на ранніх етапах, що сприяє своєчасному втручанню та усуненню потенційних причин збоїв. Це особливо важливо для високонавантажених та безпекових систем, де навіть незначна несправність може призвести до серйозних наслідків.

Зменшення ризиків відмови досягається шляхом інтеграції методів машинного навчання, багатоканального моніторингу параметрів та побудови прогностичних моделей. Такі моделі аналізують динаміку даних у режимі реального часу, формують оцінку ризику та ініціюють процеси локалізації проблем при перевищенні критичних порогів. Це дозволяє скоротити час реагування та підвищити стійкість системи до несподіваних впливів.

Точність і надійність процесу верифікації забезпечуються завдяки використанню гібридних підходів, які поєднують статистичні алгоритми, нейромережеві моделі та логічне виведення. Верифікація охоплює не тільки підтвердження відповідності вимогам, але й тестування в умовах моделювання збоїв, що надає змогу оцінити поведінку системи під навантаженням. Таке поєднання технологій підвищує рівень довіри до результатів діагностики та сприяє побудові стійкої архітектури безпеки в системах критичного призначення.

Прогностичний метод також може використовувати профілі латентної поведінки, які формуються на основі історичних даних про раніше виявлені дефекти. За допомогою машинного навчання ці профілі можна співвідносити з поточним станом системи, дозволяючи розпізнавати неочевидні ознаки майбутньої нестабільності.

Таким чином, запропонований прогностичний метод виявлення аномалій і збоїв у процесі діагностичних експериментів забезпечує високу чутливість до змін у поведінці системи, дозволяє здійснювати ранню індикацію потенційних проблем і знижує ймовірність виникнення відмов у критичних умовах. Метод доцільно інтегрувати в модулі моніторингу систем критичного призначення та використовувати як частину комплексної верифікаційної інфраструктури.

Література

1. Xianguang Jia, Jie Qu, Yingying Lyu, Mengyi Guo, Jinke Zhang, Fengxiang Guo, A Prediction-Based Anomaly Detection Method for Traffic Flow Data with Multi-Domain Feature Extraction. Appl. Sci. 2025, 15(6), 3234. https://doi.org/10.3390/app15063234

2. Henzinger, T.A. Quantitative reactive modeling and verification. Comput Sci Res Dev 28, 331–344 (2013). https://doi.org/10.1007/s00450-013-0251-7

3. Sedighin, F.; Cichocki, A. Image completion in embedded space using multistage tensor ring decomposition. Frontiers in Artificial Intelligence 2021, 4, 687176. https://doi.org/10.3389/frai.2021.687176

УДК 372.862

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Крупецький Кирило Андрійович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 123 Комп'ютерна інженерія
Міжнародний гуманітарний університет

Панков Іван Олексійович
здобувач 2 курсу першого (бакалаврського) рівня
зі спеціальності 123 Комп'ютерна інженерія
Міжнародний гуманітарний університет

ВИКОРИСТАННЯ ЦИФРОВИХ КОНТУРІВ КЕРУВАННЯ В ІМПУЛЬСНИХ ПЕРЕТВОРЮВАЧАХ НАПРУГИ КОМП'ЮТЕРНОГО ОБЛАДНАННЯ

Анотація. *Розглянуто особливості використання цифрових контурів керування в імпульсних перетворювачах напруги, які застосовуються в сучасному комп'ютерному обладнанні, зокрема у пристроях Інтернету речей та робототехнічних системах. Показано, що цифрове керування на базі мікроконтролерів загального призначення дає змогу зменшити кількість електронних компонентів, знизити габарити пристроїв і забезпечити гнучкість алгоритмів стабілізації. Наведено приклад практичної реалізації підвищувального перетворювача з цифровим керуванням без використання окремої мікросхеми контролера.*

Імпульсні перетворювачі напруги є критично важливою складовою сучасного комп'ютерного обладнання, забезпечуючи стабільне живлення його вузлів, блоків та систем. Їхня висока енергоефективність, компактність і здатність до швидкого реагування на коливання енергоспоживання в колах навантаження роблять їх незамінними в системах живлення персональних комп'ютерів, серверів, пристроїв Інтернету речей, елементів робототехнічних систем і вбудованої електроніки.

До недавнього часу контури керування імпульсними перетворювачами напруги будувалися виключно на основі спеціалізованих мікросхем-контролерів. Типовий контролер імпульсного перетворювача містить генератор пилкоподібної (лінійно наростаючої) напруги, що задає частоту роботи силової частини, та широтно-імпульсний модулятор (ШІМ), який порівнює пилкоподібний сигнал із напругою помилки (рис. 1) [1]. Остання формується підсилювачем помилки на основі різниці між вихідною напругою перетворювача та заздалегідь відомою – опорною напругою V_{REF}. На виході ШІМ-модулятора формується імпульсний сигнал керування силовим ключем, який має постійну частоту та змінну тривалість імпульсів, що дозволяє корегувати енергетичні процеси та стабілізувати вихідну напругу при зміні навантаження або параметрів живлення.

Використання спеціалізованих мікросхем-контролерів у схемах керування імпульсними перетворювачами має низку переваг, серед яких висока надійність, передбачувана поведінка та швидка інтеграція в комп'ютерне обладнання. Такі мікросхеми

забезпечують стабільну роботу в широкому діапазоні робочих умов. Водночас наявність окремої мікросхеми для керування збільшує габарити друкованої плати, підвищує загальну складність пристрою та спричиняє додаткові витрати на закупівлю і виробництво. У компактних пристроях, таких як модулі IoT або мобільна техніка, критично важливо зменшити розміри, вагу й енергоспоживання системи, що змушує розробників комп'ютерного обладнання шукати шляхи для вирішення цієї проблеми.

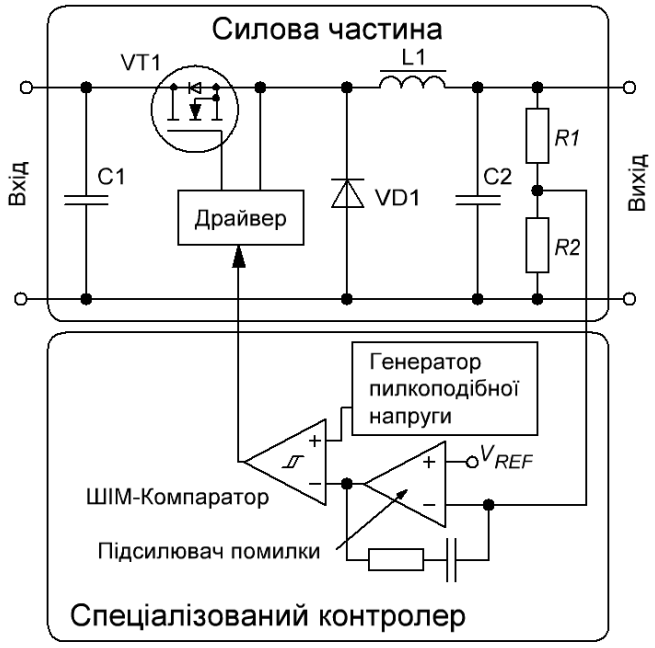


Рисунок 1 – Керування перетворювачем за допомогою спеціалізованих контролерів

Одним із способів зменшення апаратної складності, розмірів та вартості комп'ютерного обладнання є використання цифрових контурів, коли керування силовою частиною імпульсного перетворювача здійснюється за допомогою мікроконтролерів загального призначення [2, 3]. У більшості випадків мікроконтролер вже входить до складу комп'ютерного або вбудованого обладнання як центральний елемент керування, і мікроконтролер зазвичай має вільні ресурси процесорного часу, які можуть бути використані для реалізації функцій стабілізації вихідної напруги без шкоди для основних задач пристрою. Крім того, сучасні мікроконтролери містять апаратні модулі формування широтно-імпульсної модуляції, компаратори та аналого-цифрові перетворювачі (АЦП), що дає змогу реалізувати майже всі функції апаратного контролера програмно. Завдяки цьому для побудови цифрового контуру стабілізації напруги достатньо лише кількох додаткових електронних компонентів, а основна складність реалізації зводиться до розробки спеціалізованого програмного забезпечення, адаптованого до архітектури мікроконтролера.

При використанні цифрових контурів керування сигнал, пропорційний вихідній напрузі, подається на вхід АЦП мікроконтролера, за допомогою якого значення напруги вводиться в програмне середовище (рис. 2). Подальша обробка інформації про вихідну напругу, включно з порівнянням із опорною напругою, фільтрацією та розрахунком сигналу керування, виконується програмним шляхом у реальному часі. Як джерела опорної напруги можуть бути задіяні внутрішні вузли самого мікроконтролера, зокрема вбудовані джерела опорної напруги або компенсаційні стабілізатори. Формування вихідного сигналу здійснюється за допомогою апаратних таймерів загального призначення, більшість з яких дають змогу генерувати ШІМ-сигнал апаратним шляхом з мінімальними витратами процесорного часу. Таким чином, основним завданням програмного забезпечення є визначення необхідної тривалості імпульсу ШІМ-сигналу відповідно до поточного значення вихідної напруги.

Таким чином, використання цифрових контурів керування в імпульсних перетворювачах напруги має низку переваг порівняно з традиційними аналоговими схемами. Програмна реалізація алгоритмів керування забезпечує гнучкість і можливість швидкої адаптації до змін вимог або умов експлуатації без необхідності втручання в апаратну частину. Крім того, цифрові контури можуть реалізовувати складні методи фільтрації, компенсації або діагностики, які практично неможливо реалізувати в аналогових схемах без суттєвого ускладнення конструкції.

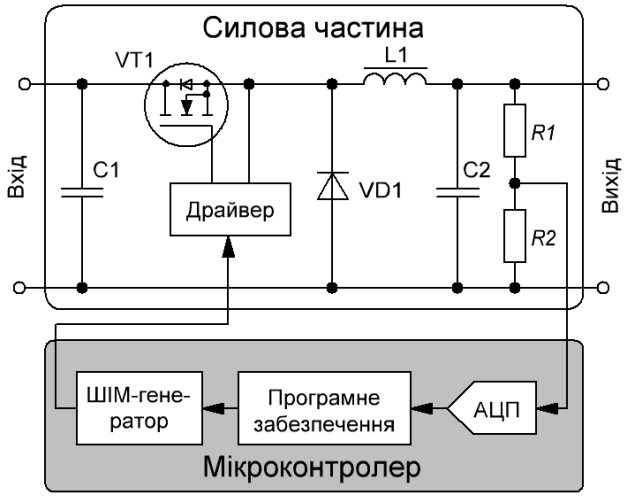


Рисунок 2 – Керування перетворювачем за допомогою цифрового контуру керування

Один із прикладів практичного використання цифрових контурів керування імпульсними перетворювачами напруги наведено на рис. 3. У цьому прикладі імпульсний підвищувальний перетворювач використовується для живлення двигунів комп'ютеризованої машинки, яка рухається по лінії. Силова частина імпульсного перетворювача, що збільшує напругу з 3,6 В до 6 В, утворена дроселем L1, транзистором VT1, діодом VD1 та конденсаторами C1–C4. Сигнал зворотного зв'язку, пропорційний вихідній напрузі, подається на вивід 13 мікроконтролера DD1 (STM8S003F3P6), з'єднаний з одним із входів АЦП. Після програмної обробки оцифрованого значення вихідного сигналу відбувається налаштування таймера, що має функцію генерації ШІМ-сигналів, вихід якого підключений до виводу 13 мікроконтролера DD1. Таким чином, керування силовою частиною імпульсного перетворювача фактично зводиться до розрахунку тривалості імпульсу керування транзистором VT1 на основі фактичної величини вихідної напруги.

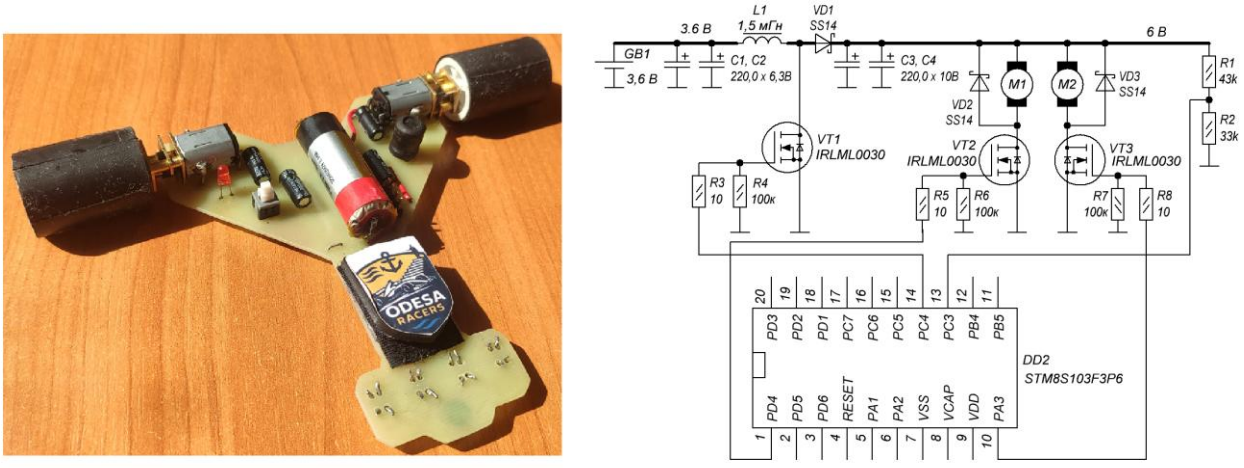


Рисунок 3 – Приклад використання цифрового контуру керування імпульсним підвищувальним перетворювачем

У наведеному прикладі для реалізації керування імпульсним перетворювачем не використовується окрема мікросхема контролера, оскільки всі необхідні функції виконує вже наявний у системі мікроконтролер. Це дозволяє суттєво зменшити кількість електронних компонентів, знизити складність друкованої плати та мінімізувати габарити пристрою, що є особливо важливим для компактних мобільних платформ, таких як роботизовані машинки.

Висновки. Цифрові контури керування в імпульсних перетворювачах напруги відкривають нові можливості для проєктування енергоефективного, компактного й функціонально гнучкого комп'ютерного обладнання. Завдяки використанню ресурсів уже наявного в системі мікроконтролера цифрове керування дає змогу відмовитися від додаткових спеціалізованих мікросхем, що позитивно впливає на зменшення апаратної складності, вартості та розмірів кінцевого пристрою. Програмна реалізація алгоритмів стабілізації вихідної напруги забезпечує високу адаптивність до змін умов навантаження і живлення, а також спрощує модернізацію пристрою за рахунок оновлення програмного забезпечення. Сучасні мікроконтролери містять усі необхідні апаратні засоби — аналогово-цифрові перетворювачі, таймери з підтримкою ШІМ, внутрішні джерела опорної напруги, — що робить цифровий контур повноцінною заміною традиційному аналоговому керуванню без втрати стабільності або швидкодії. Наведений приклад із роботизованою платформою демонструє ефективність такого підходу для мініатюрних пристроїв, де критично важливими є габарити, маса й енергоспоживання.

Література

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

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

3. Raymond G. Jacquot Modern Digital Control Systems. Routledge, 2019. 432p.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Ковальчук Д. А.
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
Науковий керівник: Йона Л. Г.
Міжнародний гуманітарний університет м. Одеса, Україна

БЛОКЧЕЙН-ТЕХНОЛОГІЇ ТА ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА НЕЗМІННОСТІ ДАНИХ

У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів даних забезпечення їхньої цілісності та незмінності стає одним із ключових аспектів кібербезпеки. Традиційні централізовані моделі зберігання інформації дедалі частіше виявляються вразливими до несанкціонованих змін, втрат або підробок даних. Це особливо критично для сфер, де дані мають правову або фінансову значущість: державні реєстри, банківські транзакції, медичні записи, ланцюги постачання.

У цьому контексті блокчейн-технології привертають значну увагу як інноваційний інструмент, що дозволяє створювати розподілені, прозорі та стійкі до фальсифікації системи зберігання даних. Завдяки використанню криптографічних алгоритмів і механізмів консенсусу, блокчейн забезпечує незмінність даних та їх перевірюваність протягом усього життєвого циклу.

Разом із тим, попри високий потенціал, впровадження блокчейн-рішень супроводжується низкою технологічних, організаційних і нормативних викликів. Таким чином, аналіз блокчейн-технологій з позиції кібербезпеки та захисту інформації є важливим кроком для формування нових підходів до гарантування цілісності, автентичності та прозорості даних у цифрову епоху.

Мета дослідження

Метою даного дослідження є всебічний аналіз потенціалу використання блокчейн-технологій як інструменту підвищення рівня кібербезпеки шляхом забезпечення цілісності, незмінності та достовірності даних у різних сферах діяльності.

Дослідження передбачає:

- розкриття ключових механізмів, за допомогою яких блокчейн гарантує захист інформації від несанкціонованих змін;
- визначення практичних переваг і недоліків впровадження блокчейн-рішень у системи, що потребують високого рівня інформаційної безпеки;
- аналіз типових викликів і обмежень (масштабованість, конфіденційність, юридичні аспекти);
- окреслення перспектив розвитку блокчейн-технологій у контексті сучасних кіберзагроз.

Отримані результати мають сприяти пошуку ефективних підходів до інтеграції блокчейн-технологій у існуючі системи захисту інформації та формуванню рекомендацій для їх подальшого наукового та практичного використання.

Механізми забезпечення цілісності та незмінності даних

Ключовою особливістю блокчейн-технологій, що робить їх перспективними у сфері кібербезпеки, є принципова архітектура з використанням розподіленого реєстру та криптографічних механізмів. Ці механізми дозволяють гарантувати цілісність та незмінність інформації навіть у разі спроби несанкціонованого втручання.

Основні елементи забезпечення цілісності включають:

- **Розподілений реєстр (Distributed Ledger):** усі учасники мережі зберігають однакові копії реєстру, що унеможливлює централізовану модифікацію або підробку даних без згоди більшості.
- **Консенсус-алгоритми (Proof of Work, Proof of Stake тощо):** забезпечують погодження між усіма учасниками щодо легітимності записів у реєстрі. Відсутність єдиної точки відмови підвищує стійкість до атак.
- **Криптографічні хеш-функції:** кожен блок містить хеш попереднього, що забезпечує ланцюговий захист. Зміна навіть одного байта даних призведе до зміни всіх наступних хешів, що миттєво виявляється.
- **Цифрові підписи та шифрування:** автентифікація транзакцій і прав доступу здійснюється на основі криптографічних ключів, що мінімізує ризик підробки або підміни даних.
- **Smart Contracts:** забезпечують автоматизацію виконання умовних операцій і перевірок, що знижує людський фактор і ризик маніпуляцій.

Поєднання цих елементів дозволяє реалізувати концепцію «середовища недовіри» (trustless environment), де учасники можуть взаємодіяти без необхідності централізованого посередника, що особливо важливо для підвищення рівня захисту критично важливої інформації.

Приклади використання

Блокчейн-технології вже знаходять практичне застосування у різних галузях, де критично важливо гарантувати цілісність, незмінність та прозорість даних. Одним із ключових аспектів їхнього використання є мінімізація ризиків шахрайства та корупційних схем шляхом створення середовища, де кожен запис є публічним, перевірюваним і незмінним.

Серед найпоширеніших прикладів можна виділити:

- **Державні реєстри та електронне урядування:** блокчейн може забезпечити прозорість ведення земельних кадастрів, реєстрів власності чи реєстрації бізнесу. Незмінність записів унеможливлює несанкціоновані виправлення чи фальсифікацію документів, що є важливим для протидії корупції у державному секторі.
- **Електронне голосування:** використання блокчейну для фіксації голосів виборців гарантує їх достовірність, унеможливлює подвійне голосування та фальсифікацію результатів.
- **Ланцюги постачання (supply chain):** завдяки блокчейну можна відстежувати походження товарів на кожному етапі логістики. Це мінімізує ризики підміни товарів, контрабанди або шахрайських схем.

- **Медична сфера:** забезпечення цілісності медичних записів пацієнтів і контроль доступу до них сприяє захисту конфіденційних даних і запобігає їхньому несанкціонованому редагуванню.
- **Антикорупційні ініціативи:** децентралізоване зберігання контрактів, тендерних процедур чи бюджетних витрат дозволяє забезпечити громадський контроль і зменшує можливості для маніпуляцій.

Таким чином, блокчейн-технології розглядаються не лише як технічне рішення для захисту інформації, а й як важливий інструмент підвищення прозорості та довіри до даних у сферах, де проблема корупції є системною.

Сучасні виклики та обмеження

Незважаючи на високий потенціал блокчейн-технологій у підвищенні рівня кібербезпеки та протидії корупції, їхнє впровадження супроводжується низкою суттєвих викликів і обмежень.

По-перше, однією з ключових проблем залишається масштабованість і продуктивність. Поширені механізми консенсусу (зокрема Proof of Work) забезпечують високу стійкість до атак, але потребують значних обчислювальних ресурсів та енергії, що робить такі системи дорогими та малоефективними для великих обсягів транзакцій.

По-друге, блокчейн за своєю природою забезпечує прозорість і публічність записів, що створює конфлікт між незмінністю даних і конфіденційністю. Для сфери захисту інформації це виклик, адже необхідно балансувати між відкритістю транзакцій та дотриманням вимог законодавства щодо захисту персональних даних.

По-третє, впровадження блокчейн-рішень у реальні бізнес-процеси стикається з організаційними та нормативно-правовими бар'єрами. Багато країн досі не мають чіткої регуляторної бази щодо використання технології розподіленого реєстру, що ускладнює її інтеграцію у державні системи та процеси, зокрема антикорупційні інструменти.

По-четверте, існують ризики, пов'язані з людським фактором та якістю початкових даних. Навіть якщо блокчейн гарантує незмінність записів, він не може забезпечити достовірність інформації, якщо вона була введена неправильно або зловмисно (проблема «сміття на вході» — garbage in, garbage out).

Крім того, для підтримки дійсно високого рівня кібербезпеки необхідно враховувати питання управління приватними ключами та захисту кінцевих точок. Компрометація ключа користувача або адміністратора може звести нанівець всі переваги блокчейн-архітектури.

Таким чином, використання блокчейну у сфері захисту інформації потребує комплексного підходу, що поєднує технологічні, організаційні та правові заходи для мінімізації потенційних ризиків і повної реалізації переваг технології.

Висновок

Блокчейн-технології демонструють високий потенціал як інструмент забезпечення цілісності, незмінності та прозорості даних у різних сферах, де питання кібербезпеки та захисту інформації є критично важливими. Завдяки використанню механізмів розподіленого реєстру, криптографії та консенсусу блокчейн здатен істотно знизити ризики несанкціонованих змін і підробок даних, а також мінімізувати прояви корупційних схем у публічних і приватних процесах.

Разом із тим впровадження блокчейн-рішень не позбавлене викликів, зокрема проблем масштабованості, конфіденційності, регуляторних невизначеностей та людського фактора. Це підкреслює необхідність комплексного підходу, що має включати не лише технічні рішення, а й чітке правове регулювання, організаційні заходи та підвищення компетенцій користувачів.

Подальші дослідження у цьому напрямі мають бути зосереджені на поєднанні блокчейн-технологій з іншими інноваційними інструментами кіберзахисту — такими як штучний інтелект чи інтернет речей — для підвищення ефективності систем контролю даних і мінімізації ризиків. У довгостроковій перспективі це сприятиме зміцненню довіри до цифрових екосистем, зростанню прозорості процесів і посиленню кіберстійкості суспільства в цілому.

Література

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
2. Swan M. Blockchain: Blueprint for a New Economy. 2015.
3. Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. Where Is Current Research on Blockchain Technology? A Systematic Review. 2016.

Головатюк К.В.
студент факультету Кібербезпека, спеціальність 125
Міжнародний гуманітарний університет
kostya93.06@gmail.com
Науковий керівник Йона Л.Г.

ФІШИНГ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ

Анотація. *Розглядається фішинг як одна з найпоширеніших і найнебезпечніших кіберзагроз сучасності, зокрема в контексті гібридної війни проти України. Аналізуються різновиди атак — spear-phishing, фармінг, вішинг — та їх цілі: викрадення даних, інфікування пристроїв, маніпуляція користувачем. Підкреслюється роль соціальних мереж у поширенні фішингових схем, а також економічна зацікавленість зловмисників. Окремо надано рекомендації для захисту користувачів і приклади дій українських кіберфахівців у виявленні та блокуванні фішингових ресурсів.*

У сучасному світі кіберзагроз фішинг вийшов на одне з перших місць за масштабами та наслідками. Це форма атаки соціальної інженерії, коли зловмисники вводять жертву в оману з метою викрадення даних або інфікування пристроїв шкідливим ПЗ. Зазвичай використовується електронна пошта, фальшиві сайти, повідомлення у месенджерах або навіть телефонні дзвінки.

Цей тип атаки побудований не лише на технічних уразливостях, а й на психологічному впливі. Атакуючі ретельно імітують комунікацію з надійним джерелом — банком, державною установою або знайомим контактом — аби викликати довіру та змусити користувача вчинити певну дію: перейти за посиланням, ввести паролі або завантажити заражений файл. Фішинг часто є першим етапом більш складної атаки, яка може завершитися повним контролем над пристроєм жертви або мережею організації.

Особливу небезпеку фішинг несе в умовах гібридної війни проти України, коли атаки націлені не лише на громадян, а й на інститути державної влади, критичну інфраструктуру, медіа та навіть благодійні організації [3].

У таких випадках фішинг є частиною цілеспрямованої інформаційно-психологічної операції, яка має на меті дестабілізувати суспільство, зірвати функціонування важливих державних механізмів або скомпрометувати осіб, дотичних до військових чи урядових процесів. Саме тому державні структури в Україні щодня фіксують сотні подібних атак, спрямованих на поширення дезінформації, крадіжку даних або зрив роботи критичних систем.

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) [2], [3].

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 [1].

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.

Фішинг — це не просто технічний виклик, а глибоко психологічна та соціальна загроза, що базується на довірі, неуважності або стресі. В умовах гібридної війни він перетворюється на ефективну зброю в руках супротивника, здатну паралізувати роботу цілих установ чи підрозділів. Успішна протидія цій загрозі можлива лише за умов поєднання технологічних рішень (фільтрів, антивірусів, моніторингових систем) та людського чинника — навчання, пильності, обізнаності. 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.

Література:

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

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

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

4. Аналітичний звіт з питань кібербезпеки в Україні: загрози та протидія. – ХНТУ, 2024. – С. 330–345.

УДК: 004.056 : 004.4

Царенко Євгеній Валентинович
Здобувач другого (магістерського) рівня вищої освіти факультету кібербезпеки, програмної інженерії та комп'ютерних наук, спеціальність «Кібербезпека та захист інформації»
Міжнародний Гуманітарний Університет
i.am.zhenya.tsarenko@gmail.com
Науковий керівник
Йона Лариса Григорівна
к.т.н., доцент

Міжнародний гуманітарний університет
yonalarisa66@gmail.com

ВПЛИВ МІКРОСЕРВІСНОЇ ТА МОНОЛІТНОЇ АРХІТЕКТУРИ НА КІБЕРБЕЗПЕКУ СУЧАСНИХ ДОДАТКІВ

Анотація. *У роботі розглядається вплив вибору архітектурного підходу - монолітного або мікросервісного на кібербезпеку сучасних програмних систем. Проаналізовано ключові відмінності між цими моделями з точки зору захисту даних, контролю доступу, вразливостей та засобів безпеки. Увага приділяється практикам, таким як використання JWT, API Gateway та secrets management, що дозволяють знизити ризики незалежно від обраної архітектури. У висновках підкреслюється необхідність інтеграції безпекових рішень на етапі проєктування архітектури, адже саме від неї значною мірою залежить стійкість додатка до кіберзагроз.*

У сучасній розробці програмного забезпечення дедалі частіше постає вибір між монолітною та мікросервісною архітектурою. Монолітна модель передбачає створення єдиної цілісної системи, тоді як мікросервіси розділяють додаток на незалежні модулі, кожен з яких виконує окрему функцію. Вибір між цими підходами впливає не лише на гнучкість і масштабованість системи, а й на її захищеність. Кібербезпека відіграє ключову роль у забезпеченні стійкості додатків до атак: архітектурні рішення визначають площу атаки, шляхи доступу, способи автентифікації та захисту даних.

Якісні архітектурні рішення сприяють кібербезпеці через впровадження таких принципів як розмежування доступу, шифрування даних та багатошаровий захист. Вдала архітектура також допомагає усувати вразливості завдяки спрощенню тестування. [1]

Наприклад, у класичній веб-програмі з монолітною структурою реалізація механізму єдиної автентифікації (Single Sign-On) можлива централізовано, через єдину точку обробки запитів. Це знижує ризик розбіжностей у логіці контролю доступу та полегшує аудит безпеки. На Рис. 1 представлено приклад монолітної архітектури.

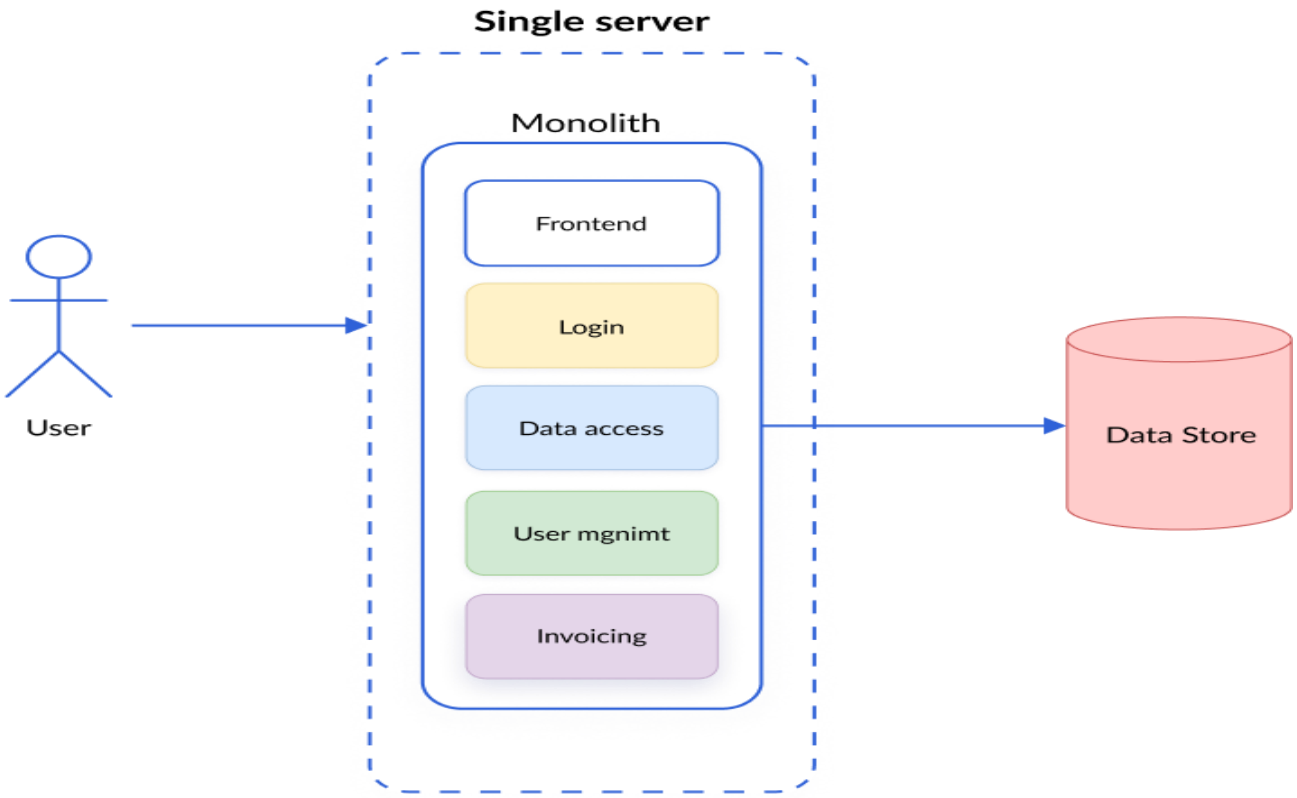


Рисунок 1 – Приклад монолітної архітектури

У мікросервісних системах збільшується кількість взаємодій між сервісами, що потребує додаткових зусиль для забезпечення автентифікації, авторизації, шифрування трафіку й моніторингу безпеки на міжсервісному рівні.

Безпека більше не може бути другорядною, коли справа стосується проектування програмного забезпечення. Кожен розробник повинен дивитися свій код через призму кібербезпеки. Жодна з архітектур не ідеальна, але розробники повинні зважити їхні переваги та недоліки, щоб забезпечити безпеку застосування [3].

В мікросервісній архітектурі одна з головних причин, чому виникають проблеми з безпекою, полягає в тому, що вона має більш складну структуру порівняно з традиційними монолітними програмами. У монолітних програмах усі компоненти знаходяться в одній кодовій базі та зазвичай працюють на одному сервері. Це полегшує впровадження заходів безпеки в центральній точці. Однак у мікросервісах кожна служба розробляється, розгортається та масштабується незалежно. Це означає, що кожна служба має власні вимоги до безпеки та має бути захищена окремо [2]. На Рис. 2 представлено приклад мікросервісної архітектури.

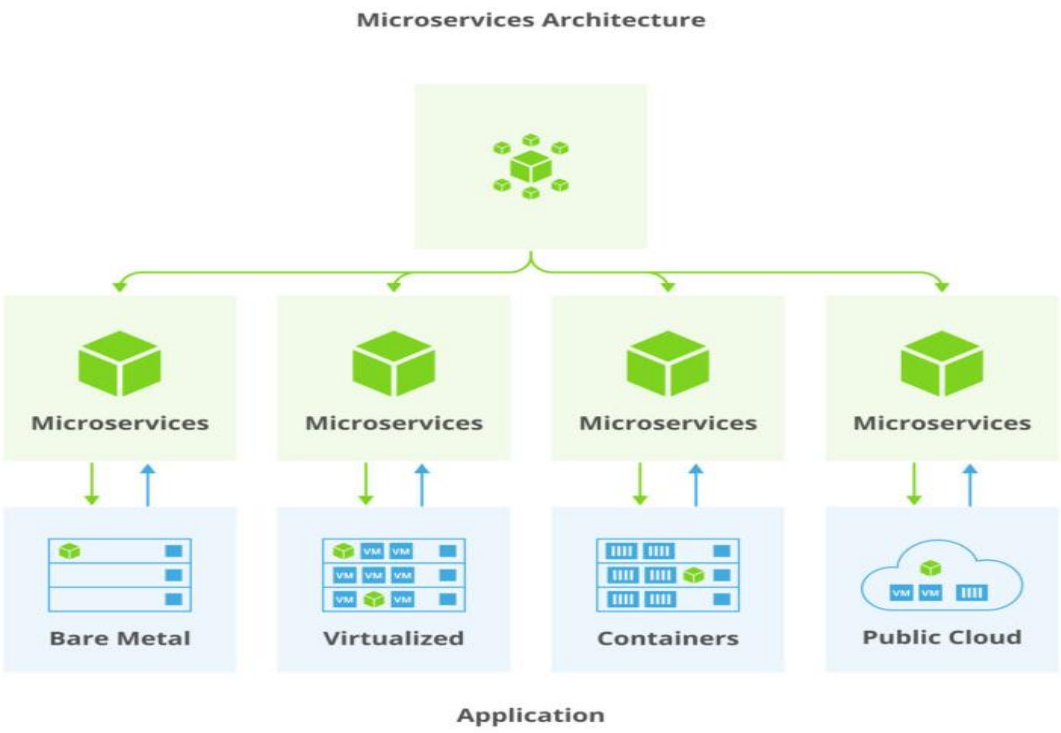


Рисунок 2 – Приклад мікросервісної архітектури

Відтак перевірка безпеки програмного забезпечення стає в розробці пріоритетом №1. Сьогодні добре продумана архітектура має бути відповіддю на загрози кібербезпеки. Вдалі патерни проєктування можуть мінімізувати вразливість системи, забезпечити захист даних та гарантувати надійність роботи ПЗ [1].

Приклади захисту додатків при різній архітектурі:

1) Використання JWT (JSON Web Tokens).

Алгоритм роботи передбачає, що один сервіс (auth) видає підписаний токен, а інші сервіси перевіряють його без звернення до auth.

У мікросервісній архітектурі JWT дозволяє безпечно передавати підтвердження ідентичності між сервісами без централізованого зберігання сесій.

2) API Gateway як захисний бар'єр.

Призначення:

— Аутентифікація та авторизація запитів
— Трафік-фільтрація (rate limiting, IP whitelist/blacklist)
— Захист від типових атак (наприклад, brute-force)

API Gateway — це перший рівень захисту мікросервісної архітектури, що знижує ризик прямого доступу до внутрішніх сервісів.

3) Secrets Management (Vault, AWS Secrets Manager)

Застосовується у CI/CD, при з'єднанні з БД, API

Призначенням є забезпечення безпечного зберігання токенів, паролів, ключів та ротація ключів без зміни коду.

Централізоване управління секретами допомагає уникнути витоку критичних даних з коду чи середовища.

Вибір між монолітною та мікросервісною архітектурою повинен враховувати не лише технічні та бізнесові потреби, а й потенційні ризики для кібербезпеки. Моноліт забезпечує

централізований контроль і меншу кількість точок входу, але вразливість в одній частині може поставити під загрозу всю систему. Натомість мікросервіси дають гнучкість та ізоляцію компонентів, проте вимагають ретельного підходу до захисту міжсервісної комунікації, автентифікації та моніторингу. У результаті, ефективна безпека додатку значною мірою залежить від правильного балансу між архітектурним підходом і впровадженими механізмами захисту.

Література:

1. Архітектура програмного забезпечення: як правильне проєктування забезпечує ефективність та безпеку. Березень 2025 року. [Електронний ресурс] URL: https://wezom.com.ua/ua/blog/arhitektura-programnogo-zabezpechennya (дата звернення 30.06.2025)

2. The Importance of Microservices Architecture and Security Challenges. Березень 2025 року. [Електронний ресурс] URL: https://www.hostragons.com/en/blog/security-challenges-in-microservices-architecture (дата звернення: 30.06.2025).

3. Microservices vs. Monoliths: Why Every Developer Must Also Be a Cybersecurity Professional. Березень 2023 року. [Електронний ресурс] URL: https://vfunction.com/blog/microservices-vs-monoliths-why-every-developer-must-be-cybersecurity-professional (дата звернення: 30.06.2025).

Пахолюк Олег Ігорович

Аспірант, спеціальність 125 «Кібербезпека та захист інформації»,

Науковий керівник

Йона Лариса Григорівна, к.т.н., доцент

Міжнародний гуманітарний університет

yonalarisa66@gmail.com

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ОПТИМІЗАЦІЇ ПРОЦЕДУР ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

***Анотація**. У статті запропоновано підхід до виявлення вразливостей інформаційних систем, що базується на вдосконаленні процедур ідентифікації та автентифікації. Розглянуто основні недоліки існуючих методів захисту, які можуть призводити до компрометації безпеки. Наведено математичну модель, яка дозволяє прогнозувати потенційні вразливості на ранніх етапах і забезпечувати високий рівень кіберзахисту.*

Вступ

Інформаційні системи є основою багатьох бізнесових, адміністративних і технологічних процесів та охоплюють етапи збереження, оброблення, видалення та передавання даних.

Проте кіберзлочинці постійно вдосконалюють свої методи атак та здатні обходити традиційні заходи безпеки, тобто загрози розвиваються так само швидко, як і технології

захисту. Серед найпоширеніших способів атак виділяються фішинг, атаки методом перебору паролів (brute force), експлуатація вразливостей програмного забезпечення, а також атаки соціальної інженерії.

Базовими елементами безпеки інформаційних систем є процедури ідентифікації та автентифікації, тому більш уваги слід приділяти саме методам їх вдосконалення. Сучасні умови вимагають запровадження прогресивних підходів, що враховують поведінку користувачів, специфіку операційного контексту та здатність систем гнучко реагувати на загрози в реальному часі.

Такі підходи спрямовані на зниження ризиків, забезпечення більшої гнучкості систем безпеки та покращення користувацького досвіду.

Метою статті є розробка підходу, що поєднує аналіз поведінкових й контекстних характеристик користувачів із адаптивними механізмами безпеки для зниження ризику несанкціонованого доступу до інформаційних систем та побудова математичної моделі виявлення вразливостей на основі оптимізації процедур ідентифікації та автентифікації.

Аналіз існуючих підходів та пропонований підхід

Основними складовими безпеки інформаційних систем є методи ідентифікації та автентифікації. До найбільш поширених методів належать паролі, біометричні технології, двофакторна автентифікація та концепція довірчої мережі (Zero Trust). Проте навіть найсучасніші методи автентифікації мають свої обмеження, які зумовлюють необхідність розробки нових підходів. Оптимальне рішення має враховувати баланс між безпекою, зручністю для користувачів та можливістю адаптації до змінних умов сучасних кіберзагроз.

Запропонований підхід дозволяє знизити ризики компрометації системи за рахунок використання трьох основних компонентів: збору даних, поведінкового аналізу та контекстної автентифікації.

Збір даних передбачає постійний моніторинг дій користувача з використанням різних джерел інформації.

Поведінковий аналіз використовує алгоритми машинного навчання, які аналізують поведінкові шаблони користувачів і виявляють аномалії.

Контекстна автентифікація є основним етапом у забезпеченні балансу між безпекою та зручністю для користувачів. У разі виявлення підозрілої активності система застосовує додаткові перевірки. При цьому в разі підтвердження автентичності, система запам’ятовує контекст, що дозволяє зменшити кількість додаткових перевірок у майбутньому за подібних умов доступу.

Використання ризик-орієнтованого підходу передбачає застосування різних заходів перевірки або блокування доступу залежно від рівня загрози. Цей підхід активно застосовується в сферах управління безпекою інформаційних систем, фінансових операцій і банківської діяльності та дозволяє автоматизовано оцінювати ризики на основі заданих параметрів, таких як ймовірність загрози або її вплив на систему, і відповідно адаптувати заходи безпеки.

Запропонована математична модель аналізу ризиків є ключовим елементом адаптивної системи автентифікації, яка дозволяє динамічно оцінювати безпеку доступу на основі поведінкових і контекстних характеристик користувача. Модель ґрунтується на комбінованій оцінці двох основних параметрів:

- ймовірність аномальної поведінки користувача (P-показник, що відображає наскільки поточна активність відрізняється від звичайного поведінкового шаблону);
- критичність доступу до системи (C- рівень важливості ресурсів або даних, до яких запитується доступ, що визначає потенційні наслідки несанкціонованого проникнення).

Модель оцінки ризиків інтегрує ймовірність аномальної поведінки користувача та критичність доступу для визначення загального рівня ризику. Математичне представлення виглядає так:

$$R = \alpha P + \beta C, \quad (1)$$

де R — загальний рівень ризику; P — ймовірність аномальної поведінки, яка визначається моделями машинного навчання; C — критичність доступу, яка попередньо класифікується; α і β — вагові коефіцієнти, що враховують значущість відповідних факторів (наприклад, $\alpha+\beta=1$).

Класифікація критичності доступу C виконується наступним чином:

— низький рівень (C=1): доступ до загальнодоступної інформації, яка не потребує значного захисту;

— середній рівень (C=2): доступ до персональних чи корпоративних даних, що мають обмежений доступ;

— високий рівень (C=3): доступ до критично важливої інформації, зокрема конфіденційних даних чи систем управління.

Ймовірність аномальної поведінки (P) визначається на основі аналізу дій користувача в реальному часі за допомогою моделей машинного навчання. Вхідні параметри для цих моделей включають: геолокацію користувача, час дії, типові дії у системі (запити до ресурсів, введення даних), попередні шаблони поведінки користувача.

Використання моделі виконується наступним чином:

— низький рівень ризику ($R<T_1$): система дозволяє доступ без додаткових перевірок;

— середній рівень ризику ($T_1 \le R < T_2$): активується одноразова автентифікація;

— високий рівень ризику ($R \ge T_2$): доступ блокується до проведення повної багатофакторної автентифікації.

Налаштування вагових коефіцієнтів:

— α більше, якщо важливіша ймовірність аномальної поведінки;

— β більше, якщо критичність доступу має визначальне значення.

Запропонована модель дозволяє динамічно адаптувати рівень безпеки до ризиків, забезпечуючи баланс між зручністю доступу та захистом інформації.

Побудова математичної моделі дозволяє прогнозувати потенційні вразливості системи, оптимізувати процедури ідентифікації та автентифікації користувачів та знизити ймовірність реалізації атак за рахунок підвищення ефективності кіберзахисту.

Система представлена множиною об'єктів, які взаємодіють через канали зв'язку, і включає етапи ідентифікації та автентифікації.

Основними компонентами моделі є: множина об'єктів системи $S = \{s_1, s_2, \ldots, s_n\}$; характеристики ідентифікації $I = \{i_1, i_2, \ldots, i_m\}$ (логіни, паролі, біометричні дані); процедури автентифікації $A=\{a_1, a_2, \ldots, a_k\}$(однофакторні та багатофакторні); вразливості системи $V = \{v_1, v_2, \ldots, v_p\}$ (помилки програмного забезпечення, неправильно налаштовані політики

доступу); потенційні атаки $T = \{t_1, t_2, \ldots, t_q\}$(фішинг, перебір паролів, експлуатація вразливостей).

Для формалізації формули, що враховує оптимізацію процедур ідентифікації та автентифікації в рамках виявлення вразливостей інформаційних систем, можна запропонувати такий підхід: позначемо: V— загальний рівень вразливості системи; P_i— ефективність процедури ідентифікації; P_A— ефективність процедури автентифікації; C— критичність ресурсів, які захищає система (від 0 до 1); R_V— ризик відомих вразливостей (оцінка рівня загроз із бази CVE або подібної системи); E_{opt}— ефективність оптимізації захисних процедур (наприклад, використання двофакторної автентифікації або біометрії); F— частота виявлення нових вразливостей у системі (наприклад, кількість нових CVE на рік). Тоді оцінку вразливостей можна обчислити за формулою:

$$V = ((1 - P_i) + (1 - P_A)) / 2 \cdot C \cdot (R_v + F) \cdot (1 - E_{opt}), \qquad (2)$$

де $(1 - P_i)$ та $(1 - P_A)$ - враховують недостатню ефективність ідентифікації та автентифікації; C - підсилює вплив уразливостей залежно від важливості даних системи; $(R_v + F)$ описує загальну ймовірність появи вразливостей; $(1 - E_{opt})$ зменшує ризик вразливостей залежно від застосованих оптимізацій.

Формула (2) дозволяє оцінити загальний рівень вразливості системи та ефективність застосування різних методів оптимізації процедур ідентифікації й автентифікації. Вона може бути адаптована залежно від конкретних сценаріїв аналізу. Та надає можливість зробити висновки щодо:

— ефективності процедур: чим нижча ефективність процедур ідентифікації (P_i) і автентифікації (P_A), тим вищий загальний рівень вразливості;

— критичності: якщо система захищає важливі ресурси ($C \to 1$), то вразливості мають більший вплив;

— оптимізації: якщо впроваджено сучасні захисні механізми ($Eopt \to 1$), рівень вразливості знижується;

— ризиків вразливостей: чим більше ризиків (R_V) і частіше з'являються нові уразливості (F), тим більше зростає загальний ризик.

Висновки щодо переваг математичної моделі:

— модель дозволяє налаштовувати параметри і вагові коефіцієнти відповідно до потреб конкретної системи, тобто є гнучкою;

— аналіз здійснюється у реальному часі, що забезпечує оперативну реакцію на потенційні загрози, тобто є динамічною;

— використання алгоритмів машинного навчання дозволяє адаптувати модель до змін поведінки користувачів, тобто є інтеграція з сучасними технологіями;

— застосування додаткових заходів лише в разі потреби, що знижує ризики, не створюючи надмірних незручностей для користувачів.

Таким чином, запропонована математична модель є ефективним інструментом для підвищення рівня безпеки інформаційних систем та забезпечує оптимальний баланс між захистом і зручністю доступу.

У подальших дослідженнях планується розширити модель, додавши механізми інтеграції з технологіями штучного інтелекту та блокчейну для ще більшої безпеки.

Література

1. Гришко, С.М. Інформаційна безпека та захист інформації: Навчальний посібник. Київ: Видавничий дім «Кондор», 2020.

2. Лаптєв, В.М., Євдокименко, В.К., Рибалко, О.Ю. Комплексний підхід до захисту інформації: Підручник. Харків: ХНУРЕ, 2018.

3. Шахов, В.В. Основи кібербезпеки. Київ: Академія, 2019

4. Bishop, M. Computer Security: Art and Science. Boston: Addison-Wesley, 2003.

5. Stallings, W. Cryptography and Network Security: Principles and Practice. 7th edition. Upper Saddle River: Pearson, 2017.

6. Alpaydin, E. Introduction to Machine Learning. 4th edition. Cambridge: MIT Press, 2020.

7. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd edition. New York: Wiley, 2020.

Димов Максим Віталійович
Студент факультету Кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність: 125 Кібербезпека
Міжнародний гуманітарний університет
mak.dymov@gmail.com
Керівник: к.т.н.,доцент Йона Лариса Григорівна,
yonalarisa66@gmail.com

РИЗИКИ ДЛЯ БЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ

Анотація. Досліджуються сучасні ризики кібербезпеки, пов'язані з використанням штучного інтелекту для створення фішингового контенту. Проаналізовано класифікацію AI-підсилених атак, методи генерації синтетичного контенту та їх застосування в дезінформаційних кампаніях. Запропоновано підходи до виявлення та протидії таким загрозам в умовах гібридних конфліктів.

Ключові слова: кібербезпека, штучний інтелект, фішинг, синтетичний контент, дезінформація, цифрові загрози.

Сучасне цифрове середовище характеризується швидким зростанням технологій розумних комп'ютерів що відкриває нові шанси як для розвитку суспільства так і для зловмисних осіб. Використання AI-технологій для створення підробленого контенту стала однією з найбільших загроз безпеки Інтернету у останніх роках [1]. Звичайні способи обману урізноманітнилися від простих текстових повідомлень та до складних мультимедійний атак із використанням deepfake-технології, AI-створеними картинками та фальшивими текстами.

Актуальність роботи пов'язана із зростанням кількості кібер-інцидентів з використанням контенту, який було створено AI, особливо під час змішаних конфліктів та боїв за інформацію [2]. По даним аналізу цифр, більше 75% організацій зустрічали нові типи фішингових атак, що використовують елементи штучного уміння для покращення соціальної інженерії.

Дослідження показує, що атаки на основі штучного інтелекту можна розділити на три головні групи згідно з типом контенту:

Перша група включає створення підроблених профілів та особистостей, де злочинці використовують мережі для генерування синтетичних фотографій, які важко відрізнити від справжніх. Такі картинки застосовуються для формування довірчих профілів у соцмережах, що дозволяє злочинцям налагоджувати зв'язки з можливими жертвами. У той же час автоматично створюються біографії і дані про осіб, яких використовують для створення фальшивих акаунтів у соціальних медіа, а також формування ботнетів.

Друга група говорить про фальшування паперів та офіційних матеріалів. Сучасні AI-програми дають змогу робити дуже хороші копії документів посвідчення особи, банківських і фінансових документів, а також офіційних листів від держави. Технічна майстерність таких підробок досягла така рівня, що візуальне впізнавання стає практично неможливим без спеціальних засобів для знаходження їх.

Третя група є найнебезпечнішою, до якої потрапляють маніпуляції з медіа-контентом голов. Технології Deepfake дають змогу виготовляти відео, на яких керівники фірм або чиновники віддають накази про переведення грошей або передачу секретної інформації [3]. Такі удари дуже дієві у випадках BEC-ударів , оскільки використовують довіру робітників до глави.

Практичні приклади AI-підсилених атак

1. **Приклад 1: Корпоративне шахрайство з використанням deepfake**

   У 2019 році британська енергетична компанія стала жертвою атаки з використанням AI-синтезованого голосу. Зловмисники створили голосову імітацію керівника німецької материнської компанії та переконали співробітника перевести 220 000 євро на рахунок в Угорщині. Атака була настільки переконливою, що жертва впізнала характерний німецький акцент та інтонації свого босса.

2. **Приклад 2: Дезінформаційна кампанія під час виборів**

   У 2020 році під час виборчих кампаній у кількох країнах було виявлено мережу фейкових акаунтів, що використовували AI-генеровані фотографії профілів. Більше 15 000 синтетичних облич були створені для поширення політичної дезінформації. Ці акаунти діяли координовано, поширюючи однакові меседжі в різних соціальних мережах.

3. **Приклад 3: Маніпуляції в фінансовій сфері**

   У 2021 році зафіксовано випадок використання deepfake-технологій для створення фальшивих відео-інтерв'ю з CEO фінансової компанії. Відео використовувалося для маніпуляцій на фондовому ринку, призвівши до короткострокового, але суттєвого коливання курсу акцій компанії.

Слід звернути увагу на дослідження використання AI-створеного контенту в дезінформаційних кампаніях під час гібридних конфліктів. Дослідження показує, що коли є військовий стан, зростає використання штучного контенту для впливу на думку людей. Зловмисники роблять фейкові фото з місць подій, вигадують неіснуючих свідків і експертів а також створюють документи та неправдиві джерела інформації. Це веде до появи альтернативної реальності, яка може дуже вплинути на прийняття важливих рішень як у індивідуальному так і у державному рівнях.

Підрив довіри до офіційних джерел інформації відбувається через створення фальшивих відео з словами політиків, підробок офіційних новин і документів, а також вигадки неправдивих новин. Скоординовані атаки за допомогою інформації використовують

сітки синтетичних акаунтів для автоматичної генерації дезінформаційного контенту та їх цілеспрямованої подачі різним групам в залежності від психології користувачів.

Для боротьби з загрозами, що посилені штучним інтелектом, потрібен комплексний підхід який поєднує технічні та організаційні заходи. Технічні способи виявлення базуються на аналізі цифрових об'єктів у синтетичних малюнках, знаходженні несумісностей метаданих файлів та застосуванні алгоритмів машинного навчання для детекції фейків [4]. Важливим елемент є аналіз поведінки підозрілих акаунтів що дозволяє знаходити координовані мережі для поширення дезінформації.

Організаційні заходи включають підвищення рівня кіберграмотності користувачів, впровадження багаторівневої верифікації важливих рішень і розробку протоколів реагування на підозрілий контент. Створення систем швидкого обміну інформацією про нові загрози між організаціями дозволяє оперативно реагувати виникнення нових типів атак.

Освітній компонент протидії включає навчання розпізнаванню ознак синтетичного контенту, підвищення критичного мислення при оцінці інформації та популяризацію методів верифікації джерел інформації. Це особливо важливо за умов інформаційних війн, коли швидкість поширення дезінформації може значно перевищувати можливості її спростування.

Висновки

Проведене дослідження показує, що використання штучного інтелекту в кіберзлочинності представляє якісно новий рівень загроз для безпеки цифрового простору. Запропонована класифікація AI-фішингових атак дозволяє систематизувати сучасні загрози та розробити цільові методи протидії.

В умовах гібридних конфліктів AI-генерований контент стає потужним інструментом дезінформаційних кампаній, що потребує розробки спеціалізованих методів виявлення та нейтралізації. Ефективна протидія можлива лише за комплексного підходу, що поєднує технічні рішення, організаційні заходи та підвищення рівня цифрової грамотності населення.

Література

1. Chesney R., Citron D. Deep fakes: a looming challenge for privacy, democracy, and national security // California Law Review. 2019. Vol. 107. P. 1753-1820. [Електронний ресурс]. – Режим доступу: https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/ (дата звернення: 06.07.2025).

2. Kietzmann J., Lee L. W., McCarthy I. P., Kietzmann T. C. Deepfakes: Trick or treat? // Business Horizons. 2020. Vol. 63, № 2. P. 135-146. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/338144721_Deepfakes_Trick_or_treat (дата звернення: 06.07.2025).

3. Vaccari C., Chadwick A. Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news // Social Media + Society. 2020. Vol. 6, № 1. [Електронний ресурс]. – Режим доступу: https://journals.sagepub.com/doi/full/10.1177/2056305120903408 (дата звернення: 06.07.2025).

4. Wang S. Y., Wang O., Zhang R., Owens A., Efros A. A. CNN-generated images are surprisingly easy to spot... for now // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2020. P. 8692-8701. [Електронний ресурс]. – Режим доступу: https://openaccess.thecvf.com/content_CVPR_2020/papers/Wang_CNN-Generated_Images_Are_Surprisingly_Easy_to_Spot..._for_Now_CVPR_2020_paper.pdf (дата звернення: 06.07.2025).

UDC 621.3:004.65

Khniunin S.H.
PhD in Technical Sciences, Associate Professor,
Department of Information Technologies,
International Humanitarian University,
Odessa, Ukraine
sergii.khniunin@gmail.com

Shvedu M.I.
2nd-year Master's student in Cybersecurity and Information Protection,
International Humanitarian University,
Odessa, Ukraine
blackangel2657@gmail.com

AN ANALYSIS OF ENTERPRISE OPERATIONAL STABILITY IN RELATION TO COMMUNICATION AND ENERGY SYSTEMS

Abstract: *This paper examines key global incidents involving damage to both power and communication lines between 2023 and 2025. It analyses their impact not only on transnational distributed enterprises, but also on entire nations, affecting critical infrastructure, economic activity, social stability, and national security. A classification of equipment failures is presented, distinguishing between natural (environmental) and intentional causes. These disruptions influence not only private entities but also state-level operations. With society undergoing complete digitalisation, such events now result in severe economic losses and casualties. The once-reliable practice of communication line redundancy has recently failed to deliver the expected level of resilience.*

Keywords: *distributed enterprises, communication networks, power outages, economic losses*

The modern world is inextricably linked to distributed enterprises—organisations that no longer operate within a single office but rely on integrated information platforms spanning multiple regions, nations, or even continents. These entities are heavily dependent on uninterrupted access to databases, communication channels, and energy systems. Disruptions in these infrastructures pose more than just technical inconveniences—they have the potential to halt supply chains, cripple infrastructure, and cause economic damage on a global scale [1].

A classification of distributed enterprises is presented in Fig. 1.

Organisations of this kind include:

- Banks – reliant on global transactions, distributed processing centres, and financial gateways.
- Pharmacies – requiring real-time data on stock availability, prices, and logistics.
- Postal and logistics services (such as UkrPoshta, Nova Poshta) – dependent on routing, tracking, and electronic documentation.
- Taxi and transport platforms (Uber, Bolt, DHL) – entirely reliant on servers, GPS systems, and route optimization.

Equally critical, though often overlooked, are sectors such as:

- Mining and oil & gas companies – employing remote sensors and offshore drilling platforms, with data centralised at headquarters.
- Chemical and metallurgical plants – frequently structured as distributed systems, where safety metrics, temperatures, and chemical reactions are monitored from a central server.

- Shipping and freight enterprises (e.g., Maersk, MSC) – dependent on global navigation systems, customs databases, and real-time cargo tracking. Any disruption in IT infrastructure can bring an entire fleet to a standstill worldwide.

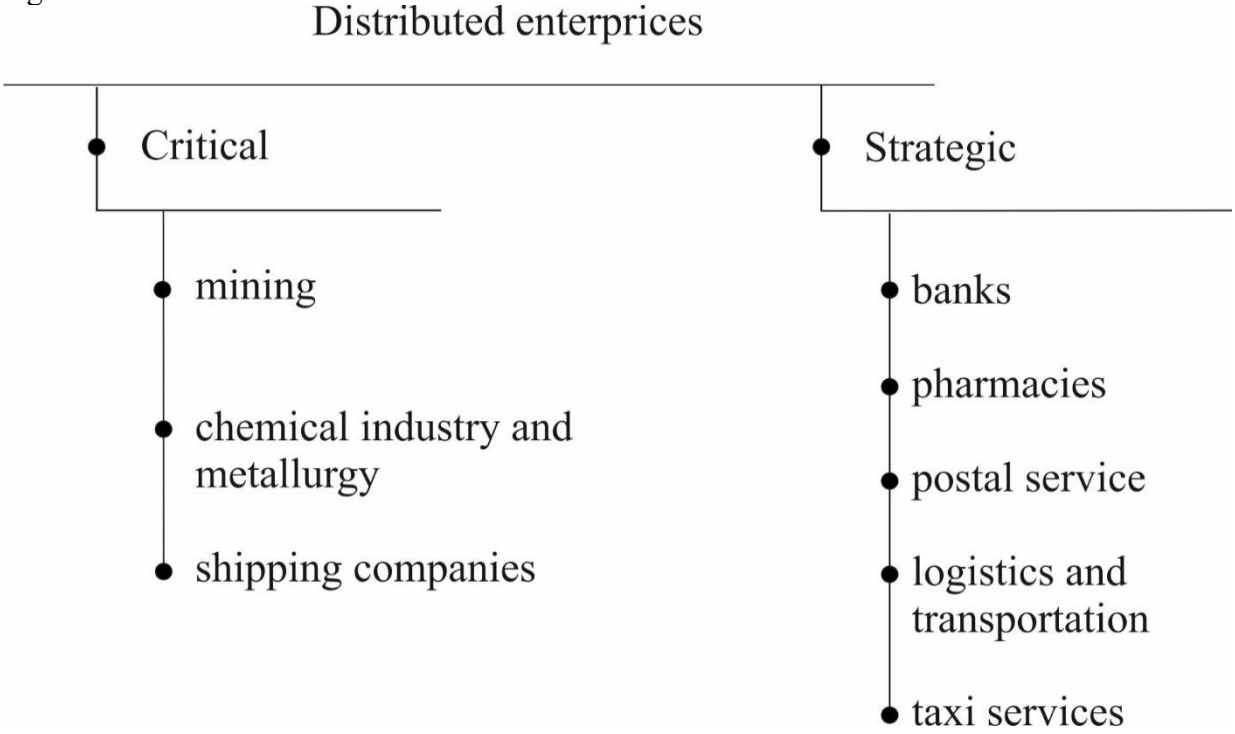


Figure 1 - Classification of distributed enterprise types

These enterprises cannot function in isolation—they are nodes in a global network. This means that a single point of failure, such as a power outage or communication breakdown in one country, can trigger cascading consequences in another.

Hence, increasing emphasis is placed on the reliability of communication and energy systems, as these underpin the uninterrupted operation of global business. Real-world case studies reveal that faults in information and power networks are not anomalies—they are part of an escalating pattern of systemic risk.

Historically, such failures received scant attention. Threats were perceived as abstract and their consequences exaggerated. Disruptions were primarily discussed within technical communities [2] and viewed more as localised mishaps [3] than as global warning signs.

Today, however, society's growing dependence on stable energy and communication infrastructure renders each new incident a cause of tangible economic, social, and political damage. Among the most significant cases in recent years are:

- Widespread power outage in Chile (February 2025) – over 70% of the country was left without electricity, affecting major hospitals and transport hubs [4].

- National blackout in Kenya (December 2024) – the entire country was plunged into darkness for several hours. The main airport ceased operations, trains halted, and communication networks largely collapsed [5].

- Complete communication loss in Gaza (October 2023) – amid military conflict, residents lost access to mobile and internet services, making emergency response and humanitarian coordination impossible [6].

- Telecommunication blackout in Libya following floods (September 2022) – after severe flooding, several regions near Derna became entirely cut off from the outside world [7].

These catastrophes can be categorised as either natural—resulting from environmental events and associated equipment failure—or intentional, including terrorism and military action. In cases of natural disaster, enterprises can mitigate risk through technical innovation and

modernisation. However, when damage is deliberate, both governments and businesses must act in unison. The effectiveness of their collaboration will determine the capacity of modern civilisation to adapt and survive in a deeply interdependent global landscape.

While such incidents were once treated with indifference, today they represent a pressing threat. With widespread digitalisation, their consequences are more profound than ever—incurring both economic losses and loss of life. Moreover, where a single backup communication line once offered sufficient protection, recent years have shown that even fibre optics and certain satellites are vulnerable to repeated damage.

In light of these developments, we must conclude that distributed enterprises operating on centralised databases are now highly exposed to emerging global risks. This vulnerability results in extensive labour hours spent on manually restoring and resynchronising data following network outages. Therefore, any organisation operating within a distributed model must integrate the following into its core strategy: preventive risk management, cybersecurity, system redundancy, and robust architectural planning. The rapid advancement of artificial intelligence offers a promising avenue to streamline and partially automate these vital processes in the near future.

References:

1. Khniunin S.H., Shvedu M.I. Ensuring the Security of Information Systems in Distributed Enterprises in Conditions of Unstable Communication System Operations // Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку: Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь: Liha-Pres, 2025. – Ч. 2. – С. 144 - 146. DOI: 10.36059/978-966-397-491-0-42

2. The US Grid Attack Looming on the Horizon. URL: https://www.wired.com/story/youre-not-ready-for-a-grid-attack/?utm_source=chatgpt.com (date of access: 06.06.2025).

3. Power Outages, Communication Failures & Healthcare. URL: https://www.domprep.com/articles/power-outages-communication-failures-healthcare?utm_source=chatgpt.com (date of access: 06.06.2025).

4. Empresario del área metalúrgica: Quién es Rudy Basualdo, el hombre secuestrado en Rancagua (February 2025). URL: https://www.emol.com/noticias/Nacional/2025/02/18/1112344/Corte-de-luz-nacional-en-Chile.html (date of access: 06.06.2025).

5. Power supply restored after major outage hits Kenya, affects internet access (December 2024). URL: https://www.reuters.com/world/africa/major-power-outage-hits-kenya-affects-internet-access-2024-12-18/?utm_source=chatgpt.com (date of access: 06.06.2025).

6. Chile declares emergency as power outage plunges country into darkness (October 2023). URL: https://www.aljazeera.com/news/2025/2/26/chile-declares-state-of-emergency-as-blackout-plunges-country-into-darkness?utm_source=chatgpt.com (date of access: 06.06.2025).

7. Communication outage hits flood-stricken city in Libya, further complicating search efforts (September 2022). URL: https://apnews.com/article/libya-derna-floods-069adb76afc3c4ec92956ee4141ad872 (date of access: 06.06.2025).

Єрьоменко Анастасія Русланівна
Студент факультету Кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність: Електронні комунікації та радіотехніка (172)
Міжнародний гуманітарний університет
ananastya1330@gmail.com
Керівник: к.т.н.,доцент Йона Лариса Григорівна,
yonalarisa66@gmail.com

МЕТОДИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Анотація. Розглянуто сучасні підходи до захисту цілісності електронних документів, зокрема новітні криптографічні методи, інтеграцію штучного інтелекту, використання блокчейну та перспективи впровадження постквантових технологій. Підкреслено необхідність переходу від класичних централізованих моделей до децентралізованих систем із високим рівнем довіри. Проаналізовано внутрішні дослідження та практичні приклади впровадження.

1. Вступ

У сучасному цифровому середовищі передача, зберігання та обробка документів часто здійснюються без використання паперових носіїв. Це вимагає створення механізмів захисту, які не лише гарантують цілісність документів, але й дозволяють безсумнівно встановити їхнє походження [4].

Сучасні виклики — зростання кіберзагроз, юридичні конфлікти, розвиток квантових обчислень — потребують інноваційних рішень, що виходять за межі класичних цифрових підписів і сертифікатів [1], [3].

2. Теоретичні основи цілісності та автентифікації

Цілісність документа — це властивість, яка гарантує незмінність даних. Автентифікація засвідчує, що джерело документа відповідає очікуваному. Класичні інструменти — геш-функції, цифрові підписи, PKI (інфраструктура відкритих ключів) — залишаються актуальними, проте потребують доповнення у зв'язку зі зростанням складності загроз [3].

Основні загрози(та сучастні протидії їм):

- Модифікація або знищення даних зловмисником (Цифрові підписи для верифікації незмінності. Резервне копіювання у захищених сховищах.[4]).
- Фальсифікація джерела походження документа (PKI-сертифікати для перевірки особи відправника. Цифрові підписи з перевіркою по відкритому ключу.[3]).
- Несанкціонований доступ до конфіденційної інформації(Шифрування даних (AES, RSA). Аудит доступу та журналювання дій користувачів.[4]).
- Підміна або підробка електронного документа (Блокчейн для фіксації автентичних копій. \ Водяні знаки або метадані з шифруванням. Штучний інтелект для виявлення аномалій у структурі документа[2],[5].).

3. Механізми програмного забезпечення цілісності

Блокчейн та децентралізація

Розподілені реєстри дозволяють фіксувати кожен факт взаємодії з документом у незмінному вигляді. Геш документа зберігається в блокчейні, що дозволяє перевірити його справжність у будь-який момент [4]. Наприклад, нотаріальні блокчейн-сервіси вже використовуються у правових процесах.

Пропонується створити міжвідомчий державний блокчейн для реєстрації дій із публічними цифровими документами, який працюватиме в режимі реального часу та надаватиме публічний API для перевірки цілісності документа будь-яким громадянином/громадянкою.

Штучний інтелект / машинне навчання (AI/ML) для верифікації

Штучний інтелект може виявляти зміни у структурі документа, які не виявляються звичайними криптографічними засобами[2]. Наприклад, аналізуючи стилістику тексту або метадані PDF-файлів. Це особливо актуально для виявлення фальсифікацій офіційних документів.

Можливе створення інтелектуальної системи фільтрів для державних установ, яка автоматично класифікуватиме та маркуватиме документи з ознаками фальсифікації на основі нейромережевого аналізу структури й стилю [2], [5].

Гомоморфне шифрування

Це підхід, що дозволяє обробляти зашифровані документи без їхнього розшифрування [1], [6]. Завдяки цьому забезпечується перевірка та обробка з повною конфіденційністю.

Переваги:

- Дані залишаються зашифрованими під час обробки.
- Мінімізується ризик витоку інформації.

Недоліки:

- Повністю гомоморфне шифрування залишається обчислювально складним і ресурсоємним.
- Ще не є практичним для всіх сценаріїв використання.

Приклад: впровадження пілотної платформи для обміну медичними даними між установами, де інформація обробляється виключно у зашифрованому вигляді з можливістю аналітики без доступу до персональних даних пацієнтів.

Постквантова криптографія

Класичні алгоритми (RSA, ECC) вразливі до квантових атак. Сучасні дослідження зосереджені на створенні стійкої до квантового зламу криптографії[3]. Розглядаються нові геш-функції (SPHINCS+, Picnic), здатні гарантувати цілісність у довгостроковій перспективі.

Напрямок — розвиток гібридних систем захисту цифрових архівів, що поєднують класичні алгоритми з постквантовими протоколами, дозволяючи поступовий перехід до нових стандартів без втрати сумісності.

4. Практичне застосування в Україні

У рамках цифровізації держави сервіси як Дія, Електронний суд, eHealth інтегрують цифрові підписи. Зростає інтерес до нових підходів: деякі стартапи працюють над верифікацією дипломів і медичних карток через блокчейн. КПІ ім. І. Сікорського досліджує багатофакторну автентифікацію на основі нейромереж [2], [5].

5. Висновки

Автентифікація та захист цілісності документів є ключовими елементами інформаційної безпеки в умовах цифрової трансформації. Інновації у сфері цілісності та автентифікації документів мають вирішальне значення для безпечного інформаційного середовища. Впровадження ШІ, блокчейну, гомоморфного шифрування та постквантових методів створює підґрунтя для нової архітектури довіри. Водночас необхідні стандартизація, нормативне забезпечення та етичне осмислення.

Література

1. Вікіпедія. Гомоморфне шифрування. URL: https://uk.wikipedia.org/wiki/Гомоморфне_шифрування

2. С. Славінський, «Застосування методів машинного навчання для виявлення фальсифікацій у цифрових документах», КПІ ім. І. Сікорського, магістерська дисертація, 2021. URL: https://ai.kpi.ua/ua/masters/thesis/28521smai-slavinskyi_magistr.pdf

3. CoinMarketCap. Повне гомоморфне шифрування (FHE). URL: https://coinmarketcap.com/academy/uk/glossary/fully-homomorphic-encryption

4. bip.net.ua. «Як підприємцю організувати електронний документообіг». URL: https://bip.net.ua/articles/yak-pidpryyemczyu-organizuvaty-elektronnyj-dokumentoobig/

5. І. М. Шевченко, С. Ю. Смоляр, «Блокчейн у забезпеченні цілісності електронних документів», Журнал якісних моделей та технологій, №2, 2023. URL: https://jqmth.donnu.edu.ua/article/download/14956/14862

6. Національний департамент інформатизації. «Сучасні загрози цифровим даним та методи захисту», Електронний репозиторій НДІППП. URL: https://repository.ndippp.gov.ua/handle/765432198/1050

Петков Євген Ігорович.
Аспірант, спеціальність 125
“Кібербезпека та захист інформації”,
Міжнародний гуманітарний 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 гуманітарного університету
yonalarisa66@gmail.com

ТИПИ СПУФІНГ АТАК ТА ЗАСОБІВ ЗАХИСТУ В ЛОКАЛЬНИХ МЕРЕЖАХ

Анотація. *Дослідження розглядає типи Spoofing-атак та засобів боротьби з ними в мережі рівня доступу.*

Атаки типу спуфінг (spoofing) — це категорія кібератак, у яких зловмисник маскується під іншу особу або пристрій, щоб обдурити користувача, систему або мережу. Основна мета таких атак — отримати несанкціонований доступ, перехопити конфіденційні дані або ввести в оману.

MAC Spoofing атаки. Як правило, мережевий коммутатор L2 рівня за замовчуванням динамічно вивчає MAC-адресу пристроя підключеного до порту, та не контролює кількість MAC-адрес, які він може вивчити на одному порту, і не блокує записи в CAM-таблиці. Зловмисник може використати ці вразливості декількома способами.

- По-перше, підробити (продублювати) MAC-адресу іншого легітимного хоста в локальній мережі. Хакер відправляє Ethernet кадр з такою ж самою MAC-адресою

відправника, і комутатор оновить в своїй CAM-таблиці запис, що посилається на викрадену MAC-адресу вже за портом підключення зловмисника, а не легітимного пристроя. Приклад атаки зображено на рис.1.

- По-друге, зловмисник може швидко заповнити CAM таблицю комутатора, надсилаючи велику кількість Ethernet кадрів, з різними підробленими MAC-адресами відправника. Після переповнення CAM-таблиці комутатор починає відправляти кадри широкомовним способом на всі свої порти, фактично діючи як хаб. Зловмисник таким чином може отримувати трафік, який йому не відправлявся. Це є MAC flooding, різновид атаки типу MAC Spoofing.

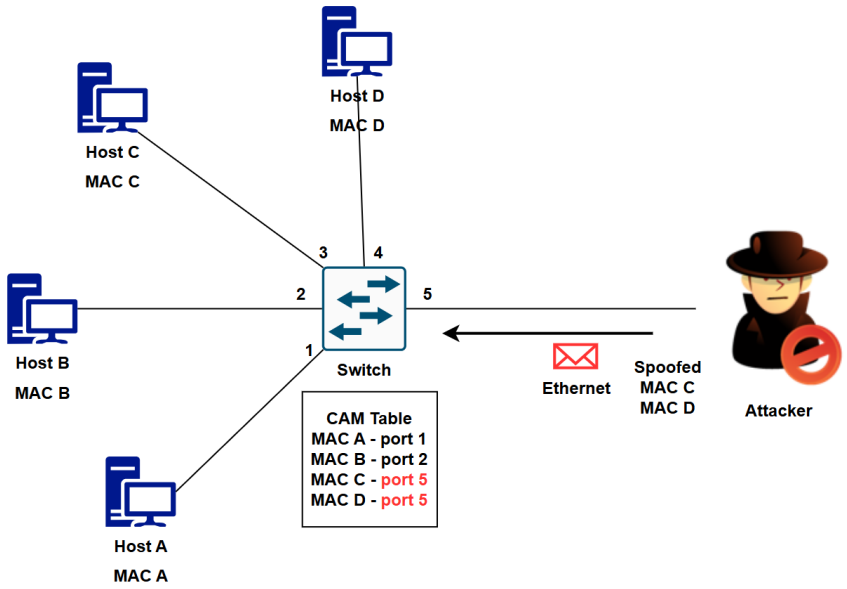


Рисунок 1 – Приклад атаки типу MAC Spoofing

Для боротьби з MAC Spoofing атаками можна використовувати такий функціонал комутаторів доступу як Port security. Активація його дозволяє: по-перше, обмежити кількість MAC-адрес вивчаємих на порту комутатора, по-друге, прив'язати певні MAC-адреси до певних портів комутатора в CAM-таблиці після їх першого вивчення.

Іншим засобом боротьби з MAC Spoofing може використовуватись протокол 802.1x для аутентифікації підключених пристроїв та запобіганню їх несанкціонованому доступу до мережі. Клієнт (який має підтримувати протокол 802.1x) отримає повний доступ до мережі тільки після успішної аутентифікації.

DHCP Spoofing атаки. В основі цього типу атаки лежить підробка зловмисником DHCP сервера в локальній мережі. Легітимні пристрої, які налаштовані на отримання конфігурації мережевого підключення по протоколу DHCP, відправляють запит в локальній мережі (при цьому перший пакет DHCP Discover як правило широкомовний і розсилається всім хостам в підмережі). На цьому етапі зловмистник (фальшивий DHCP сервер) може перехопити клієнтський запит та надіслати назад пропозицію DHCP Offer із підробленими параметрами підключення (IP-адреси, шлюза за замовчуванням, DNS серверів), а відповідно клієнт може прийняти цю пропозицію від нелегітимного DHCP серверу раніше ніж від легітимного. Приклад атаки зображено на рис.2. Таким чином, зловмисний DHCP сервер може навіть організувати атаку "людина посередині" (man-in-the-middle), наприклад, надавши клієнту свою IP адресу як шлюз за замовчуванням. Тоді скомпрометований хост буде пересилати свій трафік через пристрій зловмисника. Або з іншого боку, зловмисник може

просто перевантажити чи зробити локальну мережу непрацездатною, надсилаючи надмірну кількість підроблених відповідей DHCP сервера.

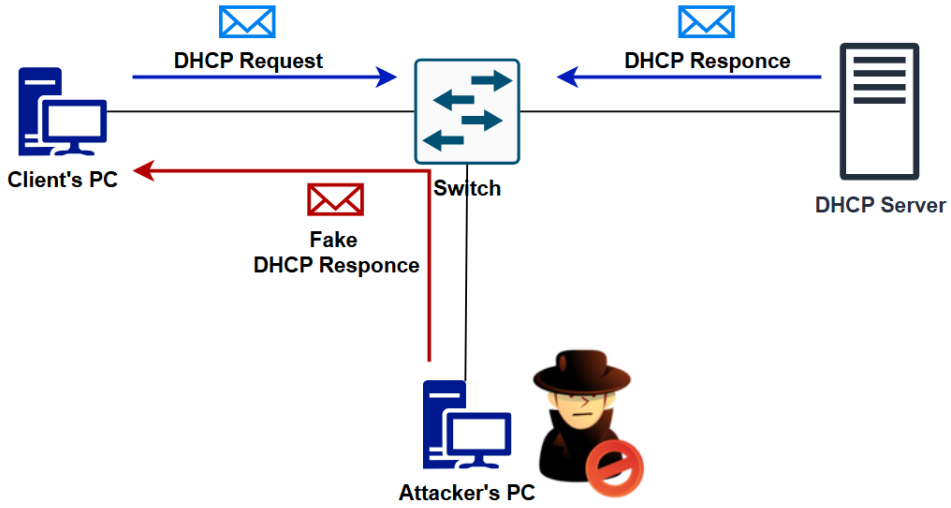


Рисунок 2 – Приклад атаки типу DHCP Spoofing

Можливий засіб боротьби з даним типом атак – це активація на комутаторах рівня доступу функції DHCP snooping. Цей функціонал дозволяє розділити всі порти комутатора на довірені та недовірені (trusted, untrusted). За замовчуванням всі порти недовірені (untrusted) – до них підключають клієнтів. З недовірених портів комутатор приймає DHCP запити, але видаляє відповіді DHCP сервера. Тільки окремі порти налаштовуються адміністратором як довірені (trusted), і тільки до таких портів підключають легітимний DHCP сервер, відповіді якого будуть передаватись комутатором на інші порти. Крім цього, комутатор з DHCP snooping аналізує інформацію в DHCP пакетах (запити від клієнтів та відповіді сервера), на основі якої будує базу прив'язки DHCP snooping binding table, яка містить по кожному клієнту: MAC адресу, порт підключення, IP адресу отриману в оренду, час оренди IP-адреси, клієнтський VLAN, тощо. Ця база прив'язки DHCP параметрів важлива і для функціонування інших функцій безпеки на комутаторах доступа, таких як Dynamic ARP Inspection, та IP Source Guard.

Треба зазначити, що таким критично важливим пристроям в локальної мережі, як сервери, маршрутизатори, як правило налаштовують статичну IP-адресу та статичні параметри підключення замість динамічного отримання параметрів IP.

ARP Spoofing атаки. Для реалізації цієї атаки зловмисник надсилає жертві підроблені ARP пакети, тим самим асоціює свою MAC-адресу з IP-адресою зовсім іншого пристрою локальної мережі. Особливістю ARP протокола є те, що зловмисник може надсилати ARP відповідь навіть якщо і не було ARP запита від клієнта, тим самим отруюючи ARP кеш жертви.

Розглянемо ситуацію на рисунку 3. Клієнт потребуючи взаємодії зі «шлюзом за замовчуванням» своєї мережі знає IP адресу шлюза (192.168.0.1), але не знає його MAC адреси. Для динамічного визначення MAC-адреси пристрою за відомою IP-адресою у локальній мережі використовується протокол ARP (Address Resolution Protocol). Також кожен пристрій підтримує свою локальну ARP-таблицю (кеш), де зберігає відповідність IP-адрес до MAC-адрес інших пристроїв мережі. Але зловмисник в цій же локальній мережі може відправляти підроблені ARP відповіді, наприклад:

- Клієнту-жертві: «IP-адреса шлюзу 192.168.0.1 має MAC-адресу C (зловмисника)»;

- Шлюзу: «IP-адреса клієнта 192.168.0.11 має MAC-адресу C (зловмисника)».

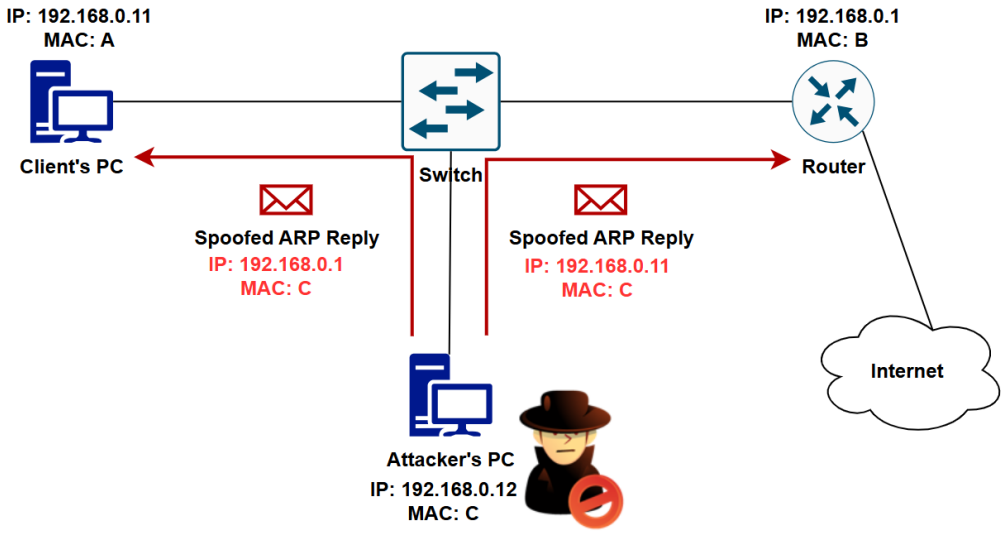


Рисунок 3 – Приклад атаки типу ARP Spoofing

Таким чином жертви ARP Spoofing атаки в локальній мережі будуть відправляти Ethernet пакети неправильному хосту (зловмиснику). Зловмисник в свою чергу, може отримувати чужий трафік з важливою інформацією, персональними даними, а також займатися підміною даних. Перенаправляючи пакети між скомпрометованими жертвами атаки, як в розглянутому випадку, зловмисник здійснює атаку "людина посередині" (man-in-the-middle).

Для боротьби з ARP Spoofing атаками можна використовувати статичні ARP записи на окремих пристроях, але це не ефективно в мережах з великою кількістю пристроїв та ускладнює адміністрування. Більш гнучкою є активація на комутаторах доступу функції Dynamic ARP Inspection (DAI), яка працює разом із функціоналом DHCP snooping. Комутатор з функцією DAI інспектує клієнтські ARP пакети та перевіряє на відповідність IP-адрес до MAC-адрес у ARP відповідях з власною базою прив'язки DHCP snooping binding table. Якщо у клієнському ARP пакеті невірна інформація – він буде відкинутий. Подібно до DHCP snooping, в конфігурації DAI також визначаються довірені та недовірені порти (trusted, untrusted). Відповідно все клієнтське обладнання підключається до недовірених портів, де DAI перевіряє ARP-пакети, а в довірені порти підключаються сервери, маршрутизатори, тощо.

IP Spoofing атаки. В цьому типу атаки зловмисник змінює свою вихідну IP-адресу в заголовку IP пакетів, щоб приховати свою особу або видати себе за інший пристрій (довірений сервер або довіреного користувача). Цей тип атаки може бути використаний як частина DoS/DDoS атаки. Наприклад, якщо зловмисник відправить велику кількість підроблених запитів на сервер від різних «відправників», а віддалений сервер буде намагатись відповідати на кожен такий запит, відкриваючи велику кількість TCP сессій і витрачаючи свої ресурси. Або з іншого боку, якщо на одну легітимну IP-адресу клієнта прийдуть відповіді від серверів, які він не замовляв – це також приклад атаки на відмову ресусів. Приклад атаки зображено на рис.4.

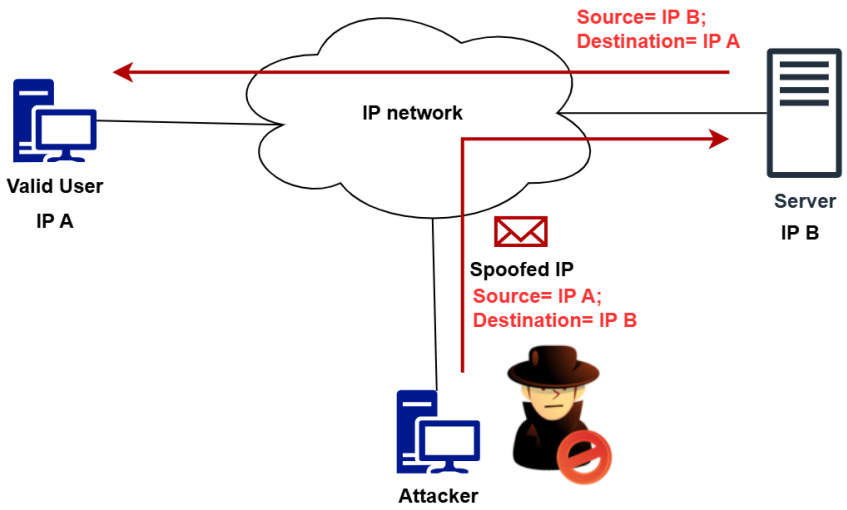


Рисунок 4 – Приклад атаки типу IP Spoofing

Для боротьби з IP Spoofing атаками можна використовувати безпосередньо на комутаторі рівня доступу функціонал IP Source Guard для перевірки дійсності вхідної IP-адреси пакета який поступає на порт комутатора. IP Source Guard може використовувати таблицю прив'язки DHCP snooping binding table (якщо такий активовано та клієнт використовує протокол DHCP для мережевого налаштування) або статичні прив'язки IP-адрес до портів підключення недовірених пристроїв. Таким чином, будь-який вхідний IP пакет з вихідною IP-адресою, відмінною від тієї, що призначена по DHCP або статичної конфігурації, буде видалено. Також на маршрутизаторах це може бути Anti-spoofing функціонал який фільтрує на основі списків контролю доступу (ACL), або перевірки в таблиці маршрутизації зворотнього маршрута до підмережі від якої прийшов вхідний IP пакет через той самий інтерфейс маршрутизатора на який був прийнятий цей пакет.

Висновок. Таким чином такі функції комутаторів рівня доступу як Port security, DHCP snooping, Dynamic ARP Inspection та IP Source Guard дають можливість заблокувати переважну більшість спуфінг атак безпосередньо в локальній мережі та якомога ближче до потенційного джерела проблеми. Перелічені функціїї безпеки підтримуються не у всіх моделях та виробниках комутаторів доступу, що потрібно враховувати при проектуванні надійної, відмовостійкої та безпечної мережі. Також протоколи аутентифікації та ідентифікації клієнтів мають важливе значення, так само, як професійне адміністрування, конфігурація мережі, моніторинг та вчасне виявлення підозрілих активностей. Безперечно, для зменшення потенційного впливу розглянутих атак типу "людина посередині" (man-in-the-middle) необхідне використання протоколів шифрування трафіку.

Література

1. The Cisco Learning Network. Layer 2 Security Features. URL: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKLCEA4/members-choice-layer-2-security-features.
2. Wikipedia. MAC spoofing. URL: https://en.wikipedia.org/wiki/MAC_spoofing.
3. Wikipedia. ARP spoofing. URL: https://en.wikipedia.org/wiki/ARP_spoofing.
4. Wikipedia. IP address spoofing. URL: https://en.wikipedia.org/wiki/IP_address_spoofing.

5. Best Practices for Securing Cisco Switches in Enterprise Environments. URL: https://community.cisco.com/t5/cisco-cafe-blogs/best-practices-for-securing-cisco-switches-in-enterprise/ba-p/5243372.
6. Cisco. Port Security. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/port_security.pdf.
7. ManageEngine. DHCP snooping. URL: https://www.manageengine.com/products/oputils/tech-topics/dhcp-snooping.html.
8. Cisco. Configuring Dynamic ARP Inspection. URL: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/security/503_u2_2/Cisco_n3k_security_cg_503_u2_2_chapter11.html?dtid=osscdc000283&linkclickid=srch.
9. Cisco. Configuring IP Source Guard. URL: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110110.html.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УДК 621.396

Пунченко Н.О. к.т.н., доцент
ОДАУ
iioonn24.01@gmail.com

БШД ЯК НАДІЙНІСТЬ ПЕРЕДАЧІ ДАНИХ

Анотація. Проаналізовано сучасний стан і перспективи впровадження бездротових широкосмугових технологій (БШД) у навігаційних системах України відповідно до діючих стандартів IALA. Розглянуто технічні особливості реалізації БШД на морських і прибережних об'єктах, а також наведено приклади цифровізації портової інфраструктури. Визначено основні виклики та напрями розвитку систем електронних комунікацій і мережевих технологій у морській галузі в умовах воєнного стану.

IALA визначає технічну політику у сфері морської навігації, зокрема щодо впровадження електронних засобів забезпечення навігації та цифрових технологій. Одним із напрямів є інтеграція бездротового широкосмугового доступу (БШД), що забезпечує високошвидкісну передачу навігаційних, гідрометеорологічних і службових даних у реальному часі. В Україні питання цифровізації морської галузі набуває актуальності у зв'язку з необхідністю підвищення ефективності, прозорості та безпеки морських перевезень [1, 2]. Пропонується огляд та рівняння технологій БШД для морського застосування.

1. LTE/4G та 5G у прибережних зонах. В Україні, як і в інших державах, для забезпечення зв'язку в прибережних районах активно впроваджуються технології LTE/4G та 5G. Технології забезпечують пропускну здатність до 1 Гбіт/с, мінімальні затримки та підтримку великої кількості IoT-пристроїв (навігаційні буї, сенсори, автоматизовані системи моніторингу) [2]. Вони мають таки відзнаки LTE/4G та 5G.

LTE/4G:

швидкість передачі даних – до 150 Мбіт/с;

покриття – до 20–30 км від базової станції, що дозволяє охоплювати значні ділянки узбережжя;

підтримка IoT – можливість підключення сенсорів, навігаційних буїв, систем моніторингу;

вартість – нижча порівняно із супутниковим зв'язком, що робить LTE/4G оптимальним для портів і прибережних об'єктів [3, 4].

5G:

швидкість передачі даних – до 1 Гбіт/с і вище;

затримка – менше 10 мс, що є значущим для автоматизованих систем управління та безпілотних технологій;

масштабованість – підтримка великої кількості пристроїв на одиницю площі (до 1 млн/км^2);

гнучкість – можливість використання приватних мереж для портових операторів, інтеграція з хмарними платформами та системами електронного документообігу [1, 2, 5].

Перевагами цих технологій при провадженні у прибережних зонах є:

висока швидкість і надійність зв'язку, що забезпечує обробку великих обсягів навігаційних, логістичних і митних даних.

Підтримка цифрових платформ портів (наприклад, DocPort, MSW), які приймають участь в забезпеченні автоматизації адміністративних процедур і зменшує час обробки суден [6].

Інтеграція IoT: підключення сенсорів для моніторингу стану інфраструктури, вантажів, екологічних параметрів.

Підвищення безпеки при оперативному обміні інформацією між суднами, портами та береговими службами, підтримка систем відеоспостереження та контролю доступу.

Зниження витрат тому що використання LTE/4G та 5G дешевше за супутниковий зв'язок у прибережних районах, особливо для масових і постійних операцій[3, 4].

В Україні перші пілотні зони 5G вже запущено в Одесі та інших містах. Планується розширення покриття на портові райони [2, 5, 7]. Впровадження цифрових платформ у портах (наприклад, DocPort) із використанням LTE/4G для автоматизації обміну даними між митницею, портовими службами та судновласниками[6]. В Китаї 5G-мережі забезпечують покриття до 50 км від берега, підтримують моніторинг риболовецьких суден, вітрових електростанцій, туристичних об'єктів і аварійно-рятувальних служб [8]. В Європі 5G використовується для автоматизації контейнерних терміналів, управління автономними суднами, інтеграції з системами електронної навігації [9].

Перевагами технології є: висока щільність обслуговування та масштабованість, підтримка віддаленого керування навігаційним обладнанням, інтеграція з цифровими платформами портів (наприклад, DocPort, MSW) [10]. При цьому необхідно розгортання інфраструктури вздовж усього узбережжя та забезпечити стійкість зв'язку в умовах складного рельєфу та погодних впливів.

2. Супутниковий зв'язок для відкритого моря.

Для об'єктів, що знаходяться поза зоною дії наземних мереж, використовуються глобальні супутникові системи (Inmarsat, Iridium, Starlink). Вони забезпечують безперервний зв'язок із судами та платформами незалежно від географічного положення. До переваг супутникового зв'язоку є глобальне покриття, надійність у надзвичайних ситуаціях, резервування каналів для критичних служб. А к недолікам відноситься во - первих висока вартість обладнання та послуг, в друге - затримки сигналу порівняно з наземними мережами, обмеження пропускної здатності у порівнянні з 4G/5G.

3. VDES та AIS

Автоматична ідентифікаційна система — базова технологія для моніторингу суден, що забезпечує передачу ідентифікаційних та навігаційних даних у VHF-діапазоні, використовуючи технологію TDMA для передачі ідентифікаційних, навігаційних та службових даних у реальному часі[10, 11]. Використовується для автоматичної ідентифікації суден, передача координат, курсу, швидкості, типу судна. Також обміна даними між суднами та береговими службами і підвищення безпеки судноплавства та запобігання зіткненням.

В Україні AIS є обов'язковою для транспортних і комерційних суден водотоннажністю понад 300 тонн, а також для риболовецьких суден довжиною понад 15 метрів. Система активно використовується у портах, на річкових і морських суднах, а також на навігаційних буях та маяках (AIS AtoN)[12].

VHF Data Exchange System — новий стандарт, що розширює можливості AIS, дозволяючи двосторонній обмін великими обсягами інформації між суднами, береговими станціями та супутниками (навігаційні повідомлення, метеодані, службова інформація). Ключові компоненти VDES:

VDE-TER (територіальний сегмент): обмін даними між суднами та береговими станціями;

VDE-SAT (супутниковий сегмент): глобальна двостороння передача даних через супутники;

розширена пропускна здатність і підтримка нових сервісів e-Navigation.

Одна з головних переваг це можливість інтеграції з іншими цифровими платформами.

Таблиця 1 – Порівняння характеристик AIS та VDES

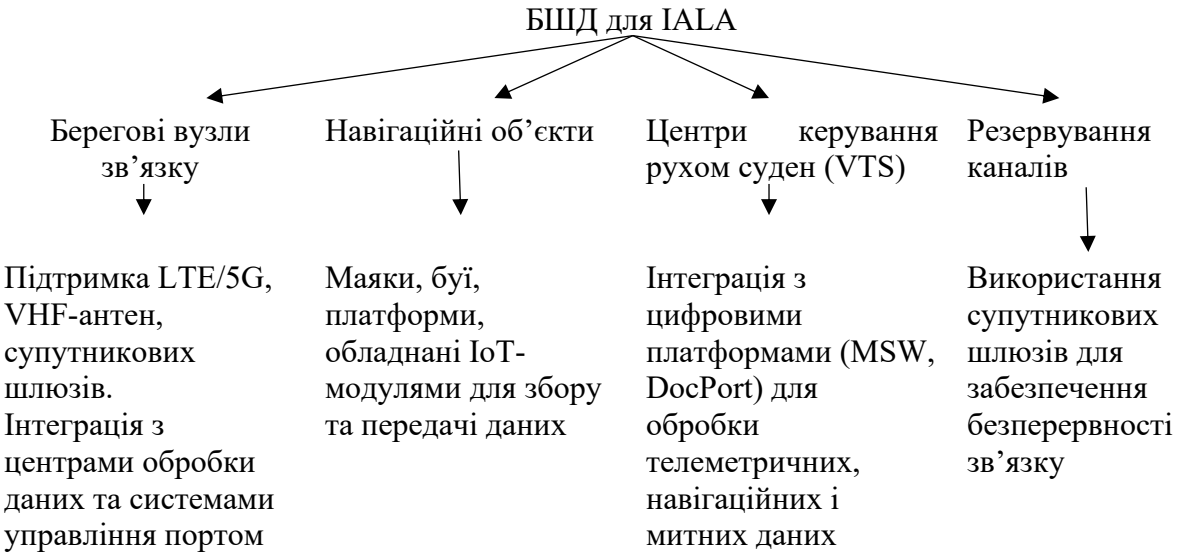
Параметр	AIS	VDES
Діапазон	VHF (162 МГц)	VHF (162 МГц) + супутникові канали
Пропускна здатність	~9,6 кбіт/с	до 307 кбіт/с
Тип обміну	Односторонній/обмежений	Двосторонній, глобальний
Підтримка IoT	Обмежена	Повна
Кібербезпека	Базова	Підвищена
Інтеграція з e-Navigation	Часткова	Повна

Загальні можливості AIS та VDES інтегруються з хмарними платформами, системами віртуалізації та електронного документообігу.

Впровадження VDES дозволяє оптимізувати інженерію трафіку, забезпечити пріоритезацію критичних навігаційних повідомлень, підтримку мультисервісних сценаріїв (навігація, екологія, безпека). Но це потребує:

1. оновлення обладнання та програмного забезпечення на суднах і берегових станціях;
2. забезпечення сумісності з існуючими системами AIS та іншими морськими радіосистемами;
3. підготовка кадрів, розробка нормативної бази, участь у міжнародних ініціативах.

В Україні реалізація БШД для IALA проходить по структурі:



В порту «Південний» йдеться впровадження – тестування морського модуля цифрової платформи DocPort — українського аналога Maritime Single Window (MSW), що автоматизує адміністративні процедури, знижує час обробки суден, підвищує прозорість і оптимізує витрати. Після тестування система масштабуватиметься на всі морські порти України з інтеграцією до IT-систем митниці та прикордонної служби[10]. Цифровізація портів Чорного моря проходить так: впровадження: 1) електронного документообігу, 2) автоматизованих систем моніторингу,3) IoT-сенсорів для контролю руху суден і вантажів[11, 12]. Проходить інтеграція з міжнародними стандартами: ви1конання вимог IMO щодо електронного обміну даними, впровадження MSW, VDES, підтримка глобальної логістики [13].

Україна орієнтується на кращі світові практики цифровізації портів (Роттердам, Сінгапур, Шанхай), де впроваджуються:

- Робототехніка та автоматизовані термінали.
- Інтелектуальні системи управління (AI, IoT).
- Технології блокчейн для безпечного обміну даними.
- Інтегровані платформи Port Community Systems (PCS) для оптимізації логістики та підвищення кібербезпеки [11].

Україна стикається з труднощами, як недостатній рівень автоматизації портових процесів, потреба у фінансуванні та підготовці кадрів, необхідність законодавчої підтримки цифрових трансформацій.

Висновки. Бездротові широкосмугові технології є ключовим чинником цифрової трансформації морської галузі України. Їх впровадження у рамках систем IALA сприяє автоматизації, підвищенню надійності навігаційного забезпечення, інтеграції до глобальної цифрової екосистеми мореплавства та виконанню міжнародних зобов'язань. Подальший розвиток БШД в Україні залежить від масштабування цифрових платформ, впровадження сучасних стандартів зв'язку (5G, VDES), інтеграції IoT та супутникових рішень, а також від активної участі у міжнародних ініціативах з цифровізації морських перевезень.

Література

1. Стратегія розвитку сфери електронних комунікацій України на період до 2030 року. Схвалено розпорядженням Кабінету Міністрів України від 4 червня 2025 р. № 546-р.

2. https://today.ua/ru/480092-oficijnij-zapusk-5g-v-ukrayini-hto-vzhe-v-zoni-nadshvidkogo-internetu/

3. https://www.maritimejournal.com/accessories-and-equipment/how-lte/5g-is-disrupting-maritime-connectivity/1467054.article

4. https://www.rivieramm.com/news-content-hub/news-content-hub/lte-and-5g-will-enhance-seafarer-communications-66244

5. https://5g.in.ua/pochatok-vprovadzhennia-5g-v-ukraini-shcho-oznachaie-dlia-korystuvachiv-ta-industrii/

6. https://agroperemoga.com.ua/morski-porty-ukrayiny-na-shlyakhu-do-povnoyi-tsyfrovizatsiyi-intehratsiya-mytnytsi-ta-port-community-system/

7. https://www.rbc.ua/ukr/news/ukrayini-pochnut-zapuskati-5g-ke-misto-pidklyuchat-1747416090.html

8. https://www.gsma.com/5ghub/5gsea

9. Мурад'ян А.О., Демидюков О.В. Особливості розвитку морських портів в умовах цифрових трансформацій: закордонний досвід. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Том 33(72). № 6. 2022. 247-252. URL: https://tech.vernadskyjournals.in.ua/journals/2022/6_2022/40.pdf.

10. https://www.yachting.com/uk-ua/news/what-is-ais-and-how-it-works?srsltid=AfmBOopRB6VPa3rn881ccIk4H8FjSOWFNzW_9c3nTSpIBNdm-aVeviue

11. https://hydro.gov.ua/?page_id=668

12. https://www.sternula.com/vdes-ais-2-0/

13. Пунченко Н.О., Цира О.В., Технологічний розвиток судноплавства, систем швартування судноплавства майбутнього, монографія./ Н.О. Пунченко, О.В.Цира // Iowa State University Digital Press, Editor-in-Chief Kotlyk S. 2022 DOI https://doi.org/10.31274/isudp.2022.121 ISBN 978-617-7867-37-0 (Print) ISBN 978-1-958291-01-6 (e-book). Стор. 220 – 291.

УДК 519.872

Уривський Л.О.
д.т.н., професор
КПІ ім. Ігоря Сікорського
leonid_uic@ukr.net

Косогор А. В.
Магістрант ІТС
КПІ ім. Ігоря Сікорського
kosogoranastasia@gmail.com

ПОРІВНЯННЯ МОДЕЛЕЙ РОЗРАХУНКУ ЙМОВІРНОСТІ БІТОВОЇ ПОМИЛКИ ДЛЯ РІЗНИХ МОДУЛЯЦІЙ У КАНАЛІ ЗВ'ЯЗКУ ЗА УМОВ ЗМІННОЇ ЕНЕРГЕТИКИ

Анотація. *У статті проведено аналіз залежностей ймовірності бітової помилки (BER) від співвідношення сигнал/шум (SNR) для чотирьох типів модуляції — BPSK, QPSK, 16-QAM та 64-QAM — у цифрових каналах зв'язку. Розрахунки виконано з використанням аналітичних формул, запропонованих Дж. Прокісом, К. Чо і Д. Юном, Л. Фінком та Л. Кантором. Особливу увагу приділено порівнянню точності моделей BER у діапазоні низьких значень SNR, де спостерігаються суттєві відмінності між результатами. Встановлено, що модель Чо і Юна забезпечує кращу відповідність фізичній суті процесів за умов слабкого сигналу, тоді як формули Прокіса схильні до переоцінки ймовірності помилки. Отримані результати дозволяють обґрунтувати вибір моделі BER при моделюванні та оптимізації телекомунікаційних систем з урахуванням умов завад та енергетичних обмежень.*

Сучасні телекомунікаційні системи функціонують в умовах постійно зростаючих вимог до якості передачі інформації, зокрема - до зниження ймовірності помилок, забезпечення стабільної пропускної здатності та адаптації до нестабільного середовища передачі. Одним із ключових факторів, що впливають на надійність інформаційного обміну, є змінна енергетика сигналу в каналі зв'язку - тобто непостійне відношення сигнал/шум (SNR), яке є типовим, наприклад, для мобільного, супутникового чи бездротового зв'язку.

За останні десятиліття цифрові комунікації вступили в фазу бурхливого розвитку, яка активно продовжується і в теперішній час. Використання сигнально-кодових конструкцій (СКК) дозволяє найбільш ефективно використовувати ресурси каналу, адже одночасно можливо отримати виграш як з енергетичної, так частотної ефективності або, у всякому разі, отримати виграш по одному показнику, не погіршуючи інший.

Важливим інструментом вибору оптимальних варіантів СКК в каналах із різноманітними параметрами є оцінка ймовірності бітової помилки (BER), яка допомогає обрати спосіб маніпуляції та спосіб кодування для досягнення потрібних показників якості передавання інформації. Для поширених видів маніпуляції, зокрема, для квадратурної амплітудної модуляції (QAM) показник BER традиційно визначається шляхом розрахунку ймовірності помилки за допомогою відомих аналітичних залежностей наведених у Таблиці 1.

Попри високу точність аналітичних виразів при високому відношенні сигнал-шум h^2, їх застосування при низьких значеннях h^2 може призводити до значних відхилень від точних значень BER.

У даній роботі проведено аналіз залежностей ймовірності бітової помилки від співвідношення сигнал/шум для чотирьох поширених видів модуляції: BPSK, QPSK, 16-QAM та 64-QAM. Розрахунки виконано з використанням формул, запропонованих Дж. Прокісом, К. Чо і Д. Юном, Л. Кантором та Л. Фінком. Оцінювання проводилося у широкому діапазоні значень SNR, зокрема в області низької енергетики, де традиційні моделі демонструють найбільші розбіжності.

Метою дослідження є з'ясування впливу вибору математичної моделі на точність розрахунку BER в умовах змінної енергетики каналу та різних модуляційних схем, а також

визначення доцільності використання тих чи інших формул у практичних завданнях телекомунікацій.

Для розрахунку зазначених показників використовуватимуться наступні формули:

Таблиця 1 – Формули для виконання розрахунків

Автор	**Формула для BPSK/QPSK**	**Формула для QAM-M**
Дж. Прокіс	$P_{b\,QPSK} = \frac{1}{2}\left[1 - F\left(\sqrt{2h^2}cos\frac{\pi}{4}\right)\right]$	$p_{b\,QAM} = \frac{4\left(1-\frac{1}{\sqrt{M}}\right)}{\sqrt{2\pi}}\int_{\sqrt{\frac{3}{M-1}h^2}}^{\infty} exp\left(\frac{-u^2}{2}\right)du$
К. Чо і Д. Юн	-	$p_{b\,M-QAM} \cong \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}} erfc\left(\sqrt{\frac{3\log_2 M\cdot h^2}{2(M-1)}}\right) + \frac{\sqrt{M}-2}{\sqrt{M}\log_2\sqrt{M}} erfc\left(3\sqrt{\frac{3\log_2 M\cdot h^2}{2(M-1)}}\right)$
Л. Кантор	$P_{b\,M-PSK} \approx \frac{2}{M} F\left(\sqrt{h^2}sin\frac{\pi}{2M}\right)$	-
Л. Фінк	$P_{b\,M-PSK} = 1 - F\left(\sqrt{2h^2}sin\frac{\pi}{M}\right)$	-

Для доведення різниці у результатах в залежності від використаної формули для визначення ймовірності бітової помилки нижче будуть закріплені графіки залежності ймовірності бітової помилки від співвідношення сигнал/шум в умовах модуляцій BPSK, QPSK, QAM-16, QAM-64.

Для розрахунку значення BER було використано програмне забезпечення “Matlab” та ПЗ “Excel” для розрахунку формул для отриманих значень та побудови і дослідження графіків. На побудованих графіках залежностей (Рисунок 1 та Рисунок 2) можна побачити закономірність зростання значень SNR в залежності від виду модуляції - відповідно, чим більша позиційність модуляції, тим більші показники. Задля зручності аналізу було обрано фіксовані значення BER: 10^{-2}, 10^{-3}, 10^{-4}, 10^{-5} та 10^{-6}, для яких обчислювали відповідні значення SNR згідно з кожною з моделей. Крім того, для всіх модуляцій будувалися графіки залежності BER від SNR, що дозволило наочно порівняти точність та поведінку моделей у різних енергетичних умовах.

Особливу увагу приділено області низьких значень SNR (0–10 дБ), оскільки саме в цій області більшість аналітичних моделей демонструють найбільші розбіжності через різні припущення, закладені в математичні вирази.

Значення ймовірності бітової помилки, що використовувалися для дослідження, а також розраховані відповідні значення співвідношення сигнал/шум для кожного типу модуляції наведено в Таблиці 2. Це дозволяє простежити, як змінюється енергетична вимога для забезпечення однакової якості передавання (BER) залежно від складності модуляційної схеми. Очевидним є той факт, що зі збільшенням кількості позицій у сигнальному просторі, необхідне значення SNR зростає.

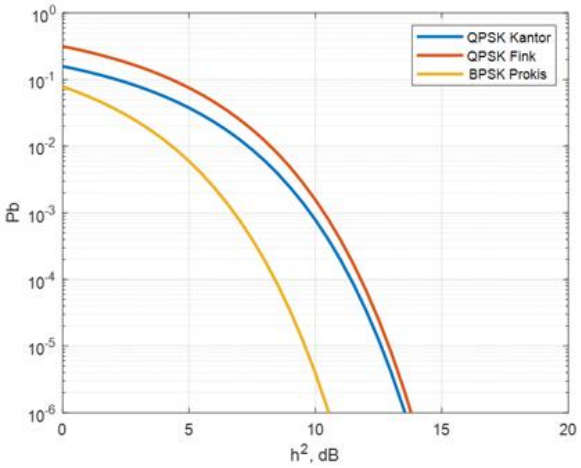


Рисунок 1 – Графік залежності ймовірності бітових помилок від SNR для сигналів бінарної BPSK та квадратурної QPSK маніпуляцій

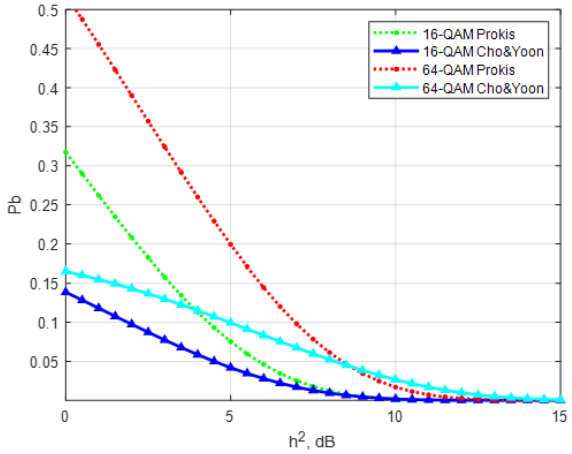


Рисунок 2 – Графік залежності ймовірності бітових помилок від SNR для багатопозиційних сигналів QAM-16 та QAM-64

Рисунок 3 – Номограма залежності ймовірності бітової помилки від SNR в дБ

Таблиця 2 – Отримані значення h^2 для кожного різновиду модуляції у випадку, якщо відома ймовірність бітової помилки

BER	BPSK	QPSK	QAM-16	QAM-64
10^(-2)	2,7378	5,4756	6,17	15,85
10^(-3)	4,805	9,61	11,22	30,2
10^(-4)	6,845	13,69	16,6	44,67
10^(-5)	8,82	17,64	22,39	60,26
10^(-6)	10,125	20,25	27,54	75,86

Загалом критерії завадостійкості сигналів бінарної та квадратурної маніпуляції визначались за формулами Дж. Прокіса, Л. Фінка та Л. Кантора, проте, наскільки ми можемо спостерігати за графіком на Рисунку 1, найбільш достовірними є результати від формули запропонованої Л. Фінком.

Залежності, які наведено на Рисунку 2 демонструють, що, за умов низької енергетики (h^2 < 8-10 дБ) формули Дж. Прокіса [1], використання яких дуже поширено в сучасних дослідження завадостійкості каналів з багатопозиційною маніпуляцією, не забезпечують достатньої точності.

При модуляції QAM-16 для $h^2 > 8$ дБ графічні залежності, отримані за виразами Дж. Прокіса і К. Чо та Д. Юна майже ідентичні. Одночасно, при $h^2 \sim 0$ ймовірність помилки за методикою Прокіса становить близько 0.32, тоді як у К. Чо і Д. Юна вона близько 0.14. Для випадку модуляції QAM-64 ситуація аналогічна, для $h^2 > 9$ дБ графічні залежності, результати майже ідентичні, але при менших значеннях h^2 результати суттєво різняться: ймовірність помилки за формулою Дж. Прокіса для QAM-M при $h^2 \sim 0$ перевищує 0.5 (що не відповідає фізичному змісту цієї помилки), а метод Cho & Yoon надає результат, близький до 0.17.

Отже, модель К. Чо і Д. Юн демонструє кращу точність при малих значеннях $h^2 <$ 8-10 дБ. При високих значеннях $h^2 >$ 8-9 дБ графіки завадостійкості сходяться, що означає, що для високої енергетики різниця між методами менш значуща.

Методика Дж. Прокіса дає перевищену оцінку ймовірності помилки на низьких значеннях h^2, що означає знижену точність для низької енергетики.

Натомість модель К. Чо і Д. Юн є більш точною та стабільною в усьому діапазоні значень h^2.

Висновки

Порівняння результатів різних методів оцінки бітової помилки свідчить про переваги та обмеження кожного з підходів. Аналітичні вирази є швидшими у реалізації і більш надійними для високих співвідношень сигнал/шум, але потребують корекції або розширення у разі низької енергетики чи нестандартних умов передачі. Зокрема, аналіз показав, що для модуляцій з високою позиційністю (QAM-16, QAM-64) формули Дж. Прокіса можуть суттєво переоцінювати значення ймовірності помилки при низьких значеннях SNR, що не відповідає фізичному змісту процесів у каналі зв'язку.

Натомість модель, запропонована К. Чо і Д. Юном, демонструє стабільні та точні результати як в області низької енергетики, так і при високих значеннях SNR. При цьому на високих рівнях сигналу всі методи дають схожі оцінки, а отже, відмінності між ними менш значущі. Це дозволяє зробити висновок, що точність визначення BER значною мірою залежить не лише від типу модуляції, а й від адекватності використаної математичної моделі до умов передачі.

Отримані результати доцільно враховувати при моделюванні та оптимізації цифрових систем зв'язку, особливо в умовах мобільного, супутникового чи бездротового середовища, де рівень шуму може динамічно змінюватися. Перспективним напрямом подальших досліджень є побудова адаптивних моделей розрахунку BER, які комбінують точність різних аналітичних підходів залежно від діапазону SNR. Такий гібридний підхід дозволить підвищити достовірність розрахунків без значного зростання обчислювальних витрат.

Література

1. Proakis, John G. Digital Communications. 4th ed. - New York: McGraw Hill, 2001.

2. Fink L. M. Discrete message transmission theory. - 1970. - 728 p.

3. Cho, K, and D. Yoon. "On the general BER expression of one- and two-dimensional amplitude modulations," IEEE Transactions on Communications, vol. 50, no. 7 (July 2002): 1074-1080. https://doi.org/10.1109/TCOMM.2002.800818.

4. Уривський Л.О., Шмігель Б.О. Визначення завадостійкості СКК в умовах низької енергетики. / К.: ІТС КПІ ім. Ігоря Сікорського, XV Міжнародна НТК «Перспективи

телекомунікацій», /Збірник матеріалів. - 2021, с.53...55. https://its.kpi.ua/sites/default/files/NDI%20TK%202021/Конференція%20ПТ/Збірники%20ПТ/Збірник%20матеріалів%20конференції%20ПТ%202021%20ISSN%20p.pdf

5. Уривський Л. О., Прокопенко К. А., Наталенко А. І. Векторно-фазовий метод для визначення показників завадостійкості багатопозиційних сигналів. — Зв'язок, № 12, 2012. - с.58...63.

6. Uryvsky L., Moshynska A., Qsypshuk S., Shmihel B. Comparison of methods for determining noise immunity indicators of a multiservice transmission system. / Advances in Information and Communication Technologies. Lecture Notes in Electrical Engineering, vol 560. / monograph. - Springer, Cham, p.p. 167...185. (2019) https://link.springer.com/chapter/10.1007/978-3-030-16770-7_8

УДК 519.872

Уривський Л.О.
д.т.н., професор
КПІ ім. Ігоря Сікорського
leonid_uic@ukr.net

Сколець А. В.
Магістр ІТС
КПІ ім. Ігоря Сікорського
kriklivanastya@gmail.com

МОДЕЛЮВАННЯ ПОКАЗНИКІВ QOS У СМО З УРАХУВАННЯМ САМОПОДІБНОГО ТРАФІКА: ПІДХІД НА ОСНОВІ РОЗПОДІЛУ ВЕЙБУЛЛА

Анотація. *Досліджено вплив властивості самоподібності трафіка на якісні показники функціонування систем масового обслуговування (СМО). Побудовано математичну модель одноканальної СМО M/M/1/∞ з найпростішим потоком та узагальнено її на випадок вхідного потоку, описаного розподілом Вейбулла, що репрезентує самоподібність (параметр Херста H=0,6-0,8). Порівняльний аналіз середнього часу очікування, часу перебування заявки в системі, довжини черги та кількості заявок показав збільшення цих величин у 2-8 разів при H→0,8 порівняно з пуассонівською моделлю, що доводить необхідність урахування самоподібності при проектуванні сучасних телекомунікаційних мереж.*

Результати численних емпіричних досліджень показали, що інтернет-трафік має властивість самоподібності, яка проявляється у вигляді довготривалої кореляції між подіями, а також наявності важкого хвоста у розподілі інтервалів між заявками. Така поведінка відрізняється від традиційних моделей, які базуються на припущенні про найпростіший (пуассонівський) потік. Ігнорування цієї властивості призводить до значних похибок при розрахунках характеристик систем масового обслуговування. У даній роботі досліджено вплив самоподібності на СМО шляхом використання Вейбуллівського розподілу, що наближує статистичні властивості реального інтернет-трафіку.

Метою є кількісна оцінка розбіжностей між показниками СМО з пуассонівським та самоподібним (Вейбуллівським) вхідним потоком і формулювання практичних рекомендації.

У класичній теорії СМО, зокрема в моделі M/M/1, використовується припущення про незалежність подій та експоненційний розподіл часу між надходженням заявок і їх

обслуговуванням [1], що значно спрощує математичний аналіз. Основною перевагою цієї моделі є аналітична зручність і наявність замкнених формул для основних характеристик (затримки, черги, завантаження тощо). Однак з часом було виявлено, що багато реальних потоків, зокрема в інтернет трафіку, не відповідають таким припущенням.

Зокрема, у 1990-х роках у серії класичних досліджень (W. Leland, M. Taqqu, W. Willinger, D. Wilson) [2] було встановлено, що інтернет-трафік має властивість **самоподібності**, яка проявляється в тому, що поведінка трафіку зберігається при масштабуванні часової осі.

Самоподібність – це статистична властивість трафіку, яка проявляється у вигляді довготривалої кореляції між подіями. Інтернет-трафік, зокрема у соціальних мережах, демонструє поведінку, за якої збільшення часової шкали не «згладжує» трафік, як це характерно для пуассонівських потоків. Така властивість описується параметром Херста [3] H∈(0.5;1). Чим ближче H до 1, тим виразніше проявляється самоподібність, зокрема у вигляді «сплесків» та «важких хвостів» у розподілах.

Для обґрунтування вибору статистичної моделі, придатної для опису самоподібного трафіку, було проведено порівняльний аналіз функцій розподілів. Встановлено, що функції з експоненційним розподілом та розподілом Вейбулла [4] мають характер показової функції, тоді як функція розподілу Парето має характер степеневої функції. Така відмінність призводить до принципово різних властивостей моделі. Крім того, розподіл Вейбулла має важливу асимптотичну властивість: при H=0,5 він збігається з експоненційним розподілом, що відповідає пуассонівському вхідному потоку. Таким чином, використання розподілу Вейбулла дозволяє узагальнити класичну модель та забезпечити поступовий перехід від випадку без самоподібності до режиму з довготривалими кореляціями при H>0,5.

Науково обґрунтовану позицію щодо доцільності використання розподілу Вейбулла при опису СМО із властивостями самоподібності можна бачити в наукових роботах [5-7].

Було сформульовано відповідні формули, які описують основні показники ефективності функціонування СМО: середній час перебування заявки в системі Wсист, середній час очікування Wоч , середню довжину черги L та середню кількість заявок у системі Q. У цих формулах ураховується вплив коефіцієнта самоподібності σ, який є функцією від параметра Херста та коригує стандартні експоненціальні вирази для більш точної апроксимації реального процесу.

Для розрахунку зазначених показників використовуються наступні формули [8]:

Таблиця 1 – Формули для виконання розрахунків

Показник	Пуассон (M/M/1/∞)	Вейбулл (M/M/1/∞)
Середня кі-сть заявок в СМО (Q)	$Q = \frac{\rho}{1-\rho}$	$Q = \frac{\rho}{1-\sigma}$
Середня довжина черги (L)	$L = \frac{\rho^2}{1-\rho}$	$L = \frac{\rho \cdot \sigma}{1-\sigma}$
Середній час перебування заявки в системі ($W_{сист}$)	$W_{сист} = \frac{1}{\mu \cdot (1-\rho)}$	$W_{сист} = \frac{1}{\mu \cdot (1-\sigma)}$
Середній час очікування заявки в черзі ($W_{оч}$)	$W_{оч} = \frac{\rho}{\mu \cdot (1-\rho)}$	$W_{оч} = \frac{\sigma}{\mu \cdot (1-\sigma)}$

Для доведення важливості врахування фактору самоподібності проведено графічне порівняння показників якості обслуговування при розподілі Пуассона і розподілі Вейбулла, використовуючи представлені формули.

Для розрахунку значення σ (сігми) для параметру Херста рівним 0,6, 0,7 та 0,8 було використано програмне забезпечення “Matlab” та ПЗ “Excel” для розрахунку формул для отриманих значень та побудови і дослідження графіків.

Будуючи графіки для кожного показника якості обслуговування, зображається залежність відповідного показника від інтенсивності навантаження для кожного параметру Херста, зокрема H=0,5, що відповідає розподілу Пуассона, та H={0,6 0,7 0,8}, що відповідає розподілу Вейбулла (як ознака самоподібності).

Деякі результати представлені у вигляді графіків залежностей кожного з показників від параметра H [9, 10].

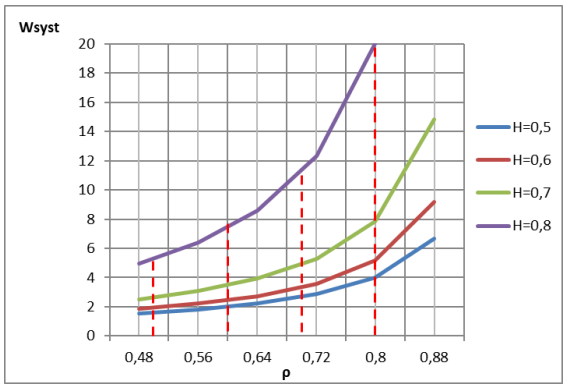


Рисунок 1 – Середній час перебування заявки в системі при різних значеннях параметру Херста для μ = 1,25

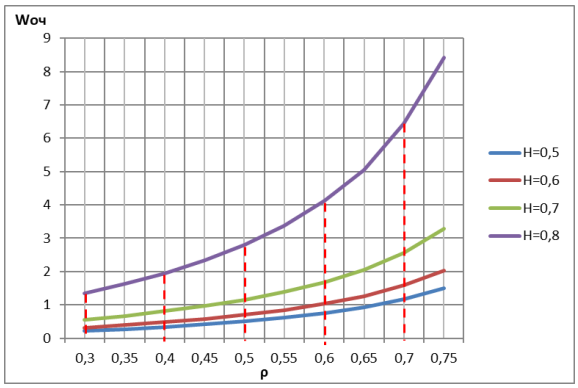


Рисунок 2 – Середній час очікування заявки при різних значеннях параметру Херста для μ = 2

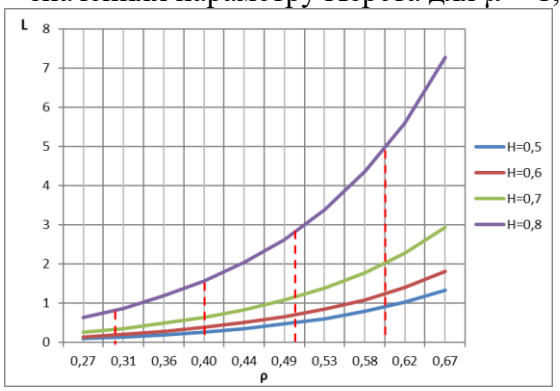


Рисунок 3 – Довжина черги заявок при різних значеннях параметру Херста для μ = 2,25

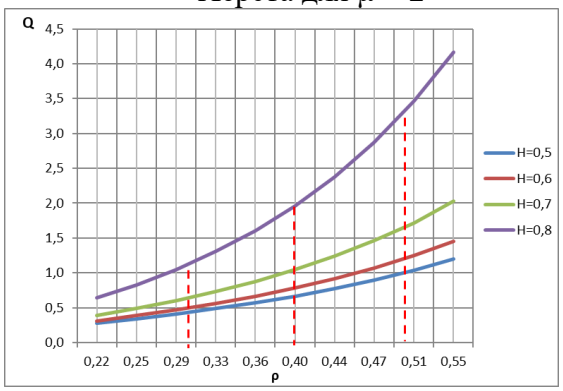


Рисунок 4 – Середня кількість заявок при різних значеннях параметру Херста для μ = 2,75

Аналізуючу результати залежностей показників самоподібного потоку від найпростішого потоку, їх можна об’єднати вирахувавши середнє значення залежностей між різнми інтенсивностями обслуговування для кожного показника якості обслуговування і отримуємо такі інтервали змін середніх значень:

Таблиця 2 – Інтервали змін середніх значень показників якості обслуговування

H	**ΔWсист**	**ΔWоч**	**ΔL**	**ΔQ**
0,6	1,2-1,3	1,3-1,5	1,3-2	1,1-1,3
0,7	1,5-2	2,1-2,5	1,8-3,3	1,4-2
0,8	2,7-5	5,3-6,3	5,3-8,3	2,6-5

З таблиці видно, що найбільш чутливим показником щодо врахування фактора самоподібності є показники середнього часу очікування Wоч та середньої довжини черги L, для яких розбіжність у показниках у порівнянні із розподлом Пуассона складає до 6-8 разів.

Решта показників теж вразлива щодо обрання умов функціонування інформаційної системи, оскільки розбіжністю у 2-3 разів теж нехтувати не можна.

Висновки

Результати проведеного моделювання свідчать про істотний вплив самоподібності вхідного трафіку на характеристики систем масового обслуговування. При зростанні параметра Херста H спостерігається багаторазове погіршення показників якості обслуговування – зокрема, середній час очікування та довжина черги можуть збільшуватися у 2-8 разів. Модель на основі розподілу Вейбулла забезпечує узагальнення класичних підходів і дозволяє точно описати перехід від пуассонівської до самоподібної поведінки трафіку.

Подальші дослідження планується спрямувати на розширення представленої моделі до випадку багатоканальної СМО з обмеженою чергою, де вплив самоподібності може виявлятися інакше внаслідок одночасного обслуговування кількох заявок та наявності ймовірності втрат. Такий підхід дозволить сформулювати прикладні рекомендації щодо ефективного використання системних ресурсів в умовах трафіку з довготривалою залежністю.

Література

1. Kleinrock, L. Queueing Systems. Volume 1: Theory // Wiley-Interscience, 1975. – 480 p.
2. Leland, W. E., Taqqu, M. S., Willinger, W., Wilson, D. V. On the self-similar nature of Ethernet traffic (extended version) // IEEE/ACM Transactions on Networking. – 1994. – Vol. 2(1). – P. 1–15.
3. Hurst, H.E. (1951). "Long-term storage capacity of reservoirs". Transactions of the American Society of Civil Engineers. v.116, p.770.
4. Weibull, W. A statistical distribution function of wide applicability. J. Appl. Mech. 1951, 18, 293–297.
5. Strelkovskaya I., Solovskaya I., Grygoryeva T., Paskalenko S. The solution to the problem of the QoS characteristics definition for self-similar traffic serviced by the W/M/1 QS // 2016 Third International Scientific-Practical Conference Problems of Infocommunications. Science and Technology / October 4-6, 2016, Kharkiv, Ukraine – p.p. 21-23.
6. Strelkovskaya I.V. at. al, Self-similar traffic in G/M/1 queue defined by the Weibull distribution», Radioelectronics and Communications Systems, V. 61, no. 3(2018), pp. 173-180, 2018. https://doi.org/10.20535/S0021347018030056.
7. Strelkovskaya I.V. at. al, Finding some QoS characteristics of self-similar traffic serviced by a mobile network // Proceedings 2nd IEEE International Conference Advanced Information and Communication Technologies-2017, July 4-7, 2017. – pp. 146-149. https://doi.org/10.1109/AIACT.2017.8020086
8. Уривський Л.О., Криклива А.В. Дослідження динаміки показників обслуговування в СМО із самоподібним трафіком // К.: НН ІТС КПІ ім. Ігоря Сікорського, XVI Міжнародна НТК «Перспективи телекомунікацій», /Збірник матеріалів. – 2022, с.53-58.
9. Uryvsky L., Skolets A. Analysis of the Influence of the Self-Similarity Factor on the Characteristics of Mass Service Systems through Quantitative Assessment / 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)/ 13-18 Nov. 2023 – p.p. 136-140.
10. Уривський Л.О., Сколець А.В. Дослідження впливу фактору самоподібності на функціонування СМО. - К.: НН ІТС КПІ ім. Ігоря Сікорського, XVII Міжнародна НТК «Перспективи телекомунікацій» / Збірник матеріалів. – / К.: НН ІТС КПІ ім. Ігоря Сікорського. – 2023, с. 68-71.

УДК 621.314

Русу Олександр Петрович, к.т.н.
Міжнародний гуманітарний університет
shurusu@ukr.net

Гінжул Владислав Михайлович
здобувач 1 курсу другого (магістерського) рівня
зі спеціальності 172 Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет

ВИЗНАЧЕННЯ РОЗМІРІВ НАКОПИЧУВАЛЬНИХ ДРОСЕЛІВ ПЕРЕТВОРЮВАЧІВ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Анотація. *У роботі розглянуто питання визначення розмірів дроселів, що застосовуються в імпульсних перетворювачах напруги телекомунікаційного обладнання. Наведено математичну модель, яка встановлює зв'язок між параметрами магнітного кола, струмового навантаження та кількості енергії, що проходить через дросель у межах одного циклу перетворення. Показано, що зменшення розмірів дроселів досягається за рахунок збільшення робочої частоти, застосування матеріалів з підвищеними характеристиками та оптимізації теплових режимів. Результати дослідження можуть бути використані для оцінки мінімально допустимих габаритів індуктивних компонентів у системах живлення з високою щільністю компонування.*

У сучасних телекомунікаційних системах для перетворення параметрів електричної енергії переважно застосовуються імпульсні методи, що забезпечують найвищу ефективність і економічну доцільність у порівнянні з альтернативними підходами. Імпульсні джерела живлення постійно зазнають змін у частині схемотехнічної реалізації, що зумовлено потребою підвищення ефективності, зниження втрат і покращення масо-габаритних характеристик. Щороку розробляються нові схеми, які спрямовані на оптимізацію окремих параметрів функціонування перетворювачів [1]. Водночас питання співставлення питомих характеристик індуктивних елементів різного конструктивного виконання залишається недостатньо вивченим. Це і визначає актуальність поставленої задачі – провести аналіз та визначити питомі параметри магнітних компонентів, що використовуються у вузлах стабілізації напруги телекомунікаційних пристроїв.

Дроселі імпульсних перетворювачів складаються з одного або кількох обвитків провідника, намотаних на магнітопровід, що концентрує магнітне поле й забезпечує зв'язок із зовнішнім електричним колом (рис. 1) [2].

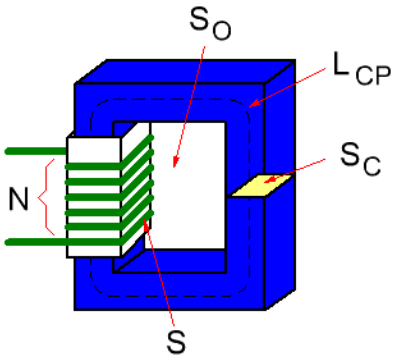


Рисунок 1 – Будова дроселя імпульсного перетворювача

Основними геометричними характеристиками магнітопроводу, окрім властивостей матеріалу, з якого він виготовлений, є довжина середньої магнітної лінії $L_{ср}$, поперечна площа сердечника S_C і площа монтажного вікна S_O, призначеного для розміщення обмоток. Об'єм робочої частини магнітного осердя, що безпосередньо бере участь у процесі перетворення енергії, визначається як добуток $L_{ср}$ на S_C: це значення відповідає фізичному об'єму магнітного матеріалу V, залученого до процесу:

$$V = S_C L_{\text{СР}}. \tag{1}$$

В процесі роботи по обвиткам обмотки протікає електричний струм I, який, відповідно до закону Джоуля-Ленца, призводить до її нагрівання. Площа S, яку займає обмотка у вікні магнітопроводу, визначається формулою:

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

Кількість витків обмотки N визначає зв'язок між зміною магнітного потоку ΔФ у сердечнику та електрорушійною силою, що виникає в провіднику. У випадку, коли на затискачах обмотки протягом інтервалу часу Δt діє напруга U, між цими величинами встановлюється співвідношення, яке формулюється згідно із законом електромагнітної індукції Фарадея:

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

Магнітний потік Ф у магнітопроводі визначається як добуток магнітної індукції B та площі поперечного перерізу сердечника S_C. Звідси випливає, що варіації потоку безпосередньо залежать від змін магнітної індукції. Тобто, при фіксованій площі S_C, зміна потоку ΔФ пропорційна зміні індукції ΔB:

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

Після вираження кількості обвитків N з рівняння (3) та підстановки цього виразу у формулу (2), а також з урахуванням співвідношення (4), можна отримати узагальнену залежність, яка встановлює зв'язок між напругою на обмотці, параметрами магнітного кола та зміною магнітної індукції:

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

Виходячи з формули (5), можна зробити висновок, що площа S, відведена під обмотку у вікні магнітопроводу, визначається рівнем енергетичного навантаження індуктивного елемента, а також значеннями густини струму J у провіднику та магнітної індукції B в осерді. Це означає, що для реалізації заданих енергетичних параметрів необхідно використовувати магнітопровід з геометричними характеристиками, які задовольняють наступну нерівність:

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

Аналіз формули (6), що геометричні розміри дроселів імпульсних перетворювачів прямо пропорційні кількості енергії, яку потрібно перетворити за один цикл перетворення. Таким чином, зменшення розмірів дроселя можливе за рахунок використання матеріалів з високим значенням магнітної індукції B, чи покращення умов охолодження, що дозволить підвищити цільність струму в обмотках J. Однак основним шляхом мініатюризації дроселів імпульсних перетворювачів є збільшення частоти перетворення, що дозволить зменшити кількість енергії, яка перетворюється в кожному циклі (добуток $UI\Delta t$).

Висновки

На основі проведеного аналізу встановлено, що геометричні параметри індуктивних елементів імпульсних перетворювачів безпосередньо залежать від величини енергії, яка передається через магнітне коло за цикл перетворення. Виведена аналітична залежність (6) дає змогу оцінити вплив густини струму в обмотках та магнітної індукції в осерді на площу, необхідну для розміщення провідника. Зменшення розмірів дроселів можливе шляхом підвищення допустимих значень J і B, що вимагає застосування відповідних матеріалів та рішень з охолодження. Найефективнішим способом мініатюризації індуктивних елементів залишається збільшення частоти роботи перетворювача, що знижує енергетичне навантаження в окремому циклі перетворення. Представлені розрахунки можуть бути використані при проєктуванні компактних телекомунікаційних джерел живлення з урахуванням вимог до ефективності та габаритів.

Література

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

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

УДК 372.862:004

Горбачов В. Е., к.т.н., доцент
Хнюнін С. Г., к.т.н., доцент
Більдюгіна С. С., студент V курсу
Міжнародний гуманітарний університет
Горбачов П. В., учень III курсу
Фаховий коледж НТІІС
physmgu@gmail.com

АДАПТИВНЕ НАВЧАННЯ В КУРСІ ІНФОРМАТИКИ ТА ПРОГРАМУВАННЯ

Анотація. *У роботі розглядаються особливості використання методики адаптивного навчання в шкільному курсі інформатики. Сформовано особливу структуру курсу вивчення інформатики та програмування, при якій учень може обрати варіанти складності навчального матеріалу та індивідуальних завдань, що відповідає його цілям, можливостям та здібностям. При такій побудові курсу, школяр чітко знає мету вивчення розділів курсу та сам приймає рішення про вибір складності шляху досягнення цієї мети, що значно підвищує вмотивованість в навчанні.*

Наразі неможливо уявити жодну сферу діяльності людини без використання інформаційних технологій, тому інформатика є найважливішою шкільною дисципліною для формування сучасного члена суспільства, незалежно від спеціальності, в якій майбутній громадянин має намір працювати. З іншого боку, інформатика і програмування є галуззю знань, що найбільш бурхливо розвивається. Щодня ми отримуємо відомості про впровадження нових рішень, методів та прийомів організації інформаційних систем. Лише останніми роками виділилися у самостійні галузі інформатики питання організації великих масивів даних, реалізації концепції побудови інформаційної мережі Інтернету речей, методів роботи зі штучним інтелектом.

Все вище сказане необхідно враховувати під час навчання інформатики та програмування у школі, тому курс інформатики безперервно збільшується як додаванням нових питань, а й навіть цілих розділів. Зараз у шкільному курсі інформатики для 10 -11 класів профільного навчання налічується дев’ять дуже перевантажених розділів [1]. В результаті школяр виявляється перевантаженим навчальною інформацією, виниклі труднощі з вивченням однієї теми тягнуть за собою відставання з інших тем, що різко знижує ефективність навчання.

Крім того, ще в загальноосвітній школі спостерігається сильна диференціація підготовленості учнів у галузі інформатики: у будь-якому класі є школярі, які вже знайомі з елементами програмування, тоді як інші мають знання лише на рівні перегляду кліпів у ТікТок. Складається ситуація, коли спрощення матеріалу веде до пасивності однієї групи учнів, а ускладнення – до труднощів засвоєння матеріалу іншою групою школярів. Тому, до навчання інформатики та програмування потрібні нові інноваційні підходи, які, з одного боку спрощували б сприйняття великого обсягу складного матеріалу, і, водночас, не знижували б інтерес найбільш підготовлених учнів до дисципліни та підвищили б вмотивованість учнів в навчанні.

Найбільш ефективним методом для вирішення цієї проблеми є адаптивний метод навчання, в якому використовується принцип досягнення учнями мети навчання шляхами різного рівню складності. Ключова особливість даного методу полягає в тому, що школяру надається можливість самому, виходячи з оцінки своїх можливостей та потреб, обрати рівень складності учбового матеріалу за яким він буде досягати мети навчання. Такий підхід

унеможливлює формальне ставлення до процесу навчання, оскільки учень повинен сам відповідально зробити вибір, а для цього чітко уявляти собі мету навчання, тобто той навчальний матеріал, який йому надається можливість вивчити. Адаптивний метод дозволяє зміцнити упевненість учнів у можливості досягнення мети навчання без проблем із вивченням складного матеріалу. Така самостійність та впевненість суттєво мотивує учнів до отримання відповідних знань.

Метою даної роботи є використання методики адаптивного навчання інформатики і програмуванню для кращого розуміння та засвоєння матеріалу, що вивчається учнями з різними рівнями підготовки.

Останні дослідження з адаптивного навчання свідчать про те, що воно ідеально підходить для навчальних цілей. Так в роботі [2] досліджено умови впровадження адаптивного навчання, та зроблено висновок, що такий підхід пропонує відповідь на очікування студентів щодо їхніх конкретних цілей і професійного розвитку, що прискорює навчання й сприяє мотивації студентів, тому дійсно являє собою майбутнє професійної підготовки. Схема адаптивні навчальні системи з використанням штучного інтелекту запропонована в статті [3], де стверджується, що адаптивне навчання дозволяє уникнути численних прогалин в індивідуальній підготовленості учня, допомагає досягати йому отримати бажаний рівень знань.

У науковій літературі можна зустріти безліч схем та алгоритмів впровадження адаптивного методу навчання, однак немає роботи з конкретними прикладами застосування цього методу на практиці для обраної дисципліни. У цій роботі досліджувалась можливість застосування адаптивного методу навчання до курсу інформатики у старших класах, а конкретний опис такого застосування розглянуто на прикладі окремого модуля цього курсу "Веб-технології", на вивчення якого, згідно до типової навчальної програми [4], планується 35 навчальних годин.

Істотною перешкодою для повсюдного впровадження адаптивного методу навчання є потреба великих трудових витрат викладача, оскільки від якості підготовки самого адаптованого контенту, організаційних питань, апаратного забезпечення суттєво залежить результат його застосування, однак час, витрачений на підготовку занять, потім з лишком окупається неприхованою зацікавленістю всіх учнів у вивченні предмета.

Першим кроком запровадження методу адаптації є структуризація учбового матеріалу з використанням методики алгоритмізації. У курсі інформатики, згідно до типової навчальної програми [1], з було виділено дев’ять послідовних самостійних частин курсу, кожна з котрих логічно закінчена та представляє самостійний елемент. У Таблиці 1 представлена структурно-логічна схема послідовності навчальних елементів шкільного курсу інформатики у вигляді окремих блоків.

Таблиця 1 – Структурно-логічна схема послідовності навчальних елементів шкільного курсу інформатики

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

Таке подання матеріалу, що вивчається, з самого початку дає можливість учням побачити об’єм всього курсу та оцінити свої можливості при його засвоєнні.

Далі було використано методику чіткої постановки мети кожного структурного блоку алгоритму процесу вивчення курсу інформатики. Наприклад, для восьмого структурного блоку – це побудова сторінки сайту на екрані монітора.

Наступним кроком було реалізовано основний принцип адаптивного методу навчання – методика диференціації навчального матеріалу за рівнями складності. Цей процес потребує найбільшого часу викладача. Рівень складності можна змінити, змінюючи час навчання або обсяг навчального матеріалу, у учня завжди повинна бути можливість вибору альтернативних способів досягнення мети навчання. У простішому макроадаптивнму випадку існують три варіанти досягнення мети навчання – це найпростіший «Базовий», «Прикладний» та «Творчий» (Таблиця 2). Учень має право змінити варіант навчання, оскільки, як показують дослідження, рушійним фактором підвищення успішності студента є завдання середньої складності.

Таблиця 2 – Розгалужена за рівнем складності спрощена структура алгоритму блоку «Веб-технології»

Рівень складності	Базовий	Прикладний	Творчий
Елементи для вивчення.	Мова розмітки гіпертексту HTML	Мова розмітки гіпертексту HTML. Правила використання каскадних таблиць стилів CSS та табличного верстання	Мова розмітки гіпертексту HTML. Правила використання каскадних таблиць стилів CSS та табличного верстання. Засоби роботи з об'єктною моделлю документа в мові сценаріїв JavaScript
Мета	Побудова сторінки сайту на екрані монітора за допомогою всіх елементів для навчання згідно з рівнем складності		

Далі було застосовано методику планування подій навчального процесу, яка істотно впливає на ефективність адаптивного навчання, оскільки будь-який збій у послідовності дій на занятті призводить до втрати інтересу і довіри учнів, отже, зводить нанівець всі зусилля вчителя з організації уроку.

И нарешті вкрай необхідна методика попередньої підготовки слухачів. На цієї частині уроку треба чітко сформулювати мету заняття (наприклад – побудова сторінки сайту), визначити шляхи її досягнення (наприклад – базовий, прикладний та творчий). Далі треба пояснити засоби досягнення мети, тобто зробити короткий опис навчального матеріалу, який необхідно вивчити. Наприклад, при базовому рівню складності учень може обмежиться вивченням мови розмітки гіпертексту HTML, при прикладному рівню складності учень, окрім мови розмітки гіпертексту HTML, повинен розібратися з правилами використання каскадних таблиць стилів CSS та табличного верстання, а при творчому рівню складності потрібно вивчити засоби роботи з об'єктною моделлю документа в мові сценаріїв JavaScript. Крім того, в ході попередньої підготовки слухачам треба чітко пояснити організаційні правила, а саме: на якому етапі відбувається вибір рівня складності, чим відрізнятимуться результати проходження відповідного рівня, в який момент та як можна змінити рівень складності.

Висновок. Таким чином, сформовано таку структуру шкільного курсу інформатики при якій учень у процесі навчання повинен обрати індивідуально сплановану послідовність 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.

УДК 378.22:004.9

Єрмакова С.С. доктор педагогічних наук, професор, практичний психолог
Міжнародний гуманітарний університет
ermakovasvitlana2011@ukr.net

ЦИФРОВІ ТРЕНДИ СУЧАСНОЇ ОСВІТИ

***Анотація**. У статті розглядаються ключові тренди формування майбутньої освіти, аналізуються такі аспекти як, персоналізоване навчання, штучний інтелект, адаптивні освітні технології, штучний інтелект в дидактиці, віртуальна і доповнена реальність, а також розвиток навичок 21 століття. Особлива увага приділяється впливу цих технологій на трансформацію особистості сучасного педагога і здобувача освітніх послуг, а також на доступність і інклюзивність освіти. Прогнозується як саме інтеграція даних трендів може призвести до створення більш гнучких, ефективних освітніх систем, спроможних відповідати викликам швидкозмінному світу.*

Сучасна освіта зазнає значних трансформацій під впливом цифрових технологій, що формують нові підходи до навчання та викладання.

Одним із ключових трендів є *персоналізація навчання*, де адаптивні платформи та штучний інтелект дозволяють створювати індивідуальні освітні траєкторії, враховуючи потреби та темп кожного учня.

Другим важливим напрямком є *змішане навчання* (blended learning), яке поєднує традиційні аудиторні заняття з онлайн-інструментами та ресурсами. Це забезпечує гнучкість, розширює доступ до навчальних матеріалів і сприяє розвитку самостійності. Мобільне навчання (m-learning) також набирає обертів, дозволяючи отримувати знання в будь-який час і в будь-якому місці за допомогою смартфонів та планшетів.

Третій тренд – це *гейміфікація та віртуальна/доповнена реальність (VR/AR)* в освітньому процесі. Використання ігрових елементів підвищує мотивацію учнів, а VR/AR створює іммерсивні середовища для симуляцій, віртуальних екскурсій та практичних занять, що значно покращує засвоєння складних концепцій.

Нарешті, *аналіз великих даних (big data analytics) в освіті* дозволяє відстежувати прогрес учнів, виявляти прогалини у знаннях та прогнозувати освітні результати, що дає

можливість викладачам та адміністрації приймати обґрунтовані рішення для покращення якості навчання.

Вище зазначені цифрові тренди не лише підвищують ефективність освітнього процесу, але й готують до викликів цифрової епохи.

Відтак, адаптивним інструментарієм цифрової трансформації освіти є інтелектуальні інформаційні технології. Увага багатьох дослідників до цього класу технологій нині набуває значущих обертів та находить своє відображення в науковому доробку. Актуальним стає інформаційно-аналітичний супровід цифрової трансформації освіти і педагогіки у цьому контексті. Потребує ґрунтовних досліджень джерелознавчий та історіографічний аспекти цієї проблеми.

Загалом, інтелектуальні інформаційні технології (ІІТ) представляють собою комплекс дисциплін і методів, що дозволяють створювати системи, здатні сприймати, обробляти, аналізувати та інтерпретувати дані, а також генерувати знання та приймати рішення, імітуючи людські когнітивні процеси. Ці технології є ключовим рушієм сучасної цифрової трансформації, змінюючи підхід до управління інформацією та її використання в найрізноманітніших сферах.

Ядром ІІТ є кілька взаємопов'язаних напрямків:

- штучний інтелект (ШІ). (На часі це широка галузь, що охоплює розробку агентів, здатних міркувати, навчатися, планувати та сприймати. У контексті ІІТ, ШІ надає інструменти для автоматизації когнітивних завдань, таких як розпізнавання образів, обробка природної мови та прийняття рішень);

- машинне навчання (МН). (Загалом МН є підгалузь ШІ, й фокусується на розробці алгоритмів, які дозволяють системам навчатися на основі даних, не будучи явно запрограмованими. Це включає в себе алгоритми класифікації, регресії, кластеризації та глибокого навчання, що є основою для багатьох інтелектуальних систем);

- обробка природної мови (ОПМ). (Дає змогу комп'ютерам розуміти, інтерпретувати та генерувати людську мову. Це критично важливо для створення чат-ботів, віртуальних асистентів, систем перекладу та аналізу текстових даних);

- комп'ютерний зір (Дозволяє системам "бачити" і інтерпретувати візуальну інформацію з зображень і відео. Застосовується у розпізнаванні обличчя, автономних транспортних засобах, медичній діагностиці та системах безпеки);

- експертні системи (Системи, що імітують процес прийняття рішень експертами в певній предметній області, використовуючи бази знань та правила виведення);

-системи підтримки прийняття рішень (СППР) (Інструменти, що допомагають користувачам приймати обґрунтовані рішення, аналізуючи великі обсяги даних та надаючи релевантну інформацію).

Враховуючи вищезазначене спостерігаємо, що ІІТ знаходять своє застосування практично в кожній галузі людської діяльності:

1) бізнес і фінанси (Оптимізація бізнес-процесів, прогнозування ринків, виявлення шахрайства, персоналізація послуг для клієнтів (рекомендаційні системи), автоматизація кол-центрів);

2) медицина та охорона здоров'я (Діагностика захворювань, розробка нових ліків, персоналізована медицина, аналіз медичних зображень, управління даними пацієнтів);

3) промисловість та виробництво (Оптимізація виробничих процесів, прогнозне обслуговування обладнання, контроль якості, робототехніка та автоматизація);

4) освіта (Персоналізоване навчання, адаптивні навчальні платформи, автоматична оцінка знань, створення інтелектуальних тьюторів);

5) державне управління та "розумні міста" (Оптимізація трафіку, управління енергоспоживанням, системи безпеки, надання інтерактивних державних послуг);

6) наукові дослідження (Аналіз великих даних, моделювання складних систем, виявлення нових закономірностей у наукових даних).

Проте незважаючи на величезний потенціал, впровадження ІІТ стикається з низкою викликів:

- етичні питання - прозорість і пояснюваність алгоритмів, упередженість даних, приватність і безпека даних, відповідальність за рішення, прийняті ШІ;
- складність і вартість впровадження - розробка та інтеграція ІІТ-рішень потребує значних інвестицій та висококваліфікованих спеціалістів;
- якість даних- ефективність інтелектуальних систем безпосередньо залежить від якості, повноти та достовірності даних, на яких вони навчаються;
- регуляторне середовище - необхідність розробки адекватних законодавчих і нормативних актів для регулювання використання ІІТ.

Саме тому, перспективи розвитку ІІТ вражають. Подальший прогрес у машинному навчанні, поява більш потужних обчислювальних ресурсів, розвиток квантових обчислень та інтеграція ІІТ з іншими передовими технологіями (наприклад, Інтернет речей, блокчейн) відкривають нові горизонти.

Отож, ми стоїмо на порозі ери, коли інтелектуальні системи стануть ще більш інтегрованими в наше повсякденне життя, змінюючи спосіб нашої роботи, навчання та взаємодії зі світом. Інтелектуальні інформаційні технології – це не просто інструменти, це каталізатор змін, що формує майбутнє, в якому інформація стає не лише даними, а й джерелом розуміння та інтелекту.

Таким чином, цифрові тренди відкривають безмежні можливості для трансформації освіти, роблячи її більш доступною, персоналізованою та ефективною. Однак важливо пам'ятати, що технології є лише інструментом. Успіх цифрової трансформації освіти залежить від здатності педагогів адаптуватися до нових реалій, розробляти інноваційні методики та зосереджуватися на розвитку всебічно розвиненої особистості, готової до викликів майбутнього.

УДК 378.22:004.9

Іванова О. С. кандидат філософських наук, доцент
Міжнародний гуманітарний університет
okmegalodon2021@ukr.net

ФІЛОСОФІЯ ОСВІТИ 4.0: ЦИФРОВІ ГОРИЗОНТИ СУЧАСНОЇ ОСВІТИ

Анотація. *Сучасна освіта стоїть на порозі глибоких трансформацій, зумовлених стрімким розвитком цифрових технологій. Стаття досліджує концептуальні засади та виклики, що постають перед освітньою системою в епоху Четвертої промислової революції. Проаналізовано вплив штучного інтелекту, великих даних, віртуальної та доповненої реальності на педагогічні парадигми, розглядають питання персоналізації навчання, розвитку критичного мислення та креативності в умовах цифрового середовища. Особливу увагу приділено етичним аспектам цифрової трансформації та формуванню нової ролі викладача як наставника в неперервному інноваційно наповненому освітньому процесі.*

У сучасному світі, що динамічно розвивається під впливом технологічних інновацій, освіта переживає глибокі трансформації. Концепція "Освіта 4.0" є прямою відповіддю на виклики та можливості Четвертої промислової революції, яка характеризується стрімким розвитком штучного інтелекту, інтернету речей, великих даних, віртуальної та доповненої реальності. Ці технології не просто змінюють методи викладання та навчання, а й переформатовують саму мету освіти, фокусуючись на формуванні навичок, необхідних для життя та роботи у цифровому суспільстві.

Філософія освіти 4.0 - це не просто чергова ініціатива чи реформа; це фундаментальний зсув у нашому розумінні мети, змісту та методів навчання в епоху Четвертої промислової революції. Освіта 4.0 – це парадигма, що виникла у відповідь на виклики та можливості, які створює Промисловість 4.0. Остання характеризується стрімким розвитком таких технологій, як штучний інтелект (ШІ), машинне навчання, інтернет речей (IoT), великі дані, робототехніка, віртуальна та доповнена реальність. Ці технології не тільки змінюють способи виробництва та управління, але й кардинально перетворюють ринок праці та суспільство в цілому. Відтак, освіта 4.0 – це проактивна відповідь системи освіти на ці зміни. Вона має на меті підготувати майбутнє покоління не лише до нинішніх умов життя, а й до майбутніх, ще невідомих викликів, розвиваючи у них навички, які дозволять їм бути гнучкими, адаптивними та інноваційними.

Враховуючи вище зазначене спостерігаємо, що Філософія освіти 4.0 базується на кількох фундаментальних принципах, що відрізняють її від традиційних освітніх моделей:

1.) персоналізація та адаптивність (навчання орієнтується на індивідуальні потреби, темп та стиль кожного учня; використання адаптивних навчальних платформ дозволяє автоматично підлаштовувати зміст і складність матеріалу, виходячи з прогресу здобувача);

2) гнучкість та доступність (освіта стає доступною будь-коли і будь-де; онлайнові курси, масові відкриті онлайн-курси, гібридні моделі навчання та мобільні додатки руйнують географічні та часові бар'єри, розширюючи можливості для неперервної освіти);

3) сфокусованість на компетенціях 21-го століття (акцент зміщується з запам'ятовування фактів на розвиток критичного мислення, креативності, співпраці, комунікації, вирішення проблем та цифрової грамотності; навички, які є незамінними у швидкозмінному світі);

4) проєктне та проблемно зорієнтоване навчання (учні залучаються до реальних проєктів та вирішення автентичних проблем, що сприяє глибшому розумінню матеріалу та розвитку практичних навичок);

5) використання новітніх технологій (інтеграція штучного інтелекту для персоналізованого навчання та аналізу даних, віртуальної та доповненої реальності для імерсивних симуляцій, інтернету речей для створення "розумних" навчальних середовищ, а також блокчейну для верифікації сертифікатів та освітніх досягнень).

Цифрові технології є каталізатором та основою освіти майбутнього. Так, наприклад,

- штучний Інтелект може аналізувати дані про навчання студентів, виявляти їхні слабкі та сильні сторони, рекомендувати індивідуальні навчальні траєкторії, надавати миттєвий зворотний зв'язок та автоматизувати рутинні завдання викладачів (наприклад, оцінювання);

- віртуальна та доповнена реальність створюють імерсивні навчальні середовища, де студенти можуть проводити віртуальні лабораторні роботи, симуляції хірургічних операцій, подорожувати в історичні епохи або досліджувати складні концепції у тривимірному просторі.

- великі дані (Big Data) та аналітика аавчання (Learning Analytics)сприяють збору та аналізу великих обсягів даних про освітній процес, що дозволяє ідентифікувати ефективні методи навчання, прогнозувати успішність здобувачів, виявляти труднощі та вдосконалювати освітні програми.

- хмарні технології забезпечують доступ до освітніх ресурсів, програмного забезпечення та платформ з будь-якого пристрою, сприяючи співпраці та обміну знаннями.

- інтернет речей у вигляді "розумних класів», що обладнані датчиками, можуть збирати дані про взаємодію здобувачів з освітнім середовищем, оптимізувати освітній простір та надавати індивідуалізований досвід.

Проте, незважаючи на значний потенціал, впровадження таких інноваційних технологій в освіту вона все ж стикається з низкою викликів, а саме:

1) цифрова нерівність (недоступність технологій та інтернету для всіх верств населення може поглибити розрив у можливостях отримання якісної освіти);

2) підготовка викладачів (необхідна масштабна перепідготовка викладачів, щоб вони могли ефективно використовувати нові технології та змінювати свої педагогічні підходи);

3) зміна освітніх програм (потреба у перегляді та адаптації навчальних планів для включення нових навичок та методів навчання);

4) кібербезпека та конфіденційність даних (захист персональних даних студентів та забезпечення безпеки освітніх платформ є критично важливими);

5) етичні аспекти штучного інтелекту (розробка етичних принципів використання ШІ в освіті, щоб уникнути упередженості та забезпечити справедливість).

Проте, принагідно зауважимо, що перспективи, які відкриває Освіта 4.0, значно переважають виклики. Вона обіцяє створити більш інклюзивну, ефективну та орієнтовану на майбутнє освітню систему, що готуватиме громадян до викликів та можливостей цифрової ери.

Таким чином Філософія освіта 4.0 – це не просто модернізація, а фундаментальна перебудова освітнього процесу, яка відповідає вимогам 21-го століття. Це синергія інноваційних технологій та педагогічних підходів, що зосереджені на розвитку критичних компетенцій, персоналізованому навчанні та доступності знань. Успішна реалізація цієї концепції вимагає злагоджених зусиль урядів, освітніх установ, викладачів та суспільства в цілому, щоб забезпечити кожному можливість реалізувати свій потенціал у світі, що постійно змінюється. Це шлях до формування гнучкого, адаптивного та конкурентоспроможного людського капіталу, який є запорукою сталого розвитку та процвітання.

УДК 378.22:004.9 – 047.22

Єрмакова С.С. доктор педагогічних наук, професор, практичний психолог
Міжнародний гуманітарний університет
ermakovasvitlana2011@ukr.net
Биков А. В. здобувач наукового ступеня доктора філософії
кафедри педагогіки та психології
Міжнародний гуманітарний університет
allanbykov@gmail.com

ЦИФРОВА ОСВІТА: ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ

Анотація. *У статті розглядаються сучасні тенденції і ключові інновації у галузі цифрової педагогіки. Аналізується вплив цифрових технологій на освітній процес, включаючи транформацію дидактичних засад освітнього процесу. Окреслено перспективи розвитку цифрової педагогіки такі як – персоналізоване навчання, гейміфікація та інтерактивні середовища, хмарні технології та співпраця, аналітика навчання та відкриті освітні ресурси. Визначено виклики з якими стикаються освітні навчальні заклади у мовах в провадження цих змін.*

Цифрова грамотність є «своєрідним каталізатором, що характеризує здатність людини навчатися впродовж життя» . Головною метою освіти у XXI столітті є формування нових професійних навичок, пов’язаних з домінуючою роллю, активним і швидким розвитком цифрового суспільства, що дає можливість впроваджувати нові форми навчання.

Цифрова педагогіка є швидкозростаючою сферою, що інтегрує цифрові технології в освітній процес для покращення навчання та викладання. Вона виходить за межі простого використання комп'ютерів, зосереджуючись на тому, як технології можуть трансформувати педагогічні підходи, сприяти індивідуалізації навчання та розвивати навички майбутнього.

Трансформація в освіті від навчання, яким керує педагог, до саморегульованого оволодіння компетентностями та уміннями, що потрібні для успішного життя в сучасному соціумі є основним завданням глобальної зміни в навчальному процесі. Відтак, сучасна цифрова педагогіка характеризується низкою інноваційних підходів та інструментів:

1. Персоналізоване навчання (використання адаптивних навчальних платформ та штучного інтелекту (ШІ) дозволяє підлаштовувати освітній контент і темп навчання під індивідуальні потреби кожного учня, що включає системи, які аналізують прогрес студента та пропонують персоналізовані завдання, ресурси та зворотний зв'язок).

2. Гейміфікація та інтерактивні середовища (впровадження ігрових елементів у навчальний процес (бали, рейтинги, квести) підвищує залученість та мотивацію учнів. Інтерактивні симуляції, віртуальна (VR) та доповнена реальність (AR) створюють імерсивні навчальні середовища, дозволяючи експериментувати та досліджувати складні концепції в безпечному та контрольованому просторі.

3.Хмарні технології та співпраця (наприклад хмарні платформи (Google Workspace, Microsoft 365) забезпечують доступ до навчальних матеріалів з будь-якого місця та пристрою, а також сприяють спільній роботі над проектами - це дозволяє студентам працювати разом у реальному часі, обмінюватися ідеями та розвивати навички командної роботи).

4.Аналітика навчання (Learning Analytics) - збір та аналіз даних про навчальну діяльність студентів дозволяє викладачам та адміністраторам відстежувати прогрес, виявляти труднощі та коригувати педагогічні стратегії. Це допомагає не лише оцінювати ефективність навчання, але й прогнозувати успішність студентів та вчасно надавати підтримку.

5.Відкриті освітні ресурси (OER) - доступність безкоштовних та відкрито ліцензованих навчальних матеріалів (онлайн-курси, підручники, відеолекції) розширює можливості для самоосвіти та доступу до якісної освіти для широких верств населення.

Створення індивідуалізованих навчальних рекомендацій допомагатиме студентам повністю реалізувати свій потенціал. Студенти будуть краще підготовлені до взаємодії з різними групами та спільнотами, вмітимуть, безпосередньо або у віртуальному просторі, компетентно спілкуватися з людьми різних культур, продовжуючи навчатися впродовж життя

До того ж, рамка компетентностей і умінь XXI століття поєднує навчальні й інноваційні уміння, так звана група «4 С»: критичне мислення (Critical thinking), комунікація (Communication), колаборація (Collaboration) і творчість (Creativeness); а також інформаційні, медіа і технологічні уміння та життєві і кар’єрні уміння. Саме тому, розвиток цифрової педагогіки відкриває значні перспективи для трансформації освіти:

- розширення доступу до якісної освіти, адже цифрові технології руйнують географічні та соціальні бар'єри, надаючи доступ до освітніх ресурсів та програм людям у віддалених регіонах або з обмеженими можливостями;
- індивідуалізація та диференціація (подальший розвиток ШІ та адаптивних систем дозволить ще точніше налаштовувати навчання під унікальні потреби кожного учня, забезпечуючи максимальну ефективність та глибоке засвоєння матеріалу);
- розвиток навичок 21 століття (цифрова педагогіка сприяє формуванню критичного мислення, креативності, колаборації та комунікації, які є ключовими для успіху в сучасному світі; навчання з використанням технологій природним чином інтегрує ці навички);
- безперервне навчання та перекваліфікація (умовах швидких змін на ринку праці цифрова педагогіка стає основою для систем безперервного навчання (Lifelong Learning), дозволяючи людям постійно оновлювати свої знання та набувати нових компетенцій);
- глобальна співпраця (цифрові інструменти сприяють міжнародній співпраці між навчальними закладами, викладачами та студентами, що відкриває нові можливості для обміну досвідом та реалізації спільних проектів).

Для формування цих умінь в учнів майбутні магістри освіти мають оволодіти медіа компететностями та уміннями проектувати цифрові наративи як одним з результативних

шляхів навчання. Підкреслимо, що необхідною умовою для оволодіння медіакомпетентностями є особистісне ставлення педагога до інформаційної продукції, його відкритість до співпраці з учнями, оскільки більшість учнів, підходять до навчання з досвідом використання інформаційно-комунікаційних технологій, котрий, іноді ширший і багатший за учительський. Тому, так важливо, щоб учителі вчилися досліджувати інформаційний простір разом з вихованцями.

У нашому дослідженні, що проходив на базі Міжнародного гуманітарного університету було доведено, що характерною особливістю професійної підготовки майбутніх магістрів освіти до формування медіа компетентності є прищеплення навичок не лише критично сприймати комунікаційний матеріал, але й збагачуватися досвідом творчої діяльності, тобто відбувається процес формування умінь «творити образний світ за допомогою комунікаційних джерел». Такий наш підхід ґрунтується на твердженні про необхідність залучення здобувачів до творчого виготовлення інформаційної продукції як обов'язкового етапу в процесі формування медіа та інформаційно-комунікаційної компетентностей.

Відтак розвиток медіакомпетентностей майбутніх магістрів освіти охоплює формування передусім таких компетентностей:

- компетентності з теорії використання медіа;
- компетентності в контексті мови й медіакомунікацій;
- компетентності вибору й аналізу медіаповідомлень;
- компетентності до творення медіаповідомлень.

Однак, незважаючи на значні перспективи та інтерес до впровадження цифрової педагогіки вона , як наука, все ж стикається з викликами, такими як-от:

1) цифровий розрив (необхідність забезпечення рівного доступу до технологій та інтернету для всіх учнів);

2) підготовка педагогів (потреба в постійному підвищенні кваліфікації вчителів та розвитку їхніх цифрових компетенцій);

3) кібербезпека (забезпечення безпеки даних та захисту конфіденційності в цифровому освітньому середовищі);

4) якість контенту (розробка високоякісного, релевантного та інтерактивного цифрового освітнього контенту).

Отож, на нашу думку для успішного розвитку цифрової педагогіки необхідні комплексні підходи, що включають інвестиції в інфраструктуру, розробку ефективних навчальних програм для педагогів, створення якісних цифрових ресурсів та формування сприятливої нормативно-правової бази.

Таким чином, цифрова педагогіка є не просто трендом, а необхідністю, що формує майбутнє освіти. Її подальший розвиток та впровадження дозволять створити гнучку, інклюзивну та ефективну освітню систему, що відповідатиме викликам та потребам 21 століття.

УДК 378.22:004.9 – 047.22

Іванова О. С. кандидат філософських наук, доцент
Міжнародний гуманітарний університет
okmegalodon2021@ukr.net
Кичка М. П. здобувач наукового ступеня доктора філософії
Міжнародний гуманітарний університет
mykola.p.kichka@gmail.com

ІННОВАЦІЙНІ SMART-ТЕХНОЛОГІЇ В ПІДГОТОВЦІ ФАХІВЦІВ ЕКОНОМІЧНОГО ПРОФІЛЮ

Анотація. *У статті досліджуються інноваційні SMART-технології та їхній вплив як на сучасне життя так і на підготовку фахівців економічного профілю. Аналізуються ключові напрями впровадження цих технологій у різні сектори життя (зокрема у промисловість, сільське господарство, логістику та сферу послуг) , а також теорію та методики професійної освіти, Особливу увагу приділено освітній продуктивності, яку забезпечує інтеграція SMART-рішень, розглядається роль SMART-технологій у підвищенні конкурентоспроможності освіти, оптимізації освітніх процесів та формуванні нових освітніх «бізнес-моделей» в умовах цифрової трансформації.*

Сучасний світ стрімко розвивається, і інноваційні SMART-технології стають дедалі важливішою частиною нашого повсякденного життя. Ці технології охоплюють широкий спектр рішень, які дозволяють керувати пристроями, системами та процесами на відстані, отримувати та передавати дані без прямого фізичного контакту. Їхнє впровадження революціонізує різні сфери, від побуту до промисловості, освіти та медицини.

Основою SMART-технологій сьогодні є поєднання інтернету речей, штучного інтелекту та високошвидкісних мереж зв'язку. Серед ключових напрямків застосування SMART-технологій можна виділити: розумний дім, дистанційне навчання та робота, телемедицина, промисловість та сільське господарство, транспорт та логістика.

Враховуючи вище зазначене сучасний світ вимагає від економічних фахівців не лише глибоких знань, а й здатності швидко адаптуватися до змін, використовувати новітні інструменти та технології. У цьому контексті SMART-технології стають ключовим елементом у підготовці конкурентоспроможних кадрів для економічної галузі.

У теоретичному етапі дослідження нами було виділено переваги впровадження SMART-технологій в освітній процес. Такими перевагами виявилися такі як-от:

- гнучкість та доступність (Дистанційне навчання дозволяє студентам отримувати освіту незалежно від їхнього географічного розташування та індивідуального розкладу. Це особливо важливо для тих, хто поєднує навчання з роботою або іншими зобов'язаннями. SMART-технології, такі як мобільні додатки та хмарні платформи, роблять навчання ще доступнішим з будь-якого пристрою);
- персоналізація освітнього процесу (Завдяки аналітичним можливостям SMART платформ, викладачі можуть відстежувати прогрес кожного студента, виявляти слабкі місця та адаптувати навчальний матеріал під індивідуальні потреби. Це дозволяє створювати персоналізовані навчальні траєкторії, що значно підвищує ефективність засвоєння знань.
- інтерактивність та залучення (Використання інтерактивних елементів, таких як віртуальні симуляції, гейміфікація, віртуальна та доповнена реальність (VR/AR), дозволяє зробити процес навчання цікавим та захоплюючим. Економічні симулятори дають можливість студентам відпрацьовувати навички управління підприємством, інвестиційного аналізу та прийняття стратегічних рішень в умовах, наближених до реальних);
- актуалізація освітнього контенту (Економічна галузь постійно розвивається, і традиційні підходи до навчання часто не встигають за цими змінами. Смарт дистанційні платформи дозволяють оперативно оновлювати навчальні матеріали, інтегрувати останні дослідження, кейси та аналітичні дані, забезпечуючи студентам доступ до найактуальнішої інформації).

Практичний етап дослідження сприяв визначенню ключових SMART-технологій у професійній підготовці фахівців саме економічного профілю. На нашу думку, варто особливо виділити такі:

1) онлайн-платформи для навчання (LMS) (системи управління навчанням, такі як Moodle, Coursera for Business, edX, забезпечують централізований доступ до курсів, завдань, тестів та комунікаційних інструментів);

2) відеоконференції та вебінари (інструменти, такі як Zoom, Google Meet, дозволяють проводити онлайн-лекції, семінари, групові обговорення та індивідуальні консультації в режимі реального часу);

3) віртуальні Лабораторії та Симулятори (програмні рішення, що імітують реальні економічні процеси та інструменти (наприклад, симулятори фондового ринку, бізнес-симулятори), дозволяють студентам здобувати практичний досвід без ризику реальних втрат);

4) штучний інтелект (ШІ) та машинне навчання (МН) (використання ШІ для персоналізації навчання, автоматичної оцінки завдань, надання зворотного зв'язку та рекомендацій, а чат-боти можуть відповідати на типові питання здобувачів);

5) Big Data та Аналітика (збір та аналіз даних про успішність студентів для оптимізації навчального процесу та прогнозування їхньої майбутньої кар'єри);

6) блокчейн (застосування блокчейну для верифікації сертифікатів та дипломів, що підвищує їхню довіру та захист від підробок).

В умовах переходу до економіки знань цінність людського потенціалу визначається можливістю використання саме неповторних особливостей потенціалу SMART-технологій в процесі як професійної підготовки майбутніх фахівців та і в процесі професійної діяльності, де працівник із досвідом, умінням, мотивами, інтересами, цінностями, стимулами, установками є стратегічним ресурсом організації. В умовах українських реалій найкращою платформою для апробації й упровадження концепції SMART-освіти є всесвітньо відома система організації та управління навчальним процесом MOODLE (Modular Object-Oriented Dynamic Learning Environment). Перевагами даного інструментального засобу є його безкоштовна ліцензія, постійне динамічне оновлення науковцями, освітянами, дизайнерами і програмістами світової спільноти та використання сучасних інновацій у сфері освітньої й педагогічної практики. Отож, спостерігаємо, поступове створення глобального інформаційного навчального середовища, що забезпечує активну взаємодію між усіма учасниками освітнього процесу, забезпечення їх доступу до глобальних освітніх ресурсів та максимальне задоволення їхніх потреб в отриманні і засвоєнні знань та отриманні стійких компетенцій у певній фаховій сфері.

Однак, незважаючи на значні переваги та актуальність, впровадження SMART-технологій у професійної підготовки майбутніх фахівців і особливо економічної сфери – такий підхід все ж має свої виклики, серед яких: необхідність значних інвестицій у технологічну інфраструктуру, підготовка викладачів до роботи з новими інструментами, забезпечення кібербезпеки та подолання "цифрової нерівності".

Проте, перспективи розвитку надзвичайно широкі. Подальше впровадження смарт дистанційних технологій в освіту дозволить формувати нове покоління економістів, які будуть володіти не лише теоретичними знаннями, а й практичними навичками роботи з сучасними технологічними рішеннями, що є запорукою їхнього успіху та сталого розвитку економіки в цілому.

Рівень розвитку трудових ресурсів відповідає за забезпечення інтенсивного економічного зростання за переходу до «нової» економіки, заснованої на знаннях (неоекономіки), за диференціацію між економічно розвиненими і країнами, що розвиваються. Головним джерелом і вирішальним чинником такого зростання є використання SMART-технологій як пріоритетного напряму в освітньому процесі в умовах глобалізації розвитку економіки України. І ключове значення у цьому процесі має саме освітній потенціал, перш за все освіченість, компетентність, творчі можливості професіоналів й умови їх реалізації. Саме знання, професійна підготовка стають головним джерелом конкурентних переваг у XXI ст

УДК 378.22:004.9

Єрмакова С.С. доктор педагогічних наук, професор, практичний психолог
Міжнародний гуманітарний університет
ermakovasvitlana2011@ukr.net
Шаповалов О.Ю. здобувач наукового ступеня доктора філософії
Міжнародний гуманітарний університет
shapovalov_76@ukr.net

ФОРМУВАННЯ МОТИВАЦІЇ РОЗВИТКУ ЦИФРОВИХ НАВИЧОК У ЗДОБУВАЧІВ ОСВІТИ ЗА КРОС-КУЛЬТУРНОЮ МЕТОДИКОЮ

Анотація. *У статті досліджується проблема формування мотивації до розвитку цифрових навичок у здобувачів, що сфокусована на крос-культурному підході. Аналізуються існуючі підходи та пропонуються нові враховуючи культурні особливості і відмінності у сприйнятті цифрових технологій. Визначенні ключові чинники формування цифрової компетентності у здобувачів освіти до навчання за крос-культурною методикою, які б сприяли підвищенню мотивації і, як правило, активному засвоєнню цифрових компетенцій. Результати дослідження можуть бути застосовані у теорії та методиці професійної освіти з метою оптимізації програм навчання цифровим навичкам.*

У сучасному світі цифрові технології відіграють ключову роль у всіх сферах життя, включаючи освіту. Ефективне використання цих технологій вимагає не лише доступу до них, а й сформованої мотивації до розвитку цифрових навичок у здобувачів освіти. Особливо актуальним це стає при впровадженні крос-культурних методик навчання, які передбачають взаємодію та обмін знаннями між представниками різних культур.

І хоча на часі цифрові навички є ключовими для успіху в будь-якій сфері діяльності. Проте, однією з головних проблем, з якою стикаються викладачі та освітні установи, є низька мотивація здобувачів освіти до розвитку цих навичок. Використання кроскультурної методики може значно покращити цю ситуацію, оскільки вона враховує різноманіття культурних особливостей та цінностей, що впливають на процеси навчання та мотивації.

Мотивація до навчання не є універсальною; вона формується під впливом безлічі культурних факторів. Наприклад, в деяких культурах домінує індивідуалістичний підхід, де акцент робиться на особисті досягнення та конкуренцію. У таких умовах здобувачі освіти можуть бути мотивовані до освоєння цифрових навичок через можливість отримати кращу роботу, підвищити свій статус або випередити однолітків. В інших культурах, які тяжіють до колективізму, важливішими є спільні досягнення, співпраця та допомога групі. Тут мотивація може бути пов'язана з можливістю використовувати цифрові інструменти для підвищення ефективності командної роботи або сприяння добробуту громади.

Крім того, на мотивацію впливають ціннісні орієнтації. У культурах, де цінуються традиції та стабільність, нові технології можуть сприйматися з обережністю, що вимагає інших підходів до формування мотивації. Навпаки, у культурах, орієнтованих на інновації та зміни, інтерес до цифрових навичок виникає природним чином.

Крос-культурна методика навчання за своєю суттю є інноваційною, оскільки вимагає від здобувачів комунікативних навичок, навичок критичного мислення, а також здатності працювати в команді. Цифрові інструменти надають унікальні можливості для реалізації цих завдань. Віртуальні навчальні середовища, онлайн-платформи для співпраці, відеоконференції та мультимедійні ресурси дозволяють здобувачам освіти з різних країн спілкуватися, обмінюватися досвідом та спільно працювати над проектами. Це сприяє не лише засвоєнню академічних знань, але й розвитку міжкультурної компетенції, толерантності та взаєморозуміння.

Кроскультурна методика передбачає адаптацію освітніх програм та методів навчання з урахуванням культурних особливостей здобувачів освіти. Це не означає просто переклад матеріалів іншою мовою, а глибоке розуміння того, як культурні норми, цінності та комунікаційні стилі впливають на сприйняття інформації та рівень залученості.

У дослідження нами було встановлено, що формування цифрової компетентності у здобувачів освіти до навчання за крос-культурною методикою є багатоаспектним процесом, що залежить від кількох ключових чинників:

- Доступність та якість цифрових ресурсів.
- Релевантність та цікавість контенту. (Навчальні матеріали повинні бути цікавими, актуальними та відповідати віковим та культурним особливостям здобувачів освіти. Використання інтерактивних елементів, гейміфікації та мультимедійного контенту значно підвищує залученість).
- Компетентність педагогів. (Вчителі повинні володіти не лише цифровими навичками, але й умінням інтегрувати цифрові інструменти в крос-культурний освітній процес, створювати умови для співпраці та фасилітувати міжкультурний діалог).
- Можливість самовираження та співпраці. (Цифрові інструменти повинні надавати здобувачам освіти можливість висловлювати свої ідеї, брати участь у спільних проектах, обмінюватися думками та отримувати зворотній зв'язок. Це створює відчуття власності та підвищує мотивацію).
- Визнання та заохочення. (Важливо відзначати успіхи здобувачів освіти у використанні цифрових інструментів та їхню активність у крос-культурних проектах).
- Подолання психологічних бар'єрів. (Деякі здобувачі освіти можуть мати страх перед новими технологіями або невпевненість у своїх цифрових навичках. Важливо створити підтримуючу атмосферу та надавати індивідуальну допомогу).

Враховуючи вище зазначені чинники, вважаємо, що для успішної мотивації здобувачів освіти до навчання за крос-культурною методикою можна використовувати такі стратегії:

1) Створення інтерактивного та залучаючого навчального середовища. (Використання віртуальних екскурсій, інтерактивних симуляцій, 3D-моделювання, віртуальної та доповненої реальності).

2) Запровадження проектної діяльності. (Залучення здобувачів освіти до спільних міжнародних проектів, що вимагають використання цифрових інструментів для комунікації, дослідження та презентації результатів).

3) Використання гейміфікації (Інтеграція ігрових елементів для підвищення інтересу та залученості).

4) Стимулювання самостійного навчання та дослідницької діяльності. Надання здобувачам освіти можливості самостійно шукати інформацію, аналізувати її та створювати власний цифровий контент.

5) Організація віртуальних зустрічей та вебінарів з носіями мови та культури. Це дозволяє здобувачам освіти безпосередньо взаємодіяти з представниками інших культур, підвищуючи їхню мотивацію до вивчення мови та міжкультурної комунікації.

6) Регулярне підвищення кваліфікації педагогів у сфері цифрових технологій та крос-культурної педагогіки.

Відтак, впровадження кроскультурної методики у формування мотивації розвитку цифрових навичок має свої виклики, такі як необхідність підвищення кваліфікації викладачів, розробка релевантних навчальних матеріалів та подолання можливих стереотипів. Проте, довгострокові переваги переважають ці труднощі. Застосування кроскультурного підходу дозволяє не лише ефективніше розвивати цифрові навички, а й сприяє формуванню глобальної компетентності, здатності працювати та взаємодіяти в полікультурному середовищі, що є надзвичайно важливим для сучасного світу.

Таким чином, інвестування в розробку та впровадження кроскультурних методик є не просто бажаним, а необхідним кроком для створення ефективної та інклюзивної системи освіти, яка готує здобувачів освіти до успіхів у цифровій епосі. А забезпечення доступу до якісних цифрових ресурсів, створення цікавого та інтерактивного контенту, компетентність педагогів та стимулювання співпраці є основними компонентами цього процесу. Інвестуючи в цифрову освіту та розвиток цифрової мотивації, ми не лише готуємо здобувачів освіти до викликів сучасності, а й сприяємо формуванню глобального громадянства та міжкультурного порозуміння.

УДК 371.3:004.8:004.946:37.018.43:37.014.5

Жигулін О. А., д. е. н., доцент
Міжнародний гуманітарний університет
zhigulin998@gmail.com

МЕТОДОЛОГІЯ ІНФОРМАЦІЙНОЇ ДУАЛЬНОСТІ, ТВОРЧОЇ РЕАБІЛІТАЦІЇ, ШТУЧНОГО ІНТЕЛЕКТУ, ДОПОВНЕНОЇ Й УЯВНОЇ РЕАЛЬНОСТІ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ НАВЧАННЯ ПІД ЧАС ВОЄННОГО СТАНУ

Анотація. *Наведено актуальність створення та результати впровадження Методології інформаційної дуальності, творчої реабілітації викладачів і студентів, штучного інтелекту, доповненої й уявної реальності для підвищенні якості навчання під час воєнного стану. Обґрунтовано дієвість складових методології, які комплексно вирішують проблему якості навчання в Україні під час кризи та інформатизації суспільства.*

Актуальність теми дослідження полягає у відсутності тісних зв'язків навчальних закладів з виробництвом, необхідності під час воєнного стану інтелектуальної, психічної й фізичної реабілітації учасників освітнього процесу, використанні штучного інтелекту, методів доповненої й уявної реальності для підвищення якості навчання.

Під терміном «інформаційна дуальність» мається на увазі залучення до формування змісту навчання досвіду підприємств, які успішно розвиваються під час воєнного стану. Наразі суспільство перебуває під тиском економічних, санітарних і соціально-політичних кризових явищ. Причиною криз є порушення Закону еволюції життя (незворотність, прискорення темпів, етичне відношення до розвитку усіх без виключень та обмежень). Наразі ліквідується бізнес, який порушує та стрімко розвивається той, що відповідає вимогам закону еволюції життя. В науковій літературі є результати досліджень, які свідчать про те, що характерною рисою успішних підприємств є задоволення інтересів і бізнесу, і суспільства, і держави або додержання вимог соціо-еколого-економічних стандартів [1]. Використання даного позитивного досвіду рекомендується реалізовувати через спільну з керівниками, менеджерами й працівниками підприємств участь у написанні підручників і навчальних посібників, надання консультаційної допомоги бізнесу та автоматизацію його бізнес-процесів, отримання від представників бізнесу пояснень вирішення складних практичних питань сьогодення.

Методологія інформаційної дуальності, творчої реабілітації, штучного інтелекту, доповненої й уявної реальності для підвищення якості навчання під час воєнного стану

пройшла апробацію на підприємствах і навчальних закладах півночі, заходу й півдня України та отримала призове місце на Всеукраїнському конкурсі Педагогічний Оскар 2025.

Результати впровадження її в навчальному закладі наведено на рис. 1. Оцінка проводилася за показником стійкості розвитку на основі самоорганізації навчального закладу. Саме самоорганізація допомагає закладам освіти й підприємствам бізнесу наразі успішно розвиватися на ринку. Для бізнесу оцінювалася динаміка чистого доходу за три цикли розвитку (9-12 років), а для закладів освіти – динаміка контингенту студентів.

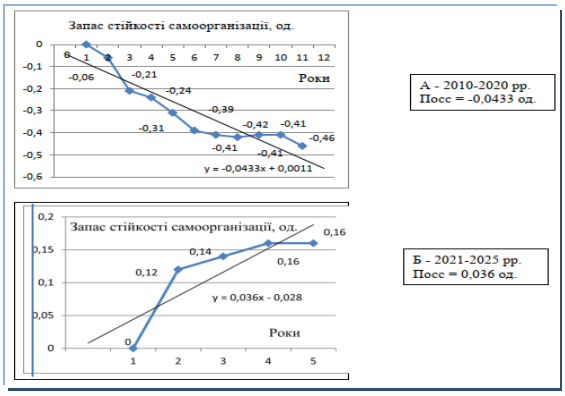


Рисунок 1 - Оцінка результатів впровадження «Методології…» у навчальному закладі

Дані рис. 1 свідчать про зміну тренду розвитку при використанні «Методології…» у період 2021-2025 рр. зі спадного на висхідний.

Для учасників освітнього процесу творча (інтелектуальна, психічна, фізична) реабілітація полягала у наступному:

1. Викладачі:

а) інтелектуальна реабілітація (перевидання підручників на основі ресурсів ШІ; автоматизація рутинних операцій пошуку інновацій за допомогою ШІ);

б) психічна реабілітація (досягнення життєвої місії викладача; нетрадиційні засідання кафедр щодо розвитку креативу за участі у творчих заходах);

в) фізична реабілітація (вправи з БЖД з помірним фізичним навантаженням; спартакіада серед викладачів з фото-винагородженням);

2. Студенти:

а) інтелектуальна реабілітація (оновлення конспектів лекцій за ресурсами ШІ; автоматизація рутинних операцій щодо розрахунків);

б) психічна реабілітація (досягнення життєвої місії за кодом типу особистості);

в) фізична реабілітація (спартакіада серед студентів).

Напрями інтелектуальної й психічної реабілітації викладачів на прикладі економіки, інформаційних технологій і безпеки праці та життєдіяльності наведено (рис. 2).


Рисунок 2 - Напрями інтелектуальної й психічної реабілітації викладачів через перевидання підручників, участь у творчих заходах, використання інтерактивних сайтів

Фізична реабілітація викладачів проводилася через вправи з БЖД з помірним фізичним навантаженням і спартакіаду з фото-винагородженням (рис. 3).

Рисунок 3 - Фізична реабілітація викладачів через спортивні змагання.

Реабілітація студентів носила індивідуальний характер. На першому занятті їх тестували (Методика ТАРТ) на встановлення бажаних галузей розвитку на шляху до виконання життєвої місії й залучали до дослідної роботи у даній сфері (рис. 4).

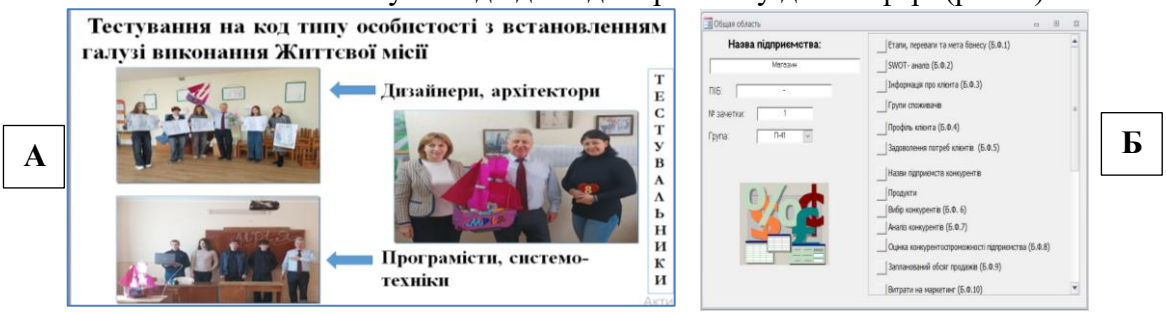


Рисунок 4 - Творча реабілітація студентів щодо тестування (А) й проведення дослідження у сфері саморозвитку з використанням програмного продукту «Розвиток» (Б)

Фізична реабілітація студентів проводилася на заняттях з БЖД та охорони праці через вправи з домедичної допомоги з помірним фізичним навантаженням (рис. 5).

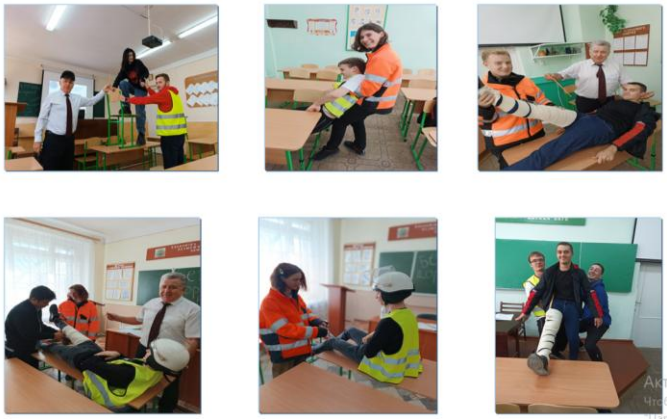


Рисунок 5 - Фізична реабілітація студентів

Висновки: 1. Розроблено й пройшла успішну адаптацію «Методологія інформаційної дуальності, творчої реабілітації викладачів і студентів, штучного інтелекту, доповненої й уявної реальності для підвищенні якості навчання під час воєнного стану».

2. Обґрунтовано дієвість складових методології, які комплексно вирішують проблему якості навчання в Україні під час воєнного стану та інформатизації суспільства.

Література

1. Жигулін О. А., Стрелковська І. В., Попа Л. М. Самоорганізація бізнесу з використанням інформаційних технологій: Монографія. Ніжин: Вид-во НДУ імені Миколи Гоголя, 2025. 276 с.